Perception Shapes Reality: How Views on Financial Market Correlation Affect Capital Availability for Cyber Insurance

Tom Johansmeyer

POLIR PhD Candidate, University of Kent, Canterbury

+1 441 799 0009

trj5@kent.ac.uk

ABSTRACT: The future of the cyber insurance and reinsurance market is uncertain, as is the case for any new and emerging market. A lack of historical data and experience constrain the analysis needed to support growth. Further, the prospect of fresh capital from the insurance linked securities (ILS) sector is constrained by a number of practical factors. Among the most important, though, is one that is nearly impossible to prove: the extent to which cyber risks are correlated with financial markets. It is an article of faith, and one that lacks clear consensus in the ILS market. If cyber is not correlated with financial markets, gaining adoption of that view could mean a significant influx of risk capital to support a new and expanding market. However, if the contrary becomes the dominant narrative, future cyber market growth could become slow and difficult to attain. Absent the ability to prove the negative, this article features makes an original contribution to the literature by presenting the findings of interviews with leading ILS managers on their views regarding the extent to which cyber risk is correlated with financial markets. The result is a new perspective on how to fuel cyber re/insurance growth.

KEYWORDS: cyber insurance, risk management, reinsurance, insurance linked securities, economic security

CONFLICT STATEMENT: I have no conflicts that informed this research. I do currently work as a reinsurance broker, but I received no funding or market input for this research. Nothing in this article would translate into a market impact, and no clients provided any feedback. All data used is publicly available.

Introduction

Historical data on the cyber insurance and reinsurance ("re/insurance") environment is thin. The class of business has a short history, and the underlying risk environment – the cyber domain – has not been around much longer. History is measured in decade for cyber risks, while other areas of the re/insurance business, like natural catastrophes, are measured in millennia. The lack of context and precedent can make analysis and judgment seemingly more difficult, with forecasts, projections, and guesswork leaning much more on assumptions than evidence and experience. While a cautious approach may seem to be safer in the near term, though, it may actually accomplish the contrary. Slow and small movements to support the nascent cyber re/insurance market, based on the belief that realistic disaster scenarios reflect extreme possibilities, may increase overall cyber insecurity by keeping capital out of the market. As a result, problems that could be managed with re/insurance market participation are forced to go unhedged, resulting in greater economic harm.

This article looks at one subset of the problem described above. There is a belief, reflected in the historical literature, that cyber attacks are correlated with financial markets. This one premise carries disproportionate weight in the global re/insurance industry, as it directly effects the extent to which

capital can be deployed to support cyber re/insurance risks. In fact, the impact that this belief has is best illustrated by looking at the property-catastrophe reinsurance market. Largely believed not to be correlated with financial markets (or very loosely correlated, with the exceptions coming in only the most extreme and remote of hypothetical cases), the diversifying effects of the property-catastrophe market have made it attractive for capital providers. What this means for cyber risks, then, is that non-correlation could make it possible for significant capital inflows to support the cyber re/insurance market, while the belief in the correlation of cyber and financial market risks could very well do the contrary.

The research question that this article seeks to address, therefore, is whether ILS market participant perceptions on the extent to which cyber risks and financial markets could enable or impede the flow of capital to support re/insurance risks. In addition to an analysis of historical events, the article focuses on interviews with ten members of the insurance linked securities (ILS) market, where discussions included the issue of cyber risk and financial market correlation. The conversations do not seek to prove or disprove the issue of financial market correlation. Instead, they seek to show the mindsets present in the ILS market and the extent to which they could enable or impede the flow of capital to support cyber re/insurance risks.

This article makes a unique contribution to the historical literature not by attempting to prove the negative on cyber and financial market correlation – with an effort to prove the negative in general a fool's errand by any measure – but rather by mining the global insurance linked securities (ILS) market for the views of its participants on the extent to which cyber risks and financial markets are correlated. While there have been several efforts to understand the role that the ILS market could play in cyber re/insurance, direct engagement with ILS market participants and their views of the market have been largely limited, as the literature review below will show.

The article begins with a review of the historical literature on the correlation of cyber risk and financial markets in general before focusing more specifically on this issue within the global re/insurance industry, after which it embarks on an analysis of past cyber events affecting multiple companies each and causing significant economic loss. The purpose of this section is to discern the extent to which cyber event and financial market correlation has occurred already and provide a foundation not just for future extrapolation but also for the discussion that follows. In addition to the review of past cyber events relative to financial market correlation, itself a unique contribution to the historical literature, this article offers the findings of interviews with ten ILS fund managers representing nearly half the ILS market as measured by assets under management (AuM) to show how the end capital providers who would support the cyber re/insurance market perceive the risks associated with how financial markets would respond to cyber events.

Background and Literature Review

The treatment of cyber security often veers into the realm of the apocalyptic – or, at a minimum, toward hyperbole (Galt 2022). From U.S. national defense worries of a "cyber Pearl Harbor" to devastating systemic loss events like "cloud down" or the decimation of major financial institutions (Reeder and Hall 2021 15, Schanz 2018 7), there is no shortage of imagined scenarios that lead to societal chaos and a strain on potentially necessary government or military responses and remedies. Moreover, "imagined" is an important concept, as Lewis of Center for Strategic and International Studies observes: "It is easier to

imagine a catastrophe than to produce it" (Lewis 2020). The effects of this imagination is as old as the connected environment itself.

Evolution of Attacks and Insurance in the Cyber Domain

Two of the earliest instances of cyber attacks (in the conventional sense) came in the 1980s. One is generally believed to be the first ransomware attack. Although the motivation of attacker Joseph Popp remains unknown, his efforts became quite the opposite. He distributed floppy discs in 1989 purporting to have information related to AIDS research (Murphy Kelly 2021), but it really included a Trojan horse virus that went on to damage researchers' data. The other, known as the "Morris Worm," decimated the internet in 1988. Originally developed to satisfy the curiosity of the malware's author, Robert Morris, the worm did not destroy any files but caused internet performance to "slow to a crawl" (FBI). Ultimately causing damage into the millions of dollars, the episode ended with criminal prosecution, a fine, and 400 hours of community service.

Such episodes as the AIDS ransomware and the Morris Worm, coming in the early days of interconnected computer use (admittedly, the ransomware used interconnectivity via traditional mail), make it easy to assume the destructive impact possible today. If one were to take the damage caused by the Morris Worm, for example, and apply it to the internet and our reliance on it now, the impact would be unthinkable. The next development in thinking around catastrophic cyber events served only to add fuel to the fire: Contemplation of cyber war. In 1993, Arquilla and Ronfeldt made their concerns clear in an article entitled, "Cyberwar is Coming!" They believed that cyber capabilities "will bring the next major shift in the nature of conflict and warfare" (1993 143), triggering a wave of speculation about the destructive potential of cyber war and systemic cyber in general.

While threats in the cyber domain are undoubtedly serious and have deserved the wide scholarly attention they have received, overestimating the threat can lead to the contemplation of unrealistic risks and extremely unlikely consequences. Entertaining what is unrealistic could lead to a perception of the risk that is disconnected from the actual threat, which in turn could result in suboptimal risk and capital management by contemplating the unrealistic while failing to prepare for what is remote but still plausible. The insurance industry has had to struggle with such challenges since the early days of its involvement with cyber risk. In fact, it was only recently that the insurability of cyber risk became taken for granted.

Although the earliest cyber insurance policies appear to have been issued in the late 1990s, the market remained small (Wolff 2022). Early efforts had low premiums and low loss ratios, and as the product gained viability, increased adoption and coverage scope led to wilder divergences in pricing and ultimately increased testing of the line of business (i.e., losses). The market gained some prominence, strictly coincidentally, around the same Rid, Gartzke, and other scholars introduced new thinking to counteract the positions exaggerating the nature of catastrophic cyber risk. The industry weathered such losses as the 2013 Target and 2014 Home Depot breaches, but remained small until 2018 and the aftermath of the WannaCry and NotPetya cyber attacks (Greenwald 2014, Hemenway 2023, Haskell-Dowland 2017). Demand for cyber insurance then spiked, and pricing adjusted based on recent loss experience to reflect the nature of the risk, a process further shaped by the ransomware epidemic soon after the 2017 events. Worldwide affirmative cyber premium surged from $3.5 billion in 2017 to $13 billion in 2023 (Schanz 2018 7, Johansmeyer 2023). Interestingly, though, penetration lagged premium growth, with the clear implication that cyber insurance was becoming more expensive than it was

prevalent. Today, total cyber limit outstanding is approximately $400 billion, with at least half of it ceded to reinsurance (Johansmeyer 2023).

Despite the rapid and substantial growth the cyber insurance sector demonstrated, skeptics remained, which contributes to the current dynamic involving the gap between premium growth and underlying protection depth. Today, the insurability of cyber risk is more firmly established – there are exceptions (e.g., Johansmeyer 2023c) – but that has come after an extensive industry-wide debate over the insurability question, raised in various forms by Eling, Elvedi, and Falco, who note that even the most extreme economic losses from cyber events are far smaller than property-catastrophe counterparts, with Hurricane Katrina above $100 billion and the 2011 Tohoku earthquake and tsunami above $200 billion (2022 430), an issue explored in more depth later in this article, with detail not presented in the historical literature (e.g., see Table 1). Eling, Elvedi, and Falco do conclude that cyber risk is insurable, a fact borne out by the state of the industry today. However, caveats remain: “Some of today’s cyber risks do not fully meet the typical characteristics of insurability” (Cellerini et al. 2022 2).

Among the concerns cyber insurers face with regard to the question of insurability is moral hazard, with the risk of insureds taking unnecessary or inappropriate risks because of the insurance in place as protection. Moral hazard could manifest as a “homeowner neglecting ageing water pipes,” for example (Grant 2012 13). In the cyber domain, moral hazard could result from reduced technology security budgets, because the insurance recoveries will ultimately cover the damage (Bailey 2013 22). This is a fairly popular view, shared also by Majuca, Yurcik, and Kesan (11), Lemay (2021), Porup (2018), and Dou et al. (2020). Yet among practitioners, moral hazard is perceived as rare (MacColl, Nurse, and Sullivan 2021 37). The reasoning is straightforward, according to research conducted by MacColl, Nurse, and Sullivan: “You wouldn’t want your house to burn down because you have an insurance policy” (2021 36). Further, this discussion overlooks the consequences of moral hazard: Once an insured has a claim, their ability to secure future cover could become much more challenging.

The practicality of moral hazard (and its being muted) is evident in industry loss ratios for cyber, where experience has offered a useful counterbalance to suspicion. Insured losses in cyber have been quite manageable. A.M. Best put the industry loss ratio at 44.6% in 2019, increasing to 66.9% in 2020, reflective largely of the increase in ransomware activity (Pain and Noordhoek 2022 8). For a tough year, 66.9% is hardly indicative of a crisis. In part because of loss experience (and an increased understanding of the risk), the issue of cyber insurance as a protection mechanism has evolved from a question of insurability to one of achieving penetration. According to Schanz, “The least researched protection gap is cyber risk” (1). While it is certainly insurable, it is not sufficiently penetrated to show how much of the economic losses above the industry could handle. Levite, Kannry, and Hoffman add, “Even though the insurance industry traditionally plays a critical role in risk channeling, at present the private sector is not fully capable of taking advantage of cyber risk insurance” (2018 9).

The growth demonstrated so far, as mentioned above, has largely focused on premium rather than overall protection, a dynamic that can be expected to continue, even if the disparity becomes less pronounced. While it would be easy to cite losses from the ransomware epidemic, there are underlying market structural factors that play an important role in how the cyber insurance sector has evolved. Among them is the industry’s heavy reliance on reinsurance, with insurers ceding as much as half their business to reinsurers (Cellerini et al. 2022 16). Absent a robust retrocession market, reinsurers had no outlet for hedging the volatility in the quota shares they assumed. Inefficient risk and capital

management thus became a major factor in the cyber insurance sector's ability to grow. Part of the inefficiency traces back to the industry's view of cyber as a systemic risk – and the belief that cyber events are correlated with global financial markets.

Literature Review

The possibility that cyber attacks could wreak such havoc in financial markets has led some to believe that cyber risks may be highly correlated with broader financial markets. While the "correlation between cyber risk and business risk isn't a foreign concept by any means," it takes a lot for a systemic event to impact financial markets as a whole (Raissipour 2023). That said, there is no shortage of alarmism. "Cyber risk is more likely to be realized with systemic ramifications than is operational risk generally, according to a note from the Federal Reserve, which continues, "Fire sales, liquidity freezes, and potential solvency issues may play out differently after a cyber shock" (Brando et al. 2022). An International Monetary Fund (IMF) working paper frets, "As the connections between cyberspace and real economy intensify – amid a widely expected further increase in interdependency, interconnectivity and complexity – the probability for an external shock to transfer to the financial system and become a systemic event is likely to increase even if steps are taken to mitigate these risks" (Kopp, Kaffenberger, and Wilson 2017 22).

Part of the problem is that cyber tends to be viewed purely in terms of aggregate exposure to loss, rather than with some sort of mitigating factors. For example, Kaffenberger and Kopp frame their concerns about systemic risk with the rapid proliferation of internet-connected devices – from 500 million in 2003 to 31 billion in 2018 – implying that the sheer number of points that could be compromised has grown to incredible scale and brought with it seemingly proportional vulnerability (2019). Issues such as "[s]ize and interconnection" are common themes, implying that big exposures that are connected to each other will easily transmit risk and lead to an accumulation of consequences (Fell et al. 2022). All of this points to the interconnected cyber risk environment being "a small world after all," but that may overstate the situation (Adelmann et al. 2020 1).

Although focused specifically on the increase in cyber risk to the financial system during the early months of the COVID-19 pandemic, one study concludes that a period of heightened risk brought with it increased correlation between cyber risk and financial markets, but that a cyber attack would have had to come "relatively quickly to achieve maximum damage" (Eisenbach, Kovner, Lee 2022 5). Other stabilizing mechanisms to offset an attack were being implemented. Further risk factors are discussed, such as the potential effects on trading books, but such discussions remain hypothetical and all imply not just an attack, but a successful one. As a result, the extent to which cyber risks are correlated with broader global financial markets remains elusive.

Insurance industry literature is split on the nature of the threat. One side of the debate has framed cyber risk as different from non-correlated risks (e.g., property-catastrophe risk), citing "clear connections to the economy" and a further claim that "the constant stream of data breaches and ransomware attacks is recognised as a direct economic drag" (Hoffman et al. 2018 9). While there are certainly economic consequences from such events, correlation with broader financial markets is quite a leap, and one as yet without justification (more on this in the coming sections of this article). The thought ends with the notion that a "major event" could possibly trigger a negative reaction from financial markets," and focus should be placed on "could possibly," which indicates that such an event has not happened (*ibid.*). Kaffenberger and Kopp go a step toward the other end of the spectrum, noting that the risks are

correlated but that a relevant situation has yet to occur (2019), and others note that correlation may exist in remote scenarios but that insurance mechanisms can still be developed (Forscey et al. 2022).

Meanwhile, what is clear is that the cyber re/insurance market needs more capital in order to achieve the growth rates that have been forecasted, with one firm suggesting that cyber insurance premium alone could reach $50 billion by 2040 and another suggesting that cyber reinsurance premium could nearly equal property-catastrophe reinsurance premium by 2032 and exceed $100 billion by 2035 – compared to worldwide cyber reinsurance premium of only around $6 billion in 2023 (Howden 2023 34, Newman, et al. 2023 12, Johansmeyer 2023). The ability of more capital to come into the cyber re/insurance market will depend in part on the extent to which ILS market participants – as well as re/insurers – believe that cyber risks are correlated with financial markets.

As to how the ILS market views cyber risk, little original research has been conducted. The only article that directly engages ILS professionals for their views on the cyber re/insurance market revealed a nuanced and uneven perspective held by, then, a relatively large number of ILS managers having taken positions in cyber trades – seven (Johansmeyer and Mican 2022 53), although several others have commented from afar. Today, at least ten ILS managers are believed to have participated in cyber re/insurance transactions, although for most of them, positions have been small and cautious (Johansmeyer 2023). Issues such as correlation have been raised, e.g. by Carter, Pain, and Enoizi, but not only as a broad concern with little exploration among members of the ILS community (2022 22).

What stands out most in the discussion about the extent to which cyber risk is correlated with financial markets is not just the lack of precedent but the acknowledgement of it. Nothing of sufficient magnitude has happened. It may be tempting to add “yet,” but the belief that what the insurance industry often calls “the hurricane Andrew of cyber” remains just that – a belief (Cuneo 2016).

This rejection of fatalism with regard to the possibility of a market-changing (or even society-changing) cyber catastrophe has finally found some purchased, with a strong statement on the potential for cyber risks to be correlated by financial markets recently published by reinsurance intermediary Guy Carpenter. The firm notes in an analysis of historical cyber attacks and financial market behavior that no such correlation has manifested, using the VIX as a point of comparison (Cordonnier et al. 2023 8). Ultimately, the firm caveats that impact can be a matter of degree, with broad financial market impact unlikely. Instead, Guy Carpenter notes that to have a systemic effect, “cyber events must ‘escape’ to the larger domains of financial activity,” like the monetary or transportation systems (Cordonnier et al. 2023 9). Finally, and impactfully, the report explains that “[w]hile many of the previously unimaginable scenarios have now indeed occurred (ransomware and wiper worms, grid and pipeline attacks, market disruptions, electoral interference, etc.), none of them has evidently produced broader impacts, at least in the financial markets” (Cordonnier et al. Guy Carpenter 10), with a nod to the view by Lewis expressed earlier in this article: “It is easier to imagine a catastrophe than to produce it” (Lewis 2020).

The analysis later in this article will review several historical cyber catastrophe events and show the absence of financial market impact. Further, it will contemplate the line between the realistic and fantastical with regard to cyber scenarios, enabling the potential for a smoother flow of risk capital into the cyber insurance market. In fact, this article makes a unique contribution to the literature on systemic cyber risk management in the insurance industry by engaging directly with ILS managers on the subject of financial market correlation with cyber risk and how it is perceived within the context of asset allocation to non-correlated (or lightly correlated) risks.

Methodology

This paper relies on a mixed methods approach to research, beginning with a compilation of key industry metrics to use as a foundation for understanding the nature, composition, and depth of the cyber re/insurance and ILS market. Using that context, the research then moves to a qualitative phase, in which ILS market participants are asked for direct feedback. The compilation of data involves secondary research using a wide range of publicly available data sources and existing publications. Primary research regarding the relationships among cyber risk, climate change, and the re/insurance industry comes from interviews with eleven cyber reinsurance executives and ten ILS managers. The interviews involved a much broader range of cyber re/insurance and security concerns, with the comments relevant to this article's research question specifically extracted for analysis.[1]

First, the use of secondary data in this article includes the development of a list of historical relevant catastrophic cyber events and their attendant economic losses. This research builds upon the sixteen-event table covering such events from 1999 through 2022 originally published in a case study comparing the effects of cyber attacks and kinetic attacks (Johansmeyer 2023b 6). Admittedly, that table was built using publicly available sources and was a supporting exhibit. As a result, it did not warrant the methodological rigor necessary to form a comprehensive and original source of historical catastrophic cyber data for analysis. The updated version of that historical list (in Table 1, later in this article) relies on additional research done for an article as-yet unpublished but currently undergoing peer review. A full methodological treatment is outside the scope of this article. In summary, the additional seven events were found through research of publicly available sources and the use of expert judgment to determine a final estimate for inclusion. Some loss estimates have been updated relative to the original sixteen-event dataset.

The events included in Table 1 have to meet specific criteria. First, economic scale must be established. Table 1 considers only events with economic losses of at least $800 million, adjusted for inflation to 2023 at an annual rate of 3%. The threshold was originally contemplated at $1 billion but was lowered to allow two more events into the dataset. Given the thin history, every additional record is helpful. There are no events after 2017. Although there has been plenty of cyber loss activity, no widespread attacks have achieved the necessary economic impact. As catastrophic events, they must have impacted a significant number of companies. Large, costly cyber attacks against single companies would not qualify, as they are limited in scope. Further, the purpose of the data in Table 1 is to establish scale for the discussion of systemic events and financial market correlation. Single-company attacks may be correlated with the share prices of those companies, and they may even have limited effect to companies in the victim's ecosystem. However, that does not meet the criteria for true market correlation. For this reason, large single-company events like the Equifax breach in 2017, the Epsilon attack in 2011, and the Veterans Affairs cyber event of 2006 are not included (FTC 2022, Firmex).

A further caveat is necessary for the use of statistics with regard to the size and scale of the global cyber re/insurance market. No independent, academic survey of the market has conducted to make that data available, leaving choices with severe limitations. Often, scholars use company reports as sources of data. Although they certainly come from entities with clear commercial agendas to advance, dismissing their usefulness for that reason is perilous, given the deep and direct insight these companies have into

[1] This research is for this author's Ph.D. in international conflict analysis, which is in progress.

the market. Alternatively, expert (but not peer-reviewed) sources have begun to appear, such as the review of cyber insurance market size in Lawfare in 2023, which is the output of academic research published in a non-academic setting (Johansmeyer 2023). This article makes use of both, favoring the latter where possible because it comes from academic research (albeit of commercial market participants).

Next, interviews were conducted and recorded using Microsoft Teams and ranged from 30 minutes to 60 minutes, with each participant interviewed once between 24 March 2023 and 8 June 2023. The project uses a thematic analysis approach, with semi-structured interviews and transcripts each coded multiple times. Information specific to the research question has been extracted from the broader interview transcripts for further examination into the issue of the interplay between natural disasters and cyber re/insurance from ten ILS managers participating. The ten ILS managers interviewed represent $49 billion in assets under management (AuM), which is approximately 47% of the $104.9 billion ILS sector (Artemis.bm Deal Directory 2023). Of them, eight engaged explicitly with the subject of whether cyber risk is correlated with broader financial markets (40% of worldwide ILS AuM). Of them, five believe that such correlation is either light or non-existent (28% of worldwide ILS AuM).

The analysis of this problem proceeds in two parts. The first is a review of historical experience – specifically, the absence of it. Although there have been systemic cyber events, none has had an impact on global financial markets. To help fill the gap left by the lack of precedent, several cases where cyber attacks caused individual company share prices to drop significantly are reviewed, with the caveat that such cases are, by definition, not systemic. Following the historical case and data review, findings from interviews with ILS managers on the extent to which they believe cyber risk is correlated with financial markets will be presented and linked to the historical cases.

Past Performance Does Not Guarantee Anything

That the past is a poor guide for the unprecedented, painfully obvious. However, it bears mentioning due to the frequency with which this guidepost is used in matters of economic security in the cyber domain. Whether it is because there have been major cyber attacks with overestimated impact (such as Stuxnet) or the lack of past events is used to signal that they are due to occur (Slayton 2017) – a view of forecasting that has absolutely no foundation in the real world – it is normal to rely on the past as guide when no other guide is available. Doing so, however, is dangerous.

Existing scholarship on the interplay between cyber risks and global financial markets relies heavily on speculation, as described earlier in this article. Nothing has caused the systemic event that worries so many, and which is largely believed to be inevitable. Consequently, the problem of financial market correlation with cyber risk – at least on a mass scale – remains theoretical. However, more fodder for savvy speculation and extrapolation exists than is often recognized. While many say the “big one” – or the Hurricane Andrew – has not yet struck, perhaps they are being seen wrong. In fact, the “big one” may have occurred already and simply was not big enough to have systemic effects on the global financial system, meaning that cyber risks would be correlated with financial markets only in the most extreme and unrealistic situations. It would also suggest that the “big one” is not necessarily as impactful as the imagination would suggest.

Unfortunately, the cyber insurance industry lacks a resource equivalent to what Munich Re NatCatSERVICE and Swiss Re *sigma* offer for historical natural disasters. There is no central database of

catastrophic cyber events and attendant economic losses. Industry loss reporting agency PCS, a division of data/analytics firm Verisk, has a database of industry-wide insured losses from cyber catastrophe events, but only one such event, NotPetya, generated sufficient loss to meet the threshold for PCS reporting (Smith 2019). To fill the gap, albeit temporarily, Table 1, below, offers a view of historical catastrophic cyber events and attendant economic losses since 1998. As discussed in the methodology chapter, the $800 million threshold for inclusion (adjusted for inflation) is the reason why there are no events listed after 2017.

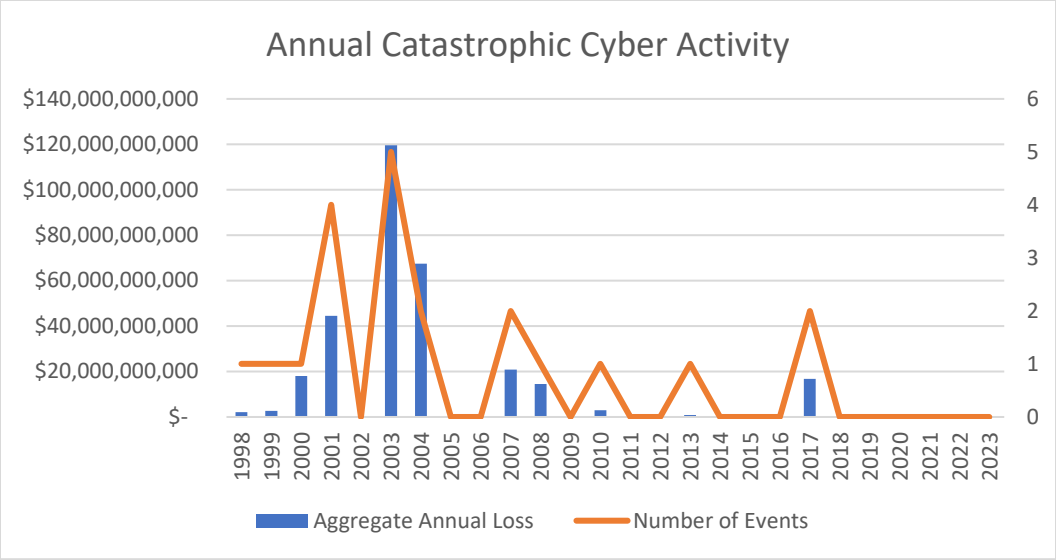
Table 1: Summary of Final Estimates for Catastrophic Cyber Events

Event	**Year**	**Economic Loss Estimate (Original)**	**Economic Loss Estimate (Adjusted to 2023)**
Chernobyl	1998	$1 billion	$2.1 billion
Melissa	1999	$1.3 billion	$2.6 billion
ILOVEYOU	2000	$9.1 billion	$18 billion
Klez	2001	$19.9 billion	$36.2 billion
CodeRed	2001	$2.25 billion	$4.3 billion
Nimda	2001	$1.1 billion	$2 billion
SirCam	2001	$1 billion	$2 billion
SoBig	2003	$36.1 billion	$65.2 billion
SQL Slammer	2003	$1.1 billion	$2 billion
Swen	2003	$9.2 billion	$16.5 billion
Minmail	2003	$8.9 billion	$16 billion
Yaha	2003	$11.1 billion	$19.9 billion
MyDoom	2004	$38 billion	$66.6 billion
Sasser	2004	$500 million	$900 million
StormWorm	2007	$10 billion	$16 billion
Conficker	2008	$9.1 billion	$14.6 billion
Zeus	2007	$3 billion	$4.8 billion
Stuxnet	2010	$2 billion	$2.9 billion
CryptoLocker	2013	$665 million	$900 million
NotPetya	2017	$10 billion	$11.9 billion
WannaCry	2017	$4 billion	$4.8 billion

Sources: 108th Congress (2003), Beattie (2012), Cyware Hacker News (2016), Gerencer (2020), Greenberg (2018), Haury (2012), Leman (2019), Mi2g (2003), Moes (2023)

As Table 1, above, shows, many cyber events with profound economic consequences have occurred over the past twenty-five years. Of the twenty-one events identified (which may not be exhaustive), few achieved significant levels of economic loss. MyDoom and SoBig are the two largest and the only two to exceed $60 billion each in economic loss. Klez, at $32 billion, is third, reflecting a large drop in quantum from SoBig. There is another large drop from Klez to Yaha's $19.9 billion. The economic losses from cyber attacks have thus not only remained small but also have become far less frequent. No catastrophic cyber event has caused an economic loss of at least $800 million since 2017, and as Chart 1, below, reveals, the economic losses from catastrophic cyber events have been thin since 2007, the last year where the annual aggregate loss from such events exceeded $20 billion.

Chart 1: Annual Catastrophic Cyber Activity



The largest cyber events in history, as measured by economic impact, clearly have failed to move the markets. Even including the two largest events on record, the economic effects of cyber attacks have generally been minimal, and they have declined over time. The most impactful came from 1998 to 2004 (ending with SoBig and MyDoom). One could argue that the older events came at a time of lower cyber security, less understanding about the risks associated with networked systems, and other factors related to sector maturity, and those are fair and reasonable conclusions to draw. That would further suggest that increased maturity and its various implications has resulted in a reduced risk of the correlation of cyber risk with financial markets, and although (again) there is little in the way of directly relevant precedent, the downward slide in economic loss estimates certainly supports that theory. While it would go too far to say that if it did not happen then, it could not happen now, it certainly seems that achieving systemic impact certainly has not gotten easier.

Further, the magnitude of economic losses from cyber events begs for context: $38 billion is a large number, and its inflation-adjusted result ($66.6 billion) may seem staggering. However, systemic events have caused greater economic losses without moving financial markets, as demonstrated by the historical losses associated with natural disaster events. In fact, tropical storms and earthquakes offer a uniquely appropriate parallel – unlike pandemic or climate change – because they occur over short periods of time, are discrete events relatively constrained by geography, and are easily measured. In fact, they have been quantified for such a long period of time that such estimates are trusted and used regularly. The losses from natural disasters are far greater than those from systemic cyber events and still have failed to move the markets, which is why they are often used as a non-correlated diversifier by global capital markets professionals (Hoffman et al. 2018 9).

The two natural disaster events that appear closest to MyDoom and SoBig, as measured by economic losses, are the 2021 European flood event (mostly affecting Germany) and 2022's Hurricane Ian (Florida). The former caused an estimated $54 billion in economic losses and the latter $65 billion (Munich Re NatCatSERVICE 2022). Both pale in comparison to the $200 billion that Hurricane Katrina could cost today (I.I.I. 2020). There have been many more natural disaster events, as well, that have caused profound economic losses, and even in aggregate they have not moved financial markets. Consequently, it appears that cyber events would have to become far more impactful before the possibility of their

impacting financial markets could even be tested. The reversibility of cyber, which acts as a constraint on the economic damage that could result from an attack, inherently limits its potential for causing runaway economic losses (Johansmeyer 2022).

NotPetya, the most recent such attack, caused an estimated $10 billion in economic damage but failed to move the market (Wolff 2021). Of course, even the largest systemic cyber events have been relatively small, a claim to be discussed in more detail later in this article. Natural disasters, for example, have been far more impactful, causing $120 billion[2] in economic losses in 2022 alone (Munich Re NatCatSERVICE 2023), yet with no systemic financial market impact. If a cyber event were to be correlated with financial market impact, it would have to be of unprecedented size – to the point that its ability to occur would be highly questionable.

Analysis by Eling, Elvedi, and Falco suggests that the projected economic impacts of extreme cyber events can range from 0.2-2% of a state's GDP (2022 429). While that is an interesting threshold and potentially a meaningful one, it remains generally untested. Three of the four losses in Table 1 from 2001 to 2004, adjusted for inflation, would reach the lower end of the threshold, using 2019's U.S. GDP estimate of $35 billion – the 2001 Klez cyber event barely so. MyDoom and SoBig would have reached 0.4% but the question of whether they could have occurred with that magnitude a decade and a half later erodes the basis for comparison.

Cyber events have not achieved the scale necessary for precedent to be set regarding correlation with broader financial markets. Absent that direct experience, one can either claim that correlation is extremely unlikely, or one could say that a sufficiently large event has yet to occur, an invitation to take patience over proof. Given that it is impossible to disprove the latter, the impatient are required to devise other ways to gauge the systemic threat posed by cyber risk. For now, it may make sense to "follow the money." End investor perception of the extent to which cyber risk is correlated with global financial markets may provide an early indicator. The ILS manager community represents a source of perspectives uniquely suited to the question, given the sector's commitment to natural catastrophe risk transfer instruments because of their low rates of correlation to global financial markets (Malesky 2012).

A Problem of Perception

The ILS sector arose from the need for capital in the global reinsurance sector, beginning with support for retrocession (the process by which reinsurers transfer risk off their books) for property-catastrophe risks. The end investors allocating to such risks seek a low level of correlation relative to broader financial markets. End investors have generally acknowledged that there is the potential for certain truly extreme natural disasters to show signs of correlation – such as the 1906 San Francisco earthquake or even the impact of Hurricane Maria on Puerto Rico's municipal bonds (Odell and Weidenmier 2004 1003, Sasseen 2019) – but such events are both rare and deep in the past. As a potential source of capital, cyber re/insurers have long eyed the ILS community, although the evolution of that relationship has been deliberate – some would say slow. The determination that cyber risk is not correlated with global financial markets could improve the flow of ILS capital into the cyber re/insurance market. If cyber is not

[2] The 2022 estimate, and other recent year estimates, could increase (or decrease) in future years based on further data and insight that emerge over time. It can take several years for the industry-wide insured loss for a particular natural catastrophe to stabilize. As a result, 2022's $120 billion total for 2022 could change.

correlated with natural catastrophe risk, it would meet end investor need for a non-correlated alternative while offering some diversification from natural catastrophe risk.

To understand the views of the ILS manager community on the extent to which cyber risks and financial markets are correlated, interviews were conducted with ten leaders in the sector, representing $49 billion in assets under management (AuM), approximately 47% of the $104.9 billion in the ILS sector (Artemis Deal Directory 2023). Four ILS managers are based in Bermuda, with three in the United Kingdom, two in the United States, and one in Switzerland. Of them, eight engaged explicitly with the theme of whether cyber risk is correlated with broader financial markets (40% of worldwide ILS AuM). Among the eight who weighed in on this issue, four see cyber as correlated with financial markets ($19.5 billion in AuM, 18.8% of the total ILS market), with two calling correlation light ($10.2 billion in AuM, 9.8% of the ILS market), and two indicating that cyber is not correlated ($10,200, in AuM, 9.8% of the market). That said, even these categorizations are heavily nuanced.

In semi-structured interviews, context becomes crucial, given that terms are not always explicitly defined at the outset of the session. The use of the term "correlation" varied, making the context of such use part of the definition. Further, the interview subjects generally caveat that their views on the correlation of cyber risks with broader financial markets are heavily nuanced, in large part because of the lack of precedent described in the previous section. Absent direct experience, they note that the past may not support an accurate projection of what could be possible. ILS manager was refreshingly straightforward: "My opinion comes from probably watching too many movies." Consequently, it is most appropriate to view the participants as split evenly on the issue of correlation, with four seeing it ($19.5 billion of global ILS AuM) and four not ($20.4 billionof global ILS AuM). The reason for this is that the two who see cyber as lightly correlated believe that such correlation exists only in extremely remote scenarios which are generally not relevant even to the transfer of remote risks.

Differing Views of Where Correlation Matters

Of the four participants who see cyber as correlated with financial markets, concerns tend to reflect the uncertainty resulting from a lack of reference events, much like the Hollywood-influenced ILS manager above. In explaining their concerns about correlation with financial markets, they do concede that their concerns are speculative and driven largely by worries about the unknown rather than specific threats or conditions. The manager recognizes that "you can argue [cyber] is more correlated to their traditional investments," although conceding that direct support for this argument is thin. The discussion continued, "We all know a massive earthquake or a massive hurricane in the right place can move the markets too for a few days," continuing "I think the evidence suggests also the same would happen in a cyber event."

The movie afficionado takes the same view, seeing cyber attacks "as a correlating event, particularly in the tail … and that's another reason why we're not looking at" investing in such risks. Another ILS manager calls cyber "heavily correlated in the tail, so if things go bad, they go bad for most of the insurance companies in a proper tail event." When pressed, those concerned about correlation in the tail, the former ILS manager "can see how correlation may be overplayed at times," noting that NotPetya did not have a significant impact: "Did that have any correlation with capital markets? No. I don't think that's the event we worry about." This signals the notion that what past precedent exists may not be indicative of the potential threat, even absent any indicators of potential severity or magnitude. NotPetya is not the event that keeps the ILS market out of cyber. Rather, the concern is something unspecified – or vaguely labeled, like cloud outage or self-replicating malware, without further detail.

When adding those who see cyber as lightly correlated to global financial markets, the total perceiving any form of correlation, however modest, increases to six ILS managers -. One of those managers differentiates between smaller and larger cyber events. He believes that there is minimal correlation between “the everyday cyber risk we’ve seen” and financial markets, leaving room for the possibility that bigger, unprecedented events - could move markets, this part echoing the thoughts of the U.S. ILS manager above. However, he goes into more detail, using the impact of NotPetya on financial markets as a starting point for extrapolation: “There's got to be some level where if there's an attack that's so fearful or shutting down such critical areas of the economy or the healthcare system that people do get scared, and financial markets react.” For context, he compares that sort of systemic cyber event with “the big one” (an earthquake) affecting Los Angeles or San Francisco: “I would imagine the world watching that on 24-hour news is probably going to be pretty spooked” and that it would probably “have some correlation in terms of the financial markets.” The ILS manager also uses the Tohoku earthquake in Japan in 2011 as an example, which led to economic losses equivalent to 3.37% of Japan’s gross domestic product (GDP) at the time (CRED 2023, countryeconomy.com 2023).

This view from a participant who falls in the “lightly correlated category” is largely similar to that of the ILS manager above who considers cyber to be correlated with financial markets – specifically the manager that compares the effects of a major cyber attack to those of a “massive earthquake or massive hurricane.” The constraints built into the response suggest a lighter degree of correlation than the respondent’s firm declaration that cyber and financial markets are correlated, offering an instance where context becomes part of the implicit definition. Essentially, these respondents see cyber risks as only correlated with financial markets in certain extreme cases, and even then, they are non-committal as to the enduring effects of such an event.

Finally two ILS managers see cyber as not correlated with financial markets, although their views are largely aligned with the respondents who see cyber risk as lightly correlated with financial markets. Essentially, the risk that a cyber attack will cause a direct and meaningful impact on global financial markets is not a concern for them, and even if they could conceive of a scenario where that does happen, the scenario would have to be so severe that the ILS protection in play would be a trivial matter – e.g., such potential impacts as societal collapse or even total financial market collapse.

Further, an ILS manager in Bermuda explains that demand for non-correlated investments has led to “a sort of saturation of the property-cat market,” leaving investors to find more non-correlated alternatives elsewhere. If cyber is indeed not correlated with financial markets (as this ILS manager believes), and if it is diversifying with natural disasters (which certainly appears to be the case), then end investors should be eager to participate. An ILS manager in the United Kingdom said it bluntly: “If you've had suffered losses in in one market, if you can offer someone non-correlated market with a similar return profile, they should be they should be biting your hand off.” In fact, the alignment between these two respondents illustrates the similarities between those who see the market as not correlated and those who see it as lightly correlated.

The other ILS manager who sees cyber as not correlated with global financial markets suggests that end investors are the problem. He notes that cyber risk is “fairly uncorrelated to the wider financial markets” but adds, “It’s not an easy question to answer, and particularly to an investor base that has a conservative risk calculator.” For him, the challenge is one of education, where he has to help end capital providers understand the nature of the risk and how it could manifest relative to the other instruments

in their portfolios. He concedes that they can "imagine some kind of threat vector that takes down everywhere all at once in practice," but is careful to add that "that's never how it's worked so far."

Correlation Not Necessarily a Barrier to Capital Allocation

Views on financial market correlation with cyber risk do not necessarily mean that an ILS manager will shy away from the category, adding further nuance. Of the three ILS managers suggesting that cyber risk is correlated with financial markets, two of them have cyber ILS positions, and one had transacted in cyber ILS in a prior role (at a different company). Both of the two LS managers who see correlation as light have transacted in cyber ILS. The perceived correlation of cyber risk and financial markets is not necessarily an impediment, as long as the ILS managers see the risk as either sufficiently remote or otherwise manageable (through hedging, managing sums deployed, or through other means). For those who see cyber as correlated far enough in the tail, it becomes analogous to property-catastrophe risks, with the familiarity making it easier to hold such positions and explain them to end investors.

There are seemingly two reasons why an ILS manager would allocate to cyber risks even with the belief that there is some correlation between them and global financial markets. The first is the likelihood of a relevant event – or, more accurately, remoteness of one. Even for those taking a comparatively more imminent view of cyber as correlated with financial markets note that such an event has not happened (at least not yet, in that view), which at least suggests reinsurability. Like natural disasters, there may be some amount of correlation, but those risks are sufficiently remote that they do not impede the flow of capital. The similarity of correlation not only makes cyber more tolerable to hold, but it also enhances the sector as a diversifier for the core property-catastrophe risks held by the ILS market.

Frankly, trading activity is the best indicator of what an ILS manager truly believes. Always, follow the money. Of the eight respondents, four have transacted in cyber ILS, four have not. Of the latter, one respondent had participated in cyber ILS in a prior role. Table 2, below, shows a specific (anonymized) breakdown of ILS managers, their perception of cyber correlation with global financial markets, and their experience with cyber ILS. The two managers who see cyber as lightly correlated have invested in cyber ILS, with the two who do not see cyber as correlated are split. One has been involved in cyber ILS for several years, and the other still has not entered the market, although he came close with a small proof-of-concept trade, he explained in his interview. Of the four who perceive cyber as correlated with financial markets, two have engaged in ILS trades, and two have not. One of those who has not, though, participated in cyber ILS activity in a prior position.

Table 2: ILS Fund Manager Perspectives on Financial Market Correlation Relative to Trading Activity

ILS Fund Manager (Anonymized)	Sees Cyber as Correlated with Financial Markets	Has Traded Cyber ILS	Notes
A	Yes	Yes	Recent market entrant with a small commitment, plans to do more
B	Light	Yes	Small cyber ILS allocation so far but plans to do more in the future
C	No	Yes	Active cyber ILS investor
D	No	No	End investor concerns are a barrier to market entry, but the manager did review a transaction that the

			counterparty withdrew … however it was “toy money”
E	Yes	No	Unlikely to allocate to cyber risks anytime soon
F	Light	Yes	Active cyber ILS investor
G	Yes	Yes	Active cyber ILS investor
H	Yes	No	Previous experience with cyber ILS

Source: Author’s interviews

The responses in Table 2 do not include each ILS manager’s AuM, as it would compromise their anonymity. However, the five with ILS experience comprise nearly $30 billion in aggregate AuM, making them nearly a third of the entire ILS market worldwide. Support for cyber ILS is not heavily constrained by concerns about the potential correlations between financial markets and major cyber attacks. This speaks not just to the reinsurability of the risk but also the nuance and subtlety involved in the correlation discussion. Two respondents could be taken as calling cyber correlated with financial markets, one of which nonetheless has experience with cyber ILS. After all, instruments could be structured for the more remote risks and still have appropriate characteristics for a portfolio, even if they are not non-correlated with financial markets. Five respondents could be seen as falling into the “lightly correlated” category, with one seeing cyber risk as not correlated with financial markets, although there were indications that he might ascribe to the “too remote to be realistic” perspective on truly extreme cyber events.

The above shows that the growth of the cyber ILS market is possible, however it is certainly not assured. The main problem is likely the mixed messages coming out of the ILS community. Although it may seem like a cohesive unit in an oversimplified world of insurance/reinsurance/ILS, but it is important to remember that ILS managers have different objectives, mandates, and strategies. The perception that cyber is at least somewhat correlated with financial markets may not be a barrier to the development of a cyber ILS market, but it may stand in the way of scaling it, at least in the near term. The discussion below examines the factors that not only characterize the role of the perception of financial market correlation today but also how that could impact the growth of the cyber re/insurance market in the future.

Discussion

Generally, the perception of cyber as a systemic threat to global financial markets is neither firmly held nor a significant barrier to the ILS fund managers who have either transacted in cyber ILS instruments or are contemplating doing so. The findings above indicate a certain fuzziness. The three major categories of perspective on correlation into which the eight respondents fall – correlated, lightly correlated, and not correlated – can bleed into one another when the context of their comments are established. Some who see correlation as established caveat that such correlation is only in remote instances, which is similar to the responses of those in the “lightly correlated” category. The same could be said of those in the “not correlated” category, who call the risk not correlated because correlation would exist in only the most extreme cases, which tend to seem unrealistic.

Ultimately, only one respondent sees cyber as correlated with financial markets to the point where he would not invest in it, and he concedes that his reasons are driven by popular culture. Another sees the risks as correlated but would invest anyway, particularly if the instruments are such that the risk could be

very clearly defined and ringfenced. Correlation is not a problem for him, as long as he can use other methods to manage the risk to which his end investors are exposed. At the other extreme, there is one ILS manager who does not see the risk as correlated, but he is constrained by the expectations of his end investors. Meanwhile, five more ILS managers – representing more than 25% of the worldwide ILS market by AuM – are somewhere in the middle, operating under the assumption that cyber is not heavily correlated with global financial markets, except in the most remote of scenarios.

It can be difficult to pick a path forward through the soft, mixed, caveated, and nuanced messages from the ILS market participants in this research project. The effort is not as simple as scanning for keywords and highlighting the market share reflected by the responses coded. With the small size of the global ILS community and the large portion represented in this research, it is possible to review responses and present them with the proper context. First, the ILS market has appetite for cyber. This is reflected – at a minimum – in the fact that five of the eight respondents have engaged in cyber ILS activities in their current roles, with one more having done so in a past role and one more having come close to completing his first such transaction. There is a salient platform for growth, and the trajectory is relatively clear. While uneven market expansion can be expected in a market as new and small as cyber ILS, the overall trend is upward, and continued trading should lead to more ILS managers engaging in cyber transactions – perhaps even the movie fan.

That growth, expansion, and maturity will not come on its own, though. There is not so much momentum that the emergence of a robust cyber ILS market – in support of an expanded cyber re/insurance ecosystem – is a foregone conclusion. The market needs to be cultivated and supported. In part, that begins with addressing the extent to which cyber risks are correlated with financial market activity and the extent to which this relationship can be measured, managed, and communicated to both ILS managers and their end investors. Further study should reveal the extent to which cyber correlation is - and should be – a barrier to the flow of capital into the cyber re/insurance market, and in fact, the responses from ILS market participant interviews lean toward the broader adoption of the belief that cyber risk is at most lightly correlated with financial markets, perhaps no more so than property-catastrophe risks are. The emerging support for the position that cyber risks are as diversifying from financial markets as natural catastrophes could support not just an influx in capital but also the optimization of existing portfolios by reflecting the lack of correlation between cyber risk and financial markets – with diversification affecting the amount of capital that re/insurers would have to hold against such risks.

As mentioned at the beginning of this article, it is a fool's errand to attempt to prove the negative, but for now, what is clear is that cyber attacks have largely failed to move financial markets. Even the largest cyber attacks in history, as measured by economic loss, have not even nudged financial markets. One could try to argue that past events may not have been as large as future attacks could become, but that runs into two challenges. First, there is a clear downward trend in the severity of economic loss from major cyber events, with those of 2017 together smaller than those of 2007 and only slightly higher than 2008, with those of 2007 and 2017 together smaller than either the SoBig event of 2003 or the MyDoom event of 2004 (adjusted for inflation). Cyber events appear to have become less impactful, although the historical data is thin. Further, the belief that a future event could be larger than those of the past – significantly larger, in fact – leaves one to wonder how big a cyber attack would have to be to have a systemic effect, not to mention whether a cyber event could even achieve such a hypothetical loss quantum. Given the many natural disaster events with economic losses far above those of SoBig and

MyDoom over the past twenty five years – including the 2011 Tohoku earthquake and Hurricanes Katrina and Ian – a cyber attack sufficiently large to move financial markets would have to reach a scale heretofore unimagined (CRED 2023).

Of course, for now, the question is one of perception – specifically, whether the perception of cyber risk as an outsized threat may be impeding the flow of capital needed to support re/insurance market growth. Although the degree of correlation is notoriously difficult to demonstrate – a problem exacerbated by the need to do the impossible and prove the negative – there seems to be a growing acceptance that cyber is not correlated with broader financial markets. Perhaps the greatest problem is putting more historical data in front of the ILS community. The assumption that there is little data available is simply not true, given the contents of Table 1 earlier in this article, a collection of historical cyber catastrophe events of economic significance that has been overlooked in both the historical cyber re/insurance literature and underwriter discussions from Lime Street in London to Front Street in Bermuda (and beyond in both directions). Although sixteen events are not much to go on, they certainly provide a reference point for potential economic severity, which can easily be benchmarked to the natural disaster events that have been the mainstay of the ILS market for nearly three decades. The lack of systemic impact from cyber events is perhaps the most effective indicator of its lack of correlation to broader financial markets.

The lack of precedent, in conjunction with the other points of comparison above, does suggest that cyber risks are unlikely to be correlated with financial markets, but the challenge in overcoming the barrier to the flow of capital that this poses likely lies in building a sufficient case to those ILS managers who either believe in correlation implicitly or lean in that direction due to influence from popular media, like the ILS manager who responded on correlation that he has probably watched too many movies. Education is likely the primary solution, along with an effort to make such education easier for the target market to find, consume, and understand. As some respondents observed, learning about cyber risk and the attendant re/insurance market has not been a priority, particularly given the demands of their core property-catastrophe obligations during a period of heightened loss activity. Fortunately, this process already appears to be in progress.

It may seem like the scaling of cyber ILS is only a matter of time. Those who believe it is not correlated with global financial markets are able to speak to the core needs of end ILS investors, who entered the natural catastrophe risk space for exactly that reason. Those who do not see cyber as non-correlated still have found a way to include it in their risk appetite, although part of the reason for that is considerable nuance on how they see the extent of correlation. As a result, a growth trajectory does seem most likely for the ILS market with regard to cyber re/insurance. That said, the market will require some cultivation in the near term. New markets can be excepted to show some volatility, particularly where precedent and historical data are in short supply. Difficult loss years may slow progress, but that should be an expectation from the start. Overall, managing the blind belief that cyber risk is correlated with financial markets could significantly improve the flow of capital into cyber re/insurance and support not just market growth but also an expansion of economic security bolstered by a growing insurance market.

Conclusion

Absent proof of the degree to which cyber risks and financial markets are correlated – or even strong support for it – all one is left with is perception. Frankly, the allocation of capital relative to prevailing risks is really driven by perception of risk anyway, as it is human beings making the decisions to accept

evidence or support for against a particular decision. This clearly manifests in the ILS market, where the decision to allocate capital to support cyber re/insurance risks faces concerns about correlation with regard to the needs and expectations of end investors. With end ILS investors hungry for non-correlated (or at least lightly correlated) investment opportunities, the prospect of low rates of correlation between cyber risks and financial markets could present a profound new opportunity for institutional investors and in important source of fresh risk capacity for the global cyber re/insurance industry.

The prospect of low-correlation returns is what drove end investors to the ILS market, with property-catastrophe reinsurance offering an opportunity to diversify away from global financial markets. If, in fact, cyber risks are not correlated with global financial markets then cyber re/insurance would offer another opportunity for such diversification, which could be particularly valuable during a period of high natural disaster activity, as has been present since 2017. However, if investors and their managers believe that cyber risks are correlated with financial markets, then there is not much in the way of diversification benefit. Yet, the holy wars over correlation do not appear to be as stark and rigid as the gravity of the issue might seem.

The interviews show, ultimately, that some amount of correlation is tolerable, as evidenced by the fact that most ILS managers who have engaged in cyber trades see some degree of correlation. Those that see the risks as correlated believe that that is only the case in relatively extreme scenarios – even by the standards of an industry that traffics in remote risks already. What ostensibly looks like a contradiction actually requires nuance and judgment. The prospect of a bad actor hypothetically "taking down the grid" is recognized by most ILS managers as quite remote, so what remains is identifying the levels at which cyber risk transfer agreements are consumable. It is a process that will take time, analysis, and even a bit of trial and error, but it will yield results.

The most effective way that existing cyber ILS players could influence the market toward growth is to lead by example. Those ILS managers who have engaged in cyber ILS activity – ten so far, as discussed above, with $27 billion in respondent AuM having done so (five) and almost $5 billion (three) more having engaged in cyber ILS activity in their prior roles – can help grow the market not just by increasing their own participation but also by showing a track record. While it may be customary to protect performance as a company secret, at least some revelation could help attract peers to the cyber market, which is more likely to bring new opportunities rather than drive competition for a static supply of deal flow. They would retain a competitive advantage through more developed and tested systems, processes, and risk familiarity, and they would be able to use increases in industry size to scale those investments faster and to greater effect. It is hardly a new story in re/insurance or in any new market.

If the ILS managers who hold that cyber risk is not meaningfully correlated with financial markets are correct, then they will have early and significant access to an important source of diversifying risk that meets the needs of their end investors, both existing and prospective. If they are wrong, then there is no telling how long they may need to wait for the "big one," although it is clear that for such an event to occur, a lot has to go wrong at the wrong time, a set of conditions that so far has proved to be profoundly difficult to meet. The worst case, of course, is that waiting to be proved right means sacrificing learning and experience for an indeterminate amount of time which would be incredibly useful when the "big one" comes (if, of course, one accepts that it both will and has not already). Frankly, this means that there is really no time like the present.

The cyber ILS market will find its footing, although the process will be both lumpy and time consuming. However, the existing market support is difficult to ignore. With more than five years of experience in a risk area that could uniquely meet the needs of end investors, cyber ILS has garnered the attention and focus that will ultimately help drive in capital with scale. For today, what remains most important is that the existing players keep pushing.

References

108 Congress. (2023, November 6). *Computer Viruses: The Disease, the Detection, and the Prescription for Protection*. House Hearing. Retrieved January 18, 2024, from https://www.govinfo.gov/content/pkg/CHRG-108hhrg90727/html/CHRG-108hhrg90727.htm.

Adelmann, F., Elliott, J., Ergen, I., Gaidosch, T., Jenkinson, N., Khiaonarong, K., Morozova, A., Schwarz, N., & Wilson, C. (2020, December). *Cyber Risk and Financial Stability: It's a Small World After All*. SDN/20/07.

Arquilla, J. & Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy.* 12, 141-165.

Bailey, L. (2013). Mitigating Moral Hazard in Cyber-Risk Insurance. *Journal of Law & Cyber Warfare.* 3(1), 1-42.

Beattie, A. (2012, December 6). *The Most Devastating Computer Viruses*. Techopedia Retrievd August 27, 2022, from https://www.techopedia.com/2/26178/security/the-most-devastating-computer-viruses.

Brando, D., Kotidis, A., Kovner, A., Lee, M., & Schreft, S. (2022, May 12). *Implications of Cyber Risk for Financial Stability*. Board of Governors of the Federal Reserve System. Retrieved June 15, 2023, from https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html.

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

Cellerini, E., Finucane, J., Lanci, L., & Holzheu, T. (2022, October). *Cyber insurance: strengthening resilience for the digital transformation.* Zurich: Swiss Re Institute.

Centre for Research on the Epidemiology of Disasters (CRED). (2022). EM-DAT Public Data. *EM-DAT: The International Disaster Database*. Retrieved February 1, 2022, from https://public.emdat.be/data.

Countryeconomy.com. (2023). *Countryeconomy.com.* Retrieved September 3, 2023, from https://countryeconomy.com/.

Cuneo, J. (2016). *AIR Worldwide: "Business interruption could be the hurricane Andrew of cyber."* Global Reinsurance. Retrieved June 21, 2023, from https://www.globalreinsurance.com/air-worldwide-business-interruption-could-be-the-hurricane-andrew-of-cyber/1418710.article..

Cyware Hacker News. (2016, August 30). *Most Expensive Computer Viruses of All Time*. Cyware Social. Retrieved August 27, 2022, from https://cyware.com/news/most-expensive-computer-viruses-of-all-time-de0d5fae.

Eisenbach, T., Kovner, A., & Lee, M. (2022). *When It Rains, It Pours: Cyber Risk and Financial Conditions.* 1022. New York: Federal Reserve Bank of New York.

Eling, M., Elvedi, M., & Falco, G. (2022). The Economic Impact of Extreme Cyber Risk Scenarios. *North American Actuarial Journal.* 27(3), 429-443.

Federal Bureau of Investigation (FBI). *History: Morris Worm*. FBI. Retrieved January 19, 2024, fromhttps://www.fbi.gov/history/famous-cases/morris-worm.

Federal Trade Commission (FTC). (2022, December). *Equifax Data Breach Settlement*. FTC. Retrieved January 19, 2024, from https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement.

Fell, J., de Vette, N., Gardo, S., Klaus, B., & Wendelborn, J.. (2022, November). *Towards a framework for assessing systemic cyber risk.* European Central Bank. Retrieved June 15, 2023, from https://www.ecb.europa.eu/pub/financial-stability/fsr/special/html/ecb.fsrart202211_03~9a8452e67a.en.html.

Firmex. *The 10 Most Expensive Data Breaches in Corporate History*. Touchpoint by Firmex. Retrieved January 18, 2024, from https://www.firmex.com/resources/blog/the-10-most-expensive-data-breaches-in-corporate-history/.

Forscey, D., Bateman, J. Beecroft, N., & Woods, B. (2022, March 7). *Systemic Cyber Risk: A Primer*. Carnegie Endowment for International Peace. Retrieved June 21, 2023, from https://carnegieendowment.org/2022/03/07/systemic-cyber-risk-primer-pub-86531.

Galt, M. (2022, July 19). Ukraine's Decentralized Cyber Army. *CYBER*.

Gerencer, T. (2020, November 4). *The Top 10 Worst Computer Viruses in History*. HP Tech Takes. Retrieved August 27, 2022, from https://www.hp.com/us-en/shop/tech-takes/top-ten-worst-computer-viruses-in-history.

Greenberg, A. (2018, August 22). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. Wired. Retrieved August 27, 2022, from https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Greenwald, J. (2014, August 6). *Target maxes out insurance coverage for 2013 data breach*. Business Insurance. Retrieved January 19, 2024, from https://www.businessinsurance.com/article/20140806/NEWS07/140809889.

Cordonnier, A., Davis, E., Awan, A., Beringer, M., & Fung, J. (2023). *Double-Whammy? Examining the Correlation Between Major Cyber Events and Broad Market Performance.* New York: Guy Carpenter.

Dou, W., Tang, W., Wu, X., Qi, L., Xu, X., Zhang, X., & Hu, C. (2020). An insurance theory based optimal cyber-insurance contract against moral hazard. *Information Sciences.* 527. Retrieved August 28, 2022, from https://www.sciencedirect.com/science/article/abs/pii/S0020025518310016.

Haury, A. (2012, May 31). *10 Of The Most Costly Computer Viruses Of All Time*. Yahoo! Finance. Retrieved January 18, 2024, from https://finance.yahoo.com/news/10-most-costly-computer-viruses-192415030.html.

Haskell-Dowland, P. (2017, June 30). *Three ways the 'NotPetya' cyberattack is more complex than WannaCry*. TheConversation. Retrieved January 19, 2024, from https://theconversation.com/three-ways-the-notpetya-cyberattack-is-more-complex-than-wannacry-80266.

Hemenway, C. (2023, December 15). *Home Depot Appeals to Get Defense Costs from CGL Policies for 2014 Breach*. Insurance Journal. Retrieved January 19, 2024, from https://www.insurancejournal.com/news/national/2023/12/15/752161.htm.

Hoffman, D., Wilson, S., & Carter, R. (2018). *Advancing Accumulation Risk in Cyber Insurance: Prerequisites for the development of a sustainable cyber risk insurance market.* Zurich: Geneva Association.

Howden. (2023). *Cyber Insurance Coming of Age.* Retrieved September 3, 2023, from https://www.howdengroup.com/sites/g/files/mwfley566/files/2023-07/howden-cyber-report-coming-of-age-03072023-final_0.pdf.

Insurance Information Institute (I.I.I.). (2020, August 18). *Swiss Re: A Katrina-like hurricane could cause up to $200 billion in damage today*. Resilience Blog: Insurance Information Institute. Retrieved June 21, 2023, from. https://resilience.iii.org/resilience-blog/hurricanes/swiss-re-a-katrina-like-hurricane-could-cause-up-to-200-billion-in-damage-today/.

Johansmeyer, T & Mican, A. (2022). Cyber ILS: How Acute Demand Could Drive a Scalable Retrocession Market. *The Journal of Risk Management and Insurance.* 26(1), 40-59.

Johansmeyer, T. (2023, June 27). *How Big Is the Cyber Insurance Market? Can It Keep Growing?* Lawfare. Retrieved September 5, 2023, from https://www.lawfaremedia.org/article/how-big-is-the-cyber-insurance-market-can-it-keep-growing.

Johansmeyer, T. (2023b). How Reversibility Differentiates Cyber from Kinetic Warfare: A Case Study in the Energy Sector. *International Journal of Security, Privacy and Trust Management.* 12(1), 1-14.

Johansmeyer, T. (2023c, July 26). *If Cyber Is Uninsurable, the United States Has a Major Strategy Problem*. Lawfare. Retrieved January 19, 2024, from https://www.lawfaremedia.org/article/if-cyber-is-uninsurable-the-united-states-has-a-major-strategy-problem.

Johansmeyer, T. (2022, June 22). *Insurance Instead of Deterrence: A Pivot in Cybersecurity Strategy*. The SAIS Review of International Affairs. Retrieved June 21, 2023, from https://saisreview.sais.jhu.edu/insurance-instead-of-deterrence-a-pivot-in-cybersecurity-strategy/.

Kaffenberger, L. & Kopp, E. (2019, September 30). *Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment*. Carnegie Endowment for International Peace. Retrieved June 15, 2023, from https://carnegieendowment.org/2019/09/30/cyber-risk-scenarios-financial-system-and-systemic-risk-assessment-pub-79911.

Kopp, E., Kaffenberger, L., & Wilson, C. (2017). *IMF Working Paper: Cyber Risk, Market Failures, and Financial Stability.*

Leman, J. (2019, October 31). *11 Malware Attacks That Nearly Wrecked the Internet*. Popular Mechanics. Retrieved August 27, 2022, from https://www.popularmechanics.com/technology/security/g29625471/history-of-malware-attacks/.

Lemay, A. (2021, April 28). *Moral Hazard of Cyber Insurance*. CYDEF. Retrieved August 28, 2022, from https://cydef.ca/blog/cyber-insurance-cyber-risk-management/.

Levite, A., Kannry, S., Hoffman, W. (2018). The Cyber Risk Environment. *Addressing the Private Sector Cybersecurity Predicament: The Indispensable Role of Insurance.* Carnegie Endowment for International Peace.

Lewis, J. (2020, August 17). Dismissing Cyber Catastrophe. Center for Strategic and International Studies. Retrieved January 19, 2024, from https://www.csis.org/analysis/dismissing-cyber-catastrophe.

MacColl, J., Nurse, J., Sullivan, J. (2021). *Cyber Insurance and the Cyber Security Challenge.* June. London: Royal United Services Institute.

Majuca, R., Yurcik, W. & Kesan, J. *The Evolution of Cyber Insurance*.

Malesky, K. (2012, June 16). *Follow the Money: On the Trail of Watergate Lore*. NPR. Retrieved June 21, 2023, from https://www.npr.org/2012/06/16/154997482/follow-the-money-on-the-trail-of-watergate-lore.

Mi2g. (2003, November 21). *Minmail to become 4th worst malware over weekend*. Mi2gRetrieved January 18, 2024, from http://www.mi2g.com/cgi/mi2g/frameset.php?pageid=http%3A//www.mi2g.com/cgi/mi2g/press/211103.php.

Moes, T. (2023). *Cybercrime Examples (2023): The 10 Worst Attacks of All Time*. Software Lab. Retrieved January 18, 2024, from https://softwarelab.org/blog/cybercrime-examples/.

Munich Re NatCatSERVICE. (2022, January 10). *Hurricanes, cold waves, tornadoes: Weather disasters in USA dominate natural disaster losses in 2021*. Munich Re. Retrieved June 21, 2023, from https://www.munichre.com/en/company/media-relations/media-information-and-corporate-news/media-information/2022/natural-disaster-losses-2021.html [Accessed 21 June 2023].

Murphy Kelly, S. (2021, May 16). *The bizarre story of the inventor of ransomware*. CNN. Retrieved January 18, 2024, from https://edition.cnn.com/2021/05/16/tech/ransomware-joseph-popp/index.html.

Newman, I., Pocock, E., & Hall, J. (2023). *CY-FI: The Future of Cyber (Re)insurance.* Retrieved September 3, 2023, from https://www.ajg.com/gallagherre/-/media/files/gallagher/gallagherre/future-of-cyber-reinsurance.pdf.

Odell, K. & Weidenmier, M. (2004). Real Shock, Monetary Aftershock: The 1906 San Francisco Earthquake and the Panic of 1907. *The Journal of Economic History.* 64(4),1002-1027.

Pain, D. & Noordhoek, D. (2022). *Ransomware: An insurance market perspective.* July. Zurich: Geneva Association.

Porup, J. (2018, June 18). *Does cyber insurance make us more (or less) secure?* CSO. Retrieved August 28, 2022, from https://www.csoonline.com/article/3280990/does-cyber-insurance-make-us-more-or-less-secure.html#:~:text=The%20moral%20hazard%20of%20cyber,since%20the%20days%20of%20sail.

Raissipour, D. (2023, June 7). *Assessing The Correlation Between Cyber Risk And Business Risk*. Forbes. Retrieved June 15, 2023, from https://www.forbes.com/sites/forbestechcouncil/2023/06/07/assessing-the-correlation-between-cyber-risk-and-business-risk/?sh=123046354e7d.

Reeder, J & Hall, T. (2021). Cybersecurity's Pearl Harbor Moment. *The Cyber Defense Review.* 6(3), 15-40.

Sasseen, J. (2019, March 8). *How Puerto Rico's financial storm is washing over the mainland*. Quartz. Retrieved July 23, 2023, from https://qz.com/1557486/puerto-ricos-bond-saga-is-messing-up-mainland-municipal-markets.

Schanz, K. (2018, May 8-9). Understanding and addressing global insurance protection gaps. *6th Polish Insurance Association Congress.* 8-Sopot, Poland.

Slayton, R. (2017, February). *Why Cyber Operations Do Not Always Favor the Offense*. Belfer Center. Retrieved July 23, 2023, from https://www.belfercenter.org/publication/why-cyber-operations-do-not-always-favor-offense.

Smith, K. (2019, June). *Going Dark*. Best's Review. Retrieved January 18, 2024, from https://news.ambest.com/ArticleContent.aspx?pc=1009&refnum=285596.

Wolff, J (2022, August 30). A Brief History of Cyberinsurance. *Slate.* Retrieved January 19, 2024, from https://slate.com/technology/2022/08/cyberinsurance-history-regulation.html.

Wolff, J. (2021, December 1). *How the NotPetya attack is reshaping cyber insurance.* TechStream: Brookings, Retrieved June 21, 2023, from https://www.brookings.edu/techstream/how-the-notpetya-attack-is-reshaping-cyber-insurance/.