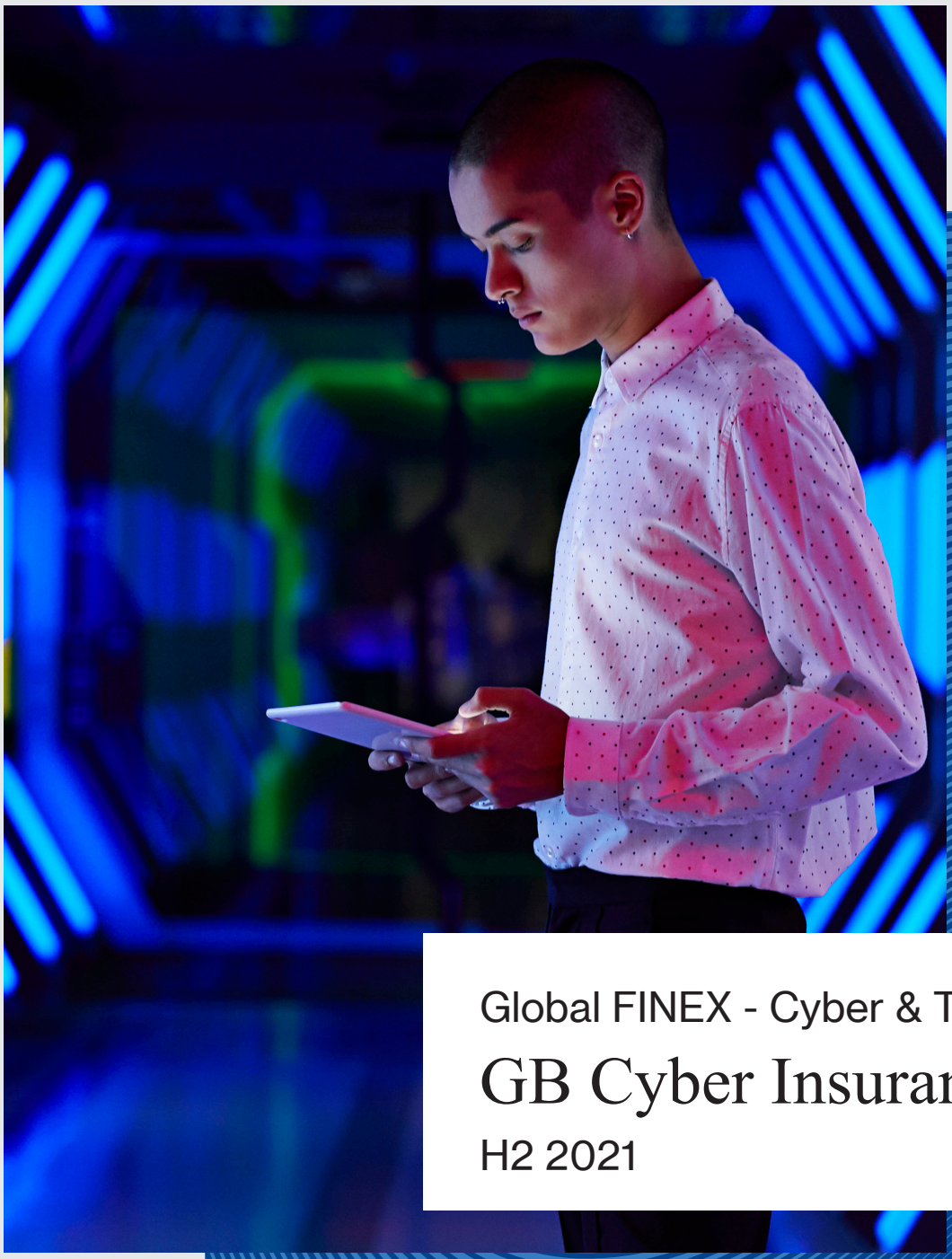
wtw



Global FINEX - Cyber & TMT

GB Cyber Insurance Update

H2 2021

wtwco.com

Executive summary

The GB cyber insurance market has experienced many challenges and changes through the second half of 2021.

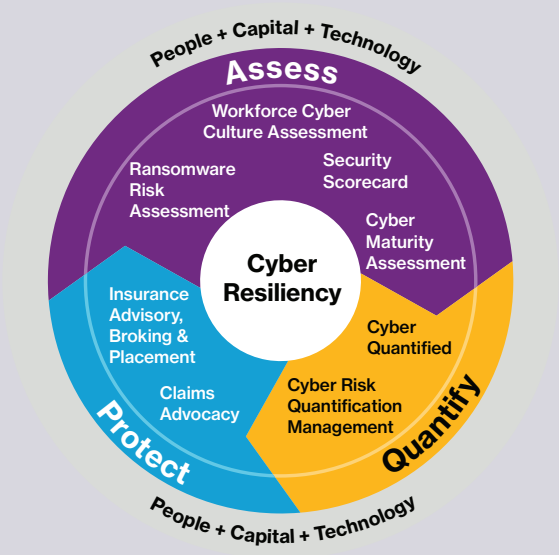
In particular:

- Further **hardening of market conditions**
- Continued **high profile / impact losses**
- Reductions to capacity
- Continued **premium increases**, exacerbated in excess layers
- **Increased policy retentions/excesses**
- **Policy coverage increasingly under review**
- More **detailed underwriting information required**

This update is a general overview of these key developments, analysing the current conditions in the GB Cyber insurance market for both international and domestic companie. The analysis is based on our own observations of the market and uses WTW proprietary data unless otherwise stated.

Simon Basham
Head of Cyber & TMT Broking (UK) / FINEX GB, WTW

T: +44 203 124 8415
M: +44 7795 855 925
Simon.Basham@WillisTowersWatson.com
www.wtwco.com



Cyber insurance market capacity

Looking back over H2 2021

Insurers continued to **reduce their capacity** and **tighten their underwriting requirements** to manage their exposure and avoid the risk of aggregation of losses from one widespread incident. This made securing capacity within the first USD/GBP/EUR50m of capacity particularly difficult.

Insurers were increasingly willing to only offer capacity for **risks fitting precisely within their appetite** in terms of pricing, attachment point and coverage. As a result, clients were forced to **retain more risk** in order to fill gaps in their programmes.

By Q4 the **capacity available for new business**, from Lloyd's syndicates in particular, became extremely limited and subject to tighter risk selection by insurers.

The capacity available for **physical property damage arising from a cyber event** cover was also under similar pressure but did not reduce at the same rate.

2022 WTW expectations

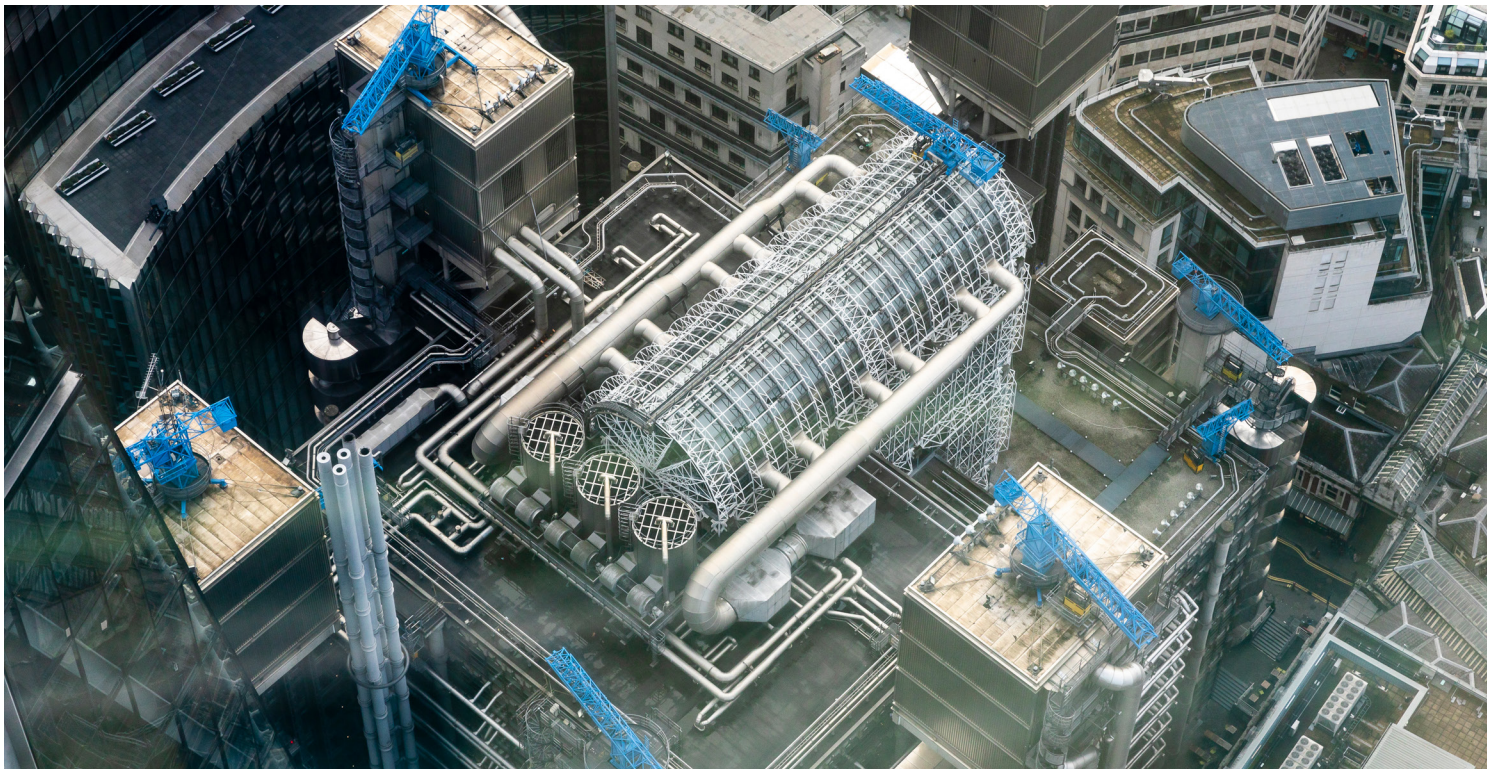
Availability of **capacity will remain a key issue** within the cyber market in 2022.

Lloyd's of London have indicated that they remain committed to cyber insurance, but **many Lloyd's syndicates have been permitted only limited growth in 2022**, with the **focus being on renewals rather than new business**. Lloyd's have also emphasised the need for syndicates to focus on best-in-class capabilities in underwriting the risk[1].

Non-Lloyd's markets will become increasingly important in 2022, with their capacity deployment strategies dictated internally rather than by Lloyd's.

There is some **new capacity coming into the market** (albeit on a limited basis) and **additional capacity will be available from existing non-traditional syndicates such as those who underwrite through the use of an algorithm**.

1. https://www.insuranceiansider.com/article/291aqbc128q6mf1c50hz4/lloyds-to-permit-cyber-growth-for-those-who-show-excellence-tiernan



Premiums & self-insured retentions

Looking back over H2 2021

Rate and premium **increases of more than 50-100% on the primary layer were not uncommon**. The percentage depended on the correction insurers deemed necessary at the date the policy incepted. Tracking those changes proved challenging as **insurers and clients adopted other policy changes**, such as increases to self-insured retentions of the primary placements, to offset premium increases.

The **increases in claims activity** prompted **regular pricing reviews by insurers**, to ensure premiums paid would meet their claims exposure. It also contributed to their **stricter risk selection**.

Thus, pricing was largely driven by each **insurer's perception of the individual risk, attachment point and structure**. Those clients with a claims history or sub-optimal cyber security controls experienced higher premium increases and a greater challenge to securing insurance. Significantly larger retentions were also imposed without premium relief. These **measures varied, dependent on factors such as a client's industry sector, size and exposures**.

Premium increases also followed on excess layers with percentages exceeding those for the primary layer. This reduced the premium discount on those excess layers compared to the primary.

2022 WTW expectations

Predicting the year-on-year percentage increase to premiums based on last year's premium is likely to prove unreliable. We **expect prices to continue to rise**, particularly in the first half of 2022.

Those pricing pressures will be exacerbated by the **reduction in supply of capacity and increased demand for it from those seeking insurance**. Virtually all placements of sizeable or substantial limits will require new capacity to fill the gaps left by incumbent insurers reducing capacity.

The first half of 2022 will also see **continued focus on tighter risk selection**, a more flexible approach to adopting **other policy changes** and **increased rate and premium rises**. To obtain insurance clients will need to prove, with help from their brokers, **the adequacy of their cyber security controls**.

Higher self-insured retention levels will remain a tool for insurers and clients, offsetting increased premiums and **the challenges of securing the first USD/GBP/EUR50m of insurance capacity**. The level of those retentions will be a strategic decision for clients planning their 2022 cyber renewal.

Policy coverage

Looking back over H2 2021

Insurers **focused on systemic risk,** with one leading insurer even limiting its exposure to widespread (systemic) events, re-writing coverage with this in mind and adding in provisions to sub-limit its exposure. How this will influence the marketplace is not yet clear, but the focus remains.

The willingness of insurers to offer **ransomware coverage was often determined on a case-by-case basis** according to a client's cyber risk profile. **Coverage of ransom payments** remained an area of focus for governments, prompting one continental European insurer to remove cover for it. **Appetite for non-IT business interruption outsource service provider coverage** all but dried up, although cover remained for third parties providing core IT outsourced goods or services.

Insurers routinely **excluded cover for wrongful collection of biometric data** where they felt uncomfortable with a client's exposure to or management of it. Once revealed, some also applied exclusions regarding the **Log4j[2] vulnerability**, although most insurers are reviewing this topic before deciding how best to respond.

The ongoing **increase in claims** and the volume of ransomware attacks led some insurers to continue imposing **sub-limits on ransomware coverage and/or co-insurance to manage their exposure**.

2022 WTW expectations

Systemic risk is expected to dominate insurers planning, with more policy exclusions, less willingness to offer Non-IT contingent business interruption cover and the sub-limiting of widespread events.

We expect to see **more war exclusions** based on the new model clauses issued by the Lloyd's Market Association (LMA)[3]. Insurers are deciding which clauses to use or amend as they deem appropriate.

Ransomware cover is likely to become **the subject of even stricter limitations,** mirroring each **insurer's exacting expectations of their client's cyber security profile.**

Pressure on Non-IT business interruption cover and full system failure will continue, as will the application of biometric data (wrongful collection) exclusions where insurers deem it necessary.

2. https://www.ncsc.gov.uk/information/log4j-vulnerability-what-everyone-needs-to-know

3. https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA21-042-PD.aspx

Claims & notifications

Looking back over H2 2021

Claim notifications and payments rose, largely due to ransomware events. Data theft (within a Ransomware attack) **added costs, regulatory exposures and long-term liabilities to potential losses**.

According to Coveware[4], the ransomware response provider, more ransomware attacks than ever were mounted through this period. They also reported that whilst average ransomware payments remained flat, attacks incorporating threats of data theft increased to 83.3% of the total.

Claim notifications involving technology supply chain issues also continued to rise, contributing to insurers concerns around the potential ramifications of a global systemic event. Examples included Kaseya, SolarWinds, Microsoft Exchange, Accellion & in December, the Log4j vulnerability.

2022 WTW expectations

Ransomware attacks are unlikely to subside in frequency or severity. Many organisations are yet to implement key cyber security controls and will remain vulnerable to ransomware until they do.

We anticipate claim notifications relating to **supply chain security issues** and the **US Biometric Information Privacy Act** will rise. This legislation may lead to US class actions alleging wrongful biometric data collection.

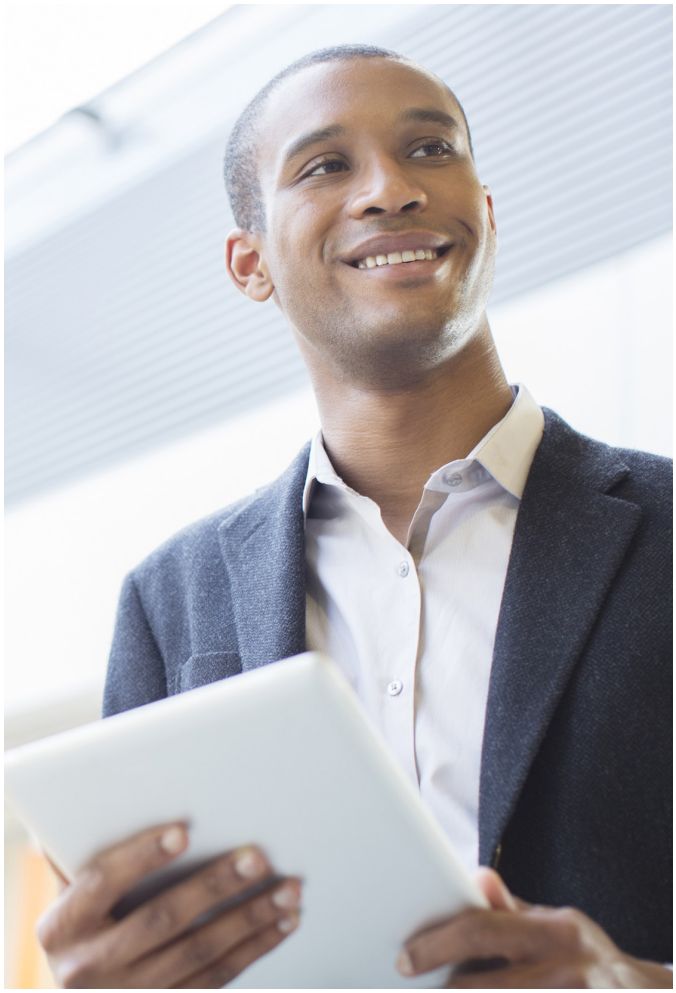
Insurers are expected to monitor these events to gauge the potential for generating systemic losses. Their development could impact insurers strategies on capacity, aggregation and coverage.

4. https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts

Cyber hygiene – control adequacy

Insurers are increasingly requiring **clients to make written cyber submissions** in addition to presentation meetings. They also require **clients to have minimum cyber security controls** in place before offering renewal or new capacity.

This echoes the findings of a report from **Allianz Global Corporate & Specialty (AGCS)** published in 2021[5] which stated that "The claims environment and the cyber threat environment is considerably worse than it was a few years ago therefore, insurers cannot continue in this market without working with clients to provide a strong baseline of acceptable controls that need to be in place." According to AGCS, an analysis of the largest ransomware claims in Europe suggests that "In around 80% of ransomware incidents losses could have been avoided if the organizations had followed best practices. In many cases we find a lack of multi factor authentication (for remote access, on privileged IT accounts or for remote maintenance) or inadequate training has been a major contributing factor to the loss".



What can clients do / being market ready?

Preparing for your renewal

- Ensure key stakeholders (for example board and CISO) **are briefed on likely renewal challenges, including increased self-insured risk retention.**
- Consider the bigger picture, what is the defining **renewal priority to guide strategy**
- **Allow plenty of time to collate renewal information & to review/refine** this with the help of your cyber brokers
- **Working with your brokers**, ensure insurers receive necessary context to frame your cyber underwriting information
- **Consider cross class leverage** with key insurer partners
- **Be self-aware in your navigation of the cyber market**, demonstrating desire to partner with insurers

'Start the renewal process early – ensure key stakeholders (for example board and CISO) are briefed on likely renewal challenges, including increased self-insured risk retention'.

5. Allianz Cyber Insights Ransomware Trends: Risks & Resilience Report (October 2021) https://www.agcs.allianz.com/news-and-insights/reports/cyber-risk-trends-2021.html

Cyber hygiene / minimum control standards

Whilst the minimum standards continue to evolve and vary between insurers, here is a selection of controls that are often critical to maintaining or securing cyber insurance coverage.

1. Utilisation of a Privileged Access Management tool for all privileged user accounts, that is subject to Multi-Factor Authentication
2. Deployment of an Endpoint Detection & Response solution on all / very high percentage of endpoints
3. Deployment of an intrusion detection and prevention solution
4. Multi-Factor Authentication required for all remote access, third party access and for access to critical information
5. Utilisation of Multi-Factor Authentication & Advanced Threat Protection for users of Microsoft Office 365
6. Limitation of the use of service accounts, in particular those in the Domain Admin group, with strong controls for such accounts such as denying interactive log-ins
7. Vulnerability scanning across all /the vast majority across your environment
8. Utilisation of offline back-ups, further measures to mitigate the likelihood such back ups are compromised (encryption, network segmentation, immutable amongst others) and back-ups made offline regularly
9. Tight management of end-of-life software and systems, with prioritised plans to replace such, particularly where the software or system is business critical and/or holds personal information
10. Regular training (at least bi-annually) for all staff to in-bed a culture of awareness regarding phishing / social engineering attacks

Disclaimer

Willis Towers Watson offers insurance-related services through its appropriately licensed and authorised companies in each country in which Willis Towers Watson operates. 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. (https://www.willistowerswatson.com/en-GB/Notices/global-regulatory-disclosures). It is a regulatory requirement for us to consider our local licensing requirements.

The information given in this publication is believed to be accurate at the date of publication shown at the top of this document. This information may have subsequently changed or have been superseded and should not be relied upon to be accurate or suitable after this date. 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 and we disclaimer all liability to the fullest extent permitted by law. 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 WTW

At WTW (NASDAQ: WTW), we provide data-driven, insight-led solutions in the areas of people, risk and capital. Leveraging the global view and local expertise of our colleagues serving 140 countries and markets, we help you sharpen your strategy, enhance organizational resilience, motivate your workforce and maximize performance. Working shoulder to shoulder with you, we uncover opportunities for sustainable success – and provide perspective that moves you. Learn more at wtwco.com.

wtwco.com/social-media

FPS2683524 WTW-503408/02/22

wtwco.com