Gallagher Re

The vital role of capital in cyber (re)insurance

MAY 2023

Executive Summary

1	Capital into the cyber (re)insurance market remains insufficient, despite recent upticks in capacity.
2	Underlying dynamics of cyber (re)insurance are materially different from other underwriting classes because of growth opportunity.
3	Customer base, both in terms of developing new products and expanding into new territories, is broadening.
4	More stringent underwriting, portfolio optimization and better use of technology has improved performance.
5	The 'winners' in this situation will be those who successfully combine better technology, data and capital.

Attracting sufficient levels of capital into cyber (re)insurance is the greatest challenge our market faces, both today and in the near term.

This may seem a strange statement, given the recent material inflow of capacity into cyber insurance and reinsurance (see Figure 2).

The common wisdom of insurance market dynamics would conclude that increasing capital flows will eventually spawn a problem for the class, perpetuating the softening of rates and broadening of coverage. Indeed, we already see evidence of rate stabilization and even rate softening in parts of the cyber market, driven in part by the increased number of participants (see Figure 3).

But what if the cyber (re)insurance market is different from all other insurance markets where the increasing supply of capital would actually fuel an increase in demand for cyber (re)insurance?

In this whitepaper, we will explain how adding capital into the cyber (re)insurance market will stimulate growth and why over-capitalization will never quite exist in cyber (re)insurance.

We will assess the impact of securing more capacity for the sector and detail how those underwriters combining capital and technology, along with the ability to use data effectively, will be the ultimate winners.

In addition, we will identify some of the obstacles we face in securing capital and how they can be overcome.

Finally, we will consider the benefit this additional capital will have for the insurance industry, and the wider economy as a whole.

The question is no longer whether cyber (re)insurance is going to grow into one of the most significant classes of (re)insurance business, but who is going to contribute to — and benefit from — the **virtuous cycle** of unlocking the full potential in cyber (re)insurance through attracting new capital to the market.

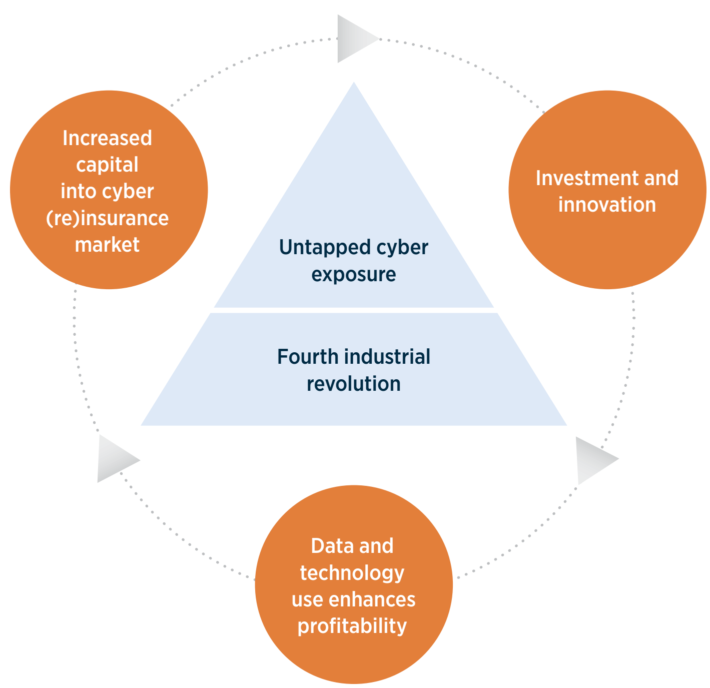

Figure 1: The virtuous cycle

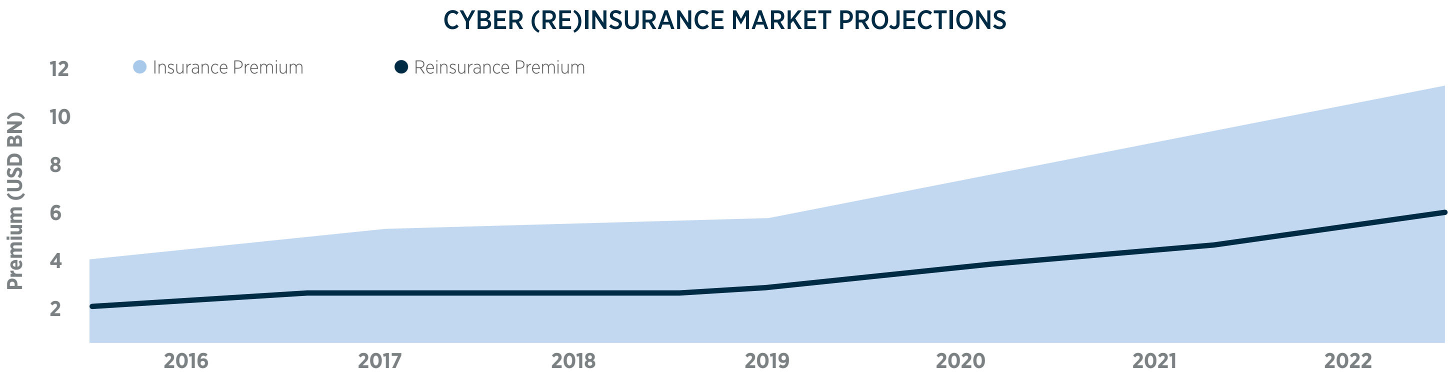

Figure 2: Premium growth in insurance and reinsurance as a proxy for capital influx
Source: Gallagher Re, NAIC, S&P Global and Swiss Re Institute calculations

Why increased capital stimulates growth (rather than the softening of terms)

Swift, wholesale and corrective action was taken market-wide to counter ransomware losses that arose in the 2019 and 2020 underwriting years (see Figure 4). The improvements in portfolio performance as a result of rate rises (see Figure 3), more stringent underwriting, portfolio optimization and more effective use of technology have resulted in a greater number of carriers looking to take on additional cyber exposure and premium.

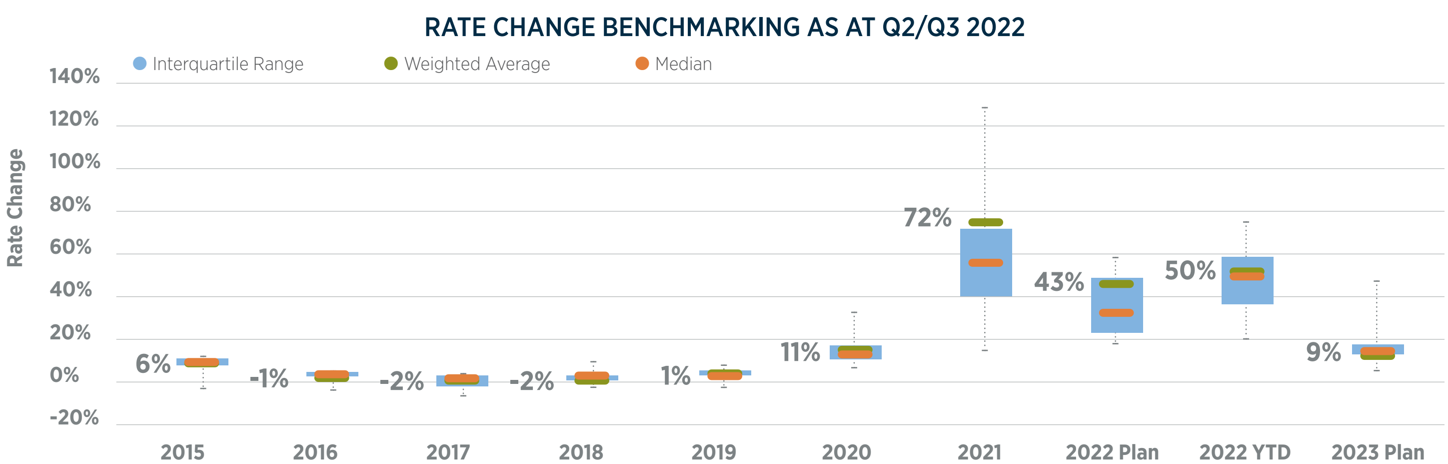

Figure 3: Rate stabilization following significant compounded rate increases related to correction for ransomware losses
Source: Gallagher Re

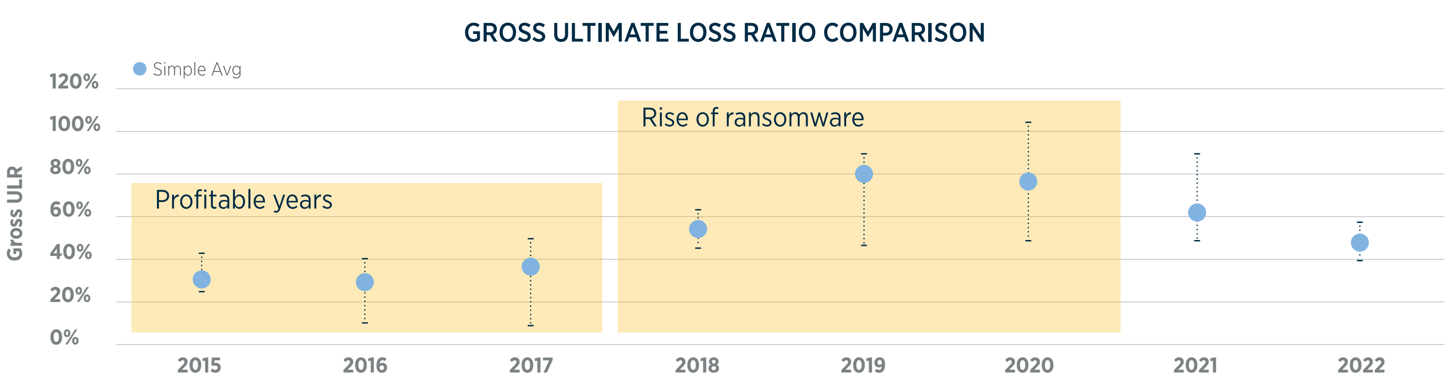

Figure 4: Gross ultimate loss ratio activity in 2016–2022 underwriting years
Source: Gallagher Re

This increased appetite is likely to intensify as we see the cumulative impact of these changes track through in the claims development triangles over the coming quarters which, in turn, will attract a further influx of capacity (as we predicted in our 2022 CyFi whitepaper).

In the short term, this influx of capacity could put downward pressure on pricing and coverage in the cyber (re)insurance chain. However, Gallagher Re believes the underlying dynamics of the cyber (re)insurance market are materially different from all other underwriting classes, in that a wave of additional capacity would not create a sustained softening in the same way as we would see in other lines of business.

This is because of the unique growth opportunity available to cyber (re)insurance. In the last few years, innovation has been stymied in what has, in its short history, been a very creative class of business. The market has been focused on remediating ransomware losses and carriers have been able to achieve their subsequent premium plan targets from underlying rate rises alone, while keeping aggregates flat. This distraction led to a stagnation in product offering and a curb on intended territorial expansion.

However, as rate increases decelerated, this dynamic diminished as a means to achieving top-line growth. We now expect to see the market pivot to attract a broader customer base, both in terms of developing new products and expanding into new territories where penetration rates are low and demand for cyber (re)insurance cover is ever-increasing.

For the market to achieve this, it requires a combination of innovation within rated carriers as well as support for MGAs. As a result, aggregates and tolerances will need to increase — and more capital will be required to support this increased demand. This stimulation in growth and profitability will likely attract further investment, in turn compounding further growth.

As a result of the unique demand and supply situation that exists currently, cyber (re)insurance can never be overcapitalized whilst this dynamic persists. Coupled with an ever-increasing digitized world and the growing dependence on cyber insurance and its associated cybersecurity services, the cyber (re)insurance market (having already demonstrated with its response to ransomware losses) will have the ability to pivot faster and more effectively than most insurance lines of business, in the event of any significant deterioration in performance.

Investment in data and technology is the key to success

To emerge as a winner in cyber (re)insurance, there are two additional key components required, alongside capital. They are data and technology.

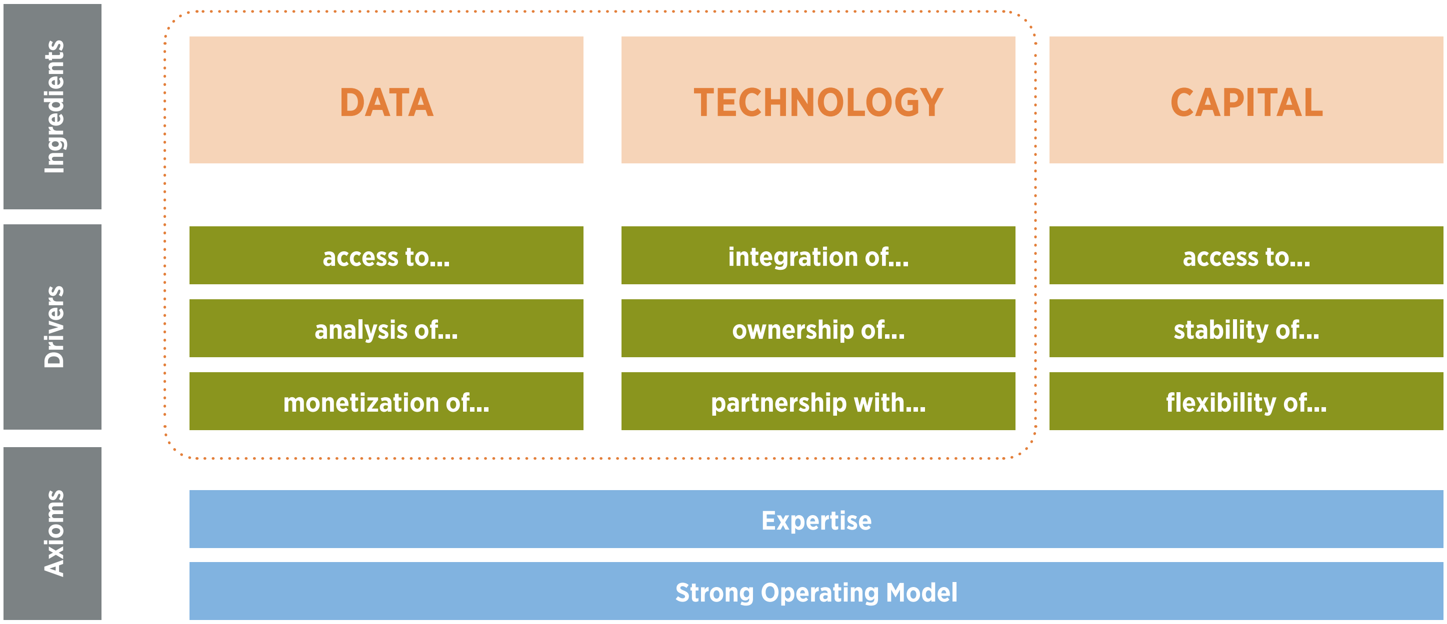

Figure 5: Winning strategy of data and technology combined with capital
Source: Gallagher Re

Gallagher Re has previously written extensively on the approaches to data and technology that are required for an underwriting company to succeed in our recent whitepaper 'Can external scanning data predict claims?', which concluded that external scanning technology has the potential to predict claims trends and positively impact loss ratios, but needs to be deployed in a targeted way in order to be successful in practice.

Here, external scanning underlines the unique dynamic of cyber insurance by offering underwriters at (re)insurers and MGAs the same information that attackers use to select and compromise targets on a near real-time basis. While the use of this technology is nearly universal amongst (re)insurers, the paper also recognized that only a minority are currently applying external scanning technology in a way that enables them to benefit from stronger risk selection. Furthermore, the use of this technology across the insurance lifecycle — to monitor aggregation risk or for loss prevention — is patchy at best.

There are multiple routes to success for data-and technology-centric (re)insurers, MGAs or vendors. Those with unrestricted access to the most powerful data are well positioned for longer-term success if they monetize this appropriately to the right target audience, while those acting as 'data mercenaries' with an ability to disentangle complex data and translate this into digestible insurance insights will prove valuable commodities.

(Re)insurers able to provide the right incentives will enjoy access beyond the firewall (or 'inside-out' data). Some are already identifying and building exclusive relationships with distribution partners that can offer long-term access to both quality risks and valuable inside-out data. Others are offering a suite of technology solutions to engage under-penetrated risks, offering them both insurance cover and a baseline standard of cybersecurity maturity.

While the MGAs do not have sole ownership of the best technology and ability to use data, (arguably some large carriers already rival them in certain areas), they do have certain structural advantages that, are allowing them to, in some cases, outperform the average of the rated balance sheet community.

This is driven by a number of key factors such as being unencumbered by legacy systems, operating with a flatter hierarchical management structure, being more nimble and embracing technology as a key strategy to achieve underwriting performance rather than merely operational efficiencies.

Exclusive ownership of proprietary market-leading data and technology are expensive endeavors and it is unclear whether MGAs will achieve adequate return on these investments through loss-ratio improvements alone. More likely, we will see some MGAs looking to monetize their technology prowess, either moving to compete with InsurTech vendors or providing solutions to noninsurers.

Despite having innovative ideas and potentially significant value-creation approaches, many MGAs continue to struggle to source capacity (as discussed in the "Overcoming capital attraction obstacles" section of this whitepaper), and as a result, a large number of them are simply unable to get off the ground. To address this capital vacuum, many MGAs are looking to secure their future by not only accessing third-party capital but also participating in their own underwriting by supplying their own risk capital.

On the flip side, the rated carriers have (or have access to) the capital, which alone gives them a higher probability of success than many of the MGAs who are looking to secure their support. The question that is often asked is who wins in the long run — is it the MGAs or the traditional insurance carriers? The answer is both.

Growth in the MGA sector is outstripping that of the market as a whole. Indeed, looking forward, MGAs will take a greater market share — most notably in the SME space, but in time, in the mid-market as well.

Furthermore, we expect to see the landscape changing materially, as underwriting entities look to bring these three key components together to create the market-leading formula of data + technology + capital.

Larger carriers will shift from simply deploying capacity behind MGAs, in the hope of creating an underwriting return and gaining knowledge (the predominant model today), to exploring joint ventures/partnerships by taking equity stakes in — or even buying out 100% of — some MGAs, so they can have access to the MGA-built technology.

This does not necessarily mean that the MGA would be absorbed in-house, as we have seen historically, but rather they may look to keep them separate to retain all the advantages of an independent MGA with the ability to invest in data and technology development, and attract/retain talent on a different structure.

Such a structure would allow access to the technology and have all the accretive benefits for the firm's overall valuation that the highly sought-after fee income would bring.

It is not just MGAs that will need capital to fund their cyber growth; so too will the traditional (re)insurance carriers. In the insurance space, we are currently seeing a huge reliance on third-party capital with close to 50% of all premium written being ceded to the reinsurance community, predominantly on a proportional basis (see Figure 6).

% Year-on-year buyers have ceded more premiums to reinsurers

YEAR	CEDED %
2019	40%
2020	43%
2021	47%
2022	50%

Cession demand remains high

Figure 6: Reinsurance growth to support insurance market
Source: Gallagher Re

As portfolios grow, and insurers' comfort levels rise, provided insurers are adequately capitalized, we are likely to see these percentage levels of cession decrease. But whilst relatively less premium and exposure may be proportionally passed over to other carriers, on an absolute basis the ceded amounts will continue to rise rapidly as the market grows.

Carriers will therefore need to continue to find new forms of capital to protect the tail risk and reduce their capital loadings.

This will also be applicable to reinsurers, as they look to grow in line with their clients' needs.

Overcoming capital attraction obstacles

Whilst traditional cyber (re)insurance will likely remain the core form of capital, Gallagher Re has long held the view that rated carriers alone won't meet the growing capacity needs of the underlying cyber insurance market.

So, where is this capital going to come from over the longer term?

Capital markets are likely to play their part in cyber (re)insurance over time. The most obvious first step is to follow the route of the property catastrophe market, which has managed to successfully source high volumes of capacity from the Insurance-Linked Securities (ILS) community over the past three decades (with upwards of USD 80 billion of limit outstanding in 2022). However, since Gallagher Re (legacy Capsicum Re) launched the first collateralized trade to cover cyber in 2017, there has been only modest growth in this area, due to a number of challenges, including:

- The infancy of models and the need for output adjustment.
- Inconsistent performance of the cyber class, particularly for attritional loss.
- Lack of consistent structural framework for investors.
- Lack of liquidity of collateralized reinsurance, compared with other products available to ILS investors, in, say, property cat.
- Historic investor preference for short-tail and geographically contained risks, with low correlation to financial markets.
- Limited understanding of aggregation language and its application to systemic cyber scenarios.
- Perceived correlation between cyber events and wider economic shocks due to its systemic properties.
- Although there is an appetite for contained and well-structured cyber risk, existing investors in cyberspace are currently not able to diversify their portfolio as successfully as they can in the property catastrophe space (e.g., Japan Typhoon vs. California Earthquake).

Gallagher Re and Gallagher Securities launched the market's first cyber catastrophe bond in January 2023. The decision to introduce the first financial security to the cyber reinsurance market centered around meeting investor (aka 'capital gatekeepers') needs.

The deal team created a liquid, tradeable and replicable instrument with features more akin to an investor's wider financial portfolio, rather than a reinsurance structure that may be perceived as being more elastic and have a longer capital duration. The bond responds to affirmative cyber catastrophes on an indemnity basis, with the limit fully collateralized to minimize credit risk.

In order to attract more capital generally, it is helpful to split the capital markets into two simple categories for the cyber peril: i) investors familiar with (re)insurance, such as ILS markets, and ii) those less experienced that may require further education. The pool of capital constituting the second category is significant and includes some of the largest financial institutions globally.

We can split the investor base further into investors looking for contained affirmative cyber risk in a familiar (re)insurance wrapper, versus those looking to partner with cyber insurance carriers (be that on their own business, providing paper for an MGA via quota share or taking on the whole balance sheet risk).

The common thread that runs through successful capital-raise efforts in the cyber (re)insurance market is education around the ever-evolving characteristics of the peril; the (re)insurance structure can follow. The level of data granularity and transparency required to draw capital markets to cyber (re)insurance is material, and the journey may be longer than for property trades. However, the sponsor benefits from obtaining brand-new capacity.

Investors are taking their time to understand and study prospective cyber cedants — and perhaps look to support fewer of them in a more significant way than in property catastrophe — with the intent to "turn on the tap" of capacity with their selected partners as the "proof of concept" develops. There is evidence of a number of major property ILS investors transitioning into cyber; over time, we may even see a completely new breed of investors (perhaps more tech-led) make up the core of the cyber (re)insurance investor base.

Although pockets of cyber-skepticism remain in the capital markets, this is noticeably lessening. Cyber risk is becoming better understood and the market need for cyber (re)insurance capacity becomes harder to deny. There could also be attractive profit margins for those that seize the opportunity and overcome some of the core challenges and misperceptions (see Figure 7).

1

Cyber is uninsurable

Opinions on whether cyber risk meets the criteria of insurability have shifted over time as cyber risk understanding has improved considerably.

2

There is no data

Insurers have been writing cyber for over 10 years—data sets continue to grow alongside the development of new tools that gather additional cyber risk data. Where data limitations exist (e.g., limited widespread CAT losses), market has invested in research overlayed with expert judgment.

3

All cyber events lead to losses

Despite media headlines, many of the supposedly "large-scale cyber events" have not yielded material industry losses.

4

Cyber cannot be modeled

Aggregation modeling has been revolutionized in the last five years. Industry has seen heavy investment from traditional modelers (RMS, AIR) and cyber-specific companies (CyberCube and Guidewire) to quantify the systemic exposures in this class as modeling credibility will be key to unlock more capacity.

5

Cyber is not profitable

Over the long term, the cyber market has been profitable. 2018–2020 saw more adverse years driven by ransomware, however, 2021–2022 have seen material rate increases, underwriting and risk management actions, returning the market to profitability as achieved in the pre-ranswomware days of 2019–2020.

6

Hackers are always one step ahead

Sensationalist media headlines are raising awareness and firms are constantly improving their cybersecurity posture and monitoring, and removing their vulnerabilities. Hackers have limited resources and low 'hanging fruit' approach no longer works.

Figure 7: Common misperceptions of cyber risk and cyber (re)insurance

Cyber capital benefits society

An inflow of capital can facilitate the growth in the breadth and strength of cyber insurance players — both traditional and tech-enabled MGAs — which in turn improves access to not only insurance itself but supports risk awareness, cyber hygiene and resilience across the wider economy.

As detailed in this whitepaper, the insurance industry — supported by both traditional and alternative capital — is driving significant investment in data and technology. While this investment is principally aimed at benefiting the underwriting performance of the industry, the ultimate benefits permeate the entire gamut of stakeholders and indeed society at large. Some of the key non-insurance benefits that the cyber insurance industry brings include:

- Scanning technology and vulnerability assessments that are becoming a mainstay of the cyber underwriting process offer policyholders valuable insights into areas of weakness in their computer networks.
- Ongoing threat monitoring and proactive alerts pushed to policyholders warn and ideally help avoid the impact of emerging vulnerabilities and threats.
- The intertwining of insurance with incident response services offers policyholders access to real-time support from experienced IT professionals to respond to and mitigate the impact of cyber incidents. This includes investigations, forensic response and triage, remediation strategy design and implementation, as well as introducing improvements to security and incident response plans post-incident.

Potentially most critically, all of the above contributes to strengthening the dialogue between the often complex and intimidating jargon of the IT security industry and the language of everyday business. This ultimately serves to promote increasing risk awareness and engagement of policyholders in strengthening their own cyber resilience.

As the underlying risk quality improves, so too will the availability of insurance, which in turn stimulates the compression of the protection gap.

While capital is not the only key to cyber (re)insurance's success, it is a core component. Although traditional (re)insurance is likely to remain the mainstay of capital, alternative capacity, in well-structured and replicable product form, will help to fill the increasing capacity and protection gaps.

The cyber cat bond market is now up and running, institutional investment houses are partnering with cyber MGAs through quota share arrangements, and technology-led investors are in discussions with brokers around the prospect of investing and supporting the market.

Capital markets have also begun entering the cyber (re)insurance market in a bigger way, and are likely to become a key ingredient of a healthier and sustainable (re)insurance market.

It truly feels as though we are at a pivotal moment for the cyber (re)insurance industry.

Authors

Ian Newman
Partner, Cyber
Ian_Newman@GallagherRe.com

Theo Norris, CFA
Cyber Account Executive, Insurance-Linked Securities
Theo_Norris@GallagherRe.com

Ed Pocock
Senior Cyber Security Consultant
Ed_Pocock@GallagherRe.com

Ryan Fitzpatrick
Chief Operating Officer, Gallagher Securities
Ryan_Fitzpatrick@AJGRe.com

Endnotes

Gallagher Re, in conjunction with Gallagher Securities, is committed to educating capital market investors that are interested and committed to pursuing an investment strategy in cyber (re)insurance, through forums, conferences and workshops. It is important we fully understand the requisite comfort levels of investment managers to secure the transfer of a proportion of their AUM into cyber (re)insurance.

Gallagher Re has the market's largest cyber analytics and consultancy team, that has established cyber cat wordings for the market and is dedicated to solving problems that will arise as an understanding of cyber risk evolves.

It's the *way* we do it.

For more information, visit GallagherRe.com.

Gallagher Re