How Cyber Model Vendors See Their Role in Closing the Cyber Insurance Protection Gap

Tom Johansmeyer

University of Kent, Canterbury

Institute of Cyber Security for Society (iCSS)

trj5@kent.ac.uk

Abstract

The developers of models for quantifying systemic cyber risk for the re/insurance industry have had little opportunity for their voice to be heard. Instead, the historical literature largely dismisses the sector as immature, inaccurate, and not up to the task of facilitating cyber re/insurance risk transfer. This characterization of the cyber modeling community may be true, but little evidence has been offered in support of such views. Further, no credible scholarly analysis of the effectiveness of cyber vendor models has been conducted. This article offers a first step in what hopefully can become a much richer and robust line of inquiry across the cyber re/insurance academic community. Consisting of qualitative research with cyber modeling vendor employees, this article offers a baseline view of how the modeling sector sees itself and its work with regard to the broader cyber re/insurance community. No such study of the model vendors themselves has been conducted. This article provides an opportunity for the modelers to say their piece in a sector that has largely overlooked their contributions.

Key Words: Cyber Insurance, Cyber Reinsurance, Catastrophe Modeling, Insurance Linked Securities, Protection Gap

1 Introduction

The flow of capital to support cyber insurance risks has been impeded by several factors, including a lack of referenceable loss history and precedent, geopolitical instability, and the prospect of better returns in more mature sectors, such as property re/insurance. However, one of the most frequently noted is that the vendor models for quantifying systemic cyber risk (also known as "cyber catastrophe" risk) are unreliable and still in their infancy. Often compared to their counterparts in the property-catastrophe business, where vendor models are considered the *lingua franca* of risk transfer, cyber vendor models tend to be seen as unready for use in quantifying risk for meaningful risk transfer activity. Without access to reliable models, capital does not flow as easily.

Concerns about the reliability of vendor models for cyber catastrophe risk has become an oft-cited reason for skepticism about the potential of the cyber re/insurance market to grow – not to mention its ability to attract new forms and sources of capital, such as those available from the insurance linked securities (ILS) market. The growing body of academic literature on cyber re/insurance risk transfer (to include access to the ILS market) tends to take a unified view on the notion that cyber model vendors are some how deficient, even if that deficiency is because the models and the sector itself are still in their infancy. According to Graham Steele, assistant secretary for financial institutions at the U.S. Department of the Treasury, the reliability of cyber models "has a long way to go" (2023).

The evolution of the cyber re/insurance market's perspective on cyber models has largely proceeded with limited input from the modelers themselves, particularly in the historical scholarship on the subject. Some articles and reports have included feedback from modelers as part of much larger efforts, with the Geneva Association a leader in this regard. However, even then, the views on modelers are often diluted by the broader respondent base and wider research objectives. Further, few such articles are peer reviewed, resulting in a dearth of literature that has been subjected to rigorous academic review standards. The resulting gap in the body of knowledge related to re/insurance risk transfer thus cries to be addressed.

This article seeks to remedy a historical shortcoming in the historical cyber re/insurance research by engaging cyber catastrophe modeling leaders in an effort to ascertain how cyber catastrophe modelers see their role in the flow of capital to the cyber re/insurance market and offer that community the opportunity to have a voice. In doing so, it represents a strong, important, and unique contribution to the literature in re/insurance scholarship and could serve as a foundation for future inquiry and research. Literature reviews in existing articles

show a clear gap with regard to modeling for systemic cyber risk, and research such as that presented below could possibly have reshaped previous lines of inquiry and even the conclusions drawn.

Nuance matters, and the historical literature has failed to capture how it manifests with regard to the vendor models focused on systemic cyber risk and how they impact the flow of capital. Improving the re/insurance community's understanding of cyber vendor models and how they are perceived could reshape the decision-making process with regard to capital allocation to cyber risks, ultimately contributing to both improved risk and capital management and the sustainable growth of the sector.

2 Literature Review

2.1 Identifying the Relevant Literature

The historical literature on cyber insurance in general is thin, due in large part to the fact that the class of business is new and emerging, as is the underlying risk it references. This becomes further limited when reviewing specific underlying issues across the cyber insurance environment, including risk transfer. For this reason, it was difficult to find diverse opinions in the literature. What little work has been done on the role of cyber vendor models in risk transfer has been done often without engaging that stakeholder group, is largely reflective of a consensus view as to the insufficiency of vendor models by re/insurers, and has come from a limited group of scholars and analysists. Given the paucity of relevant scholarship, the process of reviewing the historical literature necessarily begins with a review of the cyber insurance protection gap, how it could be reshaped by an influx of capital, and general context on engaging the ILS market. This leads naturally to the role of vendor models and the perceived challenges risk transfer parties have in using them, which speaks to this articles central research question.

The process of sourcing and reviewing literature differs from disciplines where the historical scholarship is more robust. Rather than using key words and scanning large numbers of article extracts, the narrow field – with even surrounding context narrow – makes it possible to quickly identify the universe of relevant literature and read the articles in full. It is otherwise difficult to find the small components within articles and papers that address cyber vendor modeling and its attendant context. Finally, the literature was informed by a broader review of the cyber

insurance, cyber security, and economic security literature with which this author has engaged in developing a body of work on cyber re/insurance and ILS risk transfer.

2.2 Industry and Risk Environment Review

An insurance protection gap is best described as economic exposure not covered by insurance, net of what could be supported through other economic means (Swiss Re 2019 11), and for cyber risks, it remains quite wide. According to a study by Blackberry and insurance company Corvus, only 55% of the companies they surveyed have cyber insurance (Ayers 2022). The same study finds that only 19% of companies have coverage of at least $600,000, despite a mean data breach cost of $2.4 million. Moreover, the belief that recent re/insurance market growth has contributed to a narrowing of the cyber insurance protection gap is flawed. The cyber insurance industry has shown grown rapidly since 2017 (see Johansmeyer and Mican 2022, p. 43 and Johansmeyer 2023), but increases in worldwide aggregate cyber insurance premium collected have masked an underlying staleness in the amount of protection offered. Cyber insurance revenues may be up, but the amount of protection offered in exchange has not kept pace, which means that the cyber insurance protection gap has likely expanded, if one ascribes to the belief that the digital environment continues to expand rapidly.

Fears about the potential impact of systemic cyber events further limit the industry's ability to grow, with pessimism having demonstrably kept capital away from cyber re/insurance risks. The possible damage from cloud service provider interruption events ranges from "large" at an economic loss of $46 billion to "extreme" at $53.05 billion, according to the Lloyd's analysis, with "[c]yber mass vulnerability interruption" ranging from $9.68 billion to $28.72 billion in economic loss (Schanz 2018 7). This comes within the context of annual aggregate cyber economic losses of $500 billion, according to the analysis. A major event, therefore, could represent 10% of annual global cyber economic losses, which may be possible. Within that, Lloyd's observes, insurance coverage for such events would range from 7-13%. Further, the exposure/risk environment is growing quickly. The $500 billion estimate above represents a profound increase from the 2017 Lloyd's estimated economic impact from cyber attacks: $120 billion (Disparte 2017 61).

The modeled scenarios above, to which one could add the potential for a $3.5 trillion economic impact from systemic cyber attacks on the financial services industry (Lloyd's of London 2023), stand in stark contrast to experiential data, which puts the number of systemic cyber events at only sixteen since 1999 with an aggregate economic loss (adjusted for inflation at 3% per year) at approximately $260 billion (Johansmeyer 2023c 6). Scholars note that there has never been

such a catastrophic cyber event, although some caveat it with “yet,” despite the extensive unsubstantiated assumptions with which that short word is burdened (e.g., Carter, Pain, and Enoizi 2022 9). Fears of a major catastrophic loss, which indeed persist and have perhaps even gained strength (Steele 2023), have had a clear impact on the flow of capital into the re/insurance market, to include new sources of capital, such as ILS.

2.2 Progress in Engaging the ILS Market

Long a source of additional capacity for the property-catastrophe reinsurance market, many in the cyber re/insurance community have identified the ILS market as a potential source of capital to help grow the cyber re/insurance market and close the cyber insurance protection gap (Johansmeyer and Mican 2022 43). Yet, ILS participation in cyber re/insurance has been small and growth slow, despite the fact that at least ten ILS managers have engaged in at least some form of cyber risk transfer (Johansmeyer 2023). One of the reasons for the reluctance of ILS managers to participate more robustly in the cyber re/insurance market has been a lack of confidence in cyber catastrophe models, which they believe to be less mature and less reliable than those in use in the property-catastrophe reinsurance market (Johansmeyer and Mican 2022 51).

In the re/insurance and ILS market, catastrophe modelers provide what is effectively the *lingua franca* of risk transfer, specifically estimates of the likelihood and potential impact (as measured by industry-wide insured loss) of major natural disaster events. While Johansmeyer and Mican explored how the ILS market saw cyber vendor models relative to the task of risk quantification in 2022, the market has clearly evolved. The cyber ILS market exceeded $1 billion in limit at one point in 2023 (Johansmeyer in Pain 2023 40-1), including several iterations of the Cairney private cyber catastrophe bond sponsored by Beazley (Artemis 2023), the Hannover Re/Stone Ridge collateralized quota share reinsurance transaction (Gallin 2023), and several significant private market deals. By the fourth quarter, three catastrophe bonds featuring at least nominal liquidity were brought to market: Long Walk Re, PoleStar Re, and East Lane VII Re (Artemis 2023).

2.3 How Vendor Models Have Been Understood

The future of ILS market engagement with cyber risks is likely to be limited until the modeling problem is solved, though. Scalability of the cyber catastrophe bond market will require robust, credible, and widely accepted risk quantification, and so far, the market has remained

uncomfortable with the vendor models. Criticism of the cyber catastrophe modeling community became commonplace in the early days of the cyber insurance market and has largely persisted (e.g., Eling and Schnell 2016 478, IAIS 2020 18, Johansmeyer and Mican 2022 51). Even in the most recent body of research published on cyber re/insurance, cyber catastrophe modeling is described as "immature," with results that "can be volatile and inconsistent" (Pain 2023 7). They are said to suffer from a lack of access to sufficient data, which only makes the effort more fraught (Dal Moro 2020 2). Further, the sorts of systemic event they seek to model are believed to lack precedent (Heather in Pain 2023 33). However, there has been little effort to get the perspectives of the cyber modelers themselves, resulting in a significant gap in the historical literature that this research project endeavors to remedy.

Some have engaged with the cyber catastrophe modeling community (e.g., Pain 2023 4), as mentioned above with regard to the Geneva Association. The insurance industry-focused think tank has reliably included feedback from cyber model vendors for years, but a standalone effort to interview and understand the perspectives of that community with regard to systemic cyber risk and how they evaluate and quantify it has not yet been conducted making the research in this report the first of its kind. The model vendors can be expected to respond from a position of self-interest, whether consciously or otherwise, but the fact that they have been neglected has cost the historical scholarship the directly relevant views of those being criticized. They deserve to be heard.

After all, the perspectives of those criticizing the cyber vendor models may not necessarily be correct. In fact, there is little (if any) evidence to the contrary. All one has is the historical literature, which has largely been fashioned without regard to the detailed views of the cyber model vendors themselves, and little in the way of critical comparison has occurred in academic settings. In fact, the dearth of published company reports on the reliability of cyber vendor models is thin, with the main contribution coming from reinsurance intermediary Guy Carpenter (see the discussion of Davis, et al. 2023 later in this article). Although there is a clear shortage of confidence in the models expressed by the cyber re/insurance market in the existing literature, no serious effort has been made to test those views. Moreover, as mentioned earlier, this article is the first focused attempt to capture and publish the views of the modelers themselves.

Of course, it can be difficult to determine who is correct when dealing with extremely remote risks – which is the domain of the ILS market – for which there is no precedent. For now, frankly, there is nothing but speculation, however informed that speculation may be. While the cyber re/insurance market awaits the "cyber Pearl Harbor" or "Hurricane Andrew of cyber" (Gartzke 2013 68, Cuneo 2016), there is little they can use in assessing and managing remote

risks. The inability to manage remote risks effectively, of course, impedes the flow of capital into the cyber re/insurance market, which in turn limits the ability of the sector to grow, given structural factors in the market such as an over-reliance on quota share reinsurance (Cellerini et al. 2022 16), slowing the closure of the cyber insurance protection gap and leaving attendant cyber and economic security vulnerability in place.

Given that the cyber catastrophe models are viewed as a key part of the impediment of the flow of ILS capital into cyber risk – which in turn constrains cyber re/insurance market growth and ultimately contributes to state-level economic security vulnerability – the possibility that they are not as unreliable as some re/insurance and ILS professionals claim would mean that attitudes toward cyber models are the impediment to the flow of capital. This research project does not seek to answer the question of cyber catastrophe model adequacy, which is likely to remain a hotly contested topic for years to come. Rather, the goal is to enter into the historical literature the perspectives held by the modelers themselves on the effectiveness of their tools and how they are perceived by the market they are intended to serve.

3 Research Objective and Design

This article answers the specific question: How do cyber catastrophe modelers see their role in the flow of capital to the cyber re/insurance market, relative to the cyber insurance protection gap?

The universe of cyber catastrophe model vendors is quite small, which makes standard statistical and other quantitative methods of analysis wholly inappropriate to understanding this community and how it interacts with the broader re/insurance market. The tendency of the re/insurance academic community to favor statistical methods, presumably a link to the industry's reliance on actuarial science, has long hindered the flow of new analysis on the cyber re/insurance sector in general, as articles have tended to lean on mock portfolio analysis and other hypotheticals, given that they enjoy easy alignment with the quantitative research methods standard to the sector. This article's original contribution to re/insurance scholarship, therefore, comes largely from the use of qualitative research methods to help the industry and its attendant community of scholars understand new and emerging dynamics that have so far been largely overlooked.

To understand the perspectives of cyber catastrophe modelers on the effectiveness and maturity of their capabilities, this research project is centered on five interviews, out of six

companies approached. One was not able to accommodate the scheduling requirements but otherwise indicated they would have participated. The interviews conducted comprise a cross-section of a market where three companies account for the majority of market share (CyberCube, Cyence, and RMS) and one could safely estimate the total population at less than ten companies, according to informal market conversations that were confirmed by the research below, excluding those companies where a proprietary model is used in a managing general agent (MGA) capacity. The use of interviews within a broader qualitative research context is necessary for a population this small. Additionally, the interview approach makes it possible to explore the specific experiences of each participant rather than force an external framework to guide potentially different experiences. Using semi-structured interviews allows for some basis for comparison while still maximizing the experiences and insights of a small set of influential individuals.

The decision to engage with five participants was made not only to capture the majority of perspectives, but because adding further interviews would be dilutive. In a small market, talking to presumably more than half the population and sampling across large, small, and niche participants provides full representative coverage. The five participants were able to speak frankly because of the protection afforded by anonymity. In fact, findings are only presented in aggregate and with a minimum of information about the participants to provide context, for example when providing direct quotes. The five interview subjects each sat for a thirty-minute interview via MS Teams with audio only recorded. Five of the six participants come from cyber modeling vendor, with the fifth a former employee of a vendor model provider that has since pivoted.

The five participants are representative of the underlying market. Two of the three largest cyber vendor modeling firms participated, and they are known to have diverging views of the risk, an issue that has arisen in other research currently being conducted by this author (as yet unpublished). Two more are startup companies that have gained traction in the market. Each has at least one major reinsurance customer (i.e., a top-ten cyber reinsurer). The remaining participant is no longer working for a vendor modeling firm but was with an organization that exited the cyber modeling sector. Further, this participant has used other models and spoken with several vendor model firms, which offers a unique perspective on the landscape in general.

Transcripts from the interviews were reviewed several times each to identify key themes, coded, and then analyzed to ascertain the key insights they offer. Given the small number of participants, the coding exercise was kept a bit looser than traditional thematic content analysis efforts. The potential for different themes and observations would either require codes too

generic to matter or too many to identify any real themes. A middle ground was necessary, by which a narrative could be conducted relative to the prevailing cyber re/insurance and ILS industry views on the adequacy of cyber catastrophe models for ILS risk transfer.

4 Results

Five key themes emerged from the responses gathered from the research participants above: (a) Lack of precedent (i.e., relevant historical systemic cyber events), (b) problems with the availability of data, (c) the characterization of remote risks, (d) challenges gaining the trust of the cyber re/insurance market, and (e) the need for further education for the industry. On the five themes presented below, the respondents were generally unanimous, although the underlying detail does reveal some of the specific differences among them. Although their views on the role of cyber modelers with regard to the flow capital into cyber re/insurance may be similar at a high level, how they operate within those constraints does vary.

This article focuses on the core themes where the respondents are at least superficially unanimous not just because they arose as the most important findings from the interviews, but also because they provide a foundation for future inquiry into the role of cyber vendor models with regard to the flow of capital to cyber re/insurance risks. The differences among the models and the model vendors may be interesting, but such an examination would benefit from the findings provided below. It is the author's hope that perspectives on cyber vendor models can grow into its own line of academic inquiry over time.

All five cyber modelers raised the problems associated with the lack of relevant precedent for systemic cyber loss events. Simply put, there has never been a major systemic cyber event that has had a meaningful impact on the cyber re/insurance industry. Although one could point to the sixteen major events compiled by this author, with losses ranging on an inflation-adjusted basis from $800 million to $65 billion, it is difficult to characterize them as systemic given the lack of meaningful impact on financial markets, society, and the insurance industry (Johansmeyer 2023c 6, Kasper 2023 4). The fact that there has been a paucity of catastrophic cyber events in general (using the term loosely) forces cyber modelers to rely more on speculation and extrapolation, because they do not have access to empirical and historical data. This point was raised consistently throughout the interviews: All five respondents specifically discussed the lack of relevant reference events, a problem that has cost the modelers crucial context for the development of their risk models, not to mention a basic understanding of the sorts of scenarios they seek to forecast and explain.

According to one respondent, a former modeling vendor employee, “Models are too divergent. There’s no common ground where they are consistent, which makes you wonder if any part of the risk is actually reasonably commonly known.” The respondent adds, “That make you have to question everything.” This issue has been covered extensively in the industry trade press, as well, referencing underlying research by industry participants (Howard 2023; Davis, et al. 2023), which makes it unsurprising that another respondent explains, “We’re all coming at it from different approaches,” continuing that this is because there is no common thread or starting point for the different model vendors. Without reference events, more assumptions are necessary, increasing the likelihood that models will have profoundly different outcomes for similar scenarios. Generally, model output should be sufficiently differentiated to show that each’s “secret sauce” is meaningful, but not so different as to make any comparison meaningless. There should be points of similarity and consistency, reflective of where all modeling is grounded in the same underlying reference points.

Of course, even without reference events, one could reasonably expect cyber modeling to improve with better access to relevant data – specifically data from the re/insurers who would use these models. Access to re/insurer data, in fact, could serve as another form of touchpoint. Even though the cyber modelers may not have past losses from which to draw, they could still at least use similar grist for the modeling mill. Again, all five respondents agree on this point. Three respondents – representing an inactive solution, a startup, and one of the big three modeling vendors – point specifically to insufficient data sharing from re/insurers. For one of the respondents, though, this was less an issue, given the company’s focus on modeling only the likelihood of certain types of extreme event, rather than the attendant industry-wide insured losses from such an event.

The startup representative observes that re/insurers are acting against their own interests in withholding data from modelers: “So you have people that sit on claims data, and they don’t want to share it. Or they don’t have it in a form where it could credibly be shared.” One respondent from one of the top-three model vendors explains that it is not just data that is in short supply, also noting that both claimant behavior and policy language and coverages can influence risk quantification. Says another respondent from one of the top three: “We’re all businesses with our own objectives and we haven’t been playing well together.”

Characterization of truly remote risks by the cyber vendor models has been the natural outcome of the underlying issues above. The lack of historical events makes it impossible to reference common constraints, and the absence of insurance data from re/insurance partners

leaves more to the modelers to extrapolate and estimate. Unsurprisingly, these two conditions lead to vast differences in how the modelers characterize the remote risks they are expected to quantify – the divergence discussed above. The participants have noted that the extrapolation necessary to form a view of systemic risk and scenario outcomes can lead to wildly varying results. Those results invariably have led to criticism from the cyber re/insurance community.

The strain of ongoing market conversations was evident from the interviews. For example, the representatives from two of the three largest cyber modeling vendors seem almost like they are talking to each other, with one acknowledging that their estimates are "pretty thick in the tail," while the other concedes that "we might be lower than the others." Feeding this feeling of a market conversation is the observation of the former model vendor employee who not only lived the struggle but adds, "I think the belief is that they are all high to one degree or another." However, there is room for the self-interest of their clients (i.e., cyber re/insurers) to help shape how those numbers are perceived.

Such differences lead to the fourth common theme from the research: A lack of trust from the re/insurance market in the models' quantification of cyber risk. The literature review is clear on this. However, the respondents in this research – unsurprisingly – do not share that view. According to one startup modeler, "I believe the models are being scapegoated." There are several reasons for this. The reluctance of re/insurers to share data, discussed above, is part of the problem. Models likely would improve with better access to market data. Additionally, re/insurer expectations on what constitutes a systemic cyber event – and how severe such an event could get – is the basis for comparison to the models (Johansmeyer 2023b). If the re/insurer believes a model is too punitive with respect to expected losses for extreme events – or, for that matter, too light – the model methodology is forced to respond to a perspective that may have no grounding in fact or science. It is virtually impossible to establish trust under such circumstances, and in fact, doing so would require behaviors that would be untrustworthy, such as skewing the model methodology or results to meet unscientific client expectations.

The problems with trust lead naturally to the fifth theme that emerged from the interviews with cyber vendor modeling professionals: Education. It is clear that the cyber re/insurance industry has benefitted from the education provided by the modelers, and the five respondents all agree that much more is necessary. Interestingly, the success enjoyed by the modeler focused on a narrow set of potential events(that does not delve into estimated insured losses from cyber events) does represent a potential interim step for the category as a whole. Their work has been well received by the cyber re/insurance market, and transparency was key. The respondent explains: "We had to open everything in this exercise, really showing them everything about how the models are working, how the models are built, step by step," adding,

“I think they started to gain confidence as we moved ahead.” Of course, the respondent noted that the process has been long. Compared with discussions with the other participants in this research, that company did benefit from the narrower scope on which it has opted to focus.

Transparency is inextricably linked with education – and ultimately trust. Transparency improves the depth of education, and as to trust, seeing is believing. The event-specific modeler focused on this when talking specifically about the education process used with re/insurance clients (described above), which was indicated as having helped with client adoption. The former employee of a cyber model vendor is now in a position to discuss the different options available and did suggest that transparency makes the model evaluation easier – and that it is in short supply. The problem, though, is that increasing transparency can reveal the practices that offer a competitive advantage, and modelers could even risk having clients co-opt (or at least be informed by) their core intellectual property. As a result, balancing transparency with protecting the model’s advantage is a difficult proposition. The unwillingness of some modelers to be transparent, perhaps, is matched by the unwillingness of re/insurers, per the responses above, to share data with the modeling vendors.

The five themes highlighted by the respondents generally unanimously provide the first modeler-centric view of the state of play for cyber catastrophe modeling with regard to cyber re/insurance risk transfer and the flow of capital to support cyber risk. There are plenty of barriers to address, and what is clear is that simply blaming the models as “immature” or “not there yet” vastly oversimplifies a structural problem in the cyber re/insurance sector in which all stakeholders have an opportunity to improve.

5 Discussion

The role of cyber model vendors in the re/insurance risk transfer process is more complex and nuanced than the historical literature contemplates. The five themes that emerged from the interviews conducted with representatives of the catastrophic cyber modeling vendor community consisted of: (a) Lack of precedent (i.e., relevant historical systemic cyber events), (b) problems with the availability of data, (c) the characterization of remote risks, (d) challenges gaining the trust of the cyber re/insurance market, and (e) the need for further education for the industry. These themes emerging from the interviews offer a roadmap for addressing perception of cyber model fitness for purpose in re/insurance risk transfer in a manner not yet addressed by the historical literature. While not all are addressable, there is enough opportunity in the findings to enable a significant improvement to the functioning of the cyber

re/insurance market through better engagement with the vendor models that are already available.

Of the five themes, data sharing is primary. One could contend that the most foundational problem from the interview themes coming from the interviews is the lack of precedent, and that would be the primary problem if it were addressable. There is no alternative but to wait and then compare any future catastrophic cyber events to the benchmarks from 1999 to 2017 (Johansmeyer 2023c 6). Even then, there would remain some uncertainty with regard to how big such events could get, and whether there is a more extreme event still on the horizon. The mixture of faith and fortuity means that lack of precedent is not an addressable problem and further not the primary problem on which the other themes rest.

Data sharing, on the other hand, is addressable. Moreover, it is directly relevant to the problem of how the models are perceived, which was covered in reasonable depth in the literature review above. There is certainly a case to be made for the fact that the models – like the sector itself – are in their infancy. However, maturation likely would proceed much more quickly with better information sharing and collaboration among the various stakeholders in the cyber re/insurance community. Doing so, in fact, would enable improvement across several of the other themes that arose. Access to better data would reduce the role of extrapolation in the creation of model output, which the research participants addressed directly. It would also increase trust – both through improved raw material for the models and the fact that re/insurers would have played a role by sharing data. The model results would be their work as well. Finally, education as to model function and output would proceed more easily, because it would be built on greater trust, but also on the fact that the re/insurers would see how the data they provided advanced model function and maturity.

Data sharing is the primary problem in this context (excluding historical precedent, which is unaddressable), because it directly influences the secondary problems associated with extrapolation and characterization, credibility and trust, and ultimately cyber re/insurance community education. Consequently, addressing it productively would have a positive knock-on effect through the other themes raised by the participants in this research's interviews. Overcoming the barriers to data sharing, however, will not be easy. The fact that the *status quo* has persisted suggests the degree to which it is an entrenched issue. To summarize a comment made by the startup modeling firm participant: They want you to get the right answer, will not help you get there, and when they see your answer, they tell you they do not believe it.

Within the context of the interviews, it looks as though cyber re/insurers are acting against their own best interests with their current approach to data sharing and cooperation, which could be described as limited at best. It is important to remember that withholding such data could be interpreted as in their own best interests, as well, particularly if they believe the data they hold offers a competitive advantage. A sense of this is offered in a comment made by the OECD: "[T]here are a few large providers of cyber insurance who may benefit from a competitive advantage as a result of their significantly greater access to past claims data" (2020 6). The finding, which came from conversations with reinsurers, was positioned as a reason to support data sharing, but it also acknowledged that the aim to protect a competitive advantage is a reason not to share. Further, this is not limited to claims data, as the participants from two of the largest cyber model vendors indicated. Policy and coverage data would be helpful as well.

The question thus turns to which advantage is more powerful (to include whether either is inherently advantageous), which itself offers the opportunity for further research int his space. Pursuing this thread in future research also would have implications throughout the global re/insurance industry, as the issue of proprietary data as a competitive advantage arises frequently with regard to discussions about consortium development and other initiatives regarding the development of benchmarks.

With regard to the perception of whether cyber models are ready for meaningful use in the cyber risk-transfer market, it is clear that the issue is far more complicated than the historical literature suggests, and generally, there is room for additional research with regard to the models themselves, how they are built and used, and the extent to which the cyber re/insurance community's expectations are accurate (or even realistic). For now, the problem appears to come down to one of faith rather than skepticism – or perhaps both, if one concedes that even skepticism requires a "leap of faith" (Lowith 1951 230).

6 Conclusion

This article represents a first step toward more rigorous, complete, and inclusive study in the cyber re/insurance discipline. The gap in the literature left by discussing cyber vendor models without engage that stakeholder group has left many questions unanswered and takes the users of those models at their word. Balanced scholarship does not mean correct scholarship, of course. Future research should not only focus on the nature, challenges, and opportunities associated with cyber vendor modeling but also begin to integrate research on the models and

modelers with that of the cyber re/insurers and ILS managers who use those models (or hope to) in risk transfer transactions.

This article makes a unique contribution to the historical literature by enabling the cyber vendor modeling community to explain their thinking with regard to the nature of their work, the challenges they face, and how they interact with the broader cyber re/insurance ecosystem and risk transfer process. This is the first study of its kind and hopefully not the last. The issues raised by the participants in this qualitative study share insights that tend to have been expressed in private and may arise in the commercial process but have yet to be uncovered, let alone discussed, in an academic setting. The one respondent who indicated that the cyber models are being "scapegoated" gave voice to an important and powerful sentiment in the cyber model vendor community, and it does have some merit.

While the cyber models themselves are not perfect – and, indeed, the participants in this research were willing to concede as much – the model vendors have had to contend not only with a stakeholder base that could be more supportive but also a perception regarding their work that could impact the willingness of stakeholders to be supportive. Perhaps the greatest problem is the fact that a lack of historical precedent means that the reliability of cyber models comes down to a "he said/she said" argument between the model vendors and their prospective users. With no experiential data or other reference points, the issue cannot be resolved on the merits, and instead it has been addressed by the vocalization of a lack of confidence by the re/insurance market. Since they are the companies that buy models and deploy capital, their perspective has a clear advantage. While there are ways these stakeholders could help improve both model performance and their confidence in it, such as data sharing, they have yet to do so with scale, which simply perpetuates the market's existing challenges.

The good news is that there has been progress. Despite concerns about model effectiveness, the three cyber catastrophe bonds that have come to market do use models from some of the participants issued, and more such financial transactions are likely to come to market in the near future. Although this development may fall short of a full-throated endorsement of the cyber vendor models as they exist today, it certainly represents an important first step toward broader adoption – and more important, the improved flow of capital into the cyber re/insurance market. For this momentum to continue, though, changes will become necessary. Confidence in the cyber models will have to increase in order for niche issuance activity to achieve scale, and this means not just executing on the themes covered in this article but also taking a more balanced view with regard to model output.

The path of least resistance has been to scapegoat the cyber vendor models. Future scholarship can help remedy that tendency and create a foundation for more productive study and dialogue. This article's most important contribution is most likely the precedent it sets for more disciplined research and analysis with regard to cyber vendor models and their contribution to risk transfer, a development that the more established property-catastrophe re/insurance market and attendant scholarship should contemplate. Further, the findings offer insights for the re/insurance and ILS market that have not been gathered, analyzed, and revealed in a methodical approach such as that in this paper. The historical literature largely failed to highlight the benefits associated with closer collaboration between risk transfer parties and the modeling community, and the voice finally lent to the modelers expressed an upside clearly and directly. The cyber catastrophe models may already be far more effective than they seem; nobody can know for sure. What is certain, though, is that the modeling sector deserves more opportunities for its voice to be heard.

7 References

Artemis. (2023). Catastrophe Bond & Insurance-Linked Securities Deal Directory. Retrieved 15 October 2023. *Artemis.bm.* https://www.artemis.bm/deal-directory/.

Ayers, E. (2022). Cyber insurance pays out for 'almost all' ransomware claims: Sophos. *Advisen Front Page News: Cyber Edition.* 5 May. Retrieved 5 May 2022. https://www.advisen.com/tools/fpnproc/news_detail3.php?list_id=35&email=amican@verisk.com&tpl=news_detail3.tpl&dp=P&ad_scale=1&rid=431070850&adp=P&hkg=ZDF0Vr2mAr.

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

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

Cuneo, J. (2016). AIR Worldwide: "Business interruption could be the hurricane Andrew of cyber". *Global Reinsurance.* 15 June. Retrieved 15 October 2023.

https://www.globalreinsurance.com/air-worldwide-business-interruption-could-be-the-hurricane-andrew-of-cyber/1418710.article.

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

Davis, E., Fung, J., Filimonov, V., Iida, S., & Mcauley, R. (2023). *Under the Lens: Investigating Cyber Vendor Model Divergence.* New York: Guy Carpenter.

Disparte, D. (2017). A Cyber Federal Deposit Insurance Corporation? Achieving Enhanced National Security. *PRISM*. *7*(2), pp. 52-65.

Eling, M.,& Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance.* 17(5), pp. 474-491.

Gallin, L. (2023). Hannover Re and Stone Ridge in $100m retrocession cyber quota share. *Reinsurance News.* 19 January. Retrieved 15 October 2023. https://www.reinsurancene.ws/hannover-re-and-stone-ridge-in-100m-retrocession-cyber-quota-share/.

Howard, L.S. (2023). Diverging Cat Model Results Challenge Underwriters' Risk Analysis: Guy Carpenter. *Insurance Journal.* 1 August. Retrieved 2 December 2023. https://www.insurancejournal.com/news/international/2023/08/01/732900.htm.

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

Johansmeyer, T. (2023). How Big Is the Cyber Insurance Market? Can It Keep Growing? *Lawfare.* 27 June. Retrieved 15 October 2023. https://www.lawfaremedia.org/article/how-big-is-the-cyber-insurance-market-can-it-keep-growing.

Johansmeyer, T. (2023b). If Cyber Is Uninsurable, the United States Has a Major Strategy Problem. *Lawfare.* 26 July. Retrieved 15 October 2023. https://www.lawfaremedia.org/article/if-cyber-is-uninsurable-the-united-states-has-a-major-strategy-problem.

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

Johansmeyer, T. & Mican, A. (2022). Cyber ILS: How Acute Demand Could Drive a Scalable Retrocession Market. *Journal of Risk Management and Insurance. 26*(10), pp. 40-59.

Kasper, D. (2023). Insights from the 7th ASTIN Cyber Working Group. *Cyber Economics Magazine.* November.

Lloyd's of London. (2023). *Lloyd's systemic risk scenario reveals global economy exposed to $3.5trn from major cyber attack*. 18 October. Retrieved 20 November 2023. https://www.lloyds.com/about-lloyds/media-centre/press-releases/lloyds-systemic-risk-scenario-reveals-global-economy-exposed-to-3.5trn-from-major-cyber-attack.

Lowith, K. (1951). Skepticism and Faith: In Memory of Erich Frank. *Social Research*, *18*(2), pp. 219-236.

OECD. (2020). *Enhancing the Availability of Data for Cyber Insurance Underwriting, The Role of Public Policy and Regulation.* Retrieved 3 December 2023. http://www.oecd.org/finance/insurance/Enhancing-the-Availability-of-Data-for-Cyber-Insurance-Underwriting.pdf.

Pain, D. (2023). *Cyber Risk Accumulation: Fully tackling the insurability challenge.* November. Zurich: The Geneva Association.

Steele, G. (2023). Closing Keynote Speech. *Catastrophic Cyber Risk and a Potential Federal Insurance Response.* 17 November. New York: U.S. Department of the Treasury's Federal Insurance Office and New York University Stern School of Business's Volatility and Risk Institute.

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

Swiss Re. (2019). *Global Risks, Trends and Closing the Protection Gap.* Swiss Re Reinsurance. Retrieved 15 October 2023. https://www.swissre.com/dam/jcr:b4cac90e-a60f-4e33-bed2-497e52ff04b5/como_o_resseguro_pode_ajudar_a_resolver_a_lacuna_de_protecao.pdf.