Bermuda Cyber Underwriting Report

2019

EXECUTIVE SUMMARY

The Bermuda Monetary Authority (Authority or BMA) published its first cyber report in 2018, following the incorporation of cyber information in 2017 year-end filing requirements for the insurance sector. In that report, the Authority outlined initial statistics, findings and general recommendations to the industry, both from cyber underwriting and operational cyber resiliency perspectives. This report focuses on cyber underwriting, while briefly mentioning a few areas of convergence with operational cyber risk.

The acceleration of technological advances being adopted by businesses across all sectors, coupled with increased cybercrime sophistication has created rising costs of data breaches, both in potential liabilities and in terms of resources needed to enable operational recovery. This appears to have presented an opportunity for the insurance industry to benefit from increasing demand for standalone/affirmative cyber protection across industries. Data from the Authority's 2018 statutory filings show an increased number of insurers offering this line of business and significant increases in gross affirmative cyber written premiums. There is also an increase in the number of organisations utilising Bermuda captive structures to cover some of their cyber risk exposures. However, challenges in key operational aspects such as in pricing, risk aggregation and reserving, continue for this line of business.

This report provides key affirmative cyber risk underwriting data aggregated from the 2018 regulatory returns of groups, commercial insurers and captive insurers. Based on information obtained from the returns, the Authority notes that 13 groups[1] (2017: 15 groups), 41 commercial insurers (2017: 37 commercial insurers) and 17 captive insurers (2017: 15) write affirmative cyber. The reduction noted on the number of Bermuda groups was a result of mergers and acquisitions transactions that saw two groups ceasing to be recognised as Bermuda groups.

The cyber schedule for commercial insurers and groups requested information for both affirmative cyber insurance and cyber exposure on other lines of business where cyber is not explicitly excluded (non-affirmative cyber). Of the returns submitted, over 85% of cyber policies (excluding affirmative cyber) do not contain an explicit cyber exclusion clause for both 2018 and 2017. The primary cyber exposures include all-risk and liability policies where there are no specific cyber exclusion clauses within the policies.

As the market continues to grow and mature, the Authority expects that as part of the application of prudence, insurers have the relevant skills, clear strategies and Board-approved risk appetites to address some of the

[1] Groups for which the BMA is the Group Supervisor.

challenges associated with cyber risk exposures. This reflects the wide-reaching and interconnecting nature of cyber risk in its relationship to the operating environment of all insurers, especially in this digital age.

As to next steps, the Authority will:

- Use the expanded information gathered thus far to enhance its supervisory framework and continually assess each company's affirmative cyber underwriting practices

- Continue to enhance the cyber schedule in the year-end filing returns by seeking feedback from industry to gather more meaningful information on affirmative and non-affirmative cyber exposures.

- Require commercial insurers and groups to disclose more explicitly in their Commercial Insurer Solvency Self-Assessment (CISSA) and Group Solvency Self-Assessment (GSSA) filings how they are managing both affirmative and non-affirmative cyber exposures.

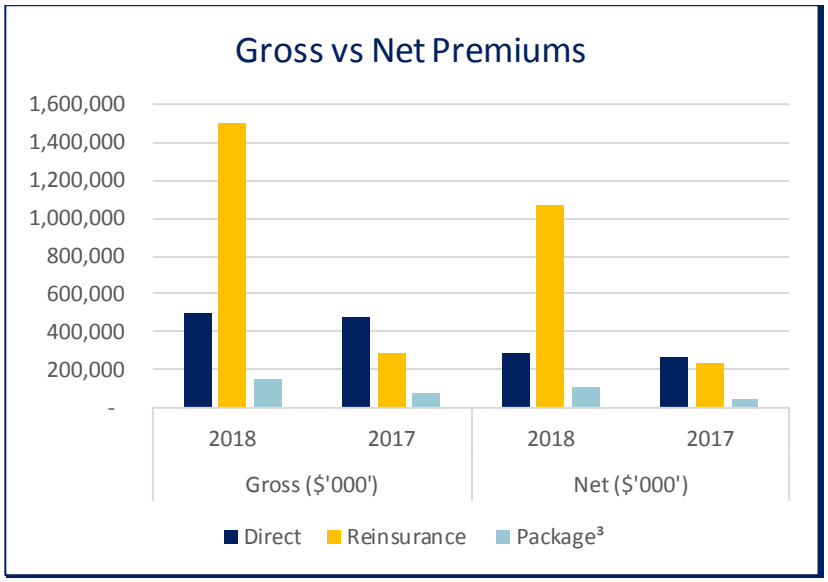
- Increase its engagement with rating agencies and vendor models to understand how models have evolved to deal with challenges related to cyber risk underwriting

- Use the information and insights gathered this year as a starting point for further discussions with insurers in its ongoing supervisory engagements, on-site visits and supervisory colleges; in the interim, insurers are welcome to send feedback or engage with the Authority about cyber underwriting practices

It is the BMA's goal to ensure that the industry has considered both affirmative and non-affirmative cyber exposure as a crucial part of its overall governance and risk management framework, and that insurers establish appropriate and holistic policies and procedures, internal control measures and an ongoing assessment of its cyber exposures.

1. Key Statistics for Commercial Insurers[2]

1.1 Gross vs Net Cyber Premiums

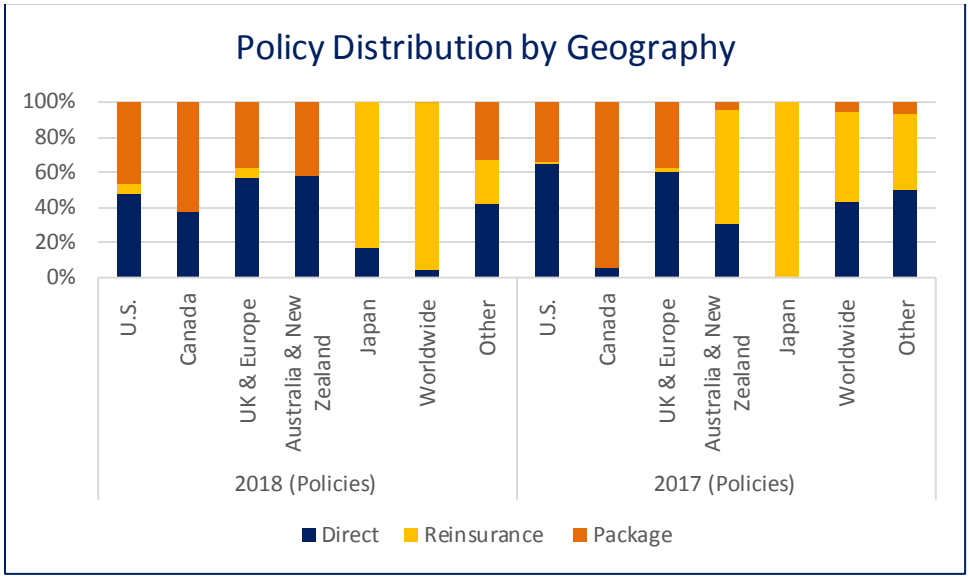


Commercial insurers reported affirmative cyber risk gross written premium of approximately $2.1 billion (2017: $845 million) and net written premium of approximately $1.5 billion (2017: $557 million) from over 100,000 policies (2017: over 31,000 policies). The spike in the reported premiums is largely related to the increase in policies written, as well as consolidation of additional subsidiaries writing cyber by Bermuda insurers. We also note that 57% of direct (2017: 55%), 71% of reinsurance (2017: 84%) and 71% of package[3] (2017: 68%) premiums were retained by commercial insurers.

Reinsurance premiums contributed the highest premiums both on a net and gross basis in 2018, potentially suggesting increased reinsurer interest in the cyber business. This is a shift from what we observed in 2017, where most of the business reported was for direct policies on both gross and net basis.

[2] Underwriting statistics are extracted from returns filed with the Bermuda Monetary Authority. For both groups and commercial insurers, not all consolidated entities are Bermuda-based, as such, the underwriting statistics will include business written on non-Bermuda paper.
[3] A cyber coverage that is included in a policy that contains other lines of business coverage.

1.2 Policy Distribution by Geography

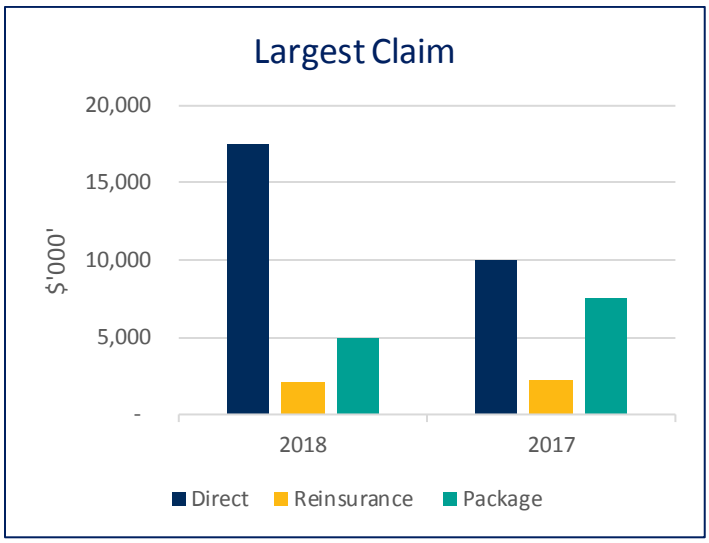


Majority of the affirmative cyber policies written by commercial insurers were for worldwide covers which accounted for 58% (2017: 26%), followed by United States of America (US) with 25% (2017: 56%) and Canada with 7% (2017: 14%). The rest of the policies were spread out amongst Japan, Australia and New Zealand, the United Kingdom and the European Union. A handful of insurers write a significant number of policies compared to the rest of the market. Increases in reported business by these major cyber underwriters created a change in regional concentration from the US to worldwide in 2018.

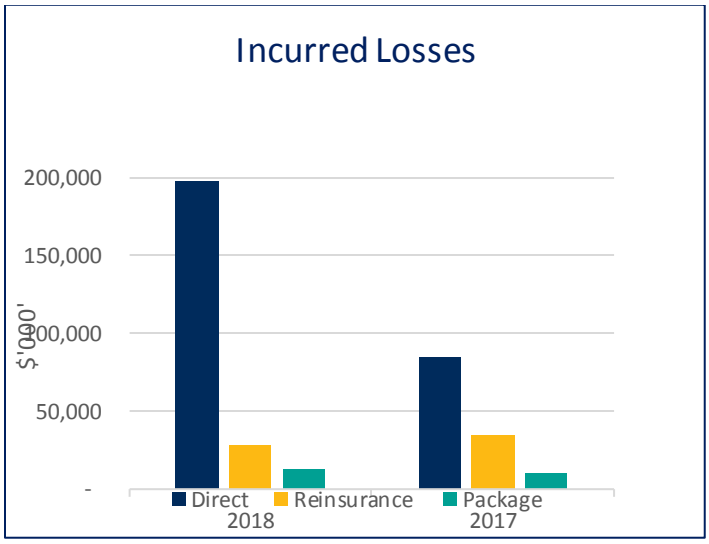
Reinsurance policies continue to be the dominant product for worldwide covers both in 2018 and 2017, while direct and package policies dominate the US business.

For groups, most affirmative cyber policies were written in the UK and Europe, followed by the US, together contributing over 80% of total policies written in both 2018 and 2017. The rest of affirmative cyber policies were spread out between Canada, Australia, worldwide and other countries.

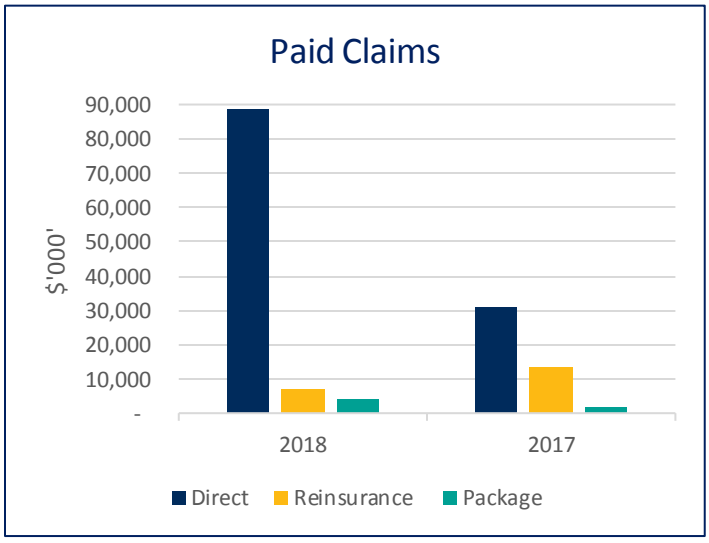
1.3 **Commercial Insurer Claims Data** *(arising out of affirmative cyber policies)*



The largest claim per underwriting category for commercial insurers was approximately $18 million (2017: $10 million) for direct, $2.1 million (2017: $2.2 million) for reinsurance and $5 million (2017: $7.5 million) for package policies. The seemingly higher individual claims contributed to the increase in total reported claims, despite the decrease in the claim count.



Aggregated incurred losses for commercial insurers for the year were approximately $239 million (2017: $130 million). Claims experienced to date for the cyber line has been low, showing loss ratios of just around 26%.



Cyber claims paid by commercial insurers were approximately $99 million for over 3,800 claims (2017: $46 million for over 6,600 claims). Direct policies contributed 89% (2017: 66%) of the total claims, whilst reinsurance contributed 7% (2017: 29%) and packages 4% for both years.

1.4 Cyber Stress Scenarios

Cyber Worst-Case Scenario (WCS)

Groups and commercial insurers were required to quantify and disclose their own cyber-specific WCS for those that write affirmative cyber policies.

For **groups,** the aggregate exposure reported for affirmative policies was over $4 billion (2017 – $7 billion) and around $2 billion after reinsurance (2017 – $5 billion), returning net retention ratio of 50% (2017 – 57%) of the aggregate exposure.

For **commercial insurers**, the aggregate exposure was over $6 billion with $3.6 billion after reinsurance, returning net retention of circa 60% (2017 – 66%). Based on the Authority's observations, both **groups and commercial insurers** have increased the use of reinsurance as a strategy to manage their overall cyber exposure.

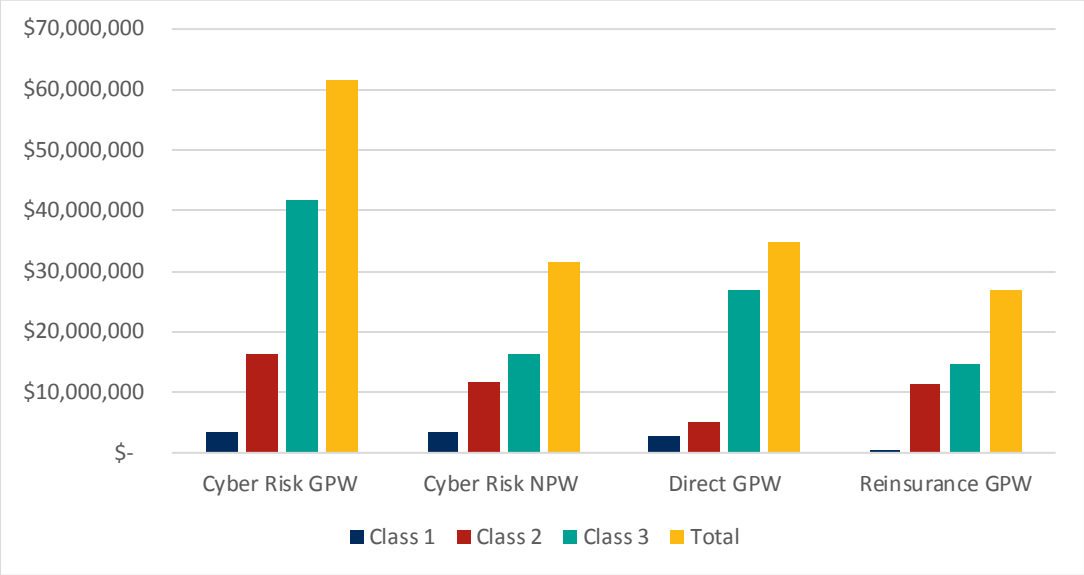
Post-WCS, both **groups** and **commercial insurers** would still be able to meet their enhanced capital requirements, reducing their statutory capital and surplus only by 5% to 8% on average. The data showed that Bermuda commercial insurers' own WCSs from affirmative cyber risk coverage would not have significant impact on their statutory capital and surplus. However, the Authority is concerned that significant losses could arise from non-affirmative exposures. Therefore, the Authority will continue its enhanced engagement with insurers next year to ensure appropriate risk management frameworks are in place to also cover non-affirmative cyber exposures, and may require more disclosures around non-affirmative cyber exposures.

2. Key Statistics for Captive Insurers

The Authority notes that many organisations are assessing how they can best utilise captives as a risk management tool to cover emerging risks such as cyber.

While this line of business remains an ever-changing landscape, Bermuda captive insurers have begun to provide solutions for cyber risk exposure to their parents and affiliates. This has increased both the number of captives writing affirmative cyber policies, as well as the volume of premiums year-on-year. This summary highlights the Bermuda captive insurers encompassing general business writers - Classes 1, 2, and 3, which are writing cyber risk line of business as reported in Electronic Statutory Financial Returns (E-SFR) for year ended 31 December 2018.

2.1 Cyber Risk - Gross Vs Net Premiums



Noting the growth in affirmative cyber-related gross premiums written by Bermuda captive insurers, there was an increase of 53.6% over the prior year, totaling approximately $61m and net premiums written of $31m. Class 3 insurers led with 67.8% of affirmative cyber written amongst the captive insurers. Further, it is noted that 56% of the total affirmative cyber gross premiums written were on a direct basis and 44% as reinsurance.

CONCLUSION

Overall, to manage this evolving risk, the Authority expects insurers to be resilient in terms of capital and liquidity. In addition, insurers should establish proper risk management and governance processes, particularly in the areas of risk quantification (especially for non-affirmative cyber exposures), aggregation and contagion from an underwriting perspective.

The Authority therefore strongly recommends insurers to take steps to ensure that aggregation risk pertaining to major cyber breaches is appropriately assessed and addressed. In addition, insurers may consider appropriate design of outward reinsurance programmes to manage non-affirmative exposures. Further, insurers should consider incorporating in their stress testing models the correlation and potential loss arising from a global cyber-attack that could impact their own operations, while at the same time being required to pay claims from their insurance business. The Authority expects all commercial insurers and groups to appropriately consider and document such assessments in the filing of their Commercial Insurer/Group Self Solvency Assessment for 2019 year-end and going forward.