BMA
BERMUDA MONETARY AUTHORITY

Bermuda Cyber Underwriting Report

2021

About this report

The Bermuda Monetary Authority's (Authority or BMA) annual Bermuda Cyber Underwriting Report is the result of analyses carried out by BMA staff on the cyber underwriting information from the 2020 annual filings for commercial (re)insurers[1] (Class 3A, 3B and 4), insurance groups[2] and limited purpose (re)insurers (Class 1, 2 and 3). The report outlines key statistics, findings and general recommendations to the industry regarding cyber underwriting.

The market is invited to review the content and insights provided in this report and reach out to the Authority should there be any questions or concerns at iwg@bma.bm.

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 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, digital asset issuances and digital asset businesses. The BMA also regulates the Bermuda Stock Exchange and the Bermuda 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

[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.

Table of Contents

1. Executive Summary

The COVID-19 pandemic highlighted growing interest and concerns around cyber risk and the need for a robust cyber insurance market. As organisations are forced to continue to operate in remote working environments, cyber threat actors continue to exploit inherent cybersecurity weaknesses. The interdependence brought by globalisation and the need for digitisation provides an avenue for multiple victims of cyber attacks across business sectors. Given this, the demand for cyber coverage continues to grow, highlighting the need for the insurance sector to continue improving on its cyber underwriting practices. While the cyber line remains a small part of the overall Bermuda insurance market (Gross Written Premiums (GWP) of <3% of overall GWP for all lines), information gathered from 2020 Year-End (YE) indicates a steady increase in both gross and net cyber exposures, at $233 and $110 billion (2019: $209 and $70 billion), respectively.

This report covers key affirmative[3] cyber risk underwriting data aggregated from 2020 financial YE statutory filings of groups, commercial insurers and captive insurers. Based on information obtained from these returns, the Authority notes that 15 groups (2019: 14 groups), 48 commercial insurers (2019: 51 commercial insurers) and 24 captive insurers (2019: 20 captive insurers) write affirmative cyber coverage, which has shown an increase in aggregate GWP from $2.96 billion in 2019 to $3.04 billion in 2020.

A slight overall increase in premium (2.7% year on year) has been observed for YE 2020, relative to the increase in both gross and net exposures, as noted above. The Authority also noted the steady rise in direct policies compared to reinsurance and package policies. The United States (US), United Kingdom (UK) and Europe continue to dominate the geographic distribution of policies written for the year, comprising 75% of the total. Cyber losses incurred during the period and loss ratios continue to rise as expected. Nevertheless, current data continues to show that the industry seems adequately capitalised to cover identified worst-case scenarios.

Furthermore, Bermuda captives continue to serve their purpose as a risk management tool for companies seeking to manage their own cyber risk exposures, as evidenced by the significant increase in the cyber gross premiums written along with the increase in the number of captives writing cyber risk as outlined in Section 3 of this report.

The Authority also outlined in this report its analysis on the aggregated results from the cyber underwriting stress scenario testing submitted by the insurers, as derived from their own worst-case scenario analyses. The Authority notes the continued resilience of the market, collectively as measured by the net impact to the insurer's capital levels post cyber stress scenarios. Nonetheless, the Authority continues to express its concern on the full impact of non-affirmative cyber exposures to the market. Therefore, as a next step, the Authority is introducing BMA-prescribed cyber stress scenarios to be completed on a best-efforts basis for 2021 YE, which will cover both affirmative and non-affirmative cyber exposures. Having a standard set of cyber stress scenarios will also give the Authority a more comparable view of the market.

Finally, the thematic review of the market's Commercial Insurer Solvency Self-Assessment (CISSA) and Group Solvency Self-Assessment (GSSA) disclosures suggest that the cyber risk management practice of some insurers could be further enhanced to improve those insurers' overall cyber risk management framework. As a result, the Authority is providing further guidelines to give clarity to the market in terms of meeting the BMA's expectations, particularly in key areas such as management of non-affirmative4 cyber risk exposure, stress scenario testing and compliance with the Insurance Sector Operational Cyber Risk Code of Conduct.

---

[3] "Affirmative cyber policy" refers to (re)insurance policies that specifically and explicitly cover cyber risk, either as a standalone policy or as endorsements added to a broader policy.

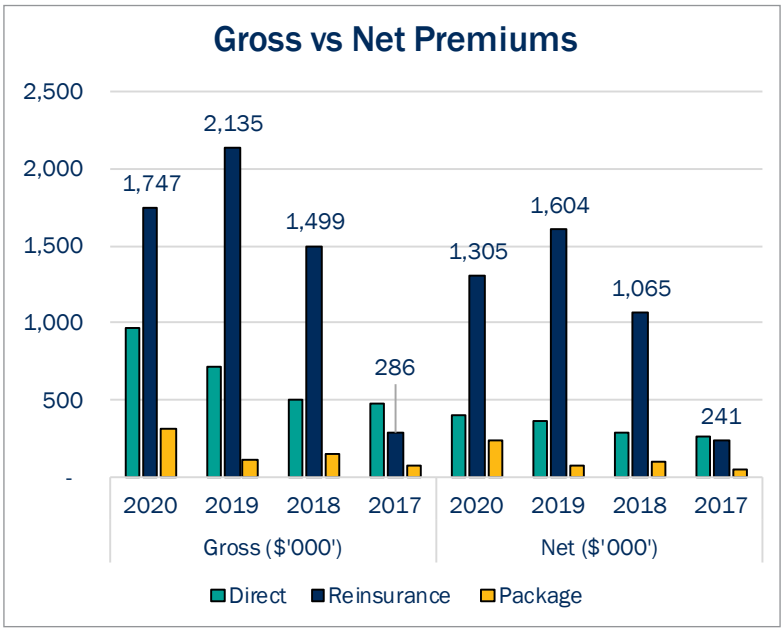
[4] "Non-affirmative cyber policies" (or silent cyber) refers to (re)insurance policies that are not specifically designed to explicitly cover cyber risk, but may be required to pay a cyber loss due to the absence of exclusionary language or an ambiguous policy structure.

2. Key Statistics for Insurance Groups and Commercial Insurers

As previously mentioned, the COVID-19 pandemic has highlighted the need for insurance groups and insurers to have a robust cybersecurity framework and sufficient cyber insurance protection. During 2020, commercial insurers reported a total GWP of $3.04 billion, or an increase of 2.7% from the previous year's $2.96 billion. The reported GWP in 2020 was generated from over 300,000 affirmative cyber policies (2019: over 400,000 policies), resulting in a slight increase in overall average premium per policy.

The increase in the total reported gross premiums is largely driven by the increases in direct and package policies, as shown in the graph below.

2.1 Gross vs. Net Cyber Premiums Written



Source: *BMA Calculations*

Net Written Premiums (NWP), however, slightly decreased to $1.95 billion (2019: $2.04 billion), indicating the continued use of reinsurance to manage cyber writers' overall exposure.

Data collected from the filings also show that cyber insurers continue to use reinsurance/retrocession covers to manage overall cyber exposure. Accordingly, direct policy writers cede the highest at 59% (2019: 50%) of their GWP to reinsurers, while reinsurance and package policy writers cede 25% (2019: 25%) and 26% (2019: 29%) of their GWP, respectively.

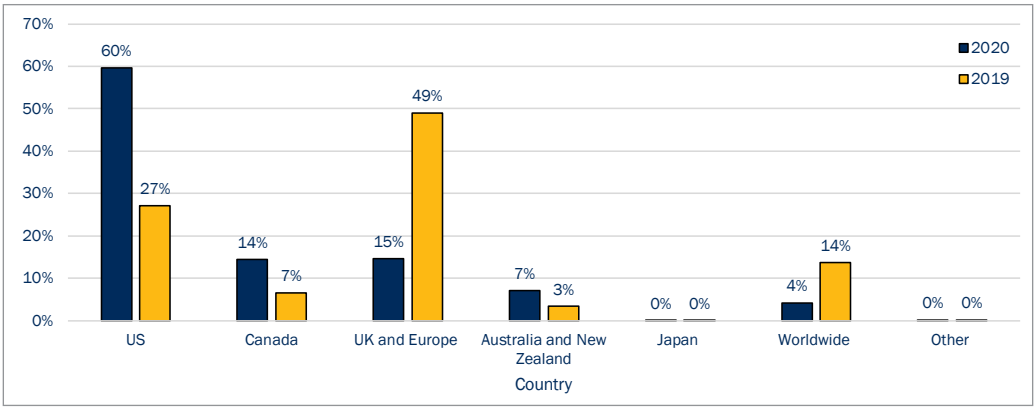
In 2020, the bulk of premiums, in value terms, written by Bermuda commercial insurers, both on a gross and net basis, continue to come from reinsurance. While the Authority expects to continue to see reinsurance covers topping the cyber offerings by Bermuda players, there is a noticeable shift in the proportion between reinsurance and direct policies, which is showing a steady rise in favor of direct policies for the last five years, as seen in the above graph.

Six commercial insurers make up 80%, which is the biggest contribution to the reinsurance premiums, writing more than $300 million each and retaining above $200 million of their GWP.

2.2 Number of Policies - Distribution by Geography

As shown below, the majority of affirmative cyber policies written by commercial insurers were for policyholders based in the US, which accounted for 60% (2019: 27%) of total policies, followed by the UK and Europe with 15% (2019: 49%) and Canada with 14% (2019: 7%). The rest of the policies were spread out among Australia and New Zealand and through worldwide covers. It is noted that there was a shift in the policy allocation from UK and Europe to US as some of the insurers have ceased to a write significant number of policies in the European Union and UK resulting in the overall policies written being lower in these locations.

2.2 Number of Policies by Country

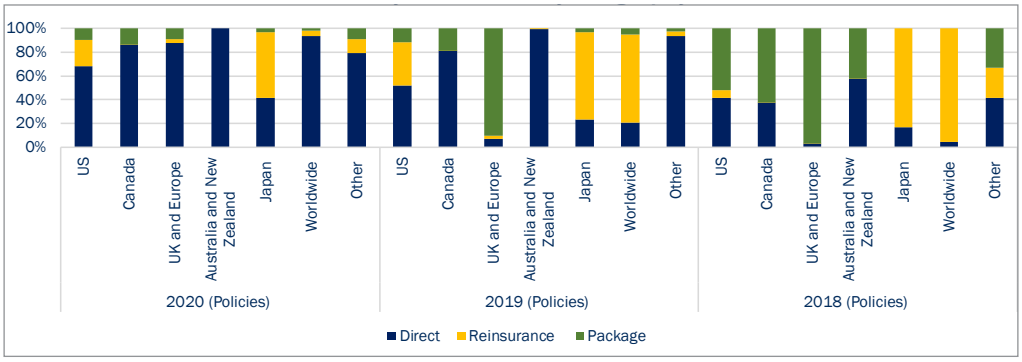


Source: BMA Calculations

For groups, affirmative cyber policies continue to cover clients in the US followed by the UK and Europe, which together contributed over 87% (2019: 80%) of total policies written. The remainder of groups' affirmative cyber policies are spread out among Canada, Australia and New Zealand, worldwide and other countries.

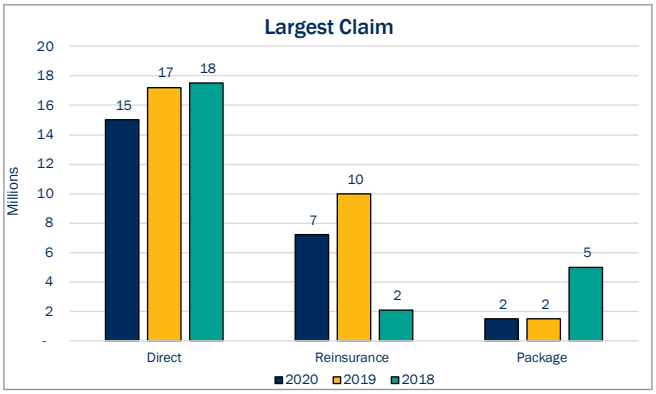
In terms of policy type, there seems to be a steady rise in the number of direct policies over reinsurance and package policies between 2019 and 2020 throughout all the major markets, consistent with the trend seen in GWP and NWP. Of particular note is the UK and Europe's switch from package to direct policies in one year as seen in the graph below. Based on this, it appears that stand-alone cyber policies continue to gain popularity, most likely as the industry begins to better understand the threats of cyber risk and the likely improvement in, and relative increase in, the available data for pricing cyber risk.

2.3 Policy Distribution by Geography



Source: BMA Calculations

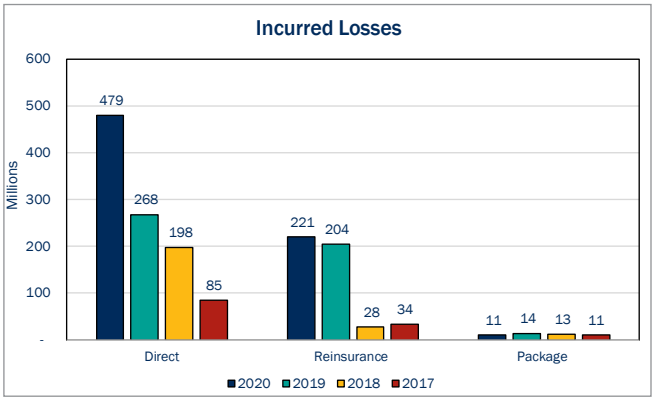
2.3 Commercial Insurer Claims Data



Source: BMA Calculations

The largest claim per underwriting category for commercial insurers generally showed a decrease in dollar value, which was approximately $15.0 million (2019: $17.2 million) for direct, $7.2 million (2019: $9.9 million) for reinsurance and $1.5 million (2019: $1.5 million) for package policies.

The largest claim for direct policies pertains to data breach, while ransomware attack is the largest reported claim for reinsurance policies.



Source: BMA Calculations

Aggregated incurred losses for commercial insurers for the year increased to $711 million (2019: $485 million). As a result, overall loss ratios to date for the cyber line increased to 37% (2019: 24%).

The increase in total incurred losses came from direct policies, consistent with the increase in premium, data breach, ransomware attack and network interruption featuring the highest types of loss event.

Cyber claims paid by commercial insurers reported an aggregate of $407 million stemming from over 8,800 claims (2019: $165 million for over 8,700 claims). An increase of approximately $221 million came from direct policies, as noted in the previous chart. Direct policies contributed 83% (2019: 70%) of the total claims paid, while reinsurance contributed 16% (2019: 29%) and package 1% (2019: 1%). Consistent with last year, a few players significantly contributed to the total claims paid. With the continued increase in the size of claims, the Authority emphasises the need for insurers to ensure that they have adequate risk management structures in place to be able to deal with a catastrophic cyber event.

3. Key Statistics for Captive Insurers

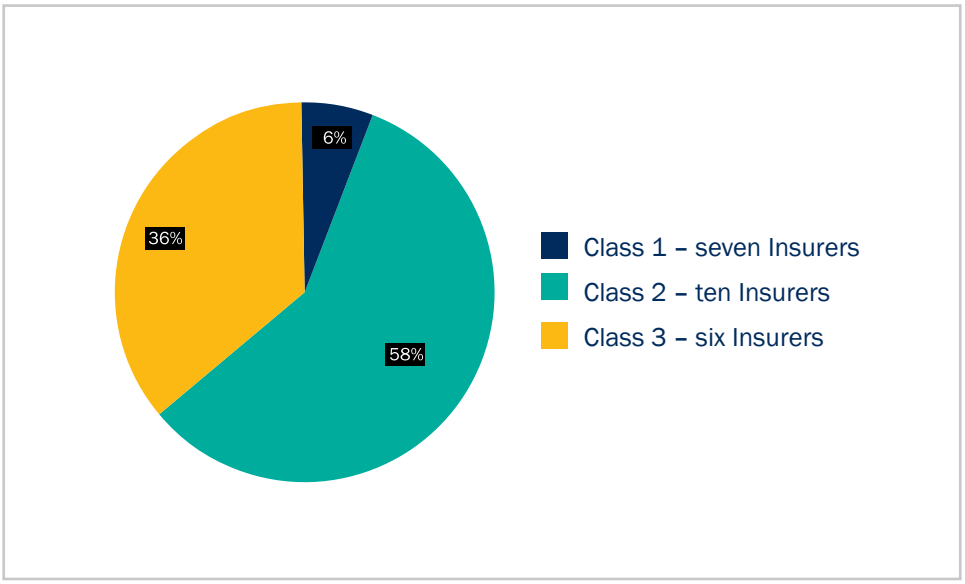
3.1 Overview

This section highlights the captives encompassing general business insurers - Classes 1, 2 and 3 writing cyber risk line of business as reported in the Electronic Statutory Financial Returns (E-SFR) for the year ended 31 December 2020.

With companies still facing the effects of COVID-19 and the recent transition to remote working arrangements, protection of company data continued to be a vital priority for all business sectors in 2020. At the height of the pandemic, companies had the opportunity to assess their needs and fine-tune their processes to ensure that their data remains well protected, highlighting the attractiveness of utilising captives as an efficient risk management tool for their overall cyber risk exposures.

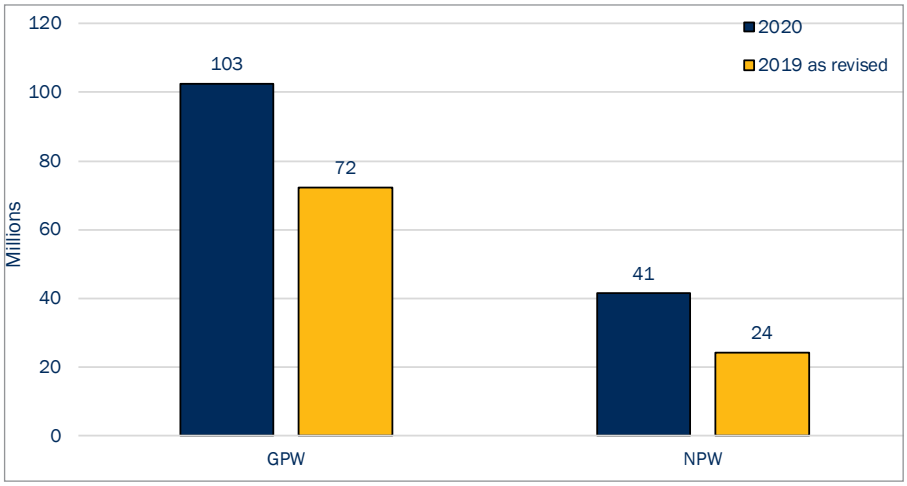
For the YE 2020, the Authority has seen an increase in cyber gross premiums written by approximately 42% (2019: 10%), with the number of captive companies writing cyber increasing from 20 to 23. Class 2 insurers dominate the overall mix, writing 58% (2019: 34%) of the total captive GWP, while Class 3 insurers trail at 36% (2019: 58%), with the remaining 6% (2019: 8%) falling within the Class 1 insurers. Nevertheless, Class 3 insurers continue to have the largest cyber GWP by a single insurer across the captive classes. The GWP by that single insurer is slightly in excess of $35 million (2019: $28 million). Of the total premium written across the Bermuda captive market, 68% (2019: 73%) is written directly by the insurers, with the remaining 32% (2019: 27%) written on a reinsurance basis.

3.1 Captive Insurers Cyber Risk Gross Written Premium



Source: BMA Calculations

3.2 Bermuda Captive Insurers Cyber Gross Written Premium and Net Written Premium



Source: BMA Calculations

As the captive market continues to prove its value to organisations in managing cyber risk exposure, the Authority expects to see a continued increase in the interest in cyber insurance within the sector as GWP for cyber business had increased by 41.9% from $72.3 million in 2019[5] to $102.6 million in 2020. The Bermuda captive market remains steady and versatile, accommodating both the new captive formations writing cyber-related exposures and the expansion of current captives adding cyber exposures or increasing premiums in existing cyber policies.

[5] 2019 figures are based on updated numbers submitted by the captives at the time of this report.

4. Cyber Underwriting Stress Scenarios

As in previous years, groups and commercial insurers were required to identify and quantify their own cyber-specific Cyber Worst-Case Scenario (Cyber WCS), particularly those that write affirmative cyber policies. Consistent with last year, groups and commercial insurers used a combination of in-house models, vendor models and publicly available cyber stress scenarios to determine their own Cyber WCS. Based on the submitted filings, there is not much change noted from last year as to the type of Cyber WCSs provided to the Authority by the insurers, including cloud service provider hack, ransomware attack, malware attack and country power outage.

For groups, aggregate Cyber WCS gross and net losses reported were approximately $4.9 billion (2019: $4.4 billion) and $2.4 billion (2019: $2.4 billion), respectively.

Commercial insurers, on the other hand, reported aggregate Cyber WCS gross and net losses of $9.5 billion (2019: $7.5 billion) and $4.4 billion (2019: $4 billion).

Overall, groups and commercial insurers are expected to meet their enhanced capital requirements after applying their own Cyber WCS; reducing their statutory capital and surplus on a gross and net basis to mean and median post Cyber WCS levels of 93% gross (94% net) and 96.7% gross (97.1% net) respectively. This continues to show the minimal impact of the affirmative cyber exposures on the Bermuda market's aggregate capital level.

However, as the Cyber WCS only accounts for affirmative cyber policies, the Authority remains concerned with the potential exposure from non-affirmative cyber. Based on 2020 filings, 42% of groups and commercial insurers continue to write non-cyber policies without explicitly providing cyber risk exclusions. As a result, aggregate potential exposure for these companies is estimated to be $26.9 billion, which is 56 times higher than the aggregate exposure for affirmative policies of these identified companies.

The Authority has designed BMA-prescribed cyber stress scenarios to help companies assess, measure and mitigate their cyber risk exposures. Designing the scenarios has been a challenge since it requires some degree of imagination and subject matter expertise to build highly severe but still plausable scenarios. The BMA has consulted the Association of Bermuda Insurers and Reinsurers' Cyber Working Group and was able to take into consideration the various points raised by the members. A draft schedule has been integrated into the BSCR model for wider consultation.

The draft scenarios consist of a systemic cloud outage, a widespread ransomware attack and a major data security breach. These scenarios were published in the 2021 YE Schedule Ve of the BSCR template to be completed on a best effort basis for the 2021 YE filing. Once finalised, this will become part of the requirement for the 2022 YE filing. The Authority's goal is to have a uniform view to measure the industry's exposure and complement the companies' assessments of their own cyber stress exposures.

5. Thematic Review of CISSA and GSSA Disclosures on Cyber Risk

In its 2020 Cyber Underwriting Report, the Authority provided its expectations for the industry on a number of areas, particularly in the management of non-affirmative cyber risk, tail risk and cyber risk accumulation. The BMA's thematic review of CISSA and GSSA filings shows a continued improvement in the disclosure of the companies' management of cyber underwriting risk. While the Authority understands that companies will have differing approaches to managing cyber, some notable observations among the top cyber writers include the following:

1. Some progress in the efforts to shift from non-affirmative and package policies to explicit and stand-alone cyber policies;
2. Setting clear risk appetites and limits for cyber risk exposure at the board level;
3. Low tolerance to cyber risk (both affirmative and non-affirmative) for some companies;
4. Using specific board committees to regularly review and monitor cyber risk exposure, particularly on cyber risk accumulation;
5. Incorporation of cyber risk exposure assessment to portfolio performance evaluation;
6. Having a more robust client-filtering process and underwriting scrutiny in relation to silent cyber exposure;
7. Using reinsurance/retrocession contracts to transfer risk and increase capacity; and
8. Seeking support from outside the traditional rated capacity via collateralised reinsurance and insurance-linked securities-based transactions.

The Authority is pleased to see these improvements and appreciates industry's efforts in this regard, particularly those who are actively offering cyber insurance products. Nevertheless, there is still a need for a large part of industry to provide more details on the nature of their cyber exposures and how companies are working to identify, quantify and manage their cyber risks as part of their CISSA and GSSA documentation. There are still many groups and commercial insurers who provided minimal information on their affirmative covers and did not include any information on cyber risk management, despite potentially having exposure to non-affirmative cyber risks, as noted in the previous section. As a result, the Authority will continue to engage with these companies respectively to improve their CISSA/GSSA disclosures as part of the respective supervisory team's engagements (e.g., onsite reviews and prudential meetings).

6. Conclusion, Expectations and Recommendations

The continuing globalisation and digitisation of business sectors, further exacerbated by COVID-19, has heightened the impact of cyber risk across all industries. While cyber line remains a relatively small part of the overall insurance offering in Bermuda (<3% of overall Bermuda GWP), the Authority notes the steady increase in the cyber market's overall premium, claims and exposures year on year. The BMA also recognises the crucial enabling role that cyber insurance plays in the digital economy. Further, current data on potential non-affirmative cyber exposures, as mentioned in Section 4, poses a significant risk to industry that warrants closer consideration.

With this in mind, the Authority maintains its view that non-affirmative cyber risks present risks and uncertainties that could amplify an insurer's risk exposures. While non-standardisation of policy wording is to be expected, particularly in the context of the Bermuda market, which is composed of writers of varying sizes and nature, there are other issues around this area that have far-reaching implications, such as, but not limited to, overlapping coverages in cyber insurance policies and types of insurance policies (e.g., business interruption, ransomware, social engineering and property damage) that need to be considered in an insurer's risk management framework for cyber risk.

The Authority also recognises other issues and challenges that groups and commercial insurers face surrounding the treatment of ransom, fines, terrorism and war risk, which raise other public policy issues relating to insurability of penalties and concerns about countering terrorism financing. Another key concern is understanding cyber risk accumulations, especially where cyber risk may entail an important systemic impact on both the insurer's own operations and in its business portfolio.

The International Association of Insurance Supervisors (IAIS) has included cyber risk underwriting among the key issues to be addressed in the context of its 2020-2024 strategic plans. As an active member of the IAIS, the BMA plans to contribute to the IAIS' efforts in providing useful guidance to the market in managing cyber risk. Given the complexity and far-reaching nature of cyber risk issues, the Authority will continue to engage the market and actively participate in international regulatory dialogues with relevant bodies in its attempt to enhance Pillar 2 regulatory and supervisory frameworks.

In light of the above points, the Authority reiterates the following recommendations to industry:

1. Silent cyber/non-affirmative cyber risk management

   Groups and commercial insurers should continue their efforts in providing clarity of cyber coverage to their policyholders. As a follow up to last year's recommendation, the Authority requires that for non-cyber policies incepting 1 January 2024, insurers must clarify whether or not they offer cyber coverage, either by including a clear exclusion language or by adding the necessary endorsements to the policies. To assist companies, bound policies before 1 January 2024 are not expected to be re-written and would be allowed to run until expiration. Nevertheless, the BMA expects the companies to ensure that any unintended exposures to non-affirmative cyber are appropriately mitigated in the interim as part of their risk management programme. For multi-year contracts, the BMA expects companies to implement the requirement as soon as it is contractually possible, such as during renewals or premium audit cycles. The Authority believes that this gives the market sufficient time to comply. Companies, at a minimum, should disclose their assessment and efforts on this area in their CISSA/GSSA submission for the 2021 YE and reflect any material updates going forward. The Authority is currently working with industry bodies and is planning on issuing a guidance note in 2022 to provide the revised reporting format in this regard.

2. Cyber stress scenario considerations and accumulation risk

As companies continue to use their own Cyber WCS to evaluate their capital levels and enterprise risk management framework, the introduction of the BMA-prescribed scenarios should provide them with an additional perspective as to where they stand in these remote but plausible stress scenarios. Accordingly, the BMA invites industry to give the Authority useful feedback on the BMA-prescribed scenarios as they complete this exercise for the coming YE filing.

In regards to their own Cyber WCS, the BMA encourages companies to continue validating their models at least once a year and, in addition, consider accumulation risk as they continue to enhance their risk management frameworks. Some issues to consider include the potential of cloud service as a single point of failure and cyber risk concentration of systemic scale. As groups and commercial insurers themselves are exposed to the same cyber threats as the companies they insure, the Authority would like industry to consider the catastrophic impact of a cyber event that can potentially halt the insurer's operations and, at the same time, requires them to pay for cyber claims from policies written. The Authority recommends that companies start articulating their assessment on these areas in their YE 2022 CISSA/GSSA submissions.

3. Operational cyber risk management

As the Insurance Sector Operational Cyber Risk Code of Conduct became enforceable beginning 1 January 2022, the Authority expects the market to have made appropriate efforts to comply with it. The BMA also invites the market to review the recently issued Bermuda Insurance Sector Operational Cyber Risk Management 2021 Report for further guidance on how their company fares against best practices set out in the code and against their peers, especially on the areas where control deficiencies are identified. Reasonable efforts must be made to comply with the recommendations in the report, as appropriate. Finally, as the cyber threat landscape continues to evolve, the Authority encourages industry to engage closely with their respective supervisors to ensure that they comply with the code and related regulations as expected.

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