ALTA SIGNA

European Cyber Insurance - A Maturing Market Entering an Attractive Phase?

Market Bulletin:

Reflections on 1 January Renewal and Outlook for 2023

www.altasigna.com

ALTA SIGNA

Contents

1:1 Cyber Renewals and 2023 Forecast

A Market Bulletin from Alta Signa

January 2023 Renewal Dynamics at a Glance

Excess Layers:

- A fundamental shift in pricing for excess layers driven by competition
- New capacity is following in with new entrants
- Existing carriers are increasing their cyber line sizes
- Increasing competition from Lloyd's in Europe
- Underwriting predominantly driven by ransomware losses
- Stronger follow form is expected in 2023 with fewer exclusions in excess layers

Primary Market:

- Primary layers still lack competition
- Adjustments still expected based on loss experience
- Retentions are increasing: cyber seen increasingly as a catastrophe cover

The history of now: Pricing has changed, but has the risk?

It is fair to say that Q4 2022 and 1.1 renewals cemented a fundamental shift in market dynamics and new capacity for excess large cap cyber risks across Europe, with regional and sector specific nuances.

The reasons for this shift are global, from the litigious and class actions in the US, to the improved perceptions of cyber risk in Europe.

The latest headline is that the cyber tide has turned in Europe, and capacity constraints on excess layers that dominated over the last few years have suddenly been relaxed through capacity from Lloyd's and companies' markets. Despite this, capacity constraints remain in primary layers, which impacted on pricing at 1.1 renewals.

This shift in dynamic is driving up demand for MGAs with local expertise, which in turn is driving greater demand for binding authority in European cyber. However, concerns regarding underwriting discipline, wordings, and claims environment in the future still remain. As a result, the market must continue to work with expert distribution partners - and stick to solid underwriting discipline in an increasingly competitive market.

The context for January's renewals

Towards the end of 2022, European excess cyber rates declined, culminating in undercutting on some accounts leading, in our view, to risky underpricing. Following fair analysis, we should be asking ourselves was this decline based on human and budget bias, or did the underlying risk actually change?

Let's leave this as an open question for now while we explore the context of what happened. When the cyber market started to harden in late 2019 and early 2020, European rates for mid-sized to large risks were significantly lower compared to the London Market equivalents.

Compared with today, insurance market penetration rates were still low and clients buying large insurance programmes could generally find the required capacity locally. Limits of EUR 25 million offered per insurer and beyond were no exception.

The pandemic and ransomware changed everything

Unfortunately, no one could have predicted what would happen next: the global COVID-19 pandemic. Faced with unforeseen challenges, the pandemic impacted every aspect of the insurance sector, including that of the cyber market.

Almost overnight, the IT requirements for businesses to adhere to the "new normal" were significantly increased as entire companies shifted to remote working. As well as a shortage in mobile devices, a lack of available secure connections quickly proved to be a real and immediate threat, causing a dramatic increase in the surface area of attacks compared to pre-pandemic times.

Understandably, the underwriting process needed to adapt to this new and uncharted situation. But this wasn't all the cyber market had to contend with; almost simultaneously, the number of ransomware claims exploded, Kickstarting what was to become the beginning of a hard market spiral.

As we moved through 2020 and 2021, capacities offered per insurer were reduced significantly to as low as EUR 5 million on primary layers, depending of course on the industry and the client's security standards. At the same time, high profile ransomware attacks in the press, together with authorities' recommendations and client's contractual requirements, led to a surge in demand.

With a constantly changing underlying risk vector, cyber was proving itself to be unique. And what's more, it encompasses systemic risk — a scenario that has been seen as uninsurable.

Market response

As a consequence of reduced available capacity and an increased demand from insureds – in many cases including primary and excess layers — rates were adjusted to single digit percentage rates per million as a new standard. Before long, even double digit percentage rates per million on primary levels weren't unique anymore.

The underwriting focus soon shifted heavily towards ransomware attacks — a main loss driver in the European cyber market and generally went much more in-depth on a technical level.

Dedicated ransomware proposal forms and underwriting considerations, together with coverage restrictions, were only one part of the community's response to the surge in ransomware cases. Even those so-called best-in-class risks — i.e. clients with the highest available security standards — struggled to get the capacity they desired, and many paid high premiums, especially for additional capacity.

Hardmarket dynamics and asymmetries

Clients renewing their existing programmes throughout the hard market, profited from year-on-year benchmarking of underwriters. But despite a more soft-gloved approach, this often nonetheless resulted in significant rate adjustments - often approaching 100%. These rates still ultimately ended up relatively low compared to fresh additional capacity coming in at new market rates.

This situation led to programmes that didn't follow any actuarial logic anymore, often with increased Limit Factors (ILFs) north of 100% on excess, and often with the most expensive capacity sitting on the least risky layer.

Coverage for ransomware-related costs was often restricted or shared with the client through co-insurance endorsements, while wordings carved out largely revolved around cyber interruptions originating at vendors. Retentions reached levels that only a few years ago seemed unsellable, increasing from below a million to multiple millions.

A change in dynamic

Between spring 2020 and spring 2022, the cyber insurance market continued to harden, leaving some market observers fearing insurers would overdo it and encourage clients to withdraw from the coverage, as they'd prefer to retain the risk on their own balance sheet. However, before summer 2022, signs of stabilisation started to emerge. Some programs saw single digit percentage increases on primary, while excess layers renewed flat. The first ransomware co-insurance endorsements were also removed.

After summer 2022, an increasing number of renewals saw slight or no rate increases on primary, while excess layer rates were generally aligned to follow the ILF curves, with decreasing rates per million across the programme.

What initially started out as stable, market conditions quickly flipped, putting pressure on excess layers with ILFs sometimes below the 70% mark compared to underlying limits, which 12 months earlier used to be above 90% as standard. If based on actuarial judgments, this would mean that the market saw the potential of devastating attacks burning entire insurance programmes as less likely than 12 months ago, a hypotheses which is difficult to verify.

Valid arguments in favour, like an on average better risk profile, allowing clients to contain a suffered attack quicker thanks to adequate tools and hence limit the damage, could be cited. Nonetheless, due to the immediate start of the changing dynamic a human bias looks more likely as a dominant driver.

The competition at 1 January 2023 renewal was especially fierce on large programmes with London Market involvement, where internationally active syndicates potentially tried to compensate for lost premiums in other territories, e.g. from non-renewed major US programmes.

When many Lloyd's syndicates struggled with their stamp capacity towards the end of 2021, the opposite was the case one year later. This further increased competition on excess layers on the continent, and for the first time some London-based underwriters offered at more competitive rates than local European players. Just as had been witnessed only two years prior, these factors came together almost simultaneously in the opposite direction.

Systemic risk and first party losses are the sword of Damocles

Barely a month passes without an executive commenting on the uninsurability of the potential systemic cyber risk. This is the very real chance that a catastrophic, cascading event could stem from a cyber attack that would have significant contagion across businesses, infrastructure and supply chains, triggering multiple insurance programs and coverages and causing massive disruption to a society and economy.

So, how do insurers view cyber systemic risk? At first, the war in Russia further increased the fear of systemic cyber threats at nation-state level, and some insurance companies tried to address this fear through an exclusion of systemic events.

However, the reality in the current market is that clients resist this kind of wording restriction, and will prefer capacity where systemic events are not excluded. This leads to a problem in that only clients with no alternative will accept this restricted coverage — resulting in potentially adverse risk selection.

Although it is questionable whether a systemic cyber risk exclusion would even be upheld in a continental European courtroom, no conversation about cyber insurance happens without touching on the challenge of systemic risk, but tangible actions are difficult to undertake.

Regarding the devastating potential of first party losses, there is certainly a human factor coming into the equation. Many European cyber underwriters have a professional lines background, with experience underwriting third party loss products which go hand in hand with a higher natural barrier for claims.

Is this shared background and higher risk tolerance potentially one reason why the devastating loss potential of business interruption seems not to be considered sufficient any longer, considering the rapidly decreasing development of ILFs? Think of a very large business with EUR 50 billion annual revenues and more, it seems unjustifiable that an ILF curve would taper off, especially when as a significant business interruption claim alone could burn a tower within very little time.

Some food for thought at the very least.

European cyber insurance:
how has underwriting adapted?

The cyber insurance market has undergone fundamental changes since 2019. The most notable shift is that cyber underwriting has had to adjust to major loss trends, a change driven predominantly by ransomware exposure. A comparison of today's proposal forms, with an equivalent from 2016 for example, starkly visualises this shift in thinking and understanding of exposure.

Calling pre-pandemic underwriting clueless, however, wouldn't be fair. Cyber insurance is still a relatively new and immature product line, and its underlying risk vectors change much faster compared to most other insurable risks.

It is, therefore, rather fair to say that today's underwriting has been forced to adapt to a completely new risk environment, one which has been heavily dominated by a shifting focus towards ransomware-related vulnerabilities. As a result, the cyber market will most likely remain one of the most dynamic markets in terms of risk analysis, and will therefore present a challenge for the underwriting community. However, a positive dynamic stemming from the hard market that may last is the shift in clients' thinking around cyber exposure and insurance as a coverage for catastrophic exposure. While today many clients have invested proper money into cyber resilience, the view on insurance has evolved into corresponding insurance structures tailored for multinational clients, who are also willing to use captive vehicles to retain the frequency exposure and transfer this risk more cost-effectively.

Such adjustment of the business line has been necessary, in terms of coverage, pricing and capacity management. On the client side, the hardening market and more technical underwriting approach left some without capacity, mainly because they were deemed uninsurable. The hardmarket was, in effect, a wake-up call.

The shifting sands of cyber psychology

The mentality among buyers of cyber insurance has evolved substantially over the last few years, with many businesses from SMEs to international corporations now appreciating that cyber is a stand-alone cover in its own right.

With a constant stream of headlines about cyber incidents, data breaches and regulatory penalties, cyber risk has for some time been a hot boardroom topic. There is also appreciation from buyers that cyber insurers have every right to insist on robust security measures and risk mitigation strategies as part of the risk transfer mechanism to secure a policy.

This risk mitigation pressure from insurers, combined with the prospect of significant fines for data breaches and the wider reputational impacts of a cyber incident on a business, are fostering a stronger than ever security culture as both a mindset and mode of operation.

This is a very positive dynamic that, if properly integrated into day-to-day thinking and decision-making within an operation as an active mindset, can improve the overall resilience — and in particular data efficiency — of an operation beyond cyber security.

Cyber risk is always somewhat a game of cat and mouse, whereby law enforcement, governments, regulators and businesses attempt to get ahead of cyber criminals. And the frontiers of cyber risk will always shift — for instance application programme interface (API) risk is likely to feature strongly in 2023 — as criminals find new ways round cyber defences, or fresh ways of exploiting new weaknesses.

Ultimately, the psychology of cyber risk mitigation for both individuals and business has matured rapidly, and continued efforts by the insurance sector to educate the market about effective risk mitigation will be key to furthering this positive trend.

The Cyber Crystal Ball:
What to expect for 2023

The cyber insurance market is difficult to make concrete forecasts for, given how quickly dynamics are changing. However, based on what we have seen at January's renewal and in the run-up, we expect the adjustment of adversely placed programmes to continue throughout the coming year, and pressure — especially on excess placements — will continue to increase.

At the same time, excess wordings will see non-follow form conditions being removed, and drop-down into sub-limits that were largely removed will likely be claimed again.

A further inflow of new capacity, either through insurers not previously active in the cyber space, or through newly established European branches or MGAs, is also expected to further accelerate the competition on excess layers.

Primary differences

The situation, however, will be different for primary placements where fewer players share the market and brokers cope with limited competition. Due to this situation, the trend towards clearer defined and more standardised wordings focusing on core coverages is expected to continue.

Regional variations

In recent years we have observed some local differences in pricing, which were unlikely to have been data driven. This is because certain regional markets benefited from local capacity that was not accessible from other countries in Europe, helping some countries' markets to avoid the extreme rate increases that were seen elsewhere.

This discrepancy between similar risks, in terms of company profile but with the insured entity being headquartered in different jurisdictions, still remains, and most likely downward pressure will be higher in the more expensive countries. It is, for example, fair to say in broad terms that it was more difficult to place cyber coverage for insurance companies for instance in France compared to Germany or Spain, while insurance for banks seemed to be more welcome by underwriters in France or Italy compared to Spain.

An end to pricing extremes?

Nevertheless, in our view the extreme swings over the past two years are on the one hand a result of unique changes in the underlying risk assumptions, and on the other hand the outcome of an immature market.

We hope that cyber penetration rates will continue to increase as the market matures, fuelling demand for additional capacity, resulting in a sustainable equilibrium over the mid and long-term, and avoiding the kind of drastic rate softening which ultimately leads to the kinds of combined ratios seen in 2019 and 2020, which reached deep red levels far above 100%.

At the same time, market education will play a far more central role in 2023. At the peak of the hard market, clients were forced to search for any capacity where available, and behind the scenes Bermudian-based reinsurers played a crucial role in helping match the need. In essence, expert local distribution knowledge seemed less crucial back then, quite simply because any available capacity was snapped up, independently of inconveniences for clients like foreign language wordings or outside the continent claims handling.

Now, the market is developing apace and returning to local language and standards for cyber policies and culture. In this respect, MGAs will play a major role in the development of the European Cyber market in 2023 and beyond, especially for those insurance companies not having the local structure to access the business directly in Europe or lacking the underwriting expertise. A further advantage of teaming up with an MGA is the possibility to outsource this kind of entrepreneurial risk, and first observe how the market further evolves.

Client perspective

For clients, the cyber market has played a crucial role for both benchmarking and as an information sharer and educator. In addition, the increasingly technically advanced understanding of the insurance market when it comes to cyber risk, and the resulting cyber security requirements within policies, have helped build resilience for many clients.

It seems that the reduction in capacity purchased by some clients seen towards the end of 2022 and into the January 2023 renewals is most likely a delayed reaction to the high premiums seen in 2021. If so, a new increase in purchased capacity by clients due to more favourable premiums is therefore likely to be seen in 2023 and at January renewals in 2024.

ALTA SIGNA

Contact

the Alta Signa Cyber Experts

Ingo Trede

Email: Itrede@altasigna.com

Tel.: +34 666 239 815

Paulina Radgowska

pradgowska@altasigna.com

+48 533 877 348

Nico Spruit

nspruit@altasigna.com

+32 456 32 63 39

www.altasigna.com