Gallagher Re

CY–FI

The Future of Cyber (Re)insurance

Executive Summary

In 2018, Gallagher Re (then Capsicum Re) wrote a white paper outlining an expectation that the reinsurance market will soon become redefined as PC&C (Property, Casualty, and Cyber). Four years later, it seems this evolution is well on the way; the COVID-19 pandemic has evidenced society's ever-expanding technological dependencies, the conclusion of the Lloyd's non-affirmative deadlines is creating momentum for standalone Cyber growth, and the demand for Cyber cover is continuing to soar as our headlines are occupied with stories of Cyber-attacks and new technologies.

So what next for the Cyber market? By 2040, we (at Gallagher Re) believe that Cyber will be comparable in size to either Property or Casualty and will have long since exceeded them in terms of annual reinsurance premium. This paper explores how we will get there.

First, we explore how the Underwriting Revolution that began in 2020 will continue into 2022. Furthermore the crunch in capacity against a backdrop of insatiable demand has led to a decoupling of premium and aggregate exposure. This has enabled (Re) insurers to leverage the full range of tools at their disposal (ranging from coverage to use of technology) as they look to deploy their budget against better quality risks. This Underwriting Revolution lays the foundations for future growth, as growing appetite for Cyber risk will stem from its increasing profitability.

2023 could see the start of Cyber's second growth wave as decreasing loss ratios, greater confidence in underlying risk quality and limited actual losses from high profile cyber events raise confidence. Unlike other markets, where enormous capital injection would seem a symptom of a softening market, capital will bring positive changes within Cyber. We explain how this will take the form of continued investment in the understanding and mitigation of potential losses through technology-led solutions.

From 2025, increasing clarity over Cyber's future as an insurance heavyweight buoyed by market confidence in the ability of data to predict claims will drive a 'data arms race' by reinsurers and Cyber Security vendors as scale is required to fully realise technology potential in loss ratio improvements. We expect this convergence between technology solutions, Cyber-security techniques, and reinsurance will create a virtuous cycle, as investors seek to protect their capital invested in the space.

Concurrently, we outline how Cyber can become the model class in regard to product innovation and diverse distribution, as it attempts to meet the growing capital base's appetite. Finally, we will review what the Cyber market will look like in 15 years time with the benefit of these changes.

While there are many factors that could influence the future of the Cyber market, much of what is explored here is, we believe, more a matter of not if, but when. Sci-fi has a strong track record for predicting the future and there's no reason Cy-Fi won't do exactly the same. We'll just have to wait 20 years to find out...

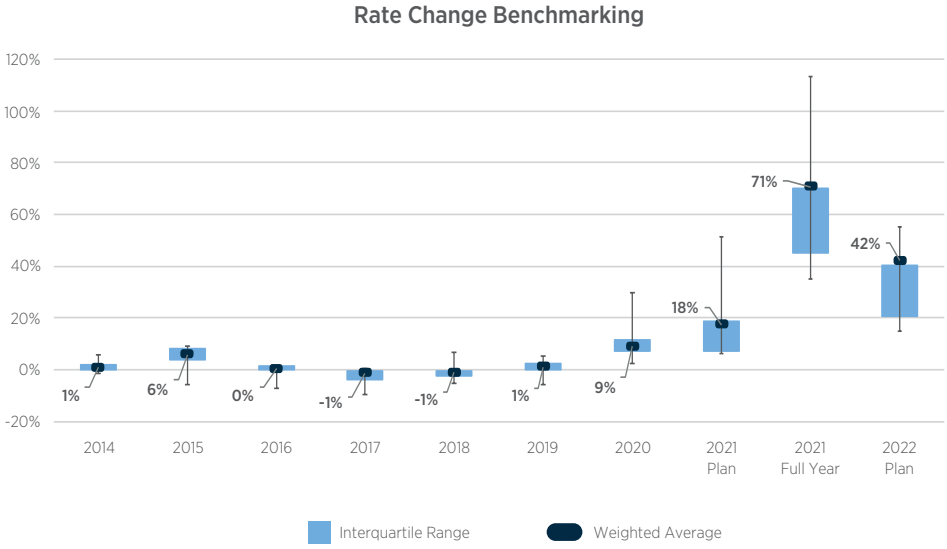
January 2021 to December 2022 – An Underwriting Revolution

When we describe the past 12 months as 'revolutionary', we do not do so lightly. The changes in rate, portfolio make-up, coverage, and underwriting (both risk selection and loss mitigation) over the past year have been staggering, and we expect this trend to continue into 2022. In this section, we outline the ingredients that have enabled this revolution over the past year and detail what lies in store for the next 12 months.

...portfolio increases of between **35%** and **113%** observed in 2021 alone...

Rate Change

Over the past year, the Cyber market has seen unprecedented rate changes, with portfolio increases of between 35% and 113% observed in 2021 alone.[1] In 2022, we expect to see the headline-grabbing rate rises observed over the past year continue. Additionally, 2022 will likely reap the benefit of the compounding rate changes. Similar to the past two years, these rate increases will be most acute for those purchasing insurance in the latter half of the year, reflecting underwriters' efforts for pricing adequacy.



Rate change benchmarking 2014-2021, Gallagher Re

These rate rises, driven in part by increased ransomware activity, are beginning to manifest in improving previously deteriorating loss ratios and 2022 is when the market could really see the loss ratio improvements manifest. We see this as an opportunity for the market to reassess and re-underwrite their portfolios.

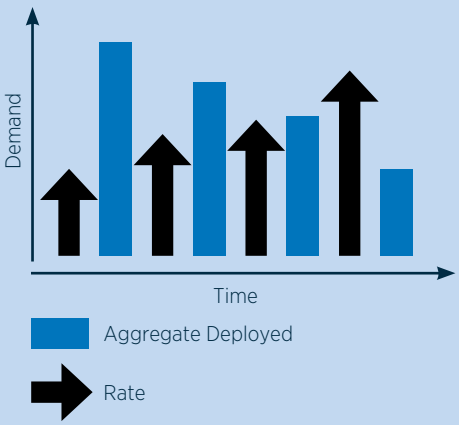
Premium Problem

Despite carriers achieving rate adequacy and the improving posture of Cyber risks (a result of other underwriting changes explored below) we anticipate rates will continue to rise in the near term. This is due to the continued capacity crunch and the market's 'premium problem', which results from business planning being conducted on a premium basis rather than exposure basis.

Business planning on the basis of premium written is a common industry standard and continues a decades-old approach. Inadvertently, this method of business planning punished Cyber as a class, as carriers accepted that every time rates went up, they would in turn write less aggregate in order to accommodate their business plans agreed by boards and/or regulators. This has resulted in a significant reduction in total aggregate limit deployed, as carriers look to stay within budget. For Cyber, at least for now, the link between premium and exposure has been severed. Now, looking ahead through 2022, we are seeing the rate momentum continue, and many insurers are already looking to adjust their targets significantly, having projected 15%-55% rate increases,[2] or face stunted growth.

As an investment heavy class of business, a continued restriction of premium will likely lead to short-term profitability, but may also stifle long-term innovation, market relevance, and impact the capabilities of carriers with smaller market share. This is a cycle we anticipate to endure in 2022 until significant additional capital is deployed or planning is rethought. Indeed, many syndicates are unable to renew existing business, let alone write new business, and have no new capacity to deploy, further widening the gap between supply and demand.

Whilst premium remains elusive, demand for Cyber cover only continues to grow. Another consequence of the ransomware activity is the increasing attention paid to Cyber as it becomes a decidedly board-level issue. A recent PwC report observes 55% of organisations significantly increasing their Cyber investment in the wake of the pandemic.[3] Cyber is also ranked second (behind pandemics) on the top concerns for CEOs this year.



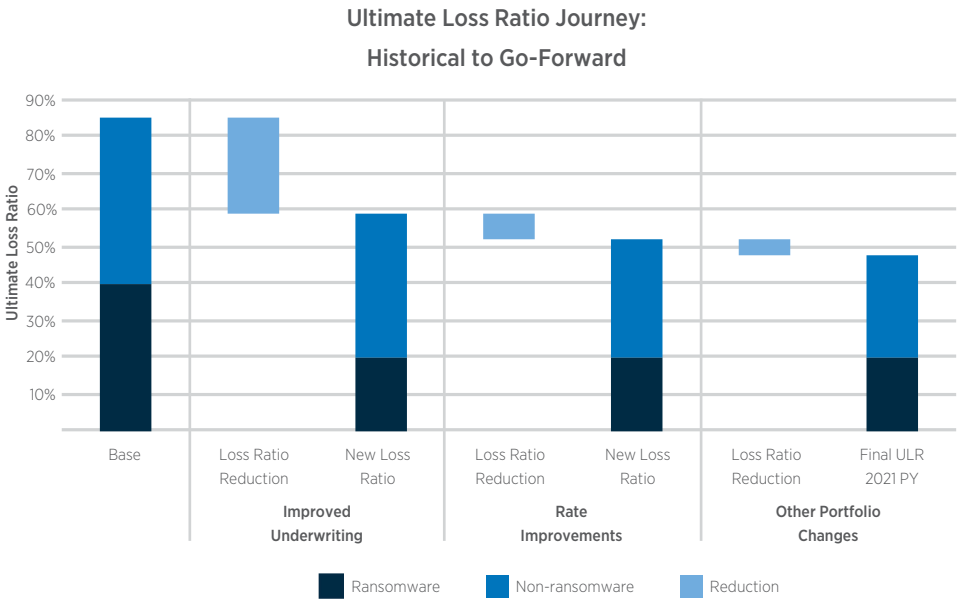
The 'premium problem', Gallagher Re

For Cyber, at least for now, the link between premium and exposure has been severed.

Underwriting Revolution

Whilst historic rate increases have grabbed the headlines, this has masked a bigger story: the underwriting revolution the Cyber market went through in 2021. For example, underwriting questionnaires have become more targeted, with many in the industry using specific 'ransomware' questionnaires with a focus on the controls effective at preventing or mitigating the conversion of incidents into claims (such as multi-factor authentication and having well-placed segregated backups). Other underwriting tactics include the tightening of terms (e.g., sublimits, coinsurance and deductibles), strengthening exclusionary language (e.g., broadening of infrastructure exclusions) and coverage restrictions (e.g., contingent business interruption). These stricter underwriting controls mean retention rates are at an all-time low, which we estimate to be between 50%-75%.[4]

These stricter underwriting controls mean retention rates are at an all-time low...



Theoretical industry waterfall

Structure	• Sublimits • Coinsurance
Technology	• Outside-in scanning
Coverage	• Exclusionary language • Per-event caps
Risk Optimisation	• RAG (red, amber, green) ranking systems for insureds • Risk tolerances for different industries

Changes to terms and conditions in the market, 2020-2021, Gallagher Re

Cyber Insurance Driving Cyber Security

As far back as the 18th century and the fire insurance plaques affixed to London properties, the insurance industry has been closely aligned with loss prevention. This remains true today as insurers look to protect their premium. In addition to the more traditional underwriting approaches outlined above, the industry has also evaluated and deployed technical solutions (e.g. outside-in scanning and aggregation modelling) to help in risk selection, pricing and portfolio optimisation. This adoption will continue to muster pace in 2022 as these technologies are integrated to: improve risk selection and underwriting, evaluate exposure to single points of failure in existing portfolios, and offer post-bind services in order to prevent claims by notifying potentially-exposed insureds as an incident unfolds.

Whilst these technologies are young and imperfect, the ability of these innovations to overcome their 'teething problems' combined with clear appetite from the insurance market to deploy them evidences that they are here to stay. Already, the ability to isolate and analyse certain data points in order to materially impact exposure is indisputable.

Gallagher Re is investing in understanding the ability of these technologies to predict Cyber claims, enabling our clients to use them most effectively. Our initial studies have shown that external scanning has some merit in predicting past claims, when used appropriately and proportionately. An illustrative example is that by denying coverage to insureds which appear to have exposed 'remote desktop protocol (RDP)', insurers can theoretically insulate themselves from a vector used to compromise victims in roughly 45% of current ransomware attacks.[5] Indeed, one carrier has claimed they had been able to reduce ransomware claims by 65% through scanning for open RDP ports.[6]

This increased use of technology extends beyond underwriting and pricing alone. One example of this is the utilisation of external scanning technology by insurers to help insureds respond to emerging and time sensitive Cyber events. For example, 2021's Microsoft Exchange vulnerabilities saw a large number of companies become exposed overnight to exploits that attackers could pursue remotely. Insurers harnessed the 'attacker's view' to notify insurers of their potential susceptibility to attack. In proactively engaging with insureds, one Cyber MGA estimated that they were able to "remediate the vulnerability for 98% of impacted policyholders within a week of the disclosure".[7]

These improved underwriting terms, efforts at portfolio optimisation, and the adoption of new technologies will further facilitate a return to profitability for the Cyber market over the next 18 months. We could begin to see the impact of these changes in industry loss ratios for 2022, but it will take longer for the full magnitude of these revolutionary changes to become fully apparent in the triangles.

Insurance Linked Securities (ILS) Enters Cyber

Whilst there has been involvement from the ILS community in Cyber since Gallagher Re did the first trade in 2016, ILS has not yet become a material part of the market. In 2021, we observed a change as both buyers and sellers grew increasingly comfortable with occurrence products, with increasing confidence in the event language and coverage triggers, as well as the potential tail losses.

Occurrence is also of increasing interest as carriers' attritional loss ratios drop significantly, and quota share and aggregates become less efficient products. Additionally, as the rated reinsurance and retro markets fail to grow in parallel to the underlying demand, (re)insurers will be forced to seek capacity in alternative forms.

...the ability to isolate and analyse certain data points in order to materially impact exposure is indisputable.

January 2023 to December 2025 – Confidence Drives Capacity Growth

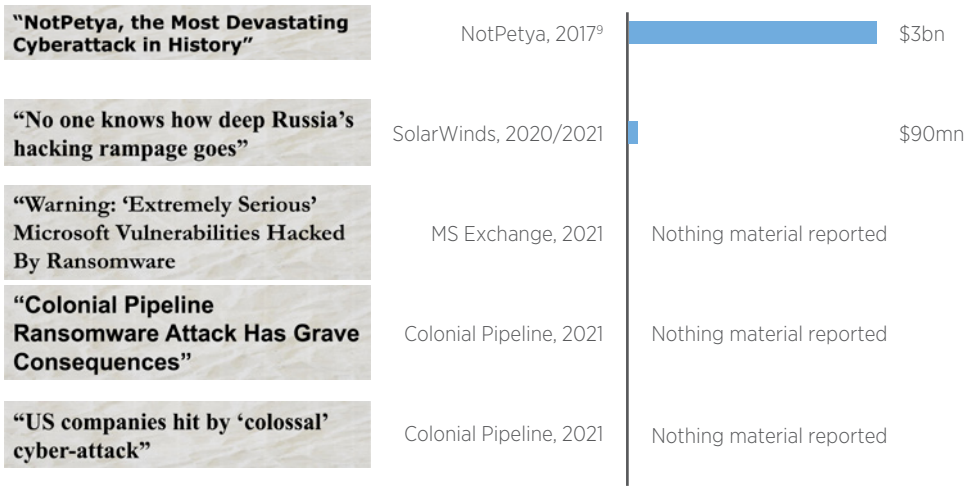
A Surge in Capacity

We've shown above that a crunch of capacity in the face of exponential demand growth has been the greatest challenge the growing Cyber market has yet faced. Without significant increase, it risks being an inefficient market with insureds finding it ever harder to obtain coverage at reasonable cost. Fortunately, by 2023, we expect the impact of the underwriting revolution in 2021-2022 to begin to show, improving confidence from capacity providers. We outline some of the major drivers for this confidence shift below.

Already, Gallagher Re sees a large disparity between the loss expectations these events produce, and the reality.

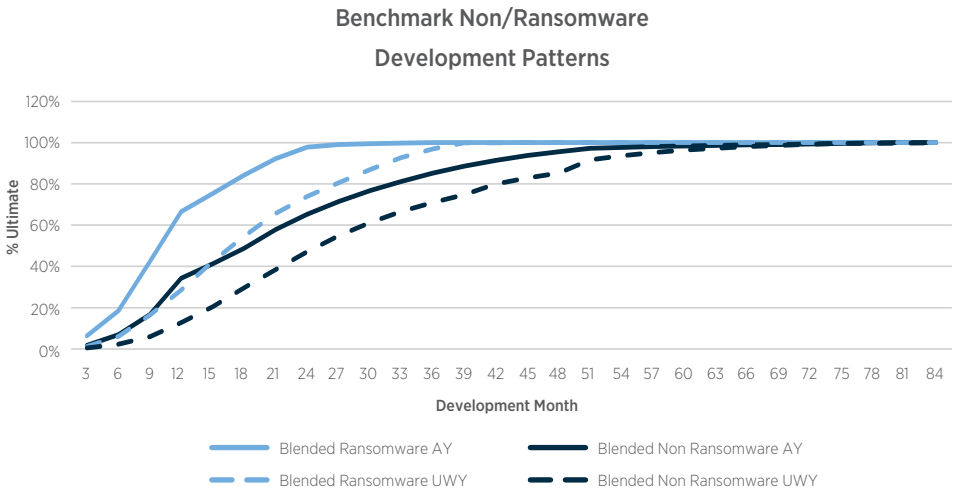
Improvement in Quality of Underlying Risk – One of the leading consequences of the underwriting revolution, and specifically the widespread harnessing of Cyber data and targeted questionnaires in the underwriting process, will be a significant improvement in the quality of the underlying insureds. Furthermore, the same data insurers have begun to harness in the underwriting revolution will enable stronger portfolio optimisation and the ability to shed the worst performing risks, again providing uplift to the quality of the underlying risk. This improvement in insurers' ability to 'cherry pick' companies with greater Cyber Security maturity is further benefited by overall improvements in risk quality by insureds and prospective insureds alike.

Understanding the Disconnect Between Cyber Headlines and Losses – As the market has grown, insurers have been concerned that sudden changes in the threat landscape in combination with the systemic nature of Cyber risk can result in significant exposure to CAT-like events. Over the course of 2023, it will become clearer that large headline enticing Cyber events—such as SolarWinds, MS Exchange and the Log4J vulnerability—didn't produce losses on the scale anticipated due to a number of disaggregating factors. These headlines were, at the time, often accompanied by doom-laden declarations questioning the very insurability of Cyber risk and understandably concerned a whole swath of the market. Already, Gallagher Re sees a large disparity between the loss expectations these events produce, and the reality.[8]



Insured losses (USD) (publicly reported as at December 2021) versus the headlines
NB. NotPetya loss includes non-affirmative cover

A Healthier Risk – As we move through 2023, the impact of changes made as part of the underwriting revolution to the long-term health of the Cyber market will likely manifest in decreasing loss ratios and development triangles. In 2021, Gallagher Re published a paper arguing that ransomware claims develop quicker when compared to other Cyber claims patterns and across other lines of business. In light of this, more efficient reserving for ransomware by the market will free up additional capital for reinvestment, whilst triangles for years 2020 and 2021 will show drastic improvement. This market greater clarity over how the underwriting revolution has impacted exposure to ransomware. This will be followed in 2024 by healthier development patterns for non-ransomware Cyber risks.



Gallagher Re has consolidated claims experience from clients to investigate and understand potential patterns in developing ransomware and non-ransomware losses independently

Pricing Stabilisation

Pricing in Cyber has always fluctuated due to the dynamic and evolving nature of the threat landscape and growing exposure surface area. However, this should stabilise as the supply-demand dynamic that is today causing the premium surge comes under control.

In almost any other market, this would result in a market softening but it is not likely to be the case for Cyber. Indeed, Cyber will unlikely be over-capitalised in the near future. This is in part due to its enormous growth potential, but we also observe the phenomena of greater investment in Cyber prompting stronger investment in product development and distribution, leading to further growth.

Second Wave Growth

The Cyber market has been exceptionally innovative. This innovation has ranged from new product creation, to new forms of distribution and offering insurance buyers incentives outside of pure indemnity, just to name a few examples. At the turn of this decade, the market has refocused from innovation towards the stabilisation of past growth, as it looks to maintain or reduce aggregate over the pursuit of growth. Much of this stabilisation, as explored above, has been directed around better understanding ransomware exposure. However, with a new influx of capital from 2023, twinned with the stronger foundations provided by more robust underwriting standards and portfolio strength, the Cyber market can truly embrace product innovation once again and provide a broader range of coverage to a greater breadth of insureds.

The Cyber market has been exceptionally innovative.

This will manifest in several ways.

Firstly, we will see significant product innovation: from the growth of personal lines Cyber, to building on existing products such as Cyber-physical damage, Cyber-marine, and Cyber-IP products.

Secondly, Cyber will expand into new territories while becoming further entrenched in more developing markets, like Europe and Asia.[10]

Thirdly, distribution will continue to evolve with insurers offering focused products for different channels to market. For example, we anticipate Cyber will become a significant part of employee benefits, with employee personal security becoming increasingly important to companies as the world embraces hybrid working.

Case Study: Cyber Personal Lines

Encapsulating each of these three aspects of innovation is Cyber Personal Lines. In 2018, the market was estimated to generate less than $500 million,[11] but forecast to reach $3 billion in 2025.[12] The risk to an individual of digital theft is approximated at higher than physical theft or damage, and yet the purchase of contents insurance is considered standard in developed markets.[13] Whilst there are early success stories with some penetration in specific markets e.g., Singapore or high-net worth individuals, uptake of Personal Lines Cyber lags well behind uptake in Cyber cover by businesses.

Gallagher Re anticipates Personal Lines Cyber to be a major beneficiary in the Cyber market's second phase of growth, becoming a common insurance purchase for individuals and families residing in developed markets by 2030. This growth will be facilitated by the merger of astute insurance products with natural distribution channels. For example, personal Cyber cover may be offered to individuals as they purchase an Antivirus Solution, as a Current Account switch incentive or even be packaged with a 'smart home device'. Personal Lines also presents an opportunity for insurers to further invest in Cyber, but diversify their risk, as the threats faced by individuals are often different from those of businesses. With this comes a new challenge for markets to understand the nature of the different aggregation risks Cyber Personal Lines inherently presents.

Through this second growth wave, Cyber insurance will continue to be a positive driver for Cyber Security change. For many companies, particularly SMEs, the cost of the Cyber tools and expertise needed to improve Cyber hygiene to an acceptable standard for insurance coverage are prohibitively expensive and complex. Insurance will continue to look to enable positive change, by providing companies impacted by this Cyber Security 'protection gap' with the services they need to become attractive insureds, all as part of an overall insurance package. There is ample space for innovation here and we can expect to see a myriad of different insurance products targeting different groups of insureds in different geographies. Technologies under this umbrella may include advanced 'CISO-as-a-Service' platforms, but will likely focus on ensuring basic security hygiene is in place for the insured. Providing the tools an insured needs to defend themselves offers an additional benefit; the ability to review and analyse data reported from these tools to better understand exposure risk. An emerging Cyber MGA aims to be a frontrunner in this space.[14]

Data Arms Race

As described above, technology has enjoyed an increasingly large impact on the profitability of (re)insurance providers, with the underwriting revolution unveiling it as a key instrument in both assessing and mitigating Cyber risk. A wide range of data vendors have been engaged by the market to facilitate the provision of this data and have typically enjoyed relatively low barriers to entry, ample investment and a receptive target audience. As (re)insurers gather an ever-stronger understanding of their data requirements and look to launch new products as the second growth wave gathers pace, they'll demand more sophistication from vendors, opting for partnerships with data vendors that provide either strong differentiation (in their product), specialism (in the type of data offered/place in data value chain) or market-leading edge.

Increased barriers to entry, twinned with M&A activity for attractive vendors will result in another surge of innovation from vendors, but also significant market consolidation from 2024 onwards. This increased demand from the market, driven by a greater appreciation that scale typically provides Cyber vendors with a data accuracy advantage, will herald a land grab by vendors, (re)insurers and other interested parties alike.
The market has already seen early movement in this space, with the purchases of BinaryEdge and ThreatInformer, respectively.[15] Early activity has also been seen outside the market with Moody's acquisition of BitSight, RMS and VisibleRisk; a move that could herald 'copycat' deals from other credit ratings agencies with ambitions in quantifying Cyber risk.[16]

January 2026 to December 2029 – The Market Reaches Maturity

Growing Barriers to Entry

The 'data arms race' we predicted above, evidences the benefits of scale afforded to Cyber data vendors providing solutions for insurance. Gallagher Re predicts this growing barrier to entry for data vendors will be mirrored for prospective new market entrants. In essence, as the level of sophistication required to compete in the Cyber insurance space increases, it becomes more and more challenging to enter the space. As such, (re)insurers that stayed the course and continued to play a role in the Cyber market, as loss ratios rose in 2019 will reap the rewards of stronger risk selection and greater fidelity in portfolio optimisation, ultimately leading to lower loss ratios.

Following an influx in capacity and new market entrants between 2023-2025, (re)insurers still uncommitted to Cyber will likely show determination to enter the space as Cyber becomes an integral part of the industry as a whole. Some carriers will be forced to enter in order to remain relevant either to their consumer base or the industry at large, as Cyber continues to converge with other classes. Whilst some will enter following massive investment in teams and capabilities, many likely seek to deploy capacity behind existing experts as they do not have the appetite or capability to compete. We anticipate Cyber data modelling companies to play a key role in 'fast-tracking' new market entrants by providing them with access to many of the technologies and datasets that incumbents enjoy.

We anticipate Cyber data modelling companies to play a key role in 'fast-tracking' new market entrants...

Insurance and Cyber Security Convergence

As 2026 arrives, we predict an even greater long-term alignment between mitigating loss in Cyber and insurance. This will take the form of (re)insurers partnering with Cyber technology companies to offer insurance at point-of-sale and benefiting from the data they provide. This may take the form of partnerships, we've already seen early relationships between cloud service providers and (Re)insurers, or as the provision of key exposure-reducing Cyber products predicted above.[17] For the latter, uptake will be high as insurance, armed with value-add products, can present a cost effective and simple package for SMEs to level-up their security controls. For (re)insurers, this offering of Cyber Security products as part of the insurance process may provide a guarantee on baseline risk quality while proving more sticky, as (re)insurers enjoy higher retention due to the complexities of an insured moving to a different insurance provider with their own partnered technologies.

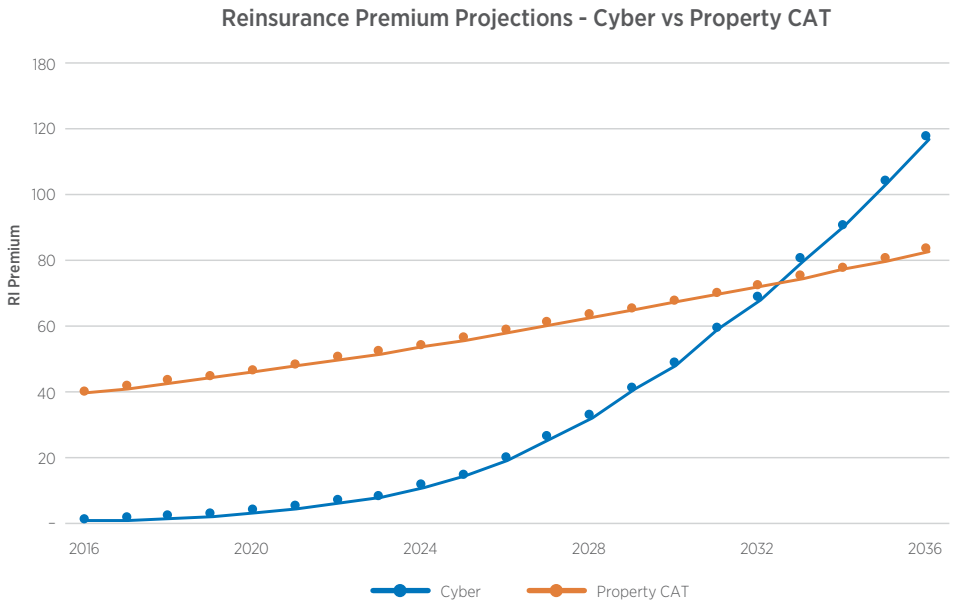
We've foreseen a land grab for Cyber data providers from 2024 as scale becomes a prerequisite for meeting the increasing expectations of an educated market. From 2026, this land grab won't be constrained to Cyber data providers and modellers alone. As the benefits of convergence between insurance and Cyber technologies becomes clearer, we'll see Cyber Security firms and traditional insurers alike race to partner with, buy, and set-up insurance companies to assist with distribution or to provide a warranty function behind their product.

2030 and Beyond – Welcome PC&C

If the Cyber market continues to grow at its current pace, it will double in size every three years.

Cyber Reinsurance Exceeds Property CAT

If the Cyber market continues to grow at its current pace, it will double in size every three years. Meanwhile, there will continue to be heavy reliance on reinsurers with what we estimate to be approximately 50% of insurance premium currently ceded to the reinsurance market. The emergence of Cyber Personal Lines and other product diversification will continue to drive the exponential demand growth, whilst new capacity will continue to emerge as loss ratios remain healthy.



Assuming average growth of 50% growth in Cyber premium in 2021 and an average of 25% for all subsequent years.

Assuming 46% premium being ceded to cyber reinsurance market in 2021, depreciating to 25% by 2040.

Assumed a growth rate of 3.9% for property for 2016-2028, reducing it to 3.5% for 2029-40 (ignoring cycles for simplicity).

In part, this profound growth is due to the prevalence of the quota share as a method of risk transfer. The predominance of quota share structures is driven by the fact that writing more Cyber will not necessarily negatively impact loss ratios. Since insurers writing Cyber will benefit from more robust data, effectively leveraging this data will enable further loss ratio improvements. Unlike other markets where loss ratio improvements increase the temptation to retain more business, markets can simply write more in Cyber, increase their net position and enjoy the benefit of the commissions and additional data this provides.

As Cyber outpaces Property, we anticipate a number of market-shifting changes. For example, we expect Cyber to become the most purchased type of insurance globally across personal lines, SME businesses, and large enterprises. We also predict the majority of Motor premium to become part of the Cyber market, as the motor product becomes a technology warranty for owners of large fleets. This will likely be paralleled in other classes like Aviation and Marine.

Cyber ILS Market Outpaces Property ILS

Cyber will be the largest driver of volatility and therefore, capital, in the industry. This is determined by both the size of Cyber and its systemic nature, i.e., it does not have the same points of disaggregation as the other key driver of capital: Property CAT. Rated carriers can therefore only take a limited amount of net exposure on their balance sheet and will look more and more to cede exposure to third-parties. The maturing of Cyber aggregation risk modelling, combined with increased trust in the ability of technology to adequately quantify and predict Cyber risk will be key to the scale of ILS influx.

Whilst Cyber may not present the most diversifying risk for capital markets, its absolute returns will encourage investors. The investor base will become far broader but also shallower than the current ILS market, and sees a larger number of parties making smaller investments. This is achieved through different structuring than we see today in ILS, where placements are done to a broader panel of investors either directly or on a secondary basis.

Conclusion

We've predicted this revolution to continue into 2022, providing the roadmap to the future of PC&C we first predicted in 2017.

Whilst Cyber remains a young class in comparison to its well-established peers, it has developed rapidly over the past 24 months as ransomware activity and capacity challenges have led to a revolution in rate and the way business is underwritten. We've predicted this revolution to continue into 2022, providing the roadmap to the future of PC&C we first predicted in 2017.

We've outlined how this revolution put in place solid foundations to restore Cyber's reputation for being one of the most profitable classes; attracting additional capital and confidence. This momentum comes as the rewards of rate changes, portfolio optimisation, and improved risk selection could be realised from 2023 in decreasing loss ratios, with Cyber insurance playing an ever-central role to improving the Cyber Security standards for insureds of all sizes.

From here, we've anticipated a second wave of growth for Cyber, not only in size, but also product innovation, with (re)insurance providing solutions for markets with lower penetration, underserved segments such as personal lines, and offering security essentials as part of the insurance package to organisations suffering a 'protection gap'. We've argued this, along with market realisation that the effective utilisation of technology, will kick-start a 'data arms race', with (re)insurers and Cyber technology vendors looking to harness, and in many cases acquire, data solutions which provide a competitive edge. We've predicted this technology 'land grab' will go one step further from 2026, with growing barriers to entry forcing a convergence of insurance and Cyber technology vendors in many places through partnerships and acquisitions.

Looking to 2030 and beyond is when we expect Cyber will not only match Property, but surpass it. This growth will also underscore Cyber becoming the largest driver of volatility in the industry, and will require the balance sheets of third-parties to manage. Cyber presents a highly attractive market dynamic in the present, but will increasingly become a prerequisite for insurers of the future as it continues its exponential growth trajectory and subsumes connected lines of business.

The potential breadth, and depth, of Cyber means an oversupply of capacity is almost an impossibility, and so therefore is a 'soft' Cyber market. As the class matures, it must be said that wider industry can perhaps learn from a peril and class like Cyber. This is true in respect of the current 'premium problem', where premium and aggregate exposure are increasingly unrelated, as well as the new ground Cyber is breaking as it breeds innovation in use of technology, product design and distribution.

Just as we did four years ago, we've foreshadowed an illustrious conclusion to Cyber as it surpasses Property in size. However, in all the greatest Sci-Fi adventures the conclusion never seems a certainty, with the journey crammed full of enticing plot twists and character defining moments. We haven't reached Cyber's conclusion yet, so this white paper remains entirely a work of fiction, but for now we'll enjoy the next chapter in the most dynamic and exciting of classes.

References

[1]Gallagher Re analysis

[2]Gallagher Re analysis

[3]PwC Global CEO Survey 2020 https://www.pwc.com/gx/en/ceo-agenda/ceosurvey/2021.html

[4]Gallagher Re analysis

[5]Coveware Ransomware Trends Report Q3: https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts

[6]Cyber insurer's security scans reduced ransomware claims by 65% (bleepingcomputer.com)

[7]Coalition H1 2021 Cyber Insurance Claims Report https://info.coalitioninc.com/download-2021-h1-cyber-claims-report.html

[8]No One Knows How Deep Russia's Hacking Rampage Goes | WIRED
PCS: NotPetya insured losses now $3bn+ | News | The Insurer
Insurers' Bill for SolarWinds Hack Estimated at Just $90 Million (bloomberglaw.com)
Warning: 'Extremely Serious' Microsoft Vulnerabilities Hacked By Ransomware Criminals (forbes.com)
Colonial Pipeline ransomware attack has grave consequences (computerweekly.com)
US companies hit by 'colossal' cyber-attack - BBC News

[9]The Untold Story of NotPetya, the Most Devastating Cyberattack in History | WIRED

[10]Understanding risks in Asia Pacific's growing cyber insurance market | Visualize | Verisk Analytics

[11]Personal cyber insurance market size U.S. 2025 | Statista

[12]Personal cyber insurance market tipped to grow (pinsentmasons.com)

[13]Crime stats show switch in focus by cyber criminals (computerweekly.com)

[14]How digital is transforming commercial insurance for customers and agents - Socotra

[15]The Secret Coalition Master Plan, or why we acquired BinaryEdge (coalitioninc.com)
https://www.cfcunderwriting.com/en-gb/resources/news/2020/01/cfc-acquires-insuretech-threatinformer/

[16]Moodys - Moody's to Acquire RMS, Leader in Climate & Natural Disaster Risk
The BitSight and Moody's Partnership: A New Era For Cyber Security | Bitsight
BitSight raises $250M from Moody's and acquires cyber risk startup VisibleRisk | TechCrunch

[17]Pioneering cyber insurance: Munich Re partners with Google Cloud and Allianz | Munich Re

Authors

Ian Newman
Global Head of Cyber

E: Ian_Newman@GallagherRe.com

Ed Pocock
Senior Cyber Security Consultant

E: Ed_Pocock@GallagherRe.com

Jemima Hall
Cyber Consultant

E: Jemima_Hall@GallagherRe.com

Additional Contributions

Justyna Pikinska
Head of Specialty Analytics

E: Justyna_Pikinska@GallagherRe.com

Liz Kim
Cyber Reinsurance Broker

E: Liz_Kim@GallagherRe.com

Simon Heather
Senior CAT Modeller

E: Simon_Heather@GallagherRe.com

Rob Ayton
Cyber Reinsurance Broker

E: Rob_Ayton@GallagherRe.com

Gallagher Re is a trading name of Arthur J. Gallagher (UK) Limited which is authorised and regulated by the Financial Conduct Authority. Registered Office: The Walbrook Building, 25 Walbrook, London EC4N 8AW. Registered in England and Wales. Company Number: 1193013. FP144-2022 Exp. 04.02.2023.

ARTUK-3348

Gallagher Re