BMA
BERMUDA MONETARY AUTHORITY

Bermuda Cyber Underwriting Report

2020

About this report

The Bermuda Monetary Authority's (Authority or BMA) annual *Bermuda Cyber Underwriting Report* was first published in 2018. This report focuses on cyber underwriting, whilst briefly mentioning a few areas of convergence with operational cyber risk. The content of this report is the result of analysis carried out by BMA staff on the cyber underwriting information from the 2019 annual filings for commercial (re)insurers (Classes 3A, 3B, 4, C, D and E), groups and limited purpose (re)insurers (Classes 1, 2, 3, A and B). The report outlines statistics, findings and general recommendations to industry regarding cyber underwriting and, to a lesser extent, operational cyber resiliency.

About the Authority

The Authority was established by statute in 1969. Its role has evolved over the years to meet the changing needs in Bermuda's financial services sector. Today it supervises, regulates and inspects financial institutions operating in the jurisdiction. It also issues Bermuda's national currency, manages exchange control transactions, assists other authorities with detecting and preventing of financial crime, and advises Government on banking and other financial and monetary matters.

The Authority develops risk-based financial regulations that apply to the supervision of Bermuda's banks, trust companies, investment businesses, investment funds, fund administrators, money service businesses, corporate service providers, insurance companies and digital asset businesses. The BMA also regulates the Bermuda Stock Exchange and the Credit Union.

BMA Contact Information

Bermuda Monetary Authority
BMA House
43 Victoria Street
Hamilton

P.O. Box 2447
Hamilton HMJX
Bermuda

Tel: (441) 295 5278
Fax: (441) 292 7471

E-mail: enquiries@bma.bm

This publication is available on the BMA website www.bma.bm

Table of Contents

1. Executive Summary

The cyber insurance[1] market continues to grow at a rapid pace as companies become increasingly digitised to keep up with a competitive global market. Although cyber underwriting as a stand-alone insurance product still appears to be relatively immature compared with other commercial insurance products, the sustained increase in technological adoption across industries, and growing knowledge on the importance of cyber insurance in a more digitised world, continues to drive market growth. This is evident from the continued rise in demand for affirmative cyber protection by insurance clients across several industries. Information obtained from 2019 Financial Year-End (FYE) statutory filings shows a steady increase in the number of insurers offering this line of business and significant increases in gross affirmative cyber premiums written. Notwithstanding this, a few insurers also reported significant reductions in exposures on slightly reduced premiums based on prior loss experiences and more clarity around the perceived loss potential. On the other hand, captive insurers continue to serve as a risk management tool for companies seeking to manage their cyber risk exposures, as evidenced by the increase in the number of captive insurers writing cyber risk.

This report covers key affirmative cyber risk underwriting data aggregated from the 2019 FYE regulatory returns of groups, commercial insurers and captive insurers. Based on information obtained from these returns, the Authority notes that 14 groups[2] (2018: 13 groups), 51 commercial insurers (2018: 41 commercial insurers) and 20 captive insurers (2018: 17 captive insurers) write affirmative cyber. The increase noted across the different company categories consists of both new and established insurers tapping into the business's cyber insurance line. Information obtained by the BMA from the returns also highlighted that a large proportion of non-cyber policies remain without cyber exclusion clauses. However, it remains a challenge to reach a market representative conclusion, as not all insurers completed the requested information under the non-affirmative section.

For 2019 FYE, commercial insurers reported gross and net premiums increased by 38% (gross) and 40% (net) reaching $2.96 billion and $1.46 billion, respectively. Premium receipts from direct policies continue to contribute the most on both a gross and net basis. Bermuda insurers continue to provide cyber coverage on a global scale, with most of the policies being written for the United Kingdom (UK) and Europe (49% of the total number of policies written). Claims continue to increase for large individual losses, total claims paid and total incurred losses.

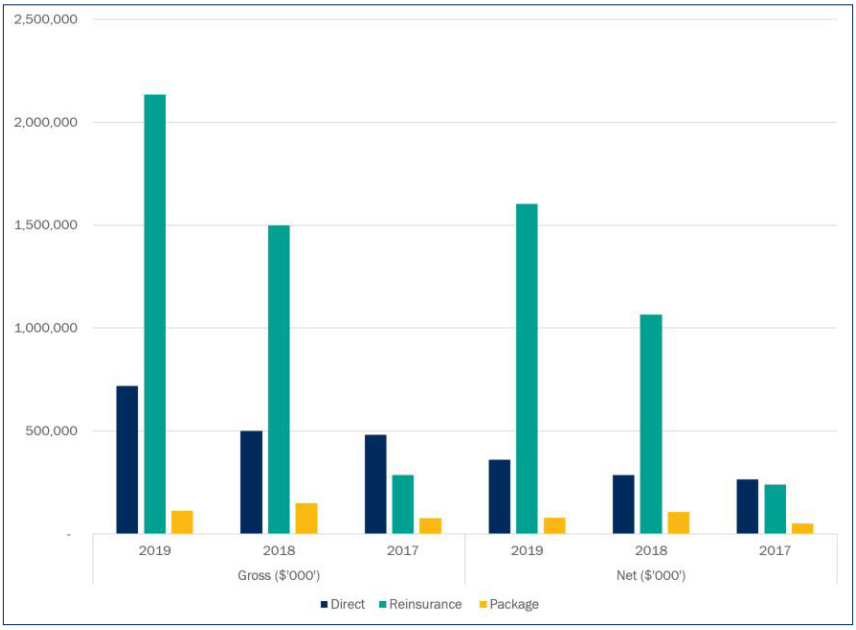
Digitisation and pandemic-induced operating environments seen at the peak of the COVID-19 pandemic are expected to result in a demand surge for cyber products. This has reemphasised the importance of cyber risk as one of the critical business risks for companies worldwide. Bermuda insurers will continue to be exposed to potential cyber risk aggregation issues. They can suffer losses from their operations and through claims from the business they write should a cyber-catastrophe occur. As such, the Authority expects Bermuda companies to be not only able to identify, quantify and manage their affirmative and non-affirmative cyber risk exposures from the business they write but also their own operational cyber risk exposures. Procedures to mitigate uncertainties around the modelling of cyber risks must be documented, including the implementing of a robust model validation process.

[1] For the purposes of this report, where reference is made to insurance, this should be taken to mean both insurance and reinsurance unless separately disclosed otherwise.

[2] Groups for which the BMA is the group supervisor.

2. Key Statistics for Commercial Insurers[3]

2.1 Gross vs. Net Cyber Premiums Written



Source: *BMA Calculations*

Commercial insurers reported affirmative cyber risk gross premium written of approximately $2.96 billion (2018: $2.15 billion) and net premium written of approximately $2.04 billion (2018: $1.46 billion) from over 400,000 policies (2018: over 100,000 policies). The increase in the reported premiums is largely driven by the increase in policies being written. The Authority also notes that 50% of direct (2018: 57%), 75% of reinsurance (2018: 71%) and 71% of package[4] (2018: 71%) premiums were retained by commercial insurers.

The bulk of Bermuda insurers continue to provide reinsurance for cyber risk. For 2019, reinsurance premiums continue to be the highest both on a gross and net basis. Coupled with the increase in retention levels for reinsurance premiums, it highlights the continued development of reinsurers' appetite for cyber risk business. This is consistent with observations from 2018 FYE filings. Two commercial insurers made the biggest contribution to the reinsurance premiums, writing more than $300 million each and retaining above $300 million of the gross premiums written. The dominance by a few insurers potentially points to the underwriting complexity and challenges of aligning cyber insurance coverage with the risk exposure; however, more insurers are steadily increasing line sizes, whilst innovating on structuring of coverage.

[3] Underwriting statistics are extracted from returns filed with the BMA. 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.

[4] 'Package' is cyber coverage which is included in a policy containings other lines of business coverage.

2.2 Number of Policies - Distribution by Geography

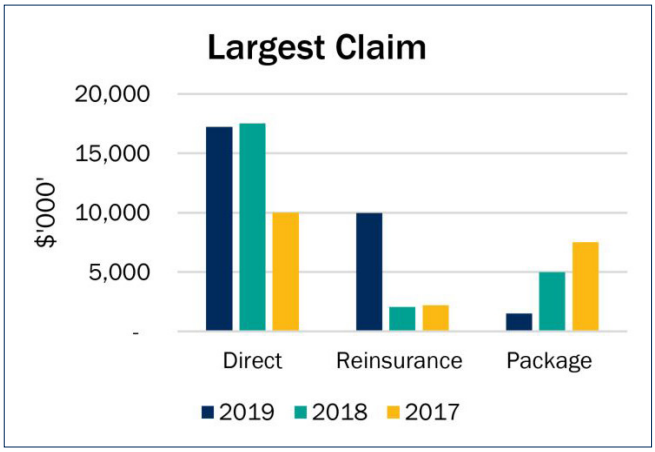
Source: BMA Calculations

The majority of affirmative cyber policies written by commercial insurers were for policyholders based in the UK and Europe, which accounted for 49% (2018: 44%) of total policies, followed by the US with 27% (2018: 13%) and worldwide covers with 14% (2018: 35%). The rest of the policies were spread out amongst Canada, Japan, Australia and New Zealand. A small number of insurers continue to write a significant number of policies compared to the rest of the market. Increases in reported business by these major cyber underwriters is reflected in regional concentration, which the UK and Europe continued to dominate in 2019. Continued shifts are expected as geographical markets develop and the demand for cyber risk protection increases.

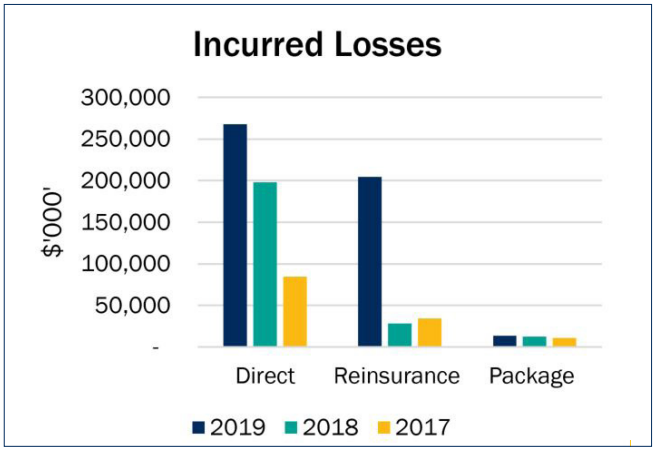
Reinsurance policies continue to be the dominant products written by Bermuda insurers worldwide covers both in 2019 and 2018. Direct policies dominated US coverage, but package policies were most prominent for the UK and Europe, mainly due to a small number of insurers. Overall, it appears that stand-alone cyber products are gaining popularity with a relative increase in market awareness about cyber exposures and the role of insurance in managing the risk.

For groups, most affirmative cyber risk exposure was reported for policies covering clients in the US, followed by the UK and Europe, which together contributed over 80% of total policies written in both 2019 and 2018. The remainder of groups' affirmative cyber policies were spread out between Canada, Australia, worldwide and other countries.

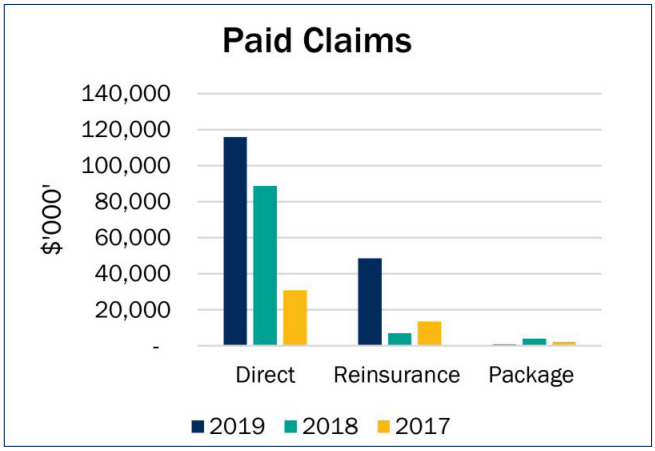
2.3 Commercial Insurer Claims Data[5]



Source: BMA Calculations



Source: BMA Calculations



Source: BMA Calculations

Ransomware attacks

The largest claim per underwriting category for commercial insurers was approximately $17.2 million (2018: $17.5 million) for direct, $9.9 million (2018: $2.1 million) for reinsurance and $1.5 million (2018: $5 million) for package policies. In the first two cases, the large losses were both related to ransomware attacks. Despite the seemingly lower individual claims loss for reinsurance and package policies, the claim count was higher and this resulted in an increase in total claims value.

Ransomware attacks and data breaches

Aggregated incurred losses for commercial insurers for the year were approximately $485 million (2018: $239 million). Direct policies continue to have the most contribution, with ransomware attacks and data breaches featuring the highest type of loss event. Loss ratios to date for the cyber line continue to increase, relative to the net premiums written (2019: 24% vs 2018: 16%).

Increase in claims paid

Cyber claims paid by commercial insurers were approximately $165 million for over 8,700 claims (2018: $99 million for over 3,800 claims). Direct policies contributed 70% (2018: 89%) of the total claims paid, whilst reinsurance contributed 29% (2017: 7%) and package 1% (2018: 4%). A few insurers writing the majority of the business reported in the 2019 filings were the significant contributor to claims paid. As the count and size of claims continue to increase, insurers must ensure that they have adequate risk management structures in place to be able to deal with potential cyber catastrophes.

[5] This information relates to affirmative cyber policies

2.4 Cyber Underwriting Stress Scenarios[6]

Cyber Worst-Case Scenario (WCS)
Groups and commercial insurers were required to identify and quantify their own cyber-specific WCS, particularly those that write affirmative cyber policies. It is important to note that insurers used varying methodologies in quantifying their own cyber-specific WCS; thus the insurers' individual results are not comparable at the market level.

For **groups**, the resulting scenarios were mainly a cloud service provider hack, a ransomware attack and a major data breach. Aggregate worst-case gross and net losses reported for affirmative policies were over $4.4 billion (2018: $3.9 billion) and over $2.4 billion (2018: $2 billion) respectively. Overall, the reported cyber risk worst-case scenario losses are not expected to significantly effect on the aggregate statutory capital and surplus for insurance groups.

The **commercial insurers** used a combination of in-house models, vendor models and publicly available cyber stress scenarios to determine WCS. A data breach, cloud outage, ransomware or country power outage were amongst the most commonly chosen scenarios. The WCS resulted in estimated aggregate losses of over $7 billion (2018: $6 billion) with $4 billion (2018: $3.6 billion) after reinsurance, returning net retention of circa 54% (2018: 60%).

Overall, both **groups** and **commercial insurers** would still be able to meet their enhanced capital requirements after applying their own WCS; reducing their statutory capital and surplus on a gross and net basis to a mean and median of 93% (94% net), and 96.7% (97.1% net) respectively. The data continues to show that Bermuda commercial insurers' own WCSs from affirmative cyber risk coverage continue to have minimal impact on the overall statutory capital and surplus. However, the Authority is concerned that significant losses could arise from non-affirmative exposures from policies such as all-risk, general liability etc. A majority of registrants continue to write non-cyber policies without explicitly providing cyber exclusions. This can pose sustainability challenges, particularly due to the catastrophic nature of cyber losses. Because of the limited industry information on cyber-related claims to date, the Authority believes that the industry needs to perform an ongoing model review, as claims experience develops over time. The Authority, therefore expects insurers to incorporate a robust model validation exercise as part of its risk management process.

2.5 Commentary Concerning Expectations for Commercial Insurers and Groups from the 2019 Cyber Underwriting Report

The Authority noted in its 2019 Cyber Underwriting Report that groups and commercial insurers were expected 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 exposures. A review of select CISSA and GSSA filings established mixed results. Some groups provided extensive affirmative and non-affirmative information, including worst case scenarios, while some groups provided information that was only limited to their affirmative cover. Some did not include any information, despite potentially having exposure to non-affirmative cyber risks. The same picture was obtained from commercial insurer filings.

Although the Authority understands the complexity and difficulty of the process of identifying and measuring non-affirmative exposures, given the potential for significant losses, the BMA expects insurers to put forth

[6] The BMA produces an annual Catastrophe Risk and Stress Testing Analysis Report which details more stress tests. This can be viewed on the following link: https://www.bma.bm/publications/bma-surveys

appropriate and proportional effort and resources to understand their potential exposure to non-affirmative cyber risks and ensure that appropriate mitigation plans are in place to address them. Therefore the Authority will continue engaging and giving explicit feedback to insurers based on the review of filings and as part of on-site reviews and supervisory college exercises.

3. Key Statistics for Captive Insurers

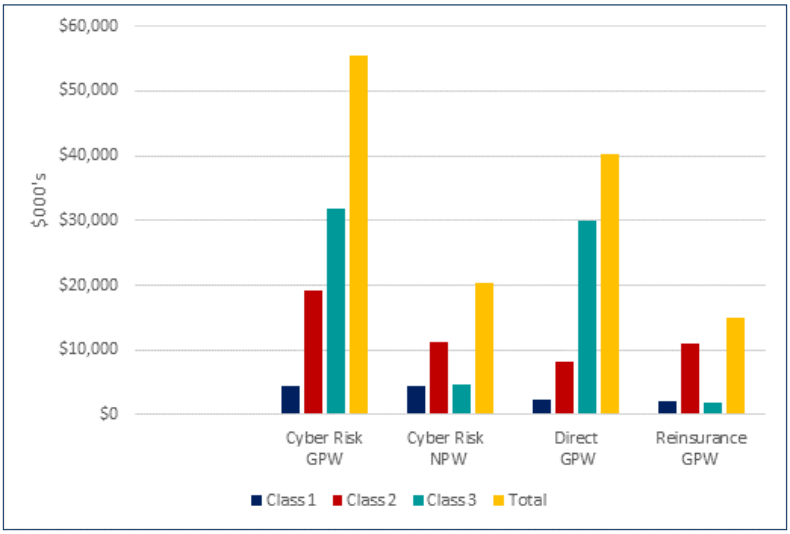
3.1 Overview

This section highlights Bermuda captive insurers, encompassing Bermuda's general business insurers - Classes 1, 2 and 3 writing cyber risk line of business as reported in electronic Statutory Financial Returns (eSFR) for the year ended 31 December 2019.

Insurers worldwide have continued to assess how their captives can be best positioned as a risk management tool. The COVID-19 pandemic has increased cyber risk exposure to these captive insurers and affected the cost and availability of the insurance coverage capacity in the market. In this new environment, the BMA continues to see growing interest in the Bermuda captive market.

As existing captives continue to prove their value to organisations, the Authority has seen new entrants to the market who see the proven benefits of owning a captive. For 2019 FYE, the number of captive insurers writing cyber risk increased from 17 to 20.

3.2 Cyber Risk - Gross vs. Net Premiums – Captive Insurers



Source: BMA Calculations

The Authority noted that 73% (2018: 56%) of the total gross premiums written were on a direct basis and 27% (2018: 44%) as reinsurance. Class 3 insurers continue to lead with 57.6% (2018: 67.8%) of cyber exposure written amongst the captive insurers.

4. Conclusion, Expectations and Next Steps

As the cyber insurance market and the cyber threat landscape continues to change, the Authority expects insurers to ensure that they adequately cover the following areas:

- **Identification, measurement, quantification, monitoring and mitigation of non-affirmative cyber risk exposures**
    - The Authority is concerned that insurers may be unaware of the magnitude and nature of their full cyber exposures. Insurers are therefore expected to implement appropriate and adequate systems in place to identify, measure, quantify, mitigate and monitor non-affirmative cyber risk exposures. The board of directors, who have ultimate responsibility for the business operations, must have a deeper understanding of non-affirmative cyber exposures to serve as a basis for its strategy formulation concerning this area
- **Management of tail risk**
    - Given the challenges of modelling cyber risk and the measurement of non-affirmative cyber risk exposures, insurers may find it difficult to manage exposures, especially from low probability and high severity events. Insurers are expected to conduct stress and scenario testing for various degrees of both affirmative and non-affirmative exposures and assess the results therein for proper mitigation measures
- **Modelling of cyber risk**
    - Given the evolving nature of cyber risk and the lack of readily available historical data for use in predicting cyber losses, the Authority expects insurers to take appropriate steps to mitigate the uncertainties associated with modelling cyber risks. Such steps must be documented and appropriately adjusted in a timely manner to reflect material changes in circumstances. As mentioned in the earlier section, insurers should implement robust model validation processes to ensure the appropriateness and usefulness of their models

As the cyber insurance market continues to develop, the BMA expects insurers to ensure that they appropriately consider, on an ongoing basis, both affirmative and non-affirmative cyber exposure as an important part of their overall governance and risk management framework.

As next steps, the Authority will:

- Require commercial insurers and groups to disclose more explicitly in their CISSA and GSSA filings how they are managing both affirmative and non-affirmative cyber exposures. The Authority expects insurers to establish appropriate policies and procedures for the identification, measurement, monitoring and mitigation of cyber insurance risk exposures
- Require insurers to clarify whether cyber coverage is provided or not, in non-cyber policies, either by having clear exclusion language or adding the necessary endorsements, beginning at the January 2022 renewal. Commercial insurers and groups will be required to document their progress in their CISSA/GSSA filings for the 2021 year-end
- Continue to engage with rating agencies and vendor model providers to understand how models adapt to deal with challenges related to cyber risk underwriting

- Continue to enhance supervisory frameworks and assess each company's affirmative cyber underwriting practices as the market gains more understanding for this line of business
- Continue to enhance the cyber underwriting schedule in the year-end FYE filing returns on both affirmative and non-affirmative cyber exposures
- Review information received from the filings to guide dialogue during on-site visits and supervisory colleges

BMA House

43 Victoria Street, Hamilton HM 12, Bermuda
P.O. Box 2447, Hamilton HM JX, Bermuda

Tel: (441) 295 5278 Fax: (441) 292 7471

Email: enquiries@bma.bm

www.bma.bm