PUBLISHED AUGUST 2021

Cyber Risk Reinsurance Issues

CYBER RISK TOOLKIT

American Academy of Actuaries
Committee on Cyber Risk, Casualty Practice Council

American Academy of Actuaries
ACTUARY.ORG

The American Academy of Actuaries' Cyber Risk Toolkit, developed by the Academy's Committee on Cyber Risk, is a series of papers addressing issues pertinent to cyber risk insurance and cyber exposure. This toolkit is intended to be a resource for interested readers of the general public, public policymakers, the actuarial profession, the insurance sector, and other stakeholders.

While the paper that follows stands alone, the complete toolkit offers a cohesive overview of the challenges posed in the cyber insurance market. The toolkit will be updated periodically to reflect new and emerging work from the committee.

American Academy of Actuaries

AMERICAN ACADEMY OF ACTUARIES
1850 M STREET NW, SUITE 300, WASHINGTON, D.C. 20036
202-223-8196 | **ACTUARY.ORG**

Cyber Risk Reinsurance Issues

Published August 2021

Like the primary cyber insurance market, reinsurers are approaching cyber insurance with caution, and many are investing heavily in cyber underwriting capabilities. Nevertheless, confidence in understanding the risk has increased, which has led to an active appetite and expansion of reinsurance capacity in recent years.

For instance, the world's largest reinsurer, Munich Re, has seen growth in premium written for cyber policies from $100 million in 2013 to $400 million in 2018. The current supply of capacity has increased in response to demand for the product, with several reinsurance towers exceeding $500 million. It is estimated that 40% of the global cyber insurance premium written flows to reinsurers,1 compared to 10% to 15% for more mature lines such as property and liability. In addition, the offerings of reinsurers sometimes extend beyond reinsurance capacity into other areas, such as assisting insurers with product development, providing advice on policy wording, and managing accumulation risk.

Despite the progress reinsurers have made over the years, underwriting to a large enough scale remains a key challenge. Underscoring the classic chicken-and-egg problem, insurers find writing cyber insurance difficult without reinsurers, but reinsurers need significant scale before the pooling effects make such reinsurance possible. Many of the challenges impacting primary insurers become more acute for reinsurers, such as lack of data and risk aggregation. Risk quantification is especially challenging for reinsurers due to aggregation potential and silent cyber risk. Enabling the scale necessary for more efficient risk-sharing is a critical element to the development of the overall cyber (re)insurance market where the top 10 carriers of cyber coverage write about half the global premium. Government backstops such as Terrorism Risk Insurance Act of 2002 (TRIA) may provide an avenue to mitigate this scaling challenge for reinsurers (and insurers)—particularly for cyber events with the potential for significant accumulation of losses.

For the many backstop programs across the world, cyber-related losses are either excluded, receive limited coverage (e.g., physical damage only), or the cyber coverage is unclear. The U. S. Department of the Treasury issued a Notice of Guidance on Dec. 27, 2016, which clarified that stand-alone "Cyber Liability" insurance policies are included under TRIA, thus demonstrating the importance of maintaining the program in the face of evolving threats.

1 "Cyber reinsurance in the 'new normal'"; Swiss Re; Oct. 5, 2020.

While the U.S. insurance industry is being pushed to cover acts of cyber terrorism under cyber-specific insurance policies, the case law is still relatively new and has not been tested by a catastrophic cyber terrorism event. Property and general liability coverages would generally still exclude this event and there is not a uniform approach under cyber-specific policies. There also is some question about coverage for widespread secondary events such as business interruption resulting from a terrorist-caused cyberattack on public utilities or internet infrastructure. Further adding to the ambiguity is that such backstop programs are usually designed to respond to terrorism attacks, which may present a challenge for cyber as such attacks are rarely attributed to terrorist organizations openly. More clarity that explicitly addresses the handling of cyber-related losses would help reduce some of the caution in the appetite of reinsurers. TRIA was reauthorized in December 2019 for seven years (expiring December 2027); nevertheless, the insurance industry and Congress has been giving increasing attention to better understanding the concerns around the handling of cyber risk. In a letter to the U.S. Government Accountability Office, the Cyber Risk Task Force of the American Academy of Actuaries shared its views on how TRIA would apply in the case of large-scale cyberattack against U.S. businesses[2]. Whether it would be best to continue extending the program in its current form or create a new program specifically designed to address these questions around the treatment of cyber perils should be part of future discussions. In several other countries, these programs are also being examined to assess the coverage being provided for cyber-related losses. For example, reinsurance for terrorism incidents provided by Pool Re, Britain's leading terrorism reinsurer, has been expanded to cover physical damage from cyber-terrorism.

Alternative risk transfer provides another avenue for reinsurance capacity, namely through insurance linked securities (ILS). The underlying complexity of cyber risk and the lack of relevant experience compared to natural catastrophes could potentially be deterrents for alternative capital providers; however, significant natural catastrophe losses in recent years has put pressure on the ILS market to improve investor returns. As a result, the ILS market is expected to be more selective with the risks it takes on in the short term. Wildfire, flood, and terrorism risks have been transferred to the capital markets successfully and so more activity is expected around cyber risk. However, in addition to the usual challenges posed by cyber risk to the traditional markets, there is a high potential for a triggering event to have an impact on bond and equity markets and therefore reduce the diversification benefits that have attracted investors to ILS covering property risks. While models are improving, data challenges contribute to not very sophisticated cyber risk models, which is also a big hurdle in transferring cyber risk to the ILS market.

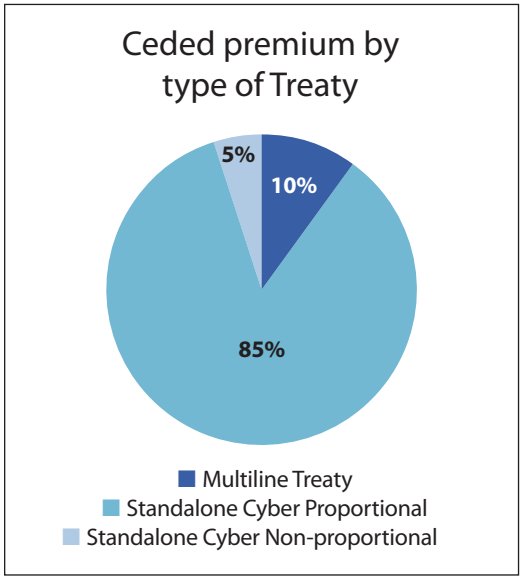
2 Academy Comments to GAO on Cyberattacks and TRIA.

A natural choice to structure a cyber risk in the ILS sector would be to follow the existing catastrophe-bond structure. One problem with this structure is that it requires upfront funding from investors, which may be a deterrent given the number of unknowns perceived to be associated with cyber risks. A potential solution to this problem could be the use of contingent capital. In this arrangement, investors would effectively promise to pay out the full amount when the structure is triggered. The drawback to this arrangement is the increased credit risk, underscoring the point that there are no easy solutions to the problem.

Availability of an industry-loss index could also be helpful in the effective retrocession of cyber risks to the ILS and reinsurance market. Such an index can be used to set up industry loss warranty arrangements (ILWs) for cyber risks. In such arrangements, loss trigger and payout after an event are typically based on the total industry losses, and in some cases the buyer's own losses too. PCS Global Cyber is one such index provided by Property Claim Services.[3] The ASTIN (Actuarial Studies In Non-life insurance) working party is also researching to provide a cyber risk index.[4]

Traditional risk transfer is currently provided primarily through standalone cyber treaties, with quota share treaties making up the vast majority.

Figure 9



Source: Swiss Re data

3 "Loss Aggregation for Cyber Events"; Verisk; 2021.
4 "ASTIN Working Party on Economic Cyber Loss Index for Parametric Covers—A Proof of Concept Study"; International Actuaries Association; May 2019.

Reinsurers have gravitated mostly to proportional (quota share) treaties due to their ability to alleviate capital requirements. In addition, proportional treaties help to fund the significant investment required to build a robust underwriting process for cyber insurance through commissions. Although proportional treaties are still the norm, non-proportional covers such as aggregate excess of loss treaties have seen increased demand due to their ability to provide balance sheet protection for insurers by ceding catastrophe risks. Aggregate excess of loss covers typically to attach at loss ratios between 90% to 200%.

Primary insurers and reinsurers have finite capital available for managing cyber risk. If reinsurers retrocede some of the cyber risk to the ILS market, additional capital could absorb a portion of the cyber risk. Further growth in the cyber market may require more innovation to attract market participants from the securities market. One such innovation could be to structure the program that allows lower barrier of entry for sponsors/cedants seeking protection from the capital market. This will enable more participants to enter the ILS market. Innovation could also be done by the modeling firms to enhance their cyber risk models. That will increase confidence of institutional investors, leading to further demand of cyber ILS instruments.

AMERICAN ACADEMY OF ACTUARIES
1850 M STREET NW, SUITE 300, WASHINGTON, D.C. 20036
202-223-8196 | **ACTUARY.ORG**