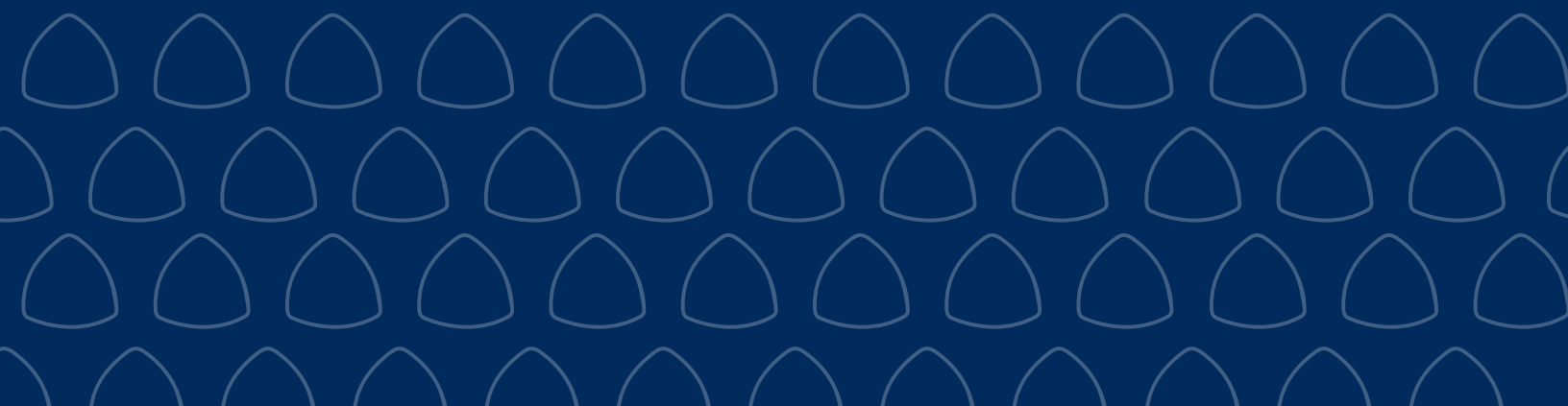




Bermuda Cyber Underwriting Report

2022



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 2021 annual filings for commercial (re)insurers¹ (Class 3A, 3B and 4), insurance groups² 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 Groups for which the BMA is the group supervisor.

² 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.

Table of Contents

1. Executive Summary	4
2. Key Statistics for Commercial Insurers	
2.1 Gross vs. Net Cyber Premiums Written	5
2.2 Number of Policies – Distribution by Country and Geography	6
2.3 Number of Policies by Country	6
2.4 Policy Distribution by Geography	6
2.5 Commercial Insurer Claims Data	7
3. Key Statistics for Captive Insurers	
3.1 Overview	9
3.2 Number of Captive Cyber Writers	9
3.3 Bermuda Captive Insurers Cyber Gross Premium Written and Net Premium Written	9
4. Cyber Underwriting Stress Scenarios	10
5. Thematic Review of CISSA and GSSA Disclosures on Cyber Risk	14
6. Expectations and Recommendations	15
7. Conclusions	17

1. Executive Summary

Over the last few years, the cyber threat landscape has continued to evolve. It has become more sophisticated, frequent and widespread, leveraging both traditional and new techniques such as ransomware, phishing, supply chain and critical infrastructure attacks, and zero-day exploits to target individuals and organisations of all sizes. Various factors introduced new security challenges, increasing cyber-attack surfaces that disrupt business operations, including critical infrastructures and supply chains. These factors include the acceleration of digitalisation due to the COVID-19 pandemic, the rise of emerging and complex business models, and a continuous move towards globalisation and the greater interconnectivity of businesses around the world. Further, the increase in legislation and regulations regarding data privacy and consumer protection has also increased the demand for cyber insurance. Similar to other lines of business, society implicitly looks at the insurance sector to provide a safety net (from a financial perspective) and promote good cybersecurity governance practices to industries in a world that has become increasingly dependent on technology.

Nevertheless, the current protection gap in cyber seems to be very high. According to a recent report by the [Global Federation of Insurance Associations](#) (GFIA), the global cyber protection gap as of 2023 is estimated to be \$0.9 trillion, second only to pensions (at \$1 trillion) but surpassing both health (\$0.8 trillion) and natural catastrophe (\$0.1 trillion). While the gap certainly provides an opportunity for insurers to expand their business, the evolving nature of this risk poses some real challenges to industry and regulators worldwide.

To this end, the Authority has proactively enhanced its regulatory and supervisory frameworks to address cyber risk from both the business and operational risk perspectives. This report covers key affirmative³ cyber risk underwriting data aggregated from 2021 financial year-end (YE) statutory filings of groups and commercial and captive insurers.

While the cyber line remains a small part of the overall Bermuda insurance market (Gross Written Premiums (GWP) of \$4.7 billion for 2021 and \$3.0 billion for 2020 (both of which remain less than 3% of overall GWP for all lines), information gathered from 2021 YE indicates that aggregate cyber loss exposures continue to be high, albeit they have slightly decreased year on year, estimated at \$194 billion gross exposure and \$108 billion net exposure (2020: \$233 and \$110 billion), respectively.

Based on the information obtained from these returns, the Authority notes that 17 groups (2020: 15 groups), 54 commercial insurers (2020: 48 commercial insurers) and 26 captive insurers (2020: 24 captive insurers) write affirmative cyber coverage.

During 2021, commercial insurers reported a total GWP of \$4.73 billion, a significant increase of 55.7% from the previous year's \$3.04 billion, with reinsurance and direct policies contributing the most. The majority of the premiums relate to United States (US) covers; however, worldwide covers have significantly increased during the year. Aggregate incurred losses increased by 69% to \$1.2 billion, with the largest claims reported being ransomware, data breach and malware. Accordingly, the largest single claim for each policy loss category reported during the year cost at least \$15 million. The overall loss ratio remains below the 40% range, but direct policies continue to be unprofitable at over 100% over both years.

In addition to market statistics, the report outlines results from the industry's first attempt to perform the BMA-prescribed cyber stress scenarios, which were only required last year on a best-efforts basis. The report then compared these outcomes against the results of the insurer's own worst-case scenario testing. Overall, most companies are still expected to meet their Enhanced Capital Requirements (ECR), post-stress for both their own and the BMA's stress scenarios. Nevertheless, a few companies were identified as falling below their Target Capital Levels (TCL) post-stress test, particularly companies whose current capital levels are already low. These insurers have been notified by their respective supervisory teams and were required to submit a detailed mitigation plan to the Authority as part of its ongoing supervisory engagement.

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.

Further, the report outlines the Authority’s findings from its thematic review of the Commercial Insurer Solvency Self-Assessment (CISSA)/Group Solvency Self-Assessment (GSSA) filings regarding disclosing the companies’ risk management approach on the various aspects of cyber risk. While some progress is noted in a few companies, a large part of the industry disclosed very little in this area.

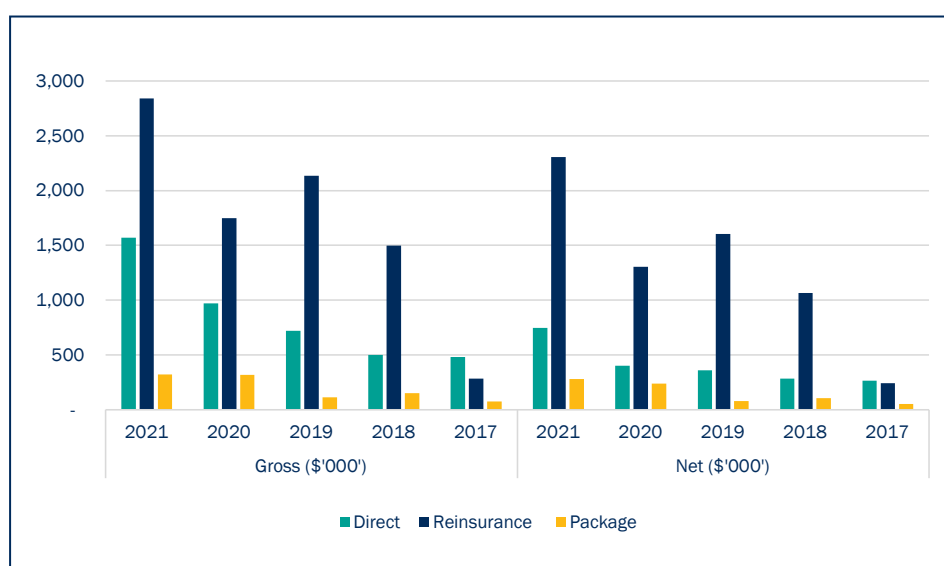
The report ends with conclusions about the market based on the current data collection and suggests expectations and recommendations for the market for the 2023 YE.

2. Key Statistics for Commercial Insurers

During 2021, commercial insurers reported a total GWP of \$4.73 billion, an increase of 55.7% from the previous year’s \$3.04 billion. Nevertheless, the number of policies shows a decrease in policy count to 200,000 affirmative cyber policies from 300,000 seen in 2020, suggesting that the growth is mainly driven by price increases rather than an increased uptake in the number of cyber policies.

Reinsurance and direct policies contributed to the overall increase in GWP, as shown in the below chart, while package policies remained flat year-over-year. This seems to indicate an increase in demand for stand-alone cyber coverage and the use of reinsurance by cyber writers to increase their capacity.

2.1 Gross vs. Net Cyber Premiums Written



Source: BMA Calculations

Similarly, Net Written Premiums (NWP) increased significantly by 70% to \$3.33 billion (2020: \$1.95 billion), indicating a continued increase in risk retention by Bermuda cyber policy writers. This is proven further when looking closely at the ceding levels per policy type, which show a declining trend; direct policy writers ceded 52% of their GWP in 2021 (2020: 59%), while reinsurance writers ceded 19% (2020: 25%) and package policy writers ceded only 13% (2020: 26%).

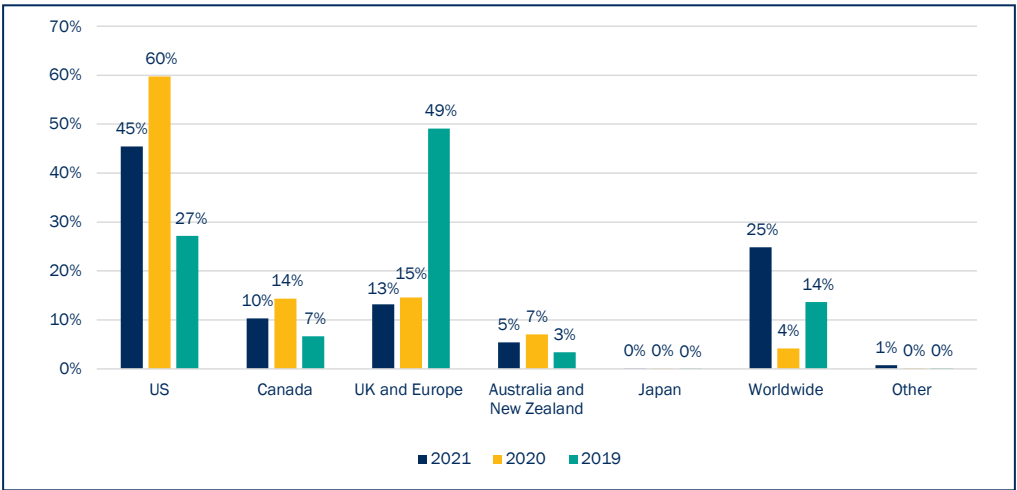
As with previous years, the bulk of premiums written by Bermuda commercial insurers, both on a gross and net basis, continue to come from reinsurance policies.

Further, a few prominent players (13 commercial insurers) made up 80% of the overall GWP in 2021, more than doubling the number from 2020—where six commercial insurers made up 80% of the overall GWP—with at least \$100 million in GWP written each year.

2.2 Number of Policies – Distribution by Country and Geography

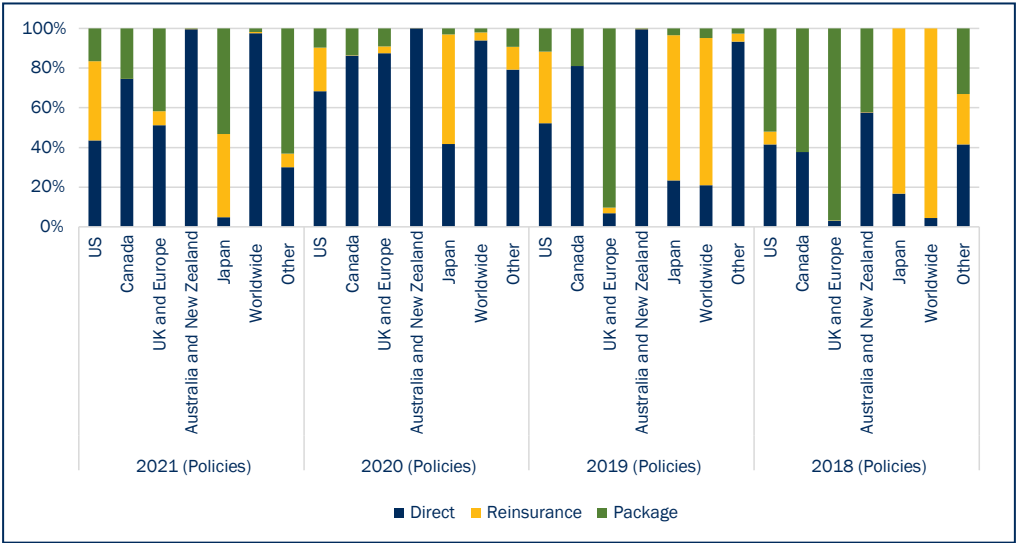
While the US still accounted for the majority of the number of policies written (2021: 45%, 2020: 60%), this year saw a significant rise in worldwide covers, now accounting for 25% (2020: 4%), only followed by the United Kingdom (UK) and Europe with 13% (2020: 15%) and Canada with 10% (2020: 14%). This seems to validate the BMA’s observation in the last few years that the cyber risk landscape has become more global in reach.

2.3 Number of Policies by Country



Source: BMA Calculations

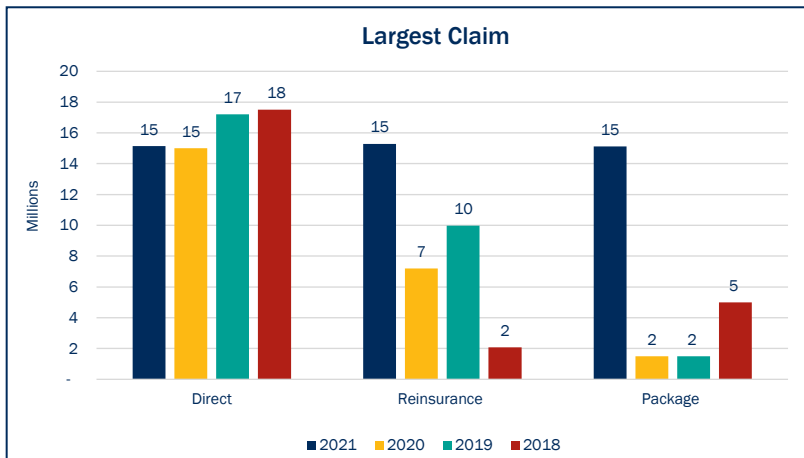
2.4 Policy Distribution by Geography



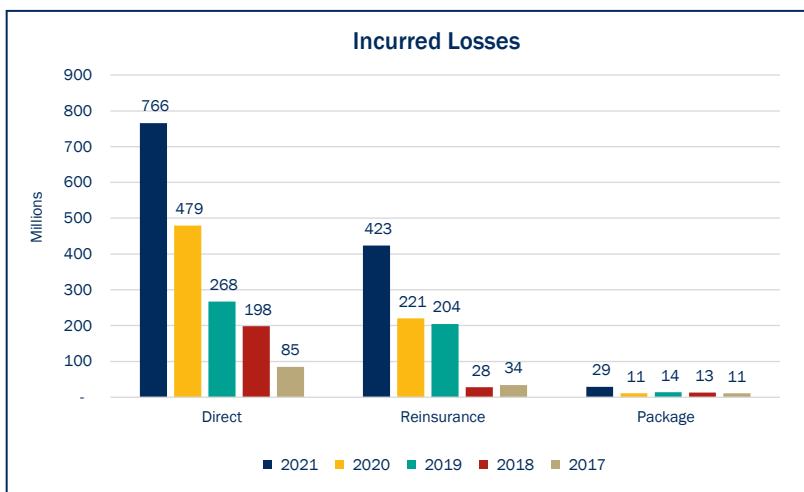
Source: BMA Calculations

Meanwhile, direct covers continue to be the largest policy type offered in most markets in terms of the number of policies. Nevertheless, there also seems to be a growing trend for the more developed markets (i.e., US, Canada, UK and Europe, and Japan) to progress towards a more balanced distribution between direct, reinsurance and package policies, as seen in the chart above, which is to be expected as the cyber line continues to mature.

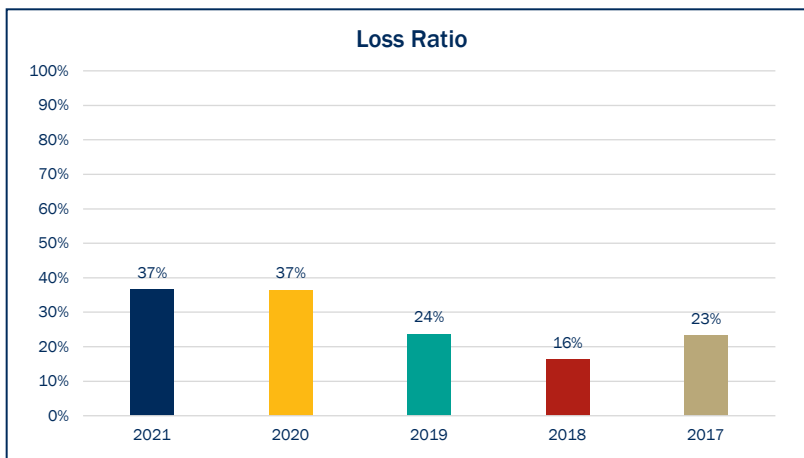
2.5 Commercial Insurer Claims Data



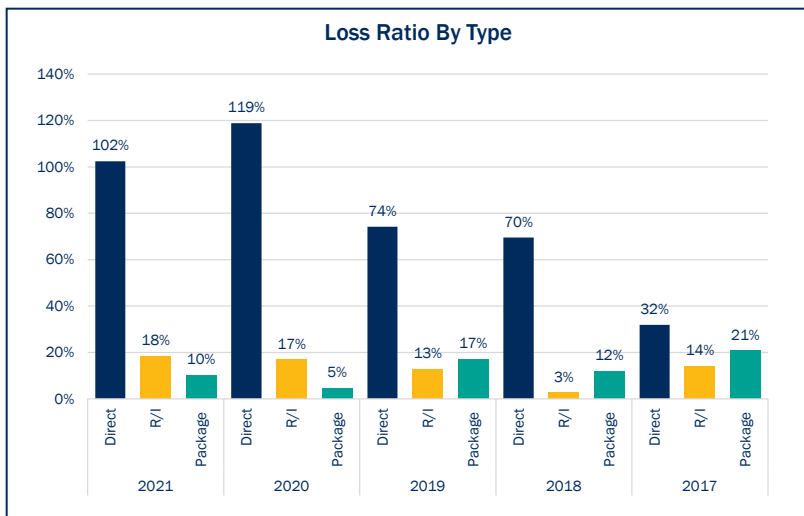
The largest claim per underwriting category reported for commercial insurers was reported at approximately \$15.1 million for data breaches for direct policies, (2020: \$15.0 million for data breaches), while reinsurance policies reported \$15.3 million for ransomware (2020: \$7.2 million for ransomware), and package policies reported its largest claim to be \$15.1 million for malware (2020: \$1.5 million for data breaches).



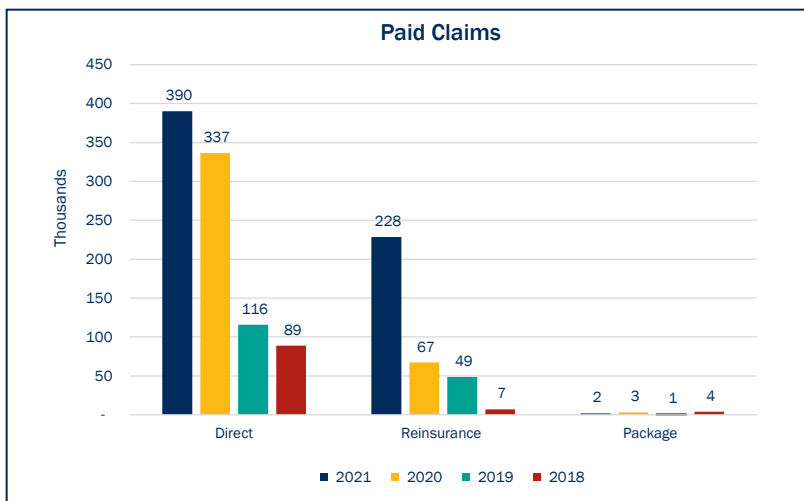
Aggregate incurred losses for commercial insurers for the year increased to a total of \$1.2 billion (2020: \$711 million), with direct policies contributing over 50% of the total, followed by reinsurance.



When coupled with the increase in GWP noted in the previous section, overall loss ratios to date for the cyber line remained the same at 37% (2020: 37%). The increase in total incurred losses came from direct and reinsurance policies, consistent with the increase in premium, with data breaches, ransomware attacks and network interruptions featuring the highest loss events.



When analysing by policy type, however, a different picture is painted. Incurred losses for direct policies have been over 100% of GWP for two years, compared to the lower ratios seen on reinsurance and package policies (below 20% in both years), indicating continuous volatility of cyber lines and the apparent immaturity in loss modelling methodologies at the primary insurance layers.



Meanwhile, cyber claims paid by commercial insurers reported an aggregate of \$620 million, stemming from over 16,900 claims (2020: \$407 million for over 8,800 claims). An increase of approximately \$287 million came from direct policies, as noted in the previous chart (2020: \$221 million).

Further, direct policies contributed 63% (2020: 83%) of the total claims paid, while reinsurance contributed 36% (2020: 16%) and package 1% (2020: 1%).

Consistent with last year, just a few companies significantly contributed to the aggregate total claims paid. With the continued increase in the size of claims year on year, the Authority continues to emphasise the need for insurers to have robust and integrated 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 captive sector, encompassing general business insurers (Class 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 2021.

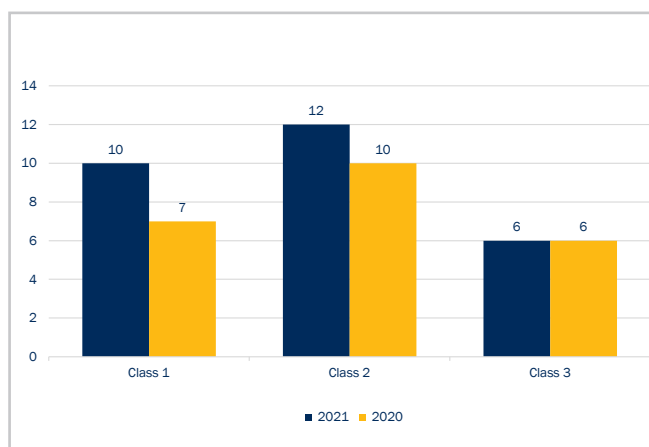
For 2021, cyber risk has been identified as one of the major emerging risks within the Bermuda captive market. Bermuda captives and their parent companies continue to closely monitor the cyber risk exposures of their organisations, with a view of effectively and efficiently managing both the exposure and increasing cost of placing cyber cover in the commercial market.

In 2021, the Authority saw the cyber gross premiums written increase by approximately 48% (2020: 42%) and the number of captive companies writing cyber increased from 23 to 28. Class 2 insurers continue to dominate the overall mix, writing 52% (2020: 58%) of the total captive GWP, while Class 3 insurers followed at 43% (2020: 36%), and Class 1 insurers at 4% (2020: 6%).

Nevertheless, a large part of the GWP was written by a single insurer, contributing approximately \$60 million (2020: \$35.6 million) of the total.

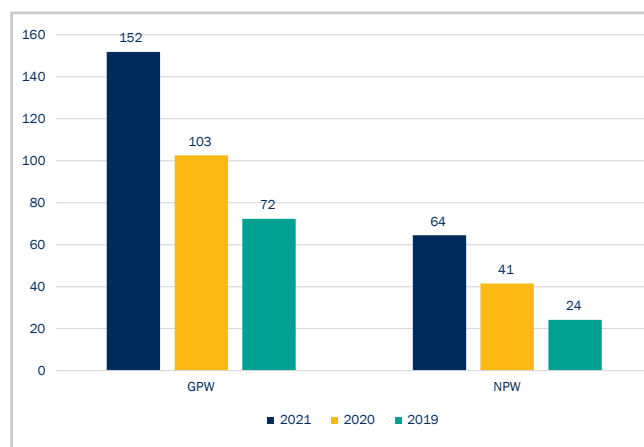
Further, of the total premium written across the Bermuda captive market, 56% (2020: 68%) was written directly by insurers, with the remaining 44% (2020: 32%) written on a reinsurance basis.

3.2 Number of Captive Cyber Writers



Source: BMA Calculations

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



Source: BMA Calculations

The use of captive insurers as part of a company's overall risk mitigation strategy allows for customisations to fit the company's specific needs and risk profile in a way that traditional carriers cannot currently address, giving companies greater control over their insurance coverage and potentially lowering their overall insurance costs.

Based on the steady growth of cyber insurance activity seen in the last three years, the captive market continues to prove its use as an effective tool to manage cyber insurance risk for companies regardless of the industry.

4. Cyber Underwriting Stress Scenarios

Insurer's Own Cyber Worst-Case Scenario Results

As in previous years, groups and commercial insurers were required to identify and quantify their own cyber-specific Cyber Worst-Case Scenario (CWCS), 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 CWCS. Based on the submitted filings, minimal change was noted over last year regarding the type of CWCSs provided to the Authority by the insurers. The most commonly mentioned types of CWCS continued to be cloud service provider hacks, ransomware attacks, malware attacks and country-wide power outages.

For groups, aggregate CWCS gross and net losses reported significantly increased to \$9.5 billion (2020: \$4.9 billion) and \$4.2 billion (2020: \$2.4 billion), respectively. Accordingly, applicable policy limits for these CWCSs are estimated to be an aggregate of \$89.8 billion (2020: \$184 billion) and \$32 billion (2020: \$86.4 billion) on a gross and net basis, respectively. To put these numbers into perspective, the current year aggregate policy limit is about the same level as the ten-year average industry loss of \$81 billion for natural catastrophes reported in 2022, [according to Swiss Re](#).

On the other hand, commercial insurers reported aggregate modelled CWCS gross and net losses of \$7.3 billion (2020: \$6.4 billion) and \$5.1 billion (2020: \$4.4 billion). While this is lower than the groups, applicable policy limits for these CWCSs are estimated to be an aggregate of \$1.8 trillion (2020: \$3.9 trillion) and \$1.1 trillion (2020: \$2.8 trillion) on a gross and net basis, respectively.

Applying the modelled CWCS losses indicated above to the Bermuda market's aggregate statutory capital and surplus, groups and commercial insurers are still expected to meet their ECR, being reduced only to mean and median post-CWCS levels of 92.2% gross (95.4% net) and 96.2% gross (97.3% net), respectively.

On an individual basis, however, the Authority noted a few commercial insurers who had minimal capital buffers and, consequently, fell below their target capital levels (120%) post-CWCS. These insurers have been notified by their respective supervisory teams and were required to submit a detailed mitigation plan to the Authority as part of its ongoing supervisory engagement.

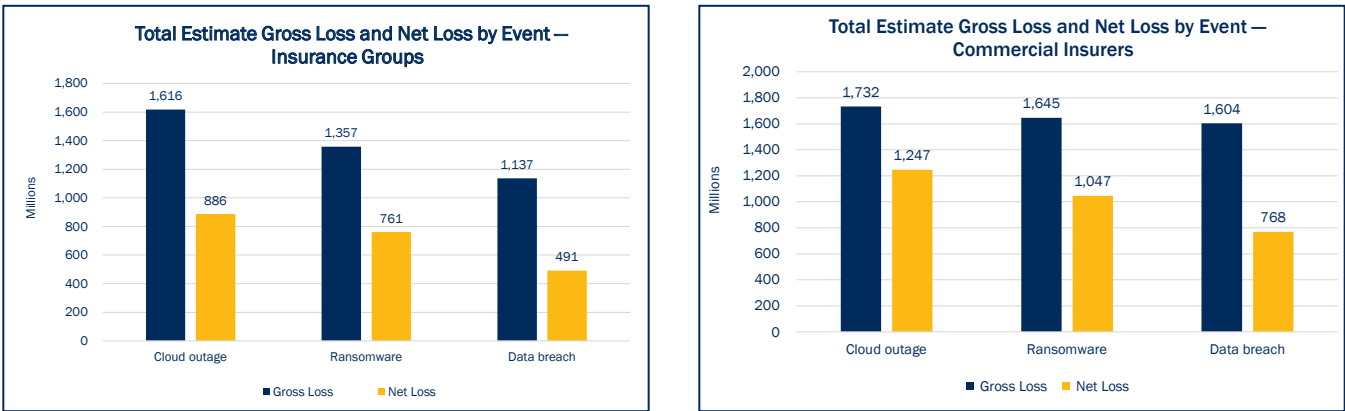
BMA-Prescribed Cyber Worst-Case Scenarios

To standardise its market analysis on the impact of extreme cyber events, the Authority designed its own prescribed cyber stress scenarios in 2022, which complemented the companies' stress tests to assess, measure and mitigate their cyber risk exposures.

The BMA engaged with the Association of Bermuda Insurers and Reinsurers' (ABIR) Cyber Working Group to obtain valuable input from the members and take it into consideration in the final scenarios. The scenarios were integrated into the Bermuda Solvency Capital Requirement (BSCR) model, and this is the first year that the Authority was able to gather such information for analysis and publication.

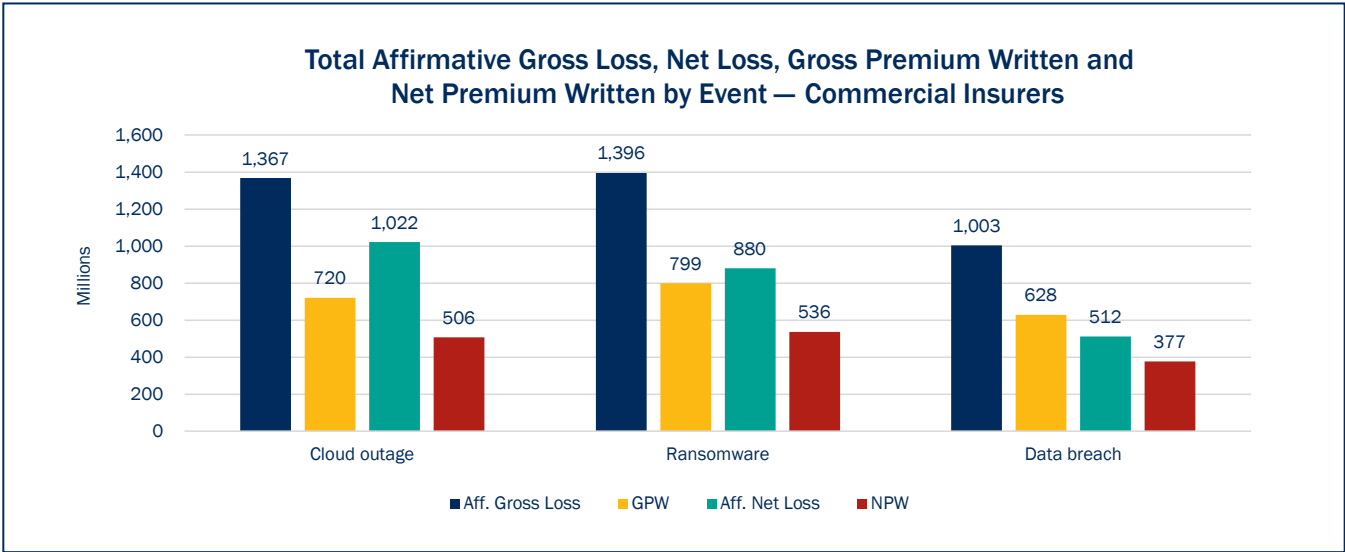
The scenarios consist of a systemic cloud outage, a widespread ransomware attack and a major data security breach. In this exercise, companies were required to estimate and report their affirmative and non-affirmative exposures for each scenario to the Authority on a best-effort basis.

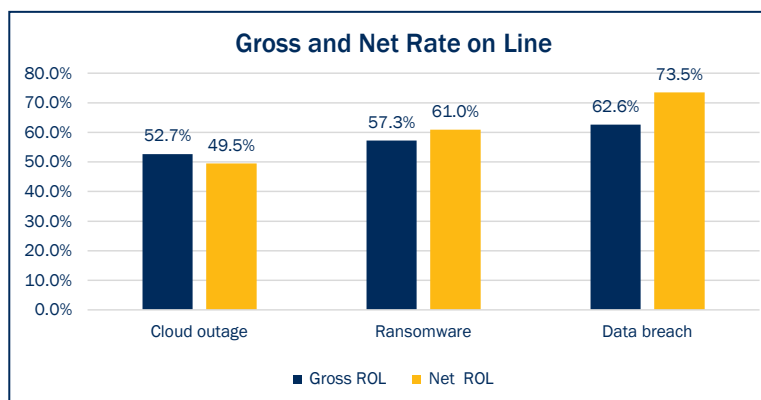
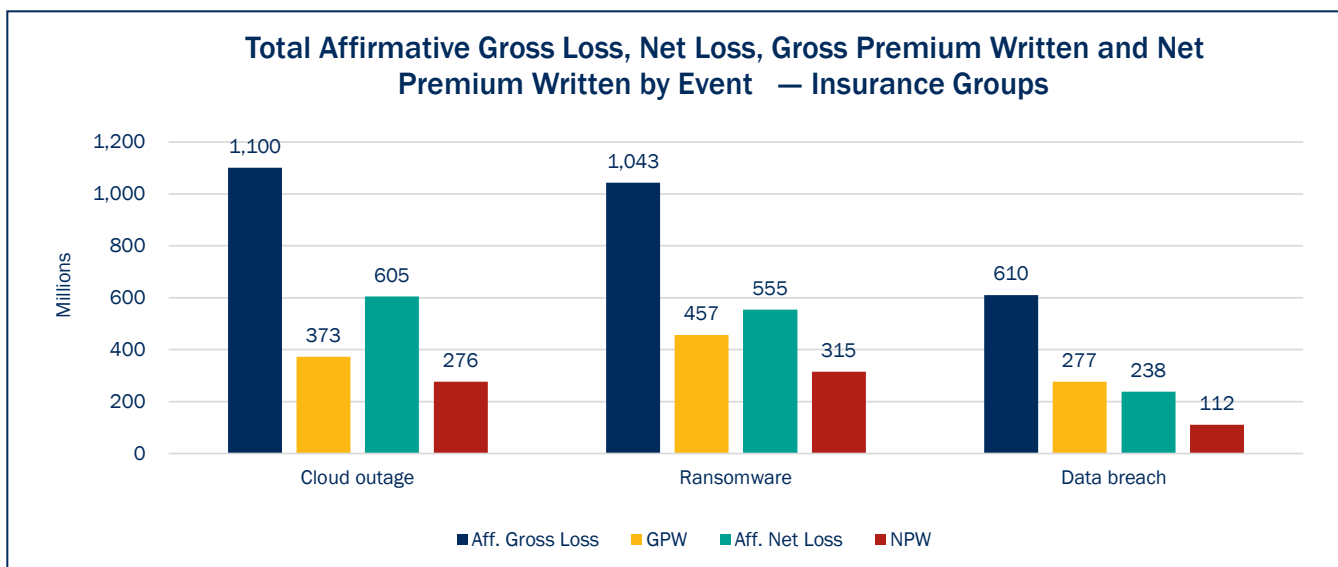
The following charts outline the aggregated results of the companies that estimated the BMA-prescribed CWCS:



Accordingly, cloud outage returned the highest aggregate loss at \$1.7 billion, albeit the numbers were closely followed by ransomware and data breach events on a gross basis. Insurance groups, accordingly, retained much lower risk than commercial insurers, as seen in the above charts.

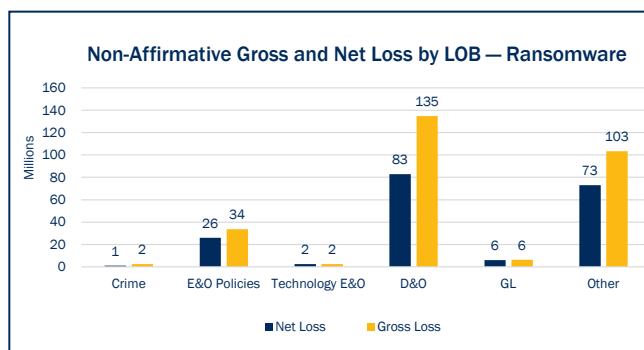
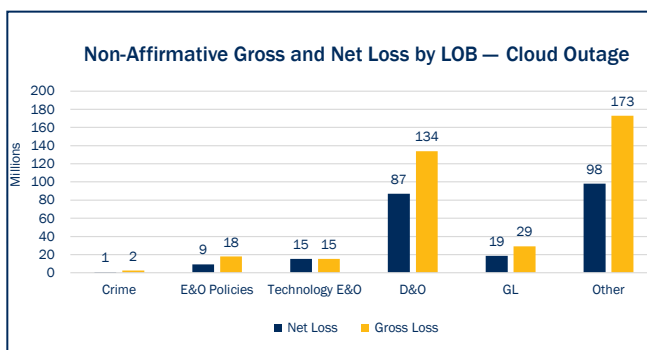
The Authority required industry to estimate their gross and net loss exposures for each of the three prescribed stress scenarios, breaking down between affirmative and non-affirmative exposures. Premiums corresponding to each of the stress scenarios were also required to estimate premium adequacy for affirmative covers. The below charts outline this information.

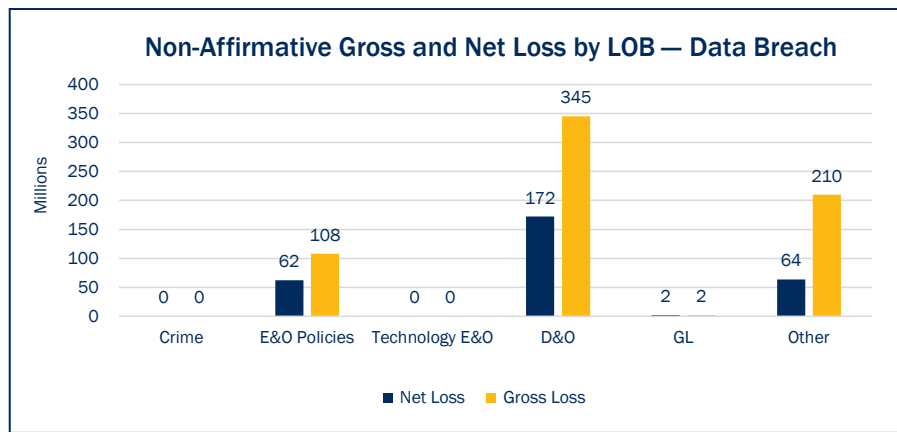




Accordingly, the premium for the estimated worse-case loss ratio ranged between 49% to 74%, relatively higher than the other lines of business.

The charts below expand the analysis to non-affirmative exposures for each stress scenario and show the estimated losses per non-cyber line that are likely to respond to the cyber stress test event for the categories of Crime, Errors and Omissions (E&O), Policies Technology E&O, Directors and Officers (D&O), General liability (GL) and other.



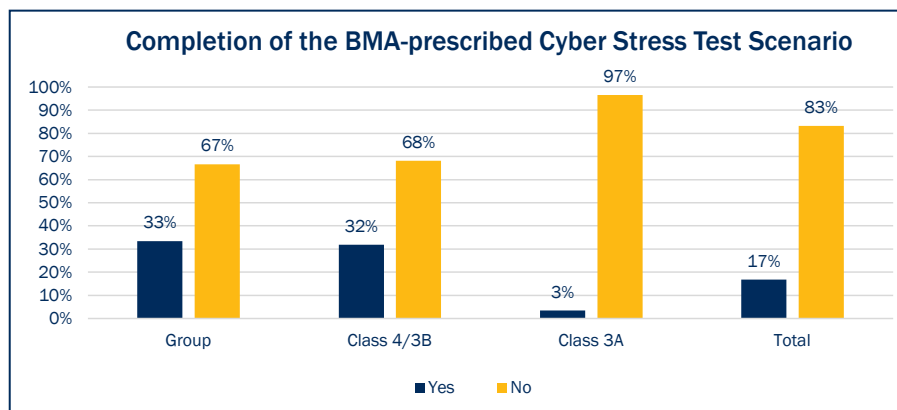


In most cases, D&O policies returned the highest exposures among the lines of business to respond to cyber events, closely followed by the ‘Others’ category. The Authority may require the industry to break down this category for the next YE filing to obtain more information about these non-cyber lines of business that are likely to respond to cyber events.

When asked about the occurrence return period for each worst-case scenario, most companies responded either a ‘1-in-100-year event’ or a ‘1-in-200-year event’ as the likelihood in which the prescribed scenarios may occur according to their models. Most companies also indicated that they used proprietary loss models or a combination of published vendor and bespoke models to estimate their exposures under the prescribed worst-case scenarios.

ECR levels were only slightly reduced when applying the respective gross and net loss estimates for each cyber stress scenario to each company's statutory capital and surplus, ranging between one to three basis points reduction from their pre-stress ECR levels. This is largely consistent with the Authority's observations when using the companies' worst-case scenarios described in the previous section. Nevertheless, similar to what is noted in the previous section, a few insurers reported that their post-stress ECRs fell below their TCL (120%) as their pre-stress ECRs closely approximated their TCLs.

It should be noted, however, that the above insights may not necessarily reflect the actual state of the Bermuda market, as many of the companies did not complete the BMA-prescribed stress test section for various reasons. The following chart shows the number of companies broken out by insurance class that did not complete the section.



As this is only the first year that the BMA implemented this stress test requirement, the market was given the option to complete this section on a voluntary and best-efforts basis. Moreover, a materiality threshold has also been provided to the market to guide the companies on whether or not they are required to complete

the section. Nonetheless, the initial results validate most of the outcomes when using the companies' own worst-case scenarios. The Authority is looking to engage industry further through the supervisory teams to get more context on those companies that did not complete this year's stress testing exercise. The exercise will also become mandatory for those who have met the BMA's materiality thresholds for next year's filing.

Non-affirmative cyber exposure

The Authority also required the companies to indicate on each of their non-cyber statutory line of business whether they have explicit exclusion clauses for cyber risks in place. Accordingly, about 42% (for 2021 and 2020) of the total groups and commercial insurers do not have explicit cyber risk exclusions in their portfolios. As a result, aggregate potential non-affirmative cyber exposure for these companies is estimated to be \$5.5 billion (2020: \$5.3 billion), which is 14 times higher (2020: 56 times higher) than the aggregate exposure for affirmative policies of these identified companies. While the gap between affirmative and non-affirmative exposure has decreased year on year, this area will continue to be one of the Authority's supervisory focuses.

Further, although having exclusionary language is the logical step to managing non-affirmative cyber risk exposures, the Authority also recognises that newly introduced exclusionary language has not been tested yet in all courts in most jurisdictions, so there remains some level of uncertainty in the effectiveness of such approach. Therefore, the Authority will continue to engage with the market to ensure that the companies adequately monitor their non-affirmative cyber risk exposures.

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

In the previous year's report, the Authority reminded companies to improve their CISSA and GSSA disclosures on cyber risk, particularly in the management of their affirmative and non-affirmative cyber risk exposures, cyber stress scenario and accumulation risk considerations, and disclosing their efforts in providing more clarity to their clients regarding cyber coverage on non-cyber policies.

Upon review of this year's filings, the BMA noted some improvements in a few companies, particularly those that write significant cyber risk. A number of large cyber writers have disclosed that they are largely complete or well underway in transforming their non-affirmative exposures into affirmative covers, as appropriate, or in providing the necessary exclusions to limit their exposures, mostly driven by similar initiatives in other jurisdictions such as Lloyd's of London's mandate to require companies to have cyber exclusions in place for all non-cyber lines.

The BMA is also pleased to see a few of Bermuda's largest cyber writers making significant progress in developing their risk appetites and tolerances on cyber risk and further developing their modelling capabilities for non-affirmative cyber loss scenarios. Some insurers have been actively enhancing their mitigation plans while seizing market opportunities, where appropriate, as part of their long-term strategy in this line of business. In addition, most cyber writers use reinsurance protection to ensure a comprehensive risk management approach.

Nevertheless, a material part of the Bermuda market still does not provide sufficient details on the nature of their cyber exposures and how they are working to identify, quantify and manage their cyber risk. A handful of large cyber writers do not disclose adequate information on their CISSA/GSSA, despite this line being one of their largest premium allocations. A significant percentage of the Class 3A and Class 3B cyber writers continue to have inadequate CISSA/GSSA disclosures despite having been notified in previous years about the BMA's requirements.

One notable gap that the BMA observed in its thematic review is the companies' disclosures regarding their cyber stress testing outcomes, both from their own and the BMA's prescribed cyber stress scenarios. Most companies also did not disclose their mitigation and recovery plans in response to these outcomes. The supervisors of these companies have been advised and will engage with these companies more closely this year to improve their CISSA/GSSA documentation.

6. Recommendations and Conclusion

The Authority would like to reiterate to companies the following expectations and recommendations for the purpose of next year's filing.

1. Silent cyber/non-affirmative cyber risk management

It is important that policyholders understand the scope of their coverage to allow them to make informed decisions when purchasing cyber (and non-cyber) covers. In this regard, groups and commercial insurers should continue their efforts to provide clarity of cyber coverage to their policyholders. The Authority has communicated in its 2021 report that companies must clarify whether or not they offer cyber coverage, either by including clear exclusion language or by adding the necessary endorsements or sub-limits to the policies beginning 1 January 2024. Bound policies before 1 January 2024 are not expected to be re-written and would be allowed to run until expiration to assist companies. For multi-year contracts, the BMA expects companies to implement this requirement as soon as contractually possible, such as during renewals or premium audit cycles.

Nonetheless, the Authority recognises that in some instances, explicit exclusions and contract language modifications are impossible, such as for policies governed by specific statutes (as in the case of workers' compensation or motor policies). In these instances, companies are asked to adequately disclose their respective circumstances in their CISSA/GSSA filing and their mitigation plans to contain their silent cyber risks within these lines.

At a minimum, companies should disclose their assessment and efforts in this area within their CISSA/GSSA submission for the 2023 YE and reflect on any material updates going forward. The BMA also requires companies to assess any unintended exposures to non-affirmative cyber and employ appropriate mitigations as part of their broader risk management programme.

2. Cyber stress scenario considerations and accumulation risk

With the BMA's publication of its own prescribed cyber stress scenarios, the Authority requires companies to consider the impact on their portfolio, reflecting both their own stress testing results and that of the BMA's. The BMA also recommends that companies review, at least annually, the impact of these various loss scenarios and work to enhance their modelling capabilities as their business grows. Tail risk, and the potential accumulation and systemic impact of these scenarios, should also be regularly assessed and considered in the companies' risk management frameworks, with the outcomes and management plans being disclosed in their CISSA/GSSA.

3. Operational cyber risk management

As the cyber threat landscape continues to expand each year, the Authority recognises that cyber insurers are also targets of cyber-attacks and breaches. The Authority, therefore, requires companies to continuously review their compliance with the applicable Bermuda [Insurance Sector Code of Conduct](#), which has been in place since 2022, to ensure that they abide by best practices.

Operational cyber risk management continued

Further, the market is invited to review the recently issued [Bermuda Insurance Sector Operational Cyber Risk Management 2022 Report](#) for further guidance on how their company fares against best practices set out in the code and against their peers, especially in areas where control deficiencies are identified.

Accordingly, some improvements are needed in a number of areas, in particular on third-party cyber risk management, data classification and data loss prevention controls. The Authority will engage with the companies, as appropriate, through the supervisors in coordination with the Cyber Risk Department on these areas.

7. Conclusion

While the cyber line remains a relatively small part of the overall insurance offering in Bermuda (<3% of overall Bermuda GWP for 2021 and 2022), the Authority notes the continued increase in the cyber market's overall premium, claims and estimated exposure over the last five years, as outlined in previous sections.

The BMA also recognises the important role of the Bermuda market in addressing the global cyber protection gap, which is estimated to be about 0.9 trillion, according to [Global Federation of Insurance Associations](#). As of this writing, Bermuda cyber writers contribute to roughly 35% of the global cyber GWP reported by the [Global Insurance Market Report](#) (GIMAR) published by International Association of Insurance Supervisors. Further, about a third of the global claims in that report were either reinsured directly by a Bermuda entity or consolidated into a Bermuda entity in 2022. Given this and the evolving nature of cyber risk, it is important for the Authority to continue to enhance its regulatory and supervisory frameworks in an effort to ensure that Bermuda cyber insurers are resilient, not only from a capital and liquidity adequacy point of view but also from an operational perspective, by promoting robust risk management practices.

To achieve this, the BMA will continue its consultative approach to policymaking and regularly engage with various industry stakeholders, particularly the industry associations (e.g., ABIR's Cyber Working Group), cybersecurity firms, modelling firms and rating agencies. Further, the BMA's innovative framework aims to encourage market innovation and development to promote the creation of enhanced and new cyber insurance products that address current threats to help close the protection gap, as well as address emerging threats.

Finally, the Authority will continue to collaborate and actively contribute to global discussions in international forums to share information, best practices and insights on cyber risk to drive the direction of policymaking in this area.

These approaches will help the Authority stay informed about emerging cyber threats and fulfill its mandate of protecting policyholders and promoting financial stability while actively contributing to developing a robust cyber insurance market.



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