IAIS Report on Cyber Risk Underwriting

December 23, 2020

Mary Frances Monroe, Senior Advisor & Insurance Lead, mmonroe@iif.com
Melanie Idler, Senior Policy Associate, midler@iif.com

INSTITUTE OF INTERNATIONAL FINANCE

The International Association of Insurance Supervisors (IAIS) recently published its report on Cyber Risk Underwriting: Identified Challenges and Supervisory Considerations for Sustainable Market Development. In addition to including cyber risk underwriting as a key theme in its 2020-2024 Strategic Plan and Financial Outlook (SPFO), the IAIS appointed a Cyber Underwriting Small Group (CUSG) to develop supervisory practices that foster a sustainable approach to cyber risk underwriting. The CUSG recently surveyed supervisors and industry participants across multiple jurisdictions about the challenges posed by cyber risk underwriting, and highlighted their key findings in this report.

Cyber Underwriting Market and Vulnerabilities

Despite the growing importance and ubiquity of cyber risk, the affirmative cyber insurance market remains small relative to other commercial insurance business lines. Despite premiums of approximately USD 4-5 billion globally, cyber insurance is just 1.7% of the size of the property insurance market and 2.9% of the general liability insurance market as of 2018. In contrast, the global annual cost of cyber incidents is estimated at USD 600 billion, an order of magnitude well above the amount of losses absorbed by the insurance sector. The sizeable protection gap, as well as growing awareness of cyber risk, suggests there is huge potential for further cyber insurance market development. At the same time, there are a number of challenges holding back both demand from prospective cyber insurance policyholders and the appetite of insurers to underwrite cyber risk. From an insurance supervisory perspective, the growth of cyber insurance has raised concerns about accumulation risk, "silent" or non-affirmative coverage, and the lack of data to accurately measure cyber risk, among other issues.

Key Challenges

The CUSG identified two key challenges affecting cyber risk underwriting:

- Measurement of risk exposure due to the evolving nature of cyber risk, which makes historical data less relevant, the limited loss experience and shortage of reliable cyber risk data, difficulties in assessing policyholder vulnerabilities, accumulation risk and non-affirmative coverage; and
- Issues related to the clarity of cyber insurance policies, which include overlapping coverage, non-affirmative coverage, and the treatment of ransoms, fines, terrorism and war risk.

Accumulation Risk:

- A cyber incident could increase the accumulation of cyber losses given concentrations of insured risks and coverages that cause substantial losses under multiple insurance policies and potentially over multiple years and geographies.
- High levels of concentration in the use of certain software and operating systems (e.g. Windows or IOS), hardware (e.g. central processing units), and cloud services providers (e.g. Amazon, Google, Microsoft, IBM, etc.), as well as the interconnectedness of information technology systems, exacerbate potential accumulation risks.

- Should a vulnerability emerge from a common information technology service provider, it could involve multiple policyholders simultaneously. This makes cyber accumulation risk different from (and potentially more worrisome than) other types of insured risks, since the degree of diversification that insurers can achieve by building large and geographically diverse cyber risk insurance portfolios is limited.
- Insurers and supervisors need to develop a better understanding of cyber risk accumulations, as it could entail important systemic risks and uncertainties.

Non-Affirmative Exposure:

- Although insurers are aware of this issue, and some supervisors and insurers are taking important steps to limit the risk, at this time non-affirmative cyber coverage may still present a dangerous hidden amplifying factor of insurers' risk exposures.
- Non-affirmative coverage presents insurers with the possibility of cyber-related losses – and, in the worst case, the accumulation of losses – for which the insurers have not collected any premiums.
- An unresolved issue is distinguishing between what is a cyber-exposure/loss and what is not – particularly with respect to certain physical losses that may arise under other type of policies (e.g. Property and Casualty) that have much higher limits.
- The industry is addressing the issue through clearer cyber exclusions in non-cyber policies, together with cyber endorsements and stand-alone cyber products.
- Supervisors have concerns that insurers are not fully aware of the extent of their potential exposure to non-affirmative cyber risk in insurance policies. Thus, the identification and measurement of non-affirmative risk remains to be further developed in terms of data adequacy and underwriting standards.

Data Collection & Risk Modeling

- Cyber risk is still a relatively new, and quickly evolving, line of business for insurers. While cyber risk modelling is becoming more sophisticated, the absence or incompleteness of historical data on past cyber losses and cyber incidents decreases the statistical reliability of actuarial models. Furthermore, the evolving nature of cyber risk makes historical data less relevant to projecting future cyber events and losses.
- Insurers tend to rely on data on cyber insurance claims, which are only a fraction of total cyber incidents given the low take-up rates of cyber insurance and the fact that not all incidents generate claims. Moreover, not all cyber incidents are disclosed unless it is mandatory in the jurisdiction or for specific sectors. Supervisory reporting on cyber underwriting is not yet widespread and comprehensive, even in jurisdictions with established regulatory reporting. Even when data is collected, it lacks a harmonized reporting taxonomy.
- These factors have raised concerns among supervisors about how insurers quantify cyber insurance risk and define the appropriate premium rate and risk management approach.

Current Supervisory Framework

Given the small size of the cyber insurance market, the majority of supervisors have not yet developed specific supervisory guidance or supervisory reporting on cyber risk underwriting. Generally, respondents considered existing risk management guidelines and recommendations broad enough to cover cyber underwriting among the emerging risks. The development of a dedicated supervisory framework will be considered once market volumes achieve a larger scale, and subject to further analysis to identify and document the issues relevant to cyber risk underwriting.

In light of increasing concerns, however, a number of supervisors indicated that they have organized awareness-raising events and engaged with the insurance sector on various occasions to discuss the challenges posed by cyber risk underwriting, particularly focusing on non-affirmative cyber exposure. Among others, EIOPA has recently defined a strategy to develop specific priorities for cyber risk underwriting in its member jurisdictions.

Recommendations to the IAIS

In light of its findings, the CUSG recommended to the IAIS' Executive Committee that the IAIS pursue a strategic approach focused on: (a) facilitating the monitoring, understanding and assessment of cyber risk underwriting exposure and impact; and (b) assisting supervisors in building relevant capacity to review cyber risk underwriting practices and exposure. Specific recommendations for future IAIS cyber-related initiatives include:

- Taking an active role in encouraging supervisors to require improved clarity of cyber risk policy coverage and monitoring progress in addressing non-affirmative cover, possibly issuing further guidance;
- Addressing heterogeneity in data capture and facilitating data sharing initiatives;
- Reviewing current supervisory reporting practices and exploring the utility of expanded supervisory reporting on cyber underwriting exposure, with particular attention given to the total exposure as part of the Holistic Framework for Systemic Risk in the Insurance Sector;
- Reviewing current industry and supervisory approaches relating to risk measurement, including development of stress scenarios to estimate cyber underwriting exposure;
- Analyzing issues related to clarity of policy terms, conditions and exclusions with a view to encouraging convergence in understanding; and
- Developing cyber awareness and expertise among supervisors and sharing good practices on supervision of cyber underwriting.