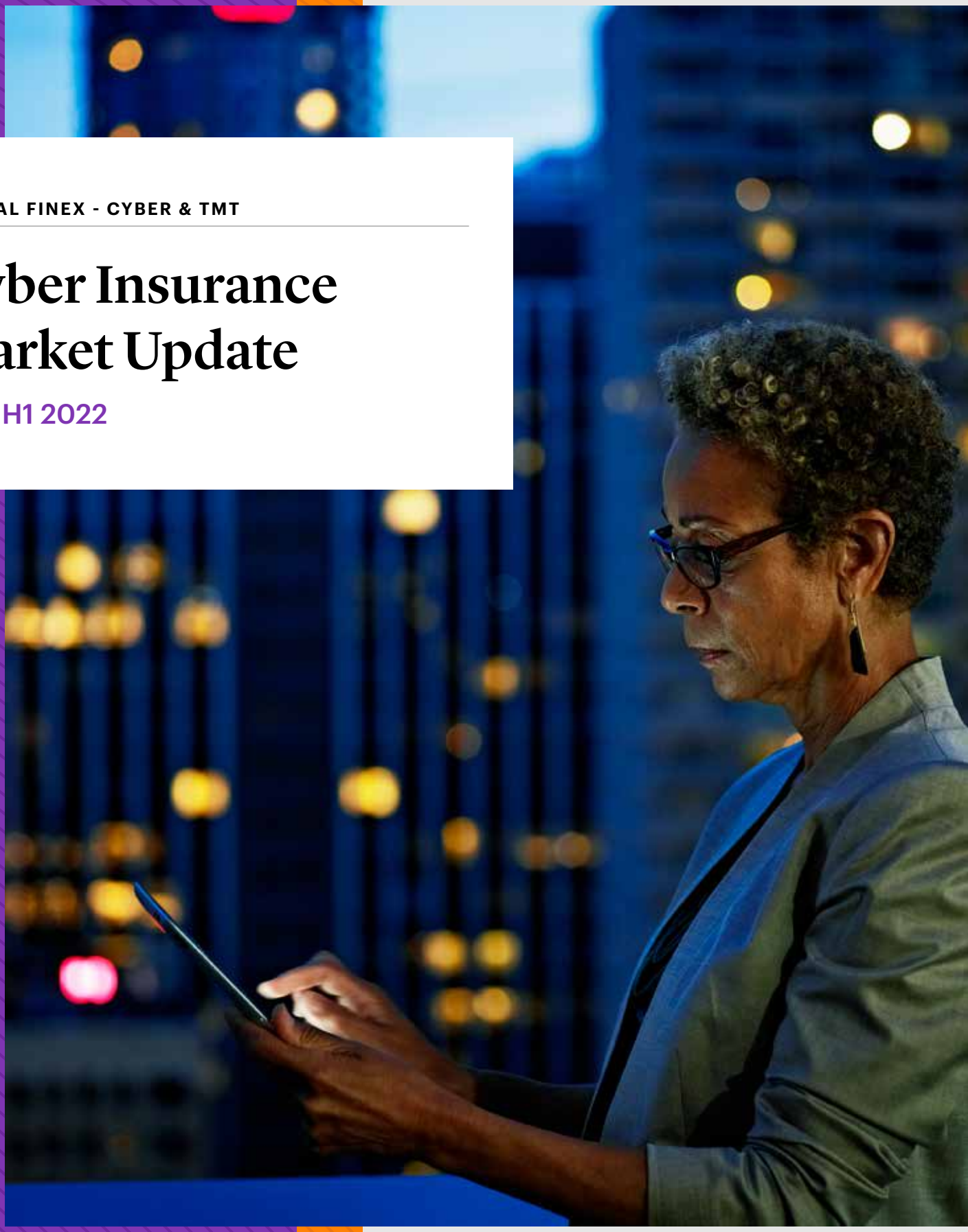
GLOBAL FINEX - CYBER & TMT

Cyber Insurance Market Update

Q2 / H1 2022



Executive summary

This update is a general overview of the key developments in the GB cyber insurance market, analysing the current conditions for both international and domestic companies using the London insurance market to transfer risk

The GB cyber insurance market has seen significant changes during Q2 2022, with the segments within the market being more distinct and nuanced than previously experienced.

In particular:

- Q2 2022 has delivered generally improving trading conditions, especially for core enterprise-scale (£1bn plus revenue) clients
- Capacity stabilising for most market segments and improving in some generating increased competition
- Focus on sustainable pricing, not a default of significant further increases
- Insurer's focus on sustainable policy retentions/ excesses remains
- Policy coverage remains under very careful review
- Continuing acute focus on war and terrorism exclusionary language
- Detailed underwriting information, and specifically context, remain key

The analysis is based on our own observations of the market and uses WTW proprietary data unless otherwise stated.

Cyber insurance market capacity

We are seeing an increasing number of insurers willing to increase their available capacity where the characteristics of the risk match their underwriting strategies.

To underline this, insurance capacity availability within the first USD/GBP/EUR50m layer has increased compared to Q1, particularly for the most attractive segments of the market (Previously less attractive/appreciated segments are also starting to see interest from insurers (focused on GBP1bn plus revenue accounts) who are increasingly showing interest in middle-market business where clients can tell a positive story and present the risk as high quality.

New insurance capacity has entered the wider market during Q2, with more likely to follow in Q3. For example, we are monitoring InsurTech insurers who have quickly established themselves in the US cyber market and may well have their eyes on competing in the middle-market space. In addition, a leading global cyber insurer has now launched an Environmental, Social & Governance (ESG) based syndicate, potentially augmenting the capacity they are already offering. Not all segments of the cyber market will benefit equally from this additional capacity.

Clients still need to show good level of risk control in order to secure capacity, however insurers are increasingly demonstrating flexibility where clients can provide the necessary context to explain their risk acceptance rationale. Insurers will have particular areas of focus and clients will need to demonstrate strong control measures in those areas. Unsurprisingly Insurers are keen to understand the business impact of events such ransomware attacks and extortion demands.

Insurers remain cautious where clients could be at risk from the Russia/Ukraine conflict, and this particularly applies to organisations in telecommunications, financial institutions and critical national infrastructure. It does seem that the level of concern is receding .

Premiums & self-insured retentions

Premium increases in Q2 2022 are far more variable than in recent quarters, as the result of insurers focus on pricing adequacy. Clients with similar profiles may receive different levels of premium increases, the key being whether their insurer feels the expiring premium levels are sufficient.

In this respect, a small but increasing number of clients received a pricing reduction compared to 2021, often where a segment most impacted by 2021 capacity challenges then benefits from increasing competition in that segment. In the same period, some accounts are still receiving increases of 50% or more, usually where their premium levels are significantly lower than their peers, demonstrating an out-performance of 2021 market conditions.

Insurers remain focused on self-insured retentions, but we are pleased to say that for an increasing percentage of accounts renewing in Q2 2022 they are seen to be adequate. We should add that clients are also considering increasing the level of self-insured retention as they plan their cyber insurance purchasing strategies.

Policy Coverage

Insurers remain very focused on systemic risk. It is common in segments with more clients and so volume sales (such as the mid-market) that insurers offer less capacity per client than they would to large enterprises of £1bn or more, who are fewer in number and so present a lower accumulated risk.

Unsurprisingly the Ukraine/ Russia crisis has made Insurers nervous. Many insurers quickly reviewed their contract language relating to War and Terrorism exclusions and are mindful that Cyber-attacks have become a modern warfare tactic. During Q2, insurers approach to this language continued to fall into the following categories:

1. Sticking with the N.M.A. 464 War and Civil War Exclusion Clause – with various amendments / cyber terrorism cover 'carved-back'
2. Drafting an updated exclusion based (to some extent) on N.M.A. 464 or drafting a new exclusion all together
3. Considering using one of the four model clauses proposed by the Lloyds Market Association LMA), predominantly LMA5567 (War, Cyber War and Limited Cyber Operation Exclusion No. 4)

Insurers continue to utilise ransomware coinsurance and/ or sub-limits where they are not satisfied that a client's security meets the insurer(s) own minimum standards. Some insurers are not willing to consider offering cyber coverage unless certain standards are met. Insurers views on required minimum controls are increasingly varied and more flexibility. This gives clients, with the support of their broker, the opportunity to advocate for their approach.

Claims & Notifications

Ransomware risk is a significant one and likely to result in significant financial losses beyond a ransomware demand itself. That said trends suggest that less ransomware demands are being paid

Here are some highlight statistics regarding Ransomware from two vendors supporting businesses impacted by ransomware incidents.

- In Q1 of 2019, 85% of the cases Coveware handled ended in the cyber-criminal receiving a ransom payment. Three years later, that number is down to 46% in Q1 of 2022.
- Data theft without encryption results in no operational disruption, but preserves the ability of the threat actor to extort the victim. Coveware expects this shift from Big Game Hunting to Big Shame Hunting to continue.[1]

82%

Increase in ransomware related data leaks in 2021 compared to 2020

Nearly 80%

of cyberattacks leverage identity-based attacks to compromise legitimate credentials and use techniques like lateral movement to quickly evade detection – how can you give insurers comfort that your organisation sufficiently protects credentials, particularly privileged credentials?[2]

1. Coveware May 3, 2022 Quarterly Report: https://www.coveware.com/blog/2022/5/3/ransomware-threat-actors-pivot-from-big-game-to-big-shame-hunting

2. Crowdstrike 2022 Global Threat Report: https://www.crowdstrike.com/global-threat-report/

Key considerations for insurance buyers

Insurers are continuing to take a careful approach when considering new or existing risks. Clients are routinely asked to provide evidence of sufficient cyber security controls before a risk will even be given consideration.

Addition written submissions Insurers are increasingly required with a focus on Ransomware controls. Insurer presentation meetings are also commonplace.

Before submitting new or renewal risk proposals clients should:

- Ensure key stakeholders (Directors and Chief Information Security Officers (CISO) for example) are briefed on likely insurer requirements. Communicate your broker's guidance regarding required levels of cyber security controls and the likely direction of premiums
- Consider the bigger picture and what would be a good outcome for the business from insurance negotiations
- Allow plenty of time to collate renewal information & to review/refine this with the help of your cyber insurance brokers.
- Present a well-articulated picture to insurers demonstrating your business has adopted a risk-based approach to cyber security. This will give insurers confidence in your cyber security strategy
- Consider your wider use of insurance and the potential to obtain more favourable terms from existing insurer partners
- Be open and collaborative with insurers in a partnership approach

Contacts

Martin Berry
Director
FINEX GB - Cyber & TMT
T: +44 1473 223 726
martin.berry@wtwco.com

Dean Chapman
Associate Director
FINEX GB - Cyber & TMT
M: + 44 7920 211 779
dean.chapman@wtwco.com

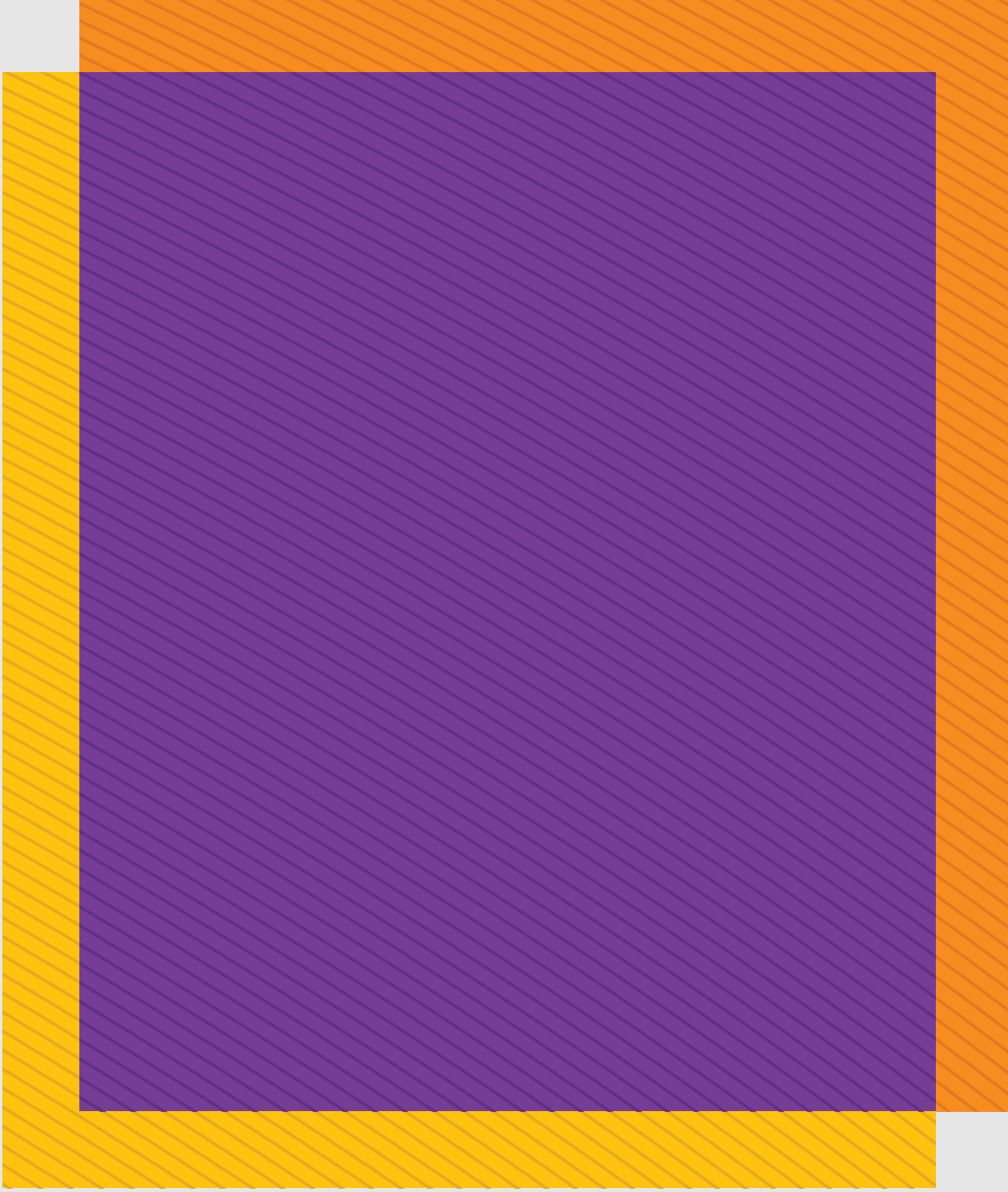
Matt Ellis BSc (Hons), MSc
Director
FINEX GB - Cyber & TMT
T: +44 20 3124 6611
M: +44 7810 831 661
matt.ellis@wtwco.com

Adrian Ruiz
Director
FINEX GB - Cyber & TMT
T: +44 20 3124 6820
M: +44 7908 070 031
adrian.ruiz@wtwco.com

Simon Basham (Global contact)
Head of Cyber & TMT Broking (UK) FINEX GB
T: +44 203 124 8415
M: +44 7795 855 925
simon.basham@wtwco.com

Jason Warmbir
Senior Director, US
T: +1 312 607 0096
M: +1 312 288 7846
jason.warmbir@wtwco.com

Ben Di Marco
Director, Australia
T: +61 478 312 988
benjamin.dimarco@wtwco.com



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 organisational resilience, motivate your workforce and maximise 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

FPS3333306 WTW-FINEX 523904/07/22

wtwco.com