Cyber ILS: How Acute Demand Could Drive a Scalable Retrocession Market

Tom Johansmeyer

PCS, Verisk, Bermuda
tjohansmeyer@verisk.com

Alex Mican

PCS, Verisk, United States
amican@verisk.com

Received: May 1, 2022
Revised: June 22, 2022
Accepted: June 24, 2022

Abstract

Increasing demand for cyber re/insurance and a shortage of supply have made the need for fresh risk capital acute. After years of seeking support from the insurance linked securities (ILS) market, re/insurers may be on the brink of a major change. Property Claim Services, a Verisk business, has conducted original research with 24 ILS funds representing nearly 80% of the sector as measured by assets under management. ILS appetite for cyber re/insurance risk has increased, with many funds interested in entering the market this year. Historical barriers such as structure and modeling may not be as problematic as they were in the past, and narrowing spreads on cyber ILS have made the risk more attainable for providers of collateralized protection. Market dynamics have pushed pricing to levels that ILS funds can reasonably contemplate, which means that scale may soon follow.

Keywords: Cyber, Insurance, Reinsurance, Risk Management, Risk Transfer, Insurance Linked Securities

1 Introduction

The cyber re/insurance market may be closer to a new source of capacity than it realizes, and it appears that the timing could not be better. For years, the global re/insurance industry have either lamented the inability to access insurance linked securities' (ILS) capacity for cyber risks or simply declared that ILS should become available to help with no reason other than the traditional market's need for capital. As a result, it appears that a mix of frustration and disinformation swirled across the global re/insurance industry regarding the ILS market, its appetite for cyber risk, and the barriers between ILS capital and the cyber re/insurance market. Along the way, there has been little discussion of these issues with the ILS community, which is evident from the narratives being advanced. Based on Property Claim Services (PCS) research, the ILS market is ready to engage with cyber re/insurance risk, provided it can do so sensibly.

Market conditions have, in part, made it easier for the gap between cyber re/insurance and ILS to be bridged. Some re/insurers have reported increased struggles with capacity shortages over the past three years, and at the January 1, 2022, reinsurance renewal, it was reported that many insurers were not able to get all the protection they sought, even on reinsurance rate increases of up to 50 percent, which itself represents acceleration from the July 1, 2021, reinsurance renewal's increases of 40 percent (Sheehan 2022, Reuters 2021). Further, many reinsurers struggled with capacity, given a lack of access to retrocession (Greenwald 2021), which would require new sources of capital, given the concentration risk observed in the cyber reinsurance sector.

ILS has often been raised to PCS by some as a potential solution to the capacity constraints experienced across the re/insurance industry, but rarely with any examinations of the conditions that have prevented for so long the connection of the ILS and cyber re/insurance markets. While many of the conventional impediments to cyber ILS are concerns – such as model maturity, potential correlation with financial markets, deal structure, and deal price – not enough focus was put on more imminent challenges in the ILS market, such as the erosion of capital due to five years of heightened natural catastrophe activity, reinsurance rates inconsistent with the realities of collateralized instruments, and buyer expectations on price, which remained low until the current shortages helped tighten spreads.

With concentration risk among the largest cyber reinsurers in the world a reported significant problem for the global re/insurance community, new capital could be crucial to future market growth. Outside capacity could support the development of a robust retrocession market, which is a role the ILS market has played before – in the property-catastrophe space. To help history repeat itself, this time in cyber, PCS surveyed more than 75 percent of the ILS community by assets under management (AuM) to gauge how they see cyber re/insurance risk and its suitability to the ILS market. Contrary to popular belief, there is already consistent cyber ILS activity, although it remains limited in scope. Based on responses, many more ILS funds, however, have already evaluated the cyber re/insurance market, contemplated how they would assume the risk, and have even expressed an interest in engaging in cyber ILS trading in 2022.

2 What cyber insurance is and what it includes

Cyber insurance is notoriously difficult to define. The Association of British Insurers (ABI) offers the succinct effort: "Cyber insurance covers the losses relating to damage to, or loss of information from, IT [information technology] systems and networks" (ABI). The ABI further

explains that such policies may also offer support related to managing cyber incidents. Other similar definitions can be found, but they ultimately fall short of an overarching definition. That is to be expected in a market that is still relatively new, experiencing rapid growth (at least until recently), and is continuing to evolve both to market demands and the threat environment itself.

While there is no single, coherent definition of the cyber insurance in the global market, what is generally accepted as the cyber insurance market includes the insurance used to protect customers in the event of breaches of proprietary systems, disruption of systems' use and operation (which could be internal or external, unintentional or intentional), and ransomware and cyber extortion (Romanosky et al. 2019). Other scenarios may be relevant, as well. There is a lack of standardization in the cyber insurance market, with some narrow programs addressing only specific scenarios, such as breach, and other taking a broader scope, to include technology errors and omissions ("tech E&O"). The use of manuscript policies over standard forms results in further definitional challenges (NetDiligence 2022).

Cyber insurance is typically considered along two lines: first-party and third-party coverage (Romanosky et al. 2019), with the former regarding losses "directly suffered by the insured" and the latter those "brought by parties external to the contract" (ibid.). The former tend to be seen as more straightforward, given that they involve the insured itself, according to conversations with cyber re/insurers. The belief that third-party issues could profoundly elongate the cyber insurance claims process has yet to be thoroughly tested, at least among losses of at least US$100 million, according to data from PCS Global Cyber, a Verisk business, because there have been so few single losses of that size and because the economic losses in those cases have tended to be much larger than the insurance in place (Johansmeyer 2018).

Finally, particularly in the reinsurance market, the cyber is increasingly seen according to yet another distinction: privacy and business interruption. In this context, privacy refers mostly to data breach events, while the latter refers to the disruption of systems to the point where the ability of the business to operate is impeded. Business interruption tends to be seen as having the greater potential for insured loss between the two, according to client conversations across the market. However, the data does not bear this out, at least not yet. The largest insured loss on record with PCS Global Cyber is for a breach event, at an industry-wide insured loss of approximately US$350 million (Insurance Day 2018). On the other hand, the largest industry-wide insured loss for a wiper or ransomware so far is only US$275 million, with the total affirmative cyber loss from NotPetya (including Merck) still falling short of the Marriott total (Artemis (2017). This oversimplification does omit a wide range of other loss types, but it reflects the general sentiment of the sector, with those writing more specific areas, like tech E&O, consisting of smaller pockets of the broader segment.

The lack of a broadly accepted definition for cyber insurance, to include differences in how policies function (e.g., some include threat assessments and post-event consultant support), has largely been addressed through the use of the distinctions provided above, at least in general conversations. Specific reinsurance agreements either mirror the underlying scope or specify what risks the reinsurer would assume, which essentially ports the discussion of definition into the agreement itself. The ambiguity of definition regarding the category may not specifically manifest as a risk transfer concern, but it has been a barrier to learning about and understanding the sector. The ILS market, for example, may struggle to understand the universe to which they would deploy capital in entering the cyber re/insurance sector, which could influence early decisions to wait for

further market developments. That said, the ILS community may not be content to continue to wait on the sidelines, as is explained further in this article.

3 Historical misconceptions about cyber ILS

Much has changed since Strupczewski wrote that "reinsurers remain conservative about their cyber risk exposure," when premium was estimated to be a mere US$525 million (2017 496). Today, PCS estimates that each of the three largest cyber reinsurers writes more premium than that (which will be discussed later in this article). Worldwide affirmative cyber reinsurance now sits at approximately US$2.8 billion, based on PCS client discussions, with the four largest accounting for US$2.1 billion in premium and the next three almost US$350 million. The cyber reinsurance sector has grown with remarkable speed over the past five years, even if that pace has ground to a near halt recently.

In addition to size, the cyber reinsurance sector has undergone structural changes, as well. The liberal use of quota shares noted by Strupczewski five years ago, has reportedly given way to more frequent adoption of excess of loss treaties and a willingness to evaluate other risk transfer structures, including the index-triggered instruments he mentions, such as industry loss and parametric (2017 496-7). Some of this apparently comes from an appetite to manage risk and capital more effectively, although the growing flexibility in risk transfer likely has much more to do with the availability of capacity. Even with the rapid growth in cyber reinsurance over the past five years, PCS has seen underlying demand increase even faster, allowing reinsurers more of a voice in structure and terms.

The increased use of new forms of risk transfer in the cyber reinsurance market appears to have renewed discussions about the potential role insurance ILS could play in the sector. The ILS market originally formed as a way to bring fresh capital to the property-catastrophe when demand was acute and capital was in short supply (Carter and Mainelli 2018, 20-21), and similar characteristics appear to be present for cyber, if not to the extent witnessed for property-catastrophe after Hurricane Andrew 30 years ago. While the ILS community could certainly play a role in enabling greater cyber re/insurance sector flexibility and growth, little attention appears to have been paid in the scholarly community to the mechanics of the ILS market, to include structural barriers that have prevented broad adoption of ILS by the cyber re/insurance market so far.

Attitudes on cyber re/insurance and ILS tend to be as polarized as they are blunt. Some simply posit a role for various forms of risk transfer – to include industry loss warranties (ILWs) and parametric instruments – using ILS capital with no justification other than the need for capacity in the cyber re/insurance market. There has been little use of either approach in cyber re/insurance so far, with some early efforts in 2020 for parametric triggers (trigger details not disclosed) and progress toward ILWs with no completed transactions yet (Sheehan 2020, Bermuda:Re+ILS 2018). For cyber ILW triggers, PCS would be the likeliest reporting agent for data used in the trigger, given that no other organization provides relevant industry-wide insured loss reporting.

Dal Moro, for example, attempts to advance a role for ILWs and parametric instruments without justification when claiming, "[o]ne way to increase the available cyber capacity of the risk transfer market, and to achieve an additional atomization of this accumulation exposure, are alternative risk transfer (ART) solutions, involving the capital market via insurance linked securities (ILS), i.e., cyber cat bonds, and parametric and industry loss warranties" (2020 2). He

then proceeds to describe potential solutions but offers no discussion of ILS sector appetite for cyber, preferred deal structures, or impediments to the consumption of cyber risk.

The prospect that "peak cyber risks will be … transferred to the capital markets" remains a possibility, according to Carter, Pain, and Enoizi, claiming that there have been "few, if any, transactions, at least in the public domain" (2022 23), a caveat that fall a bit short in capturing the volume of cyber ILS transactions completed, although still accurately reflecting that the sector has been small even within the context of cyber re/insurance. They identify some key impediments to the scaling of cyber ILS, including modeling and potential "correlation between major cyber events and capital markets outcomes" (Biener, Eling, and Wirfs 2014, 19; Carter, Pain, Enoizi 2022 23).

Ammar, Braun, and Eling note that "the opinions of our experts diverge" when it comes to whether cyber re/insurance risk can be transferred to the ILS market, explaining the fact that some see the potential for significant returns, while others believe that with "cyber risk there is in fact a high correlation with the market" (2015 56). The same concern is echoed by Hofmann, who comments that "a major event, perhaps disrupting one or more industry sectors, could trigger a negative reaction from financial markets" (2018 9).

The divergence of opinion leaves room for consistency with actual market activity. Cyber ILS trades have been completed, and several of them have apparently become strategic relationships that have been renewed several times, according to PCS market sources, even in what is largely perceived as an increasing threat environment (Johansmeyer *Global Policy* 2021). While there have been many barriers to cyber ILS – including modeling, historical loss activity, and general discussions about price and familiarity with the risk – some of it comes down to end-investor expectations and ILS fund manager strategy. ILS funds historically have sought to deliver diversification from broader financial markets, with "little or no correlation" to them," according to Hofmann, but "cyber-based securities are different" (2018 9).

Some market dynamics have become significant impediments to the use of ILS by the cyber re/insurance industry. Through 2018 and 2019 in particular, PCS observed that efforts to engage in cyber ILS transactions were often stymied by wide price spreads that showed no signs of narrowing. In working with the market to help develop alternative sources of capital (particularly in ILW form), PCS saw that certain protection buyers sought fairly low attaching cover at low single-digit rates on line (ROL), arguing that in the past, cyber cover was often included in property-catastrophe treaties at little or no cost. Meanwhile, some protection sellers contended that they had to price aggressively early, on the assumption that rates only decrease over time – and that they would never make what they do early on. They were willing to hold out for sufficient novelty premium. Low ROL deals, in particular, were unlikely to get much traction, even with stratospheric attachment points. The attendant low ROLs would likely not be realistic alternatives for ILS funds that collateralized their transactions. Without the leverage enjoyed by rated reinsurers, constraints on capital flexibility effectively set a floor that could only be pierced for rare exceptions.

Additionally, property-catastrophe volatility has impeded ILS entry into the cyber re/insurance sector. Starting with Hurricanes Harvey, Irma, and Maria in 2017 (not to mention large several wildfire catastrophes that year), losses have been significant, particularly in the United States, Canada, and Japan, with additional events in Australia – markets where PCS reports industry-wide insured catastrophe losses, which gives the organization unique insights into loss

events in these countries. The 2021 flood in Continental Europe (Evans 2021), like the Texas winter storms earlier that year (Aon Securities 2021 16), was unexpected and costly. While high rates of property-catastrophe loss may seem like a driver for expanding to new classes of business, such as cyber, the mechanics are a bit more involved.

Losses require focus. With the past five years being loss-intensive – and with major catastrophe losses requiring fund manager attention for years after the wind has stopped blowing – the ILS sector has had to spend time and effort understanding loss events, reserving, communicating with end investors, and revisiting their portfolios. Many have raised additional capital. Although property-catastrophe risks have been problematic, ILS funds specialize in that category and have needed to address the loss events, a process that continues, particularly with Hurricane Ida in 2021 (Gallin 2021). Reduced capital positions have also made it more difficult to experiment with new classes of business, particularly one as large, high-profile, and difficult to understand as cyber. Even at attractive ROLs, cyber has not been able to find an easy home in the ILS sector (Howard 2021).

Of course, cyber pricing likely would have to increase not just from what had been quoted in the past; it would also have to compete with the higher property-catastrophe ROLs that come with a hardening market. Based on many PCS client conversations over the past five years, ILS funds would require a premium for cyber relative to property-catastrophe risk (effectively a novelty premium) for theoretically commensurate risks. Even then, though, many ILS funds would likely sacrifice a generous novelty premium to stay with familiar classes of business.

4 An important change in the cyber re/insurance market

An initial sense of discouragement would be as forgivable as it is intuitive. PCS client conversations might seem to suggest a stasis in ILS appetite regularly reinforced by increasing property-catastrophe ROLs, to the point that cyber ILS could not be a realistic alternative. However, despite the headwinds detailed above, ILS interest in cyber re/insurance risk has shown signs of increasing over the past 18 months, even in the face of the ransomware epidemic and a wide range of geopolitical considerations (Seals 2021, Temple-Raston 2021). In casual client conversations, part of the reason for this comes down to simple fatalism – many just feel that cyber will become part of the ILS market eventually. It is hard to see that much demand for a cover so broadly needed go unaddressed for too long. Underlying that fatalism, however, is an important market dynamic that is helping to hasten the entry of cyber reinsurance risk into the ILS sector: A lack of access to retrocession.

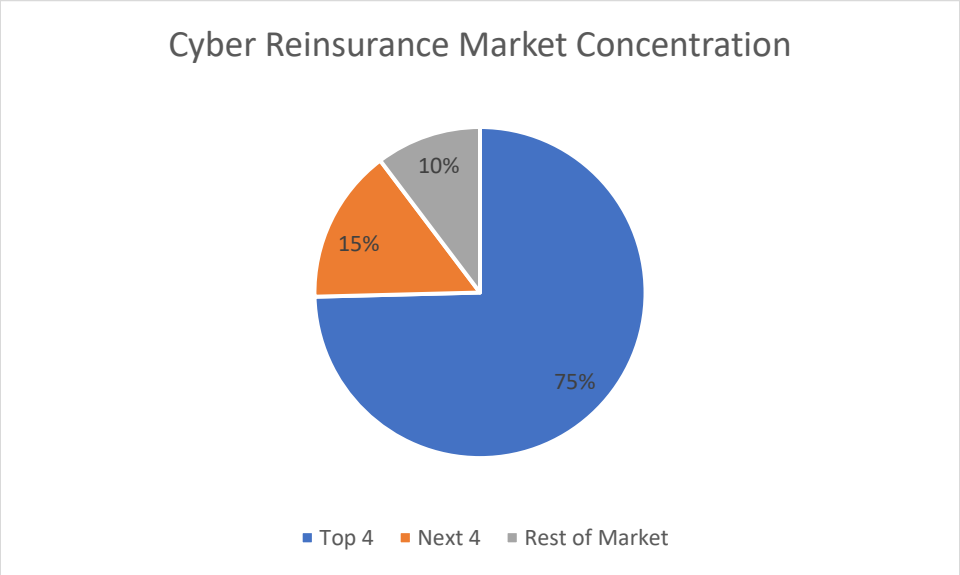
Reinsurance has become a fundamental factor in the growth of the cyber insurance industry (Johansmeyer *Harvard Business Review* 2021), identified as far back as 2014 by Biener, Eling, and Wirfs, who observe, “The development of a viable cyber market could thus benefit from increasing reinsurance capacity for the risks” (2014 12). Insurers cede approximately 55 percent of what they write to reinsurers, PCS has learned through many client conversations, and they generally remain reluctant to grow by retaining more risk. For a while, many reinsurers reported they were content with this relationship, but as industrywide affirmative cyber reinsurance premium surpassed US$2.5 billion in 2020, according to PCS internal estimates growth began to slow, still reaching US$2.8 billion by the end of 2021. While the prospect of a government body as “an insurer of last resort” has not been necessary to fuel profound cyber re/insurance market growth, a discussion noted by Biener, Eling, and Wirfs, the issue tends to arise whenever growth

appears to be constrained – whether that constraint be on premium or the ability to expand cover across more of the market (2014 17).

The increase in premium growth does not imply an expansion of the overall cyber re/insurance market. In fact, the contrary is probably true: Cyber re/insurance likely contracted (or at best remained the same) while premiums simply rose. Some re/insurers were able to charge more for the underlying risk as a result of the changing threat environment and increased insured loss activity. At the same time, reinsurance dependence is increasing, indicating the concerns insurers have about holding cyber risk. Cession rates, according to PCS market sources, climbed (another) 10 percent from 2020 to 2021, to the 55 percent mentioned above. The rate of cession provided here is higher than the 40 percent ascribed to Swiss Re by IAIS in 2020 and leave room for significant differences in estimates based on the opaque nature of the industry and the possibility of variability in a siloed and still new sector of the re/insurance market (2020 16). Had there been more reinsurance capacity available, the cession rate likely would have climbed even more aggressively. The fact that reinsurance cannot meet cedents' demand has seized up the market, making further rapid growth seemingly impossible – and even the characteristics of recent growth questionable.

The four largest cyber reinsurers together account for approximately 75 percent of dedicated global cyber reinsurance premium, according to internal PCS estimates at the end of 2021, up sharply from approximately 65 percent only a year earlier. While some of this is from measured and intentional growth, there are concerns across the industry that some of the increased concentration may not have been. However, to treat the top four as a cohort simply because of their size would be to ascribe a level of commonality across them that would not be appropriate. PCS understands from client conversations that there were instances of deliberate aggressive growth among the top four.

Figure 1: Cyber Reinsurance Market Concentration



Source: PCS internal research

Based on PCS estimates, the drop from the fourth largest cyber reinsurer to the fifth is quite steep (more than US$250 million). In fact, the "next four" (reinsurers ranked fifth through eighth based on cyber reinsurance premium) show US$425 million in aggregate premium, making them together only slightly larger than the fourth-largest cyber reinsurer. Even the entirety of the cyber reinsurance market below the top four amounts to just over US$700 million in premium. The concentration of premium among such a small cohort – and the lack of alternatives below them – indicates some of the structural challenges faced by the cyber re/insurance market. Concentration risk could be one of the biggest difficulties the sector faces, and it manifests in a practical manner in several ways.

First, the four largest reinsurers struggle to gain access to retrocession capacity with any scale, according to PCS market sources, given that trading among them would likely result in only further increases in concentration risk. This has been evidenced in the market with at least two such risk-transfer transactions, both of which have become only more difficult to place, according to conversations with clients that have direct visibility into or experience with those placements. While ILS capacity has played a role in those placements, they represented part of what only was a small amount of capacity, which became even harder to find at the January 1, 2022, reinsurance renewal. Those placements have involved the participation of smaller cyber reinsurers, but as evidenced by their share of the market, they can provide only little relief to major players in the sector. In fact, the strain that large reinsurer retrocession demands have placed on smaller reinsurers is salient, resulting in significant under-placement, in some cases, and broad syndication across a large panel.

Additionally, it can be difficult for mid-sized and smaller reinsurers to engage in retrocession with each other, for the same concentration reasons. While the demand for capital may not be early as large as it is for retrocession placements among the top four, smaller players still encounter the same issues around capacity constraint and concentration risk. Two smaller players may have the same challenges as two larger players, for example. The result is a logjam in the cyber reinsurance market as a result of limited access to retrocession capacity, and it comes at a time when demand has been higher than ever.

Two of the four largest cyber reinsurers, according to PCS knowledge and client discussions, and two more in the top ten, have engaged in cyber retrocession transactions over the past two years (although there could be more). At least three more cyber reinsurers are looking for retrocession capacity as of this writing. Further, there could be significant uncommunicated demand, with reinsurers not looking for cyber retrocession capacity because they do not believe any is available, and further still, some reinsurers might look to cyber retrocession, if it becomes available, as a way to fuel a new or revised strategy for that class of business. Given sufficient capacity and the reasonable expectation that more will become available, demand for cyber retrocession could accelerate rapidly.

The flow of additional cyber reinsurance capacity – to include retrocession – has been limited to a trickle so far according to market sources, with some new players engaging at the January 1, 2022, reinsurance renewal. Far more capacity will be necessary to make a difference in the smooth functioning of the market as it is today, let alone to bring the original cyber insurance industry back to a trajectory of rapid growth. While many have identified the ILS sector as a potential source of capital – including Dal Moro, Carter (S.) and Mainelli, and the teams writing for the Geneva Association (Carter, R.A.; Pain; Enoizi; and Hofmann) – nobody has tried to

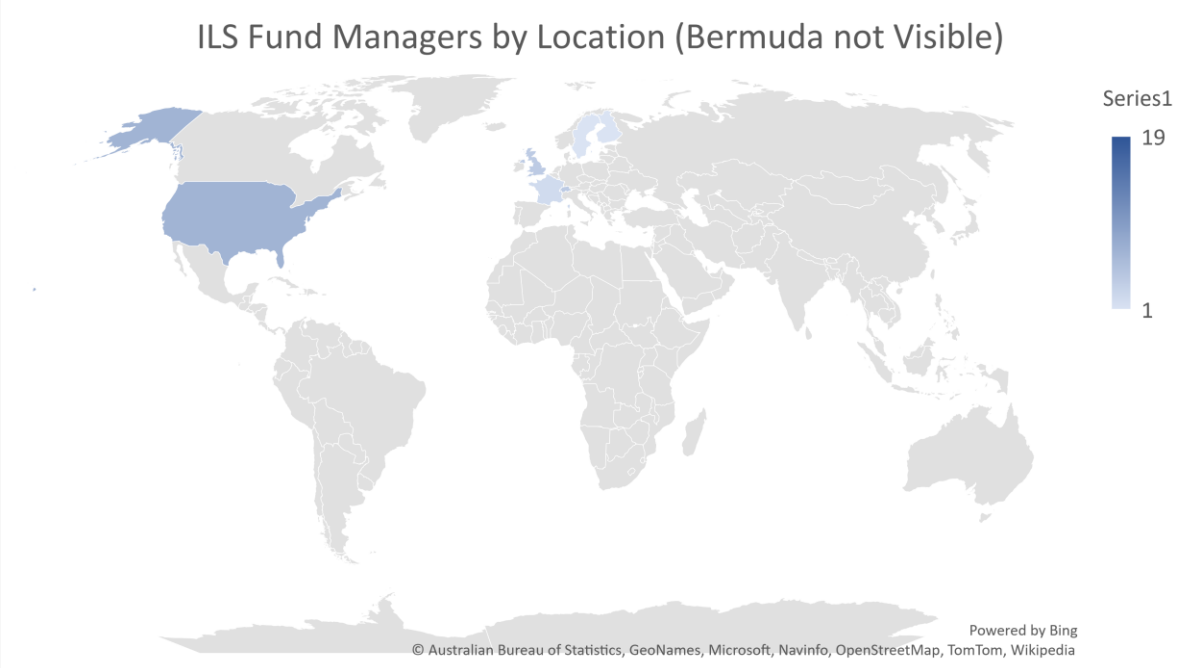
ascertain what developments would be necessary to bridge the rest of the gap between the cyber re/insurance market and the ILS sector.

What has been missing has been the perspective of the ILS sector in the discussion about the role they could play in the cyber re/insurance market. There appears to have been no thorough, direct engagement with the ILS fund managers who have so far made the decision to write cyber re/insurance business (or not), their reasons for doing so, and what their plans are for the future. PCS has engaged in what we believe to be the first study of this type, surveying nearly three-quarters of the global ILS community specifically on their perceptions of, attitudes toward, intentions regarding, and activities within the cyber re/insurance market. Their responses can help form a foundation for productively engaging the ILS market on cyber re/insurance matters, and could provide an opportunity to enable the flow of capital that cyber re/insurers need to return to a period of reliable growth.

5 ILS market cyber survey: Methodology and findings

Around the world, there are more than 40 ILS fund managers, and their aggregate assets under management exceed US$107 million (Artemis 2022). The majority of that is with the 25 ILS funds that have at least US$1 billion in AuM. Originally developed to meet the demand for capital in the property-catastrophe market (Artemis 2018), the ILS community has participated in other segments of re/insurance risk, such as specialty classes like marine and energy, political violence, property per risk, and aviation. Some have also engaged in casualty lines of business (Koch 2018). Some have engaged in cyber ILS activity as well, as the findings below illustrate, although the ILS market is still split on whether cyber will be a significant driver of growth (Evans 2019).

Figure 2: ILS Fund Managers by Location



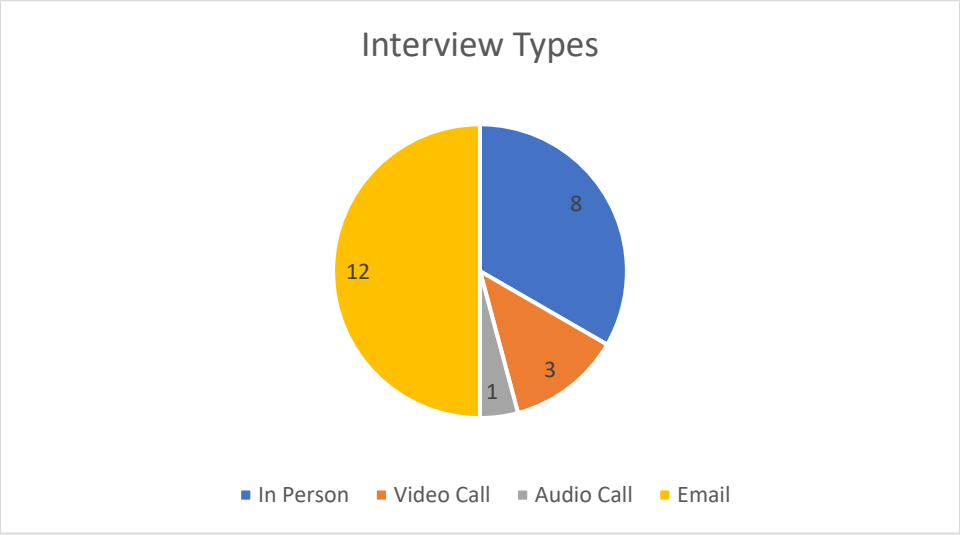
Source: Artemis.bm

Cyber has generally been difficult to place in the ILS market, although it has been done before (Gallin 2019, Shah and Dyson 2018). Popular perceptions have focused on the reported small size and infrequency of the transactions completed, as well as the fact that so few have made it into the public domain (Carter, Pain, and Enoizi 2022 23). As a result, misconceptions about the ILS market and its appetite for cyber re/insurance risk appear prevalent. To address this development, PCS engaged with 24 ILS funds (78 percent of the ILS market by AuM), reflecting approximately US$84 billion in AuM. That includes most of the ten largest in the world, as well as five with AuM of under US$1 billion. One respondent has no direct commercial relationship with PCS, as of this writing. Not all respondents subscribe to PCS Global Cyber. The one respondent with "N/A" answers throughout the survey did not engage with PCS on this research but is known not to be active any longer.

PCS contacted 27 ILS fund managers to conduct confidential interviews consisting of the six questions below (plus one that was used for a separate paper). Twenty-four ILS fund managers responded and participated in interviews. The names and companies of the participants cannot be revealed, and the presentation of aggregate statistics is done in a manner that protects the confidentiality of the participants and seeks to minimize the risk that any identities could be deduced. The interviews themselves were designed to increase response rate overall and also to increase the flow of information with respondents once engaged. Participants were encouraged to communicate comfortably and freely when responding to each question.

Each participant was asked the same six questions followed by open discussion to maximize the opportunity to gather practical insights as yet unknown to the broader cyber re/insurance market. Of the 24 interviews, eight were conducted in person, three via video call, one via audio call, and 12 by email. Email interviews were not necessarily limited to one exchange. Where necessary to clarify responses or elicit further information, follow-up correspondence was used. However, specific answers that did not call for further exploration were respected. In-person interviews and those conducted live by audio or video call were scheduled for 30 minutes. In some cases, the interviews were much shorter, particularly for participants with no plans to enter the cyber ILS market. Calls were not recorded in order to provide further comfort of anonymity. Instead, notes were taken and are held privately.

Figure 3: Interview Types



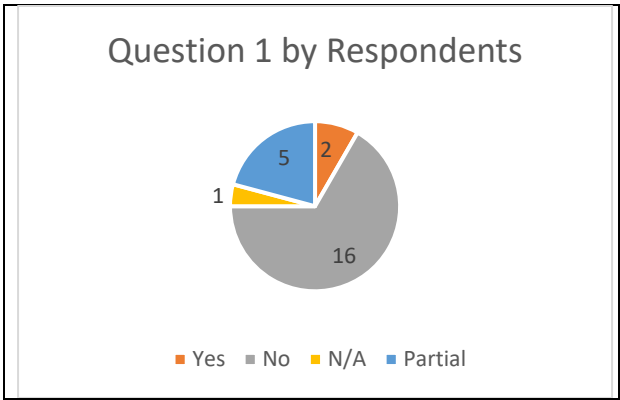
Source: PCS, a Verisk business

PCS employed a certain amount of flexibility during the interview process given the unique nature of this opportunity. The ILS market has been known for opacity, as noted by Carter, Paine, and Enoizi above (2022 23). As a result, some rigor was intentionally sacrificed for the benefit of maximizing actionable information for the global cyber re/insurance market.

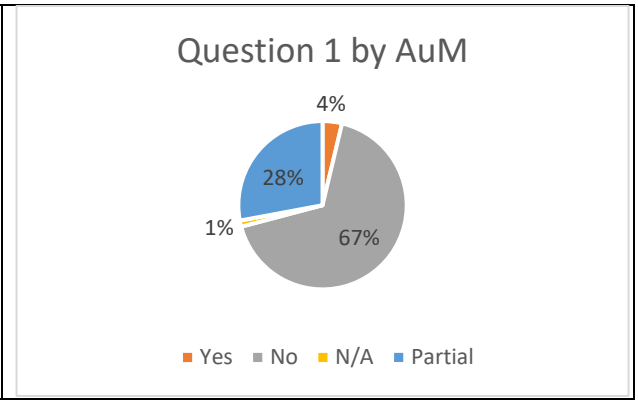
Question 1: Do you have a mandate preventing you from trading cyber?

To address the persistent belief in the global cyber re/insurance market that ILS fund mandates do not allow for trading in cyber and other man-made risks, PCS first asked participants if this is true. The sentiment arose during research conducted by PCS in 2021 on ILS fund appetite for political violence risk (see, for example, Johansmeyer *Security Magazine* 2021), and the parallels to cyber were evident. The notion that ILS funds are prohibited from trading cyber re/insurance by mandate is generally not true, although there was some nuance among responses. PCS found that 95 percent of respondents by AuM (22 of 24 respondents) have no such prohibition by mandate, although 28 percent do have partial prohibitions (5 respondents).

Figure 4: Question 1 Respondents



Source: PCS, a Verisk business



Source: PCS, a Verisk business

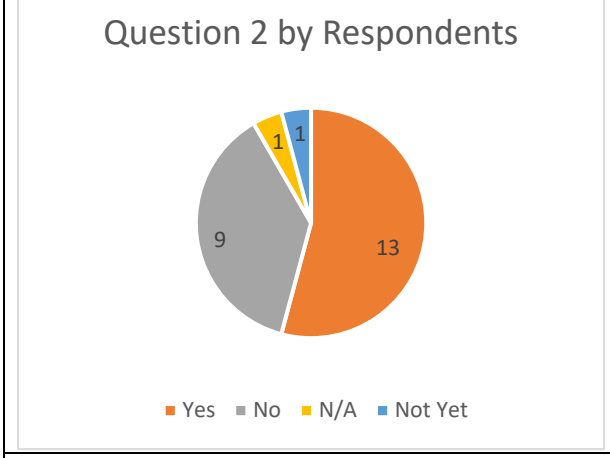
One of the two respondents that reported a prohibition on cyber re/insurance risk trading by mandate indicated having no interest or appetite for that class of business. The other indicated a willingness to explore cyber re/insurance risk, which would also require revisiting the issue with their investors. This respondent suggested that favorable market conditions would be sufficient to discuss with investors the possibility of revising those mandates. Additionally, some ILS fund managers indicated that they are not interested in cyber re/insurance risk, regardless of mandate (a topic explored in more detail below). Thus, while there is some credence to the notion that many ILS funds are averse to cyber risk, it is not necessarily because of a specific prohibition in their mandates.

Question 2: Are you interested in trading cyber?

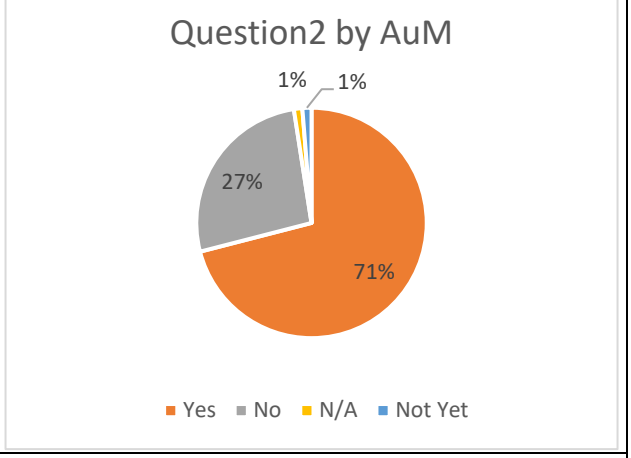
The ILS sector struggles with the misperception that it is generally not interested in consuming cyber re/insurance risk. PCS found the contrary to be true. ILS fund managers, in fact, showed a general openness to the cyber class of business, with 13 respondents (71 percent by AuM) indicating interest, although prospective timeframes varied. The "not yet" response offered

by one fund manager was shared in other forms by others who want to enter the cyber re/insurance market when they are ready. Readiness ranged from pricing and terms being adequate for their portfolios to the manifestation of pressure to engage because their peers have.

Figure 5: Question 2 Respondents



Source: PCS, a Verisk business



Source: PCS, a Verisk business

To be reviewed more thoroughly in Question 4 below, five respondents have engaged in cyber re/insurance transactions already (as well as two more who did not participate in the research but separately confirmed their cyber re/insurance activity). They generally suggest that they will remain committed to cyber ILS and might have further appetite, although that would depend on deal flow. For those who have not yet traded cyber but are interested in doing so, some impediments remain, including the risk that cyber is correlated with financial markets (although this is a point of disagreement in the market), pricing and structure, and whether a separate portfolio specifically for cyber risk would be necessary.

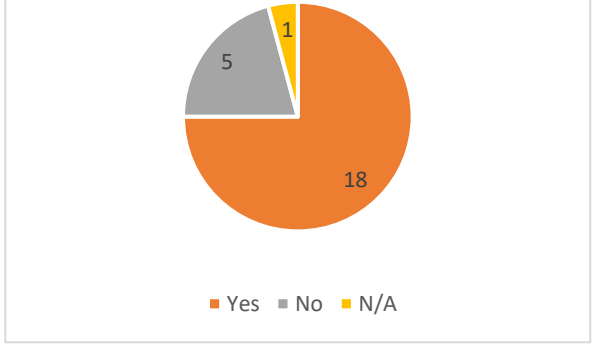
One large ILS fund (in the top five by AuM) responded that it was not "desperate" to get into cyber re/insurance but remained interested in seeing opportunities and would enter when a transaction met their standards. Another got quite close, but specific terms prevented the transaction from being completed. Many cited deal structure and pricing as particularly problematic; they were not being offered potential transactions that either paid enough or made sense structurally. Many respondents specifically cited the lack of a mechanism for efficient capital release, the long-tail nature of the risk, and the lack of liquidity they expected from such instruments. Additionally, many ILS fund managers stated that (related to pricing), the independent vendor models are not as reliable in cyber as they are for property-catastrophe transactions. However, a subset of those respondents did suggest that they would look past structural or modeling issues if the deal economics were favorable.

Respondents not interested in consuming cyber re/insurance risk echoed the skepticism of their interested peers but saw such issues – e.g., modeling, pricing, and deal structure – as greater barriers to engaging with cyber re/insurance risk. Most of the respondents who do not want to trade cyber did suggest that the market may carry them along. The implication of such momentum, though, is that the underlying concerns they addressed would likely be addressed at least to some degree.

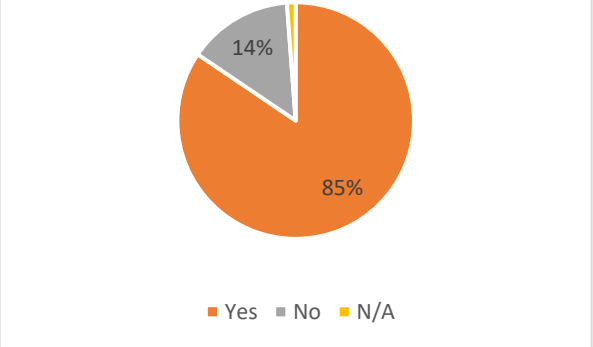
Question 3: Have you analyzed/reviewed the cyber market?

The overwhelming majority of respondents to the PCS survey have analyzed or reviewed the cyber re/insurance market. With 18 respondents representing 85 percent of the response base by AuM having engaged in such activity, it is clear that a decision to enter the sector would not have been made lightly. The response rate speaks to the broad understanding that cyber re/insurance has the potential to become a large segment of the market, which could bring significant opportunity along the entire risk and capital supply chain. Further, respondents tended to express a sense of inevitability, given the amount of original cyber exposure that exists, resulting in demand for insurance that would require further reinsurance and retrocession support.

Figure 6: Question 3 Respondents



Source: PCS, a Verisk business



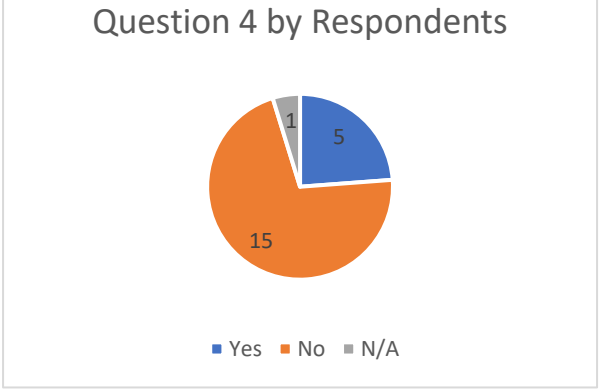
Source: PCS, a Verisk business

Three of the five companies that respondent that they have not reviewed the cyber re/insurance market have less than US$1 billion in AuM and further said they have no interest in cyber re/insurance at all. However, that position could change in the future based on substantial changes in market conditions, evolution of strategy, and other large trends and factors, even given a "never cyber" posture at present. At the other end of the spectrum, a larger respondent explained that the size of the investment necessary to explore a segment in which they are not interested was too large to be worth it. Even that perspective, though, suggests a sense of the cyber re/insurance market that can only have been informed by a preliminary inquiry.

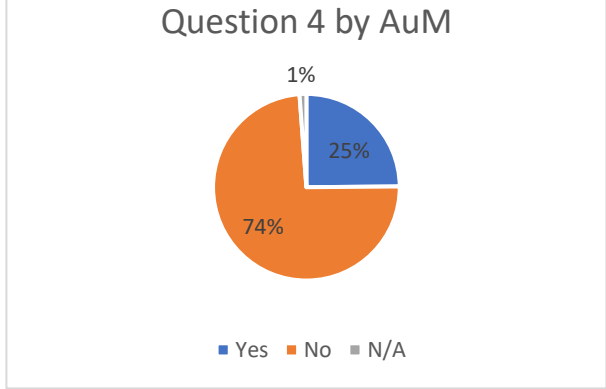
Question 4: Have you traded cyber?

The ILS market is no stranger to cyber re/insurance, although the underlying experience has been uneven. Five ILS fund managers indicated that they have engaged in cyber ILS transactions, representing US$21 billion in AuM. That is 25 percent of participants in this study (by AuM) and almost 20 percent of the ILS market as a whole. ILS participation in cyber re/insurance remains smaller than other specialty lines (e.g., marine and energy, terror, and aviation), but engagement is much larger than the broader re/insurance market appears to have realized.

Figure 7: Question 4 Respondents



Source: PCS, a Verisk business



Source: PCS, a Verisk business

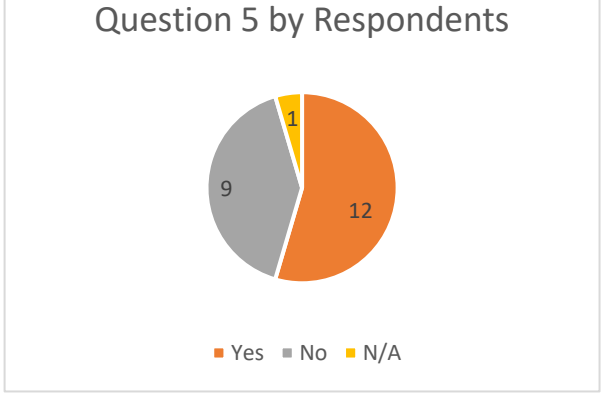
Little information is available on the number and size of transactions completed so far (which was outside the scope of this survey). There are few instances of ILS funds taking several deals per year, particularly over multiple years, according to further client conversations outside this research, and when that has happened, the trades have tended to be smaller. However, there have been instances of private transactions that have not been discussed in broader circles, as well as larger transactions that have been completed. Outside this survey, PCS has learned of transactions of at least US$20 million having been completed, and using both survey responses and separate client conversations, PCS estimates that the amount of cyber ILS completed over the past five years may approach US$500 million.

Additionally, outside our respondents, PCS understands (through conversations with several sources) that two more ILS funds that have engaged in ILS transactions. They are not included in the totals above, given that the information came from outside our respondents and when included bring the total of ILS funds engaging in the cyber re/insurance market to seven, and total AuM will not be revealed out of respect for a non-participating companies privacy.

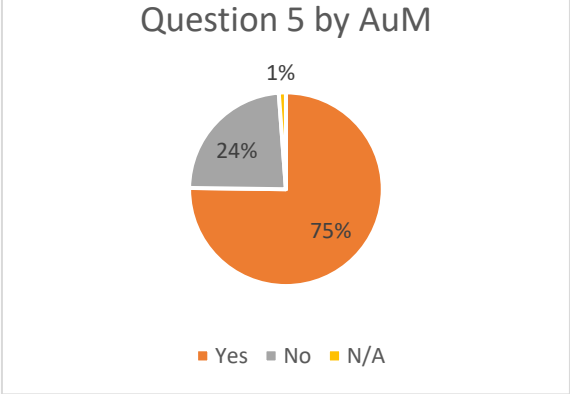
Question 5: Have you been shown cyber trades?

Respondents advised that reinsurance brokers turned to the ILS market for support much less than PCS expected, given the shortage of capacity that characterized the global cyber reinsurance market at the January 1, 2022 reinsurance renewal. The fact that 12 ILS funds (including most of the top 10 by AuM) were shown cyber reinsurance deals by reinsurance brokers is less interesting than the fact that some funds have been reviewing such opportunities for several years and still have no plans to enter the sector. The fact that they have reported monitoring with no plans to act suggests the sense of inevitability mentioned above in the discussion of question 3. The ILS fund manager community seems to think that cyber re/insurance may ultimately become unavoidable.

Figure 8: *Question 5 Respondents*



Source: PCS, a Verisk business



Source: PCS, a Verisk business

Several ILS funds surveyed have reviewed ILW trades over the past 12 months, particularly given that bid/ask spreads are narrowing to levels close enough that an ILW trade could clear. The introduction of ILWs with more realistic pricing and terms appears to have directly resulted in more engagement between reinsurance brokers and ILS funds on cyber, with several deals reportedly being actively discussed as of this writing.

In the broader reinsurance market, brokers have had to contend with an acute shortage of cyber reinsurance capacity relative to cedent demand. To support their clients, particularly at the January 1, 2022, reinsurance renewal, a number often sent cyber reinsurance submissions to reinsurers that had previously indicated they were not interested in that class of business, behavior that seemed less present in the ILS market. ILS fund managers who reported having no interest in cyber re/insurance transactions reported that they were left alone (nine respondents representing 24 percent of the respondent base by AuM). PCS asked the question above with the broader reinsurance market in mind – to see if brokers were expanding their efforts to the ILS market in order to source the capacity their clients needed.

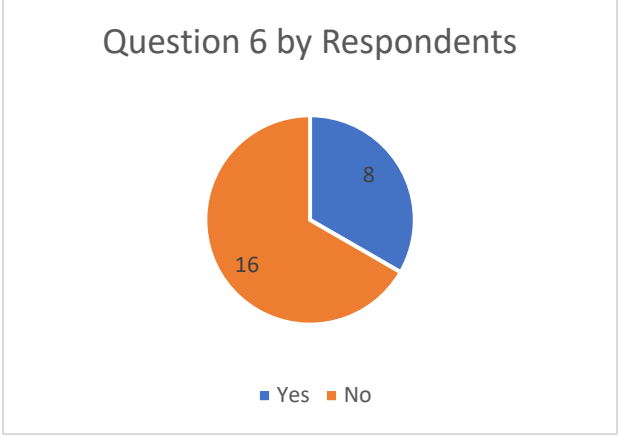
Question 6: Do you plan to trade cyber this year?

The eight respondents who answered this question favorably heavily caveated their interest, as would be appropriate. Answers include "soft yes," "only if it makes sense," and even initially targeting 2023 but would trade in 2022 if the right deal came along. Another suggested that a 2022 transaction was more likely, given the progress made in 2021. One respondent answered "maybe," which has been included here with the "yes" answers. First, this was done to protect the confidentiality of the respondent, as a single "yes" with the attendant AuM could have made it possible to determine which respondent answered in that manner. Further, the "maybe" response does not differ in substance from the "soft yes" and other heavily qualified affirmative responses that PCS received. Of course, underlying all responses was the reported need for deal flow with appropriate price and structural characteristics.

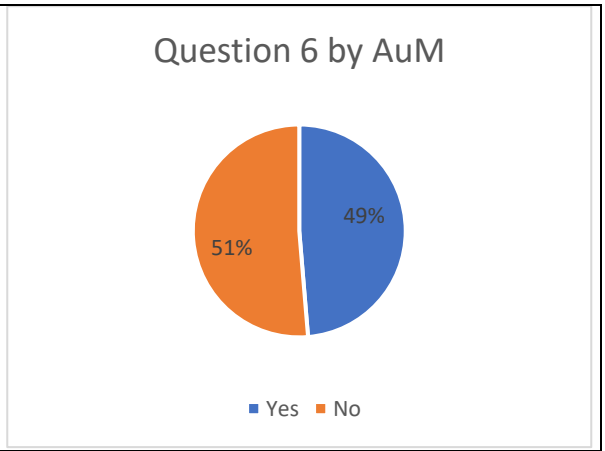
Not all five ILS fund managers who have traded cyber ILS in the past are among the eight planning to do so in 2022, although there is significant overlap. One who responded with a lack of interest in trading cyber this year indicated a willingness to reconsider based on end-investor

appetite. Several new entrants seem particularly eager to join the market, as evidenced by the fact that they have reached out to reinsurance brokers specifically to engage in their first cyber ILS transactions.

Figure 9: Question 6 Respondents



Source: PCS, a Verisk business



Source: PCS, a Verisk business

The format in which a cyber transaction is offered may make a difference in appetite – both in general and over the coming year. Several ILS funds indicated a preference for cyber risk in catastrophe bond form, citing the benefits of liquidity, the additional rigor in structuring and documentation, and the likely benefit of many market participants on the same transaction. While the speed and flexibility of collateralized reinsurance and ILWs might seem easier to manage intuitively, the infrastructure surrounding catastrophe bonds may provide a layer of comfort, in addition to structural discipline.

ILS fund respondents varied on trigger type preference when talking about trading appetite for 2022. Those already engaged in the cyber ILS sector reported using traditional reinsurance structures and could continue to trade on that basis. Most potential new entrants indicated a preference for ILWs or parametric transactions. The latter were cited as a way to narrow the coverage to specific perils, which many protection sellers see as favorable. However, adoption has been quite limited, given that buyers reported seeking broader coverage to reflect their underlying books of business more accurately. Market conversations suggest further trading in collateralized reinsurance, as well as likely first trades in the cyber ILW market.

PCS learned outside the research project of one more ILS fund that would like to trade cyber this year but was not a respondent to this survey.

6 Next steps for the development of a cyber ILS market

The fact that traditional re/insurance perspectives about cyber attitudes toward ILS were not correct oddly failed to change underlying market dynamics, largely because of other impediments to the ILS sector's adoption of ILS. However, an increase in interest in cyber re/insurance among many ILS funds suggests that better alignment of expectations between cyber re/insurers and the ILS community could be an important first step toward turning the occasional

transaction into a repeatable and scalable market that can provide robust and reliable support to the worldwide cyber re/insurance market.

Most ILS funds surveyed have at least a foundational understanding of the cyber re/insurance market and are open to evaluating cyber ILS deals. Even those unwilling to consider such transactions have a sense that there will come a day when they are pulled into the cyber ILS market. Ultimately, these sentiments are quite favorable, in that they all end with deeper ILS market engagement for the cyber re/insurance sector, which may translate to increased capital availability, a return to strong growth, and a more mature market that is not constrained by concentration risk at key value chain choke points. A primary challenge at present is to identify the mechanisms by which barriers to adoption can be removed.

Some problems may take a while to solve, but as standalone concerns, they could be managed, in part, through increased trading volume in the near term. The perceived lack of maturity among risk models, for example, is almost universally cited as an impediment to the growth of cyber ILS. That said, five funds have already transacted, and many more reported that they want to. Those that want to engage in cyber ILS, particularly in the next year, may not wait for cyber models to mature, indicating that they see bilateral trades (particularly in ILW form) as manageable through internal actuarial and analytical exercises. Further, several ILS fund managers have indicated a willingness to tolerate "best efforts" in modeling in order to see cyber catastrophe bonds come to market (which itself suggests that private perceptions of model maturity may be more positive than those offered publicly).

Price and structure have historically been problematic for cyber ILS deal completion, with a lack of historical data and uneven market penetration often noted as complicating factors. It seems that acute demand for capacity has lifted protection buyer expectations on price and increased their flexibility on terms, which means that clearing prices should be easier to attain for structures that buyers have avoided in the past, such as index-triggered transactions including ILWs and parametrics. ILS funds reported seeing potential returns increasing to levels that are worth exploring in detail, which could help repeatable deal structures get completed, an important first step toward the commoditization of the risk. That commoditization should drive scale, which ultimately may support broader cyber re/insurance market growth.

What is most evident from the responses offered by more than 75 percent of the global ILS community is that cyber ILS is still very much a work in progress. The responses suggest that the sector generally wants to consume cyber re/insurance risk and is looking for ways to do so. Short-term barriers outside the cyber re/insurance market (such as several years of high property-catastrophe losses) do not appear to be slowing cyber ILS progress as much as they used to, particularly for funds that are willing to take on cyber risk as a diversifier in their portfolios, even if it does potentially introduce some end-investor correlation. From 12 months of this writing, the amount of cyber ILS transactions completed is likely to increase substantially from where it is today, if for no other reason than the combination of acute protection buyer need and the increased interest among ILS funds in providing such cover.

As the ILS market formed to help a re/insurance industry beleaguered by Hurricane Andrew 30 years ago, today it seems poised to play that role again in support of a market that requires an infusion of capital to serve its end customers.

Disclaimer

The authors are the head of PCS and director of specialty lines product development. The views expressed herein are those of the authors, based on research conducted by the authors, and may not necessarily represent the views of others, unless otherwise noted. PCS, a Verisk business, generally provides data and analytics to the global re/insurance and ILS markets. PCS captures reported loss information on certain events, which may encompass, on average, approximately 70% of the market. Any reference to industry-wide is based on this research and the authors' view of trends in the industry, and do not necessarily represent the view(s) of others in the industry.

References

Ammar, S.B., Braun, A., & Eling, M. (2015). *Alternative Risk Transfer and Insurance-Linked Securities: Trends, Challenges and New Market Opportunities.* St. Gallen: Institute of Insurance Economics.

Aon Securities. (2021). *ILS Annual Report 2021: Alternative Capital: Continuing Growth Momentum*.

Artemis. (2017). PCS puts Merck malware cyber loss estimate at $275m. *Artemis.* 18 October. Retrieved 21 June 2022, from https://www.artemis.bm/news/pcs-puts-merck-malware-cyber-loss-estimate-at-275m/.

Artemis. (2018). Property cat still key area for ILS market growth, cyber close behind. *Artemis.* 23 November. Retrieved 6 February 2022, from https://www.artemis.bm/news/property-cat-still-key-area-for-ils-market-growth-cyber-close-behind/.

Artemis.bm. (2022). Insurance Linked Securities Investment Managers & Funds Directory. *Artemis*. Retrieved 31 January 2022 from https://www.artemis.bm/ils-fund-managers/.

Association of British Insurers (ABI). [No year given] Cyber risk insurance. *ABI.* Retrieved 21 June 2022, from https://www.abi.org.uk/products-and-issues/choosing-the-right-insurance/business-insurance/cyber-risk-insurance/.

Bermuda:Re+ILS. (2018). Hiscox introduces new cyber ILW. *Bermuda:Re+ILS.* 16 March. Retrieved 22 June 2022, from https://www.bermudareinsurancemagazine.com/news/hiscox-introduces-new-cyber-ilw-3850.

Biener, C., Eling, M., & Wirfs J.H. (2014). Insurability of Cyber Risks; An Empirical Analysis. *The Geneva Papers*. *1*(28), 1-28.

Carter, R.A., Paine, D., & Enoizi, J.. (2022). *Insuring Hostile Cyber Activity: In search of sustainable solutions.* January. Zurich: Geneva Association.

Carter, S., & Mainelli, M. (2018). *Cyber-Catastrophe Insurance-Linked Securities On Smart Ledgers.* Long Finance – Distributed Futures, SSRN.

Dal Moro, E. (2020). Towards an Economic Cyber Loss Index for Parametric Cover Based on IT Security Indicator: A Preliminary Analysis. *Risks 8*(45), 1-12.

Evans, S. (2019). Cyber a growth compartment for the ILS industry: Millette, Hudson Structured. *Artemis.* 8 November. Retrieved 6 February 2022, from https://www.artemis.bm/news/cyber-a-growth-compartment-for-the-ils-industry-millette-hudson-structured/.

Evans, S. (2021). Munich Re expects €1.8 billion losses from Ida & European floods. *Artemis.* 19 October. Retrieved 31 January 2022, from https://www.artemis.bm/news/munich-re-expects-e1-8bn-losses-hurricane-ida-european-floods/.

Gallin, L. (2019). No fast way into cyber for ILS, say experts. *Artemis.* 27 November. Retrieved 6 February 2022, from https://www.artemis.bm/news/no-fast-way-into-cyber-for-ils-say-experts/.

Gallin, L. (2021). PCS explores the complex development of Hurricane Ida: Interview. *Reinsurance News.* 7 December. Retrieved 6 February 2022, from https://www.reinsurancene.ws/pcs-explores-the-complex-development-of-hurricane-ida-interview/.

Greenwald, J. (2021). Reinsurers can strengthen cyber market: Standard & Poor's. *Business Insurance.* 29 September. Retrieved 6 February 2021, from https://www.businessinsurance.com/article/20210929/NEWS06/912344890/Reinsurers-can-strengthen-cyber-market-Standard-&-Poor%E2%80%99s.

Hofmann, D.M. (2018). *Advancing Accumulation Risk Management in Cyber Insurance: Prerequisites for the development of a sustainable cyber risk insurance market.* Zurich: Geneva Association.

Howard, L.S. (2021). Re/Insurance Cyber Rates Could Double Before 2023, as Attacks Skyrocket: S&P. *Insurance Journal.* 30 September. Retrieved 6 February 2022, from https://www.insurancejournal.com/news/international/2021/09/30/634535.htm.

International Association of Insurance Supervisors (IAIS). (2020). *Cyber Risk Underwriting: Identified Challenges and Supervisory Considerations for Sustainable Market Development.* Basel: IAIS.

Johansmeyer, T. (2021). Can Cyber Insurance Survive without Diplomatic Support? *Global Policy*. 5 October. Retrieved 31 January 2022, from https://www.globalpolicyjournal.com/blog/05/10/2021/can-cyber-insurance-survive-without-diplomatic-support.

Johansmeyer, T. (2021). Cybersecurity Insurance Has a Big Problem. *Harvard Business Review*. 11 January. Retrieved 6 February 2022, from https://hbr.org/2021/01/cybersecurity-insurance-has-a-big-problem.

Johansmeyer, T. (2021). Political violence and resilience: A capital markets solution. *Security Magazine.* 30 July. Retrieved 31 January 2022, from https://www.securitymagazine.com/articles/95748-political-violence-and-resilience-a-capital-markets-solution.

Johansmeyer, T. (2018). Cyber: don't catch your tail in the door. *The Actuary.* 6 February. Retrieved 21 June 2022, from https://www.theactuary.com/opinion/2018/01/2018/02/06/cyber-dont-catch-your-tail-door.

Koch, A.C. (2018). Casualty: The Next ILS Frontier? *Insurance Journal*. 6 August. Retrieved 6 February 2022, from https://www.insurancejournal.com/news/national/2018/08/06/497146.htm.

Mainelli, M, Von Gunten, C., & Duff, M. (2015). Promoting UK Cyber Prosperity: Public-Private Cyber-Catastrophe Reinsurance. *Public-Private Cyber-Catastrophe Reinsurance – Long Finance, 2015.* 1 July. Retrieved 22 June 2022, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3676352.

NetDiligence. (2022). Cyber War: Legal Issues, Coverage & Exclusions. *Cyber Risk Summit Philadelphia: June 2022.* 1 June 2022. Retrieved 21 June 2022, from https://netdiligence.com/virtual-programming/#philadelphia-22.

News. (2018). PCS designates Marriott hotel hack as a global cyber loss event. *Insurance Day*. 4 December. Retrieved 21 June 2022, from https://insuranceday.maritimeintelligence.informa.com/ID1124684/PCS-designates-Marriott-hotel-hack-as-a-global-cyber-loss-event.

Reuters. (2021). Cyber reinsurance rates rocket at July renewals – Willis Re. *Reuters.* 1 July. Retrieved 6 February 2022, from https://www.reuters.com/technology/cyber-reinsurance-rates-rocket-july-renewals-willis-re-2021-07-01/.

Romanosky, S, Ablon, L, Kuehn, A, & Jones, T. (2019). Content analysis of cyber insurance policies: how do carriers price cyber risk? *Journal of Cybersecurity*, *5*(1), 1-19. Retrieved 21 June 2022, from https://academic.oup.com/cybersecurity/article/5/1/tyz002/5366419.

Sheehan, M. (2022). Renewal rate increases imply dramatically better returns: KBW. *Reinsurance News.* 6 January. Retrieved 6 February 2022, from https://www.reinsurancene.ws/renewal-rate-increases-imply-dramatically-better-returns-kbw/.

Seals, T. 2021. Ransomware Volumes Hit Record Highs as 2021 Wears On. *ThreatPost.* 3 August. Retrieved 31 January 2022, from https://threatpost.com/ransomware-volumes-record-highs-2021/168327/.

Shah, S.S., & Dyson, B. (2018). Cyber insurance-linked securities have arrived, but market still in infancy. *S&P Global Market Intelligence.* 12 October. Retrieved 6 February 2022, from https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/cyber-insurance-linked-securities-have-arrived-but-market-still-in-infancy-46915334.

Sheehan, M. (2020). Hiscox comments on new cyber parametric transaction. *Reinsurance News.* 21 January. Retrieved 22 June 2022, from https://www.reinsurancene.ws/hiscox-comments-on-new-cyber-parametric-transaction/.

Strupczewski, G. (2017). Current State of the Cyber Insurance Market. In *10th Economics & Finance Conference* (pp. 491-501).

Temple-Raston, D. (2021). A 'Worst Nightmare' Cyberattack: The Untold Story of SolarWinds. *NPR.* 16 April. Retrieved 31 January 2022, from https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.