BMA
BERMUDA MONETARY AUTHORITY

Bermuda Cyber Underwriting Report

2023

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 2022 annual filings for commercial 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 for the industry regarding cyber insurance underwriting.

The market is invited to review the content and insights provided in this report and contact the Authority with any feedback, questions or concerns at enquiries@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 the 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, HM12

P.O. Box 2447
Hamilton HMJX
Bermuda

Tel: (441) 295 5278

E-mail: enquiries@bma.bm

This publication is available on the BMA's 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] Insurance Groups for which the BMA is the group supervisor.

Table of Contents

1. Executive Summary

The cyber insurance landscape has undergone significant transformation in the last five years, driven by increasing scale and sophistication of cyberattacks globally. Emerging technologies, notably the rise of generative AI, show strong potential to exacerbate cyber risks by enabling more sophisticated and targeted attacks and increasing the demand for cyber insurance products across industries. Recent data indicates a significant increase in cyberattacks targeting Small and Medium-sized Enterprises (SMEs).

According to Tripwire, 73% of small business owners reported experiencing data breaches or cyberattacks in 2023, a substantial rise from previous years. This trend underscores the growing vulnerability of SMEs, which often have fewer tools and technical resources to defend against sophisticated cyber threats compared to larger organisations. With the evolution of the cyber threat landscape, the cyber insurance market has also responded with substantial growth and diversification in policy offerings, as outlined in this report, coupled with some improvements in terms of cyber modelling capabilities by the market in general.

The global cyber insurance market was valued at $13.5 billion in 2023 and is projected to grow to $120.47 billion by 2032, exhibiting a 24.5% compounded annual growth rate, according to Fortune Business Insights. However, while the cyber insurance market grows in value, cybercrime is also estimated to cost between $6 to 10 trillion annually, dwarfing the size of insurance coverage in place, according to CyberCube.

As one of the leading global reinsurance hubs, Bermuda provides significant capacity for cyber insurance risks. A substantial portion of the global cyber insurance premiums is either ceded to Bermuda-based reinsurers or consolidated into a Bermuda group or a large Bermuda commercial insurer. Bermuda is also home to the greatest number of cyber captives as well as large Insurance-Linked Securities (ILS) vehicles. This provides reinsurance capacity to traditional insurers to cover their own risk and enables cyber insurance coverage for large-scale and systemic cyber events. In consideration of this, the Authority continues to view cyber risk as a critical risk that requires ongoing review and a tailored approach in implementing its regulatory and supervisory frameworks.

The report begins with an update on key Bermuda market statistics from 2022 year-end (YE) filings. The report demonstrates significant growth over the previous year, with commercial insurers reporting a total cyber insurance Gross Written Premium (GWP) of **$7.75 billion**, marking a 63.7% increase from the prior year's $4.73 billion. The aggregate number of cyber insurance policies also surged from 200,000 in 2021 to **500,000** in 2022. Reinsurance policies continue to dominate the market, accounting for 58% of the overall distribution in GWP, while direct and package policies also saw significant growth. Geographically, the United States continues to lead in the number of policies written, accounting for 49% in 2022 (up from 45% in 2021), followed by worldwide covers (20%), the United Kingdom (14%) and Canada (12%).

Incurred losses on the other hand remained stable at **$1.2 billion** aggregate in 2022, with reinsurance policies contributing nearly 50% of the total. Loss ratios appear to have improved significantly, with an overall loss ratio of 22% in 2022 compared to 37% in 2021. This is comparable to the decrease in the global cyber loss ratio from 43% to 68% previously, likely driven by both increases in premium rates and lower losses reported during the year.

The Bermuda captive insurance sector also experienced steady growth, with cyber GWP increasing by 14% to **$172 million** in 2022, coupled with an increase in the number of captive insurers offering cyber policies.

This report further showed aggregate information regarding the results of the stress/scenario testing exercise required by the BMA as part of the YE regulatory filings, comparing the outcomes between the company's own stress testing and the BMA's prescribed Cyber Worst Case Scenarios (CWCS). On the aggregate, the market is generally resilient in terms of capital levels after applying post-cyber stress scenarios. However, a number of insurers are expected to fall below their Enhanced Capital Requirement (ECR) ratio. This highlights the need for insurers to monitor and enhance their capital buffers to manage this risk.

This report also indicates improved data for the number of companies explicitly stating that they do not have exclusions in place for non-cyber policies. Responding to feedback from the market during the year, the Authority provided further clarification, guidance and practical examples pertaining to the implementation of the guidelines that were issued in the previous year. Beginning 1 January 2024, companies were required to explicitly state within their policies whether or not cyber triggers are covered in non-cyber policies. The BMA also provided specific guidance on the key areas to be incorporated in the company's Commercial Insurer's Solvency Self Assessments (CISSAs)/Group Solvency Self-Assessment (GSSAs). Overall, while the insurance industry has made strides in managing silent cyber exposures, data shows that the risk remains substantial. Continued efforts in policy clarification, risk assessment and regulatory collaboration are essential to effectively mitigating and managing these risks.

Furthermore, this report highlights the role of the cyber ILS sector, which currently shows significant potential for growth over the next few years. In 2023, Bermuda-based ILS vehicles issued a total of **$670 million** of aggregate insurance protection in cyber-specific ILS, which provided critical additional capacity to meet the rising demand for cyber insurance protection.

Companies were also reminded to review their ongoing compliance with the Insurance Sector Operational Cyber Code of Conduct and to refer to the recently issued *Operational Cyber Risk Management Report 2023* to address deficiencies and continuously improve their governance and risk management frameworks.

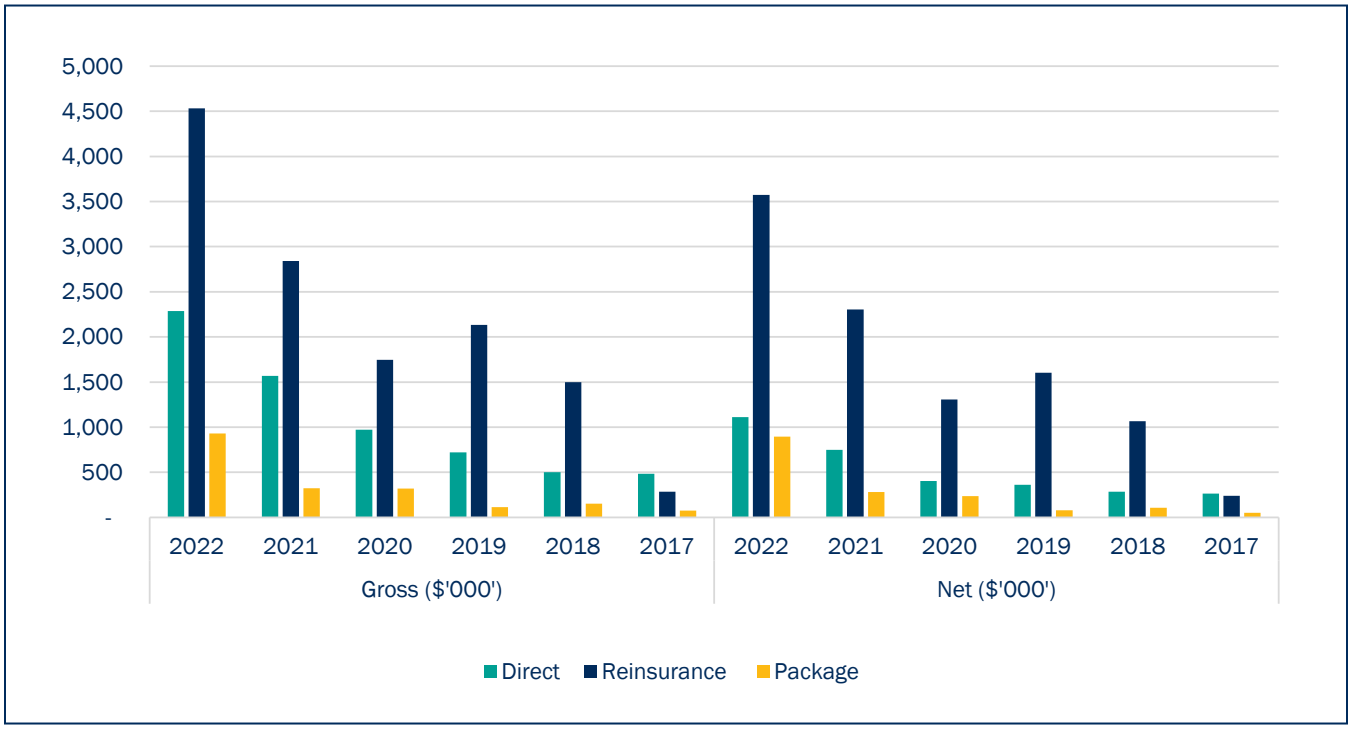
Finally, this report recognises Bermuda's pivotal role in covering a substantial portion of the cyber protection gap within the global cyber insurance landscape. Enhancements to the BMA requirements and guidance are also outlined, which include the removal of the materiality threshold and making the completion of the BMA-prescribed CWCS mandatory for all groups and commercial insurers regardless of their size, increased supervisory reviews of CISSA and GSSA submissions for the following year's filing, and the publication of a subsequent guidance note on cyber underwriting next year.

2. Key Statistics for Commercial Insurers

During 2022, commercial insurers reported a total cyber insurance GWP of **$7.75 billion**, an increase of 63.7% from the previous year's $4.73 billion. This is consistent with the rise in the number of policies written (500,000 affirmative cyber policies compared to 200,000 for 2021), suggesting a significant growth year on year in both the number of policies and premium rates.

As we look closely at the types of policies issued, reinsurance continues to dominate, accounting for 58% of GWP's overall distribution of policies, while direct and package policies have also significantly increased, respectively.

2.1 Gross versus Net Cyber Premiums Written



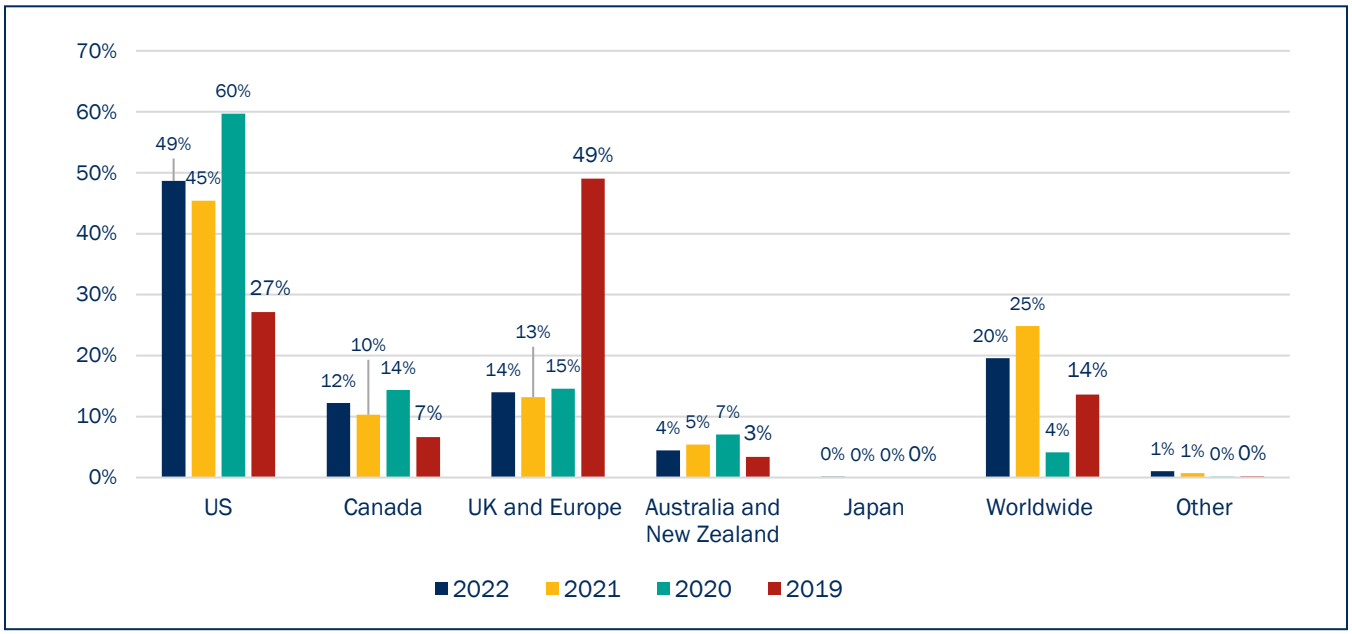
Source: *BMA Calculations*

Net Written Premiums (NWP) also increased by 67% to $5.58 billion in 2022, compared to $3.33 billion in 2021, indicating a continued increase in risk retention by Bermuda cyber policy writers as cyber models continue to develop. Further, a few prominent players consisting of 15 commercial insurers, compared to 13 in 2021, comprised 80% of the overall GWP for both years, with at least $100 million in GWP written each year.

2.2 Number of Policies — Distribution by Country and Geography

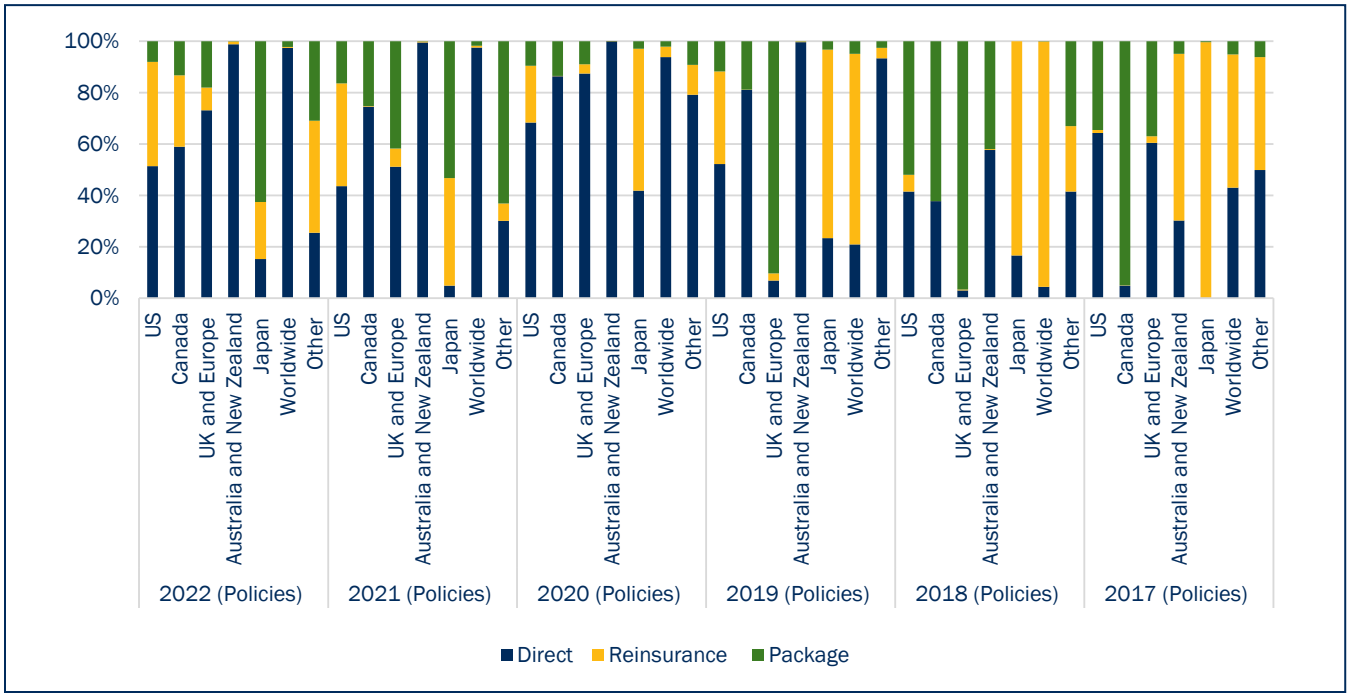
In terms of geographical distribution, the US still accounted for the majority of the number of policies written (2022: 49%, 2021: 45%), while worldwide covers accounted for 20% (2021: 25%), followed by the United Kingdom (UK) and Europe together with 14% (2021: 13%) and Canada with 12% (2021: 10%).

2.3 Number of Policies by Country



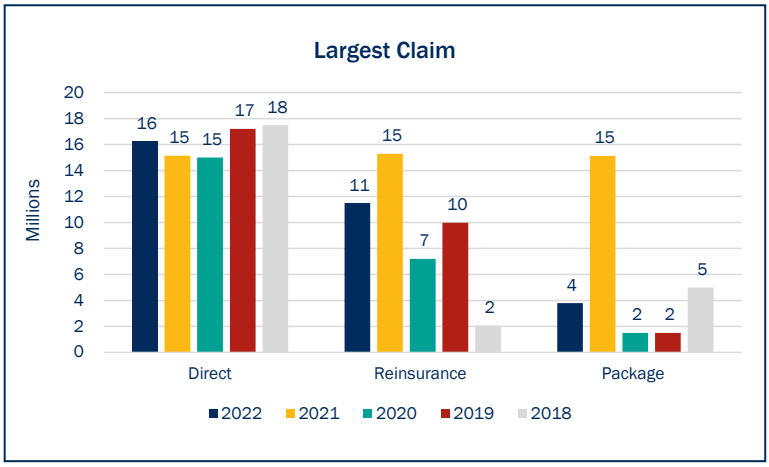
Source: BMA Calculations

2.4 Policy Distribution by Geography

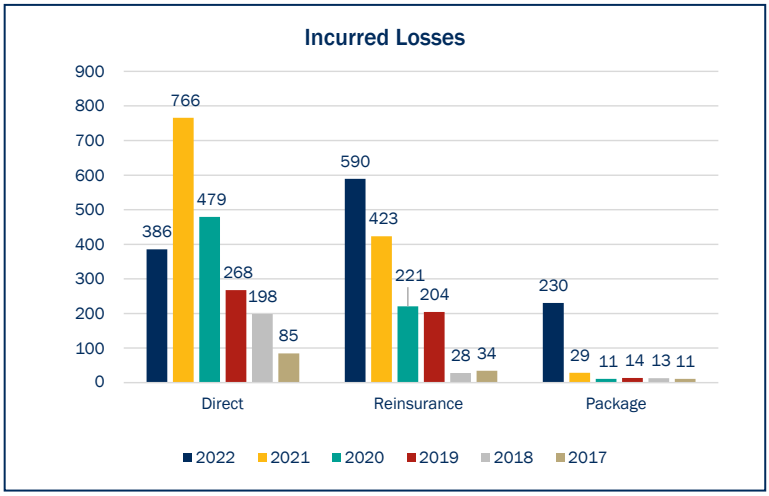


Source: BMA Calculations

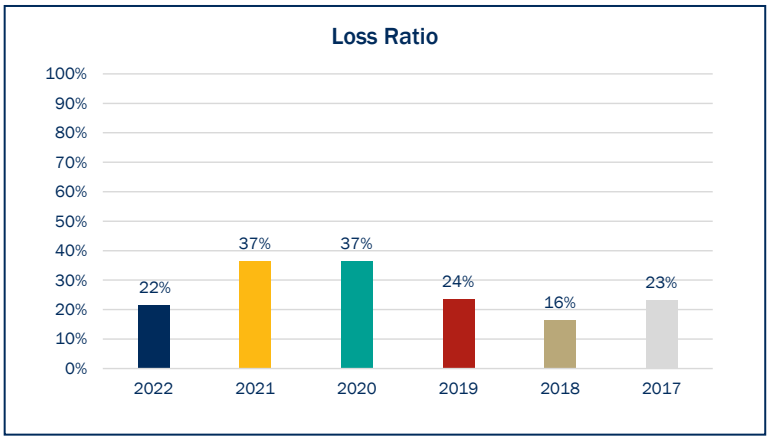
2.5 Commercial Insurer Claims Data



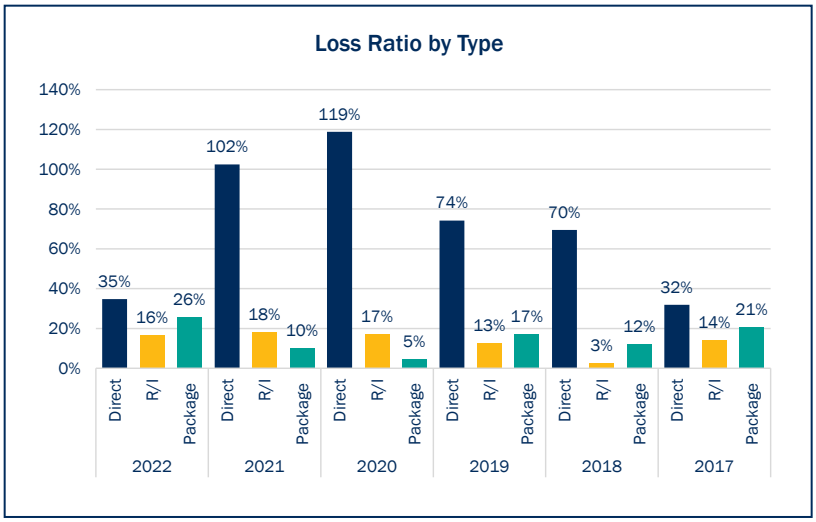
Commercial insurers reported the largest cyber claim per underwriting category, which was approximately $16.3 million for a single data breach for direct policies, compared to $15.1 million in 2021. Reinsurance policies reported their highest loss claim at $11.5 million for ransomware, the same as in 2021. Package policies reported their largest claim to be $3.8 million for malware compared to $15.1 million in 2021. Direct policies have consistently been within the $15 to 18 million range over the last five years. In contrast, reinsurance and package policies saw significant decreases in their largest claim by dollar amounts.



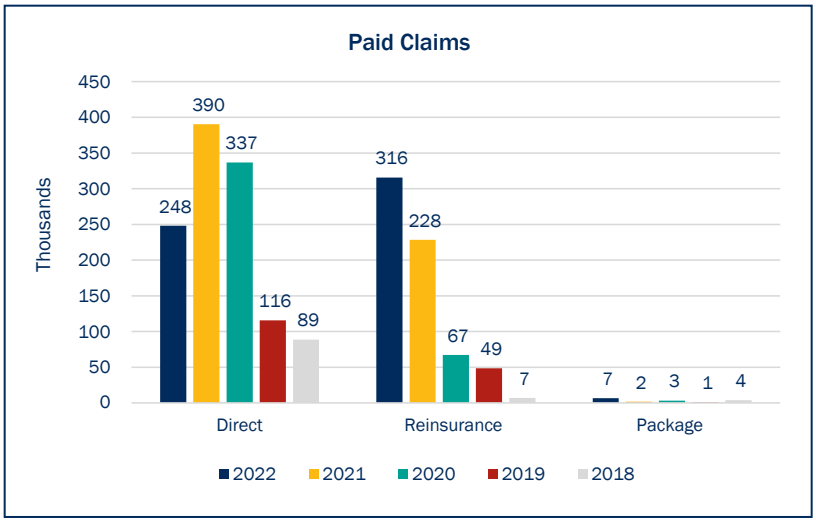
In aggregate, however, incurred losses for commercial insurers remained at $1.2 billion, the same as in 2021, with reinsurance policies contributing nearly 50% of the total, followed by direct policies. Direct policies saw a 50% reduction in incurred losses, while reinsurance and package policies reported a steady increase in incurred losses, respectively.



Consequently, loss ratios seem to have improved, with an overall reported loss ratio of 22% compared to 37% in 2021. This was likely driven by the noted decrease in reported loss claims during the year, coupled with an increase in overall premium rates.



Loss ratios for direct and reinsurance policies significantly improved, while package policy loss ratios doubled yearly, albeit still comparably lower than direct policies.



Similarly, actual cyber insurance claims paid during the year reported a reduced aggregate amount of $570 million, stemming from nearly 12,800 claims compared to $620 million for over 16,900 claims in 2021. These losses primarily resulted from reinsurance and totalled $315.6 million in 2021, compared to $228.2 million in 2020. This shift represents a significant change from prior years, where direct policies were the primary source of losses. Further, reinsurance policies contributed 55% of the total claims paid in 2022 compared to 37% in 2021, while direct policies contributed 44% of the total claims paid in 2022. Consistent with 2022, a few companies significantly contributed to the aggregate total claims paid.

3. Key Statistics for Captive Insurers

3.1 Overview

This section highlights the captive sector and encompasses general business insurers (Class 1, 2 and 3) that write cyber insurance risk as reported in the Electronic Statutory Financial Returns (E-SFR) for the last three years.

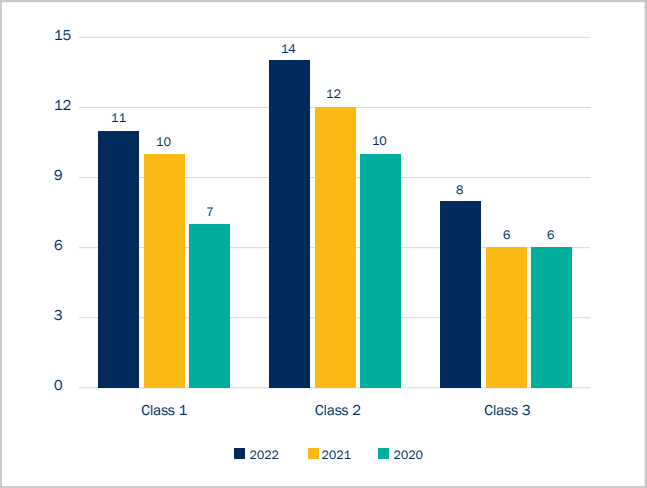
In 2022, the Authority saw cyber insurance GWP increase by approximately 14%, from $172 million in 2022 to $172 million in 2021, while the number of captive companies writing cyber insurance risks increased from 28 in 2021 to 33 in 2022.

Class 2 insurers continued to write the highest number of cyber insurance policies, while Class 3 insurers wrote about 62% of the total captive GWP in 2022, compared to 43% in 2021. This was followed by Class 2 insurers at 32% in 2022, compared to 52% in 2021 and Class 1 insurers at 7% in 2022, compared to 4% in 2021.

Similar to last year, a large part of the cyber insurance GWP continues to be written by a single captive insurer. One insurer contributed approximately $89.9 million in 2022 (2021: $59.8 million), which was 52% of the total GWP during the year.

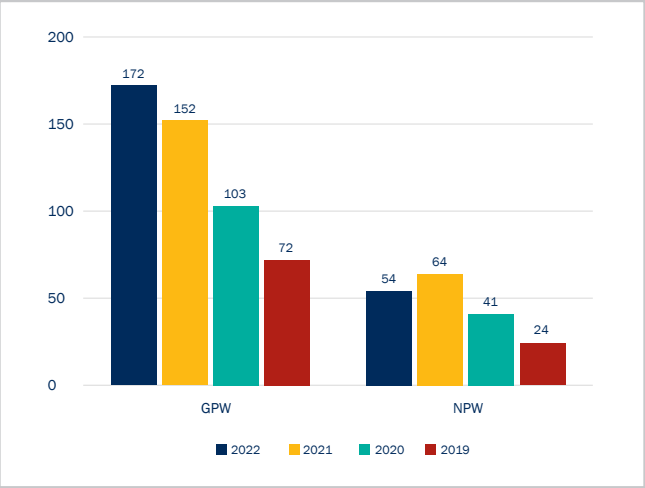
Furthermore, of the total cyber insurance premium written across the Bermuda captive market, 69% was written directly by insurers in 2022, compared to 56% in 2021, with the remaining 31% written by reinsurers in 2022, compared to 44% in 2021.

3.2 Number of Captive Cyber Underwriters



Source: BMA Calculations

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



Source: BMA Calculations

Based on the steady growth of cyber insurance activity over the last three years, the captive market continues to prove effective as a tool for managing cyber insurance risk for companies regardless of their industry. The Authority recognises that the captive sector plays a critical role in the growth and development of the cyber insurance market by offering tailored risk management solutions, cost efficiencies and enhanced control over claims and coverage. Using captives is expected to become increasingly important as cyber threats evolve to help organisations effectively manage their cyber risk exposures.

4. Cyber Underwriting Stress Scenarios

4.1 Insurer's Own Cyber Worst-Case Scenario Results

Insurance groups and commercial insurers have been required to identify and quantify their own CWCS, particularly those that write affirmative cyber policies. Based on the submitted regulatory filings, minimal change was noted over the last year regarding the type of CWCSs provided to the Authority by the insurers. The most commonly- reported types of CWCS continue to be cloud service provider hacks, large-scale ransomware and malware attacks, and large data breaches.

However, aggregate estimated CWCS gross and net losses significantly increased in dollar terms. Groups reported **$13.1 billion** in gross losses in 2022 compared to $9.5 billion in 2021 and **$6.8 billion** in net losses in 2022 compared to $4.2 billion in 2021. Accordingly, the applicable aggregate policy limits for these CWCSs were estimated to be **$240.2 billion** on a gross basis in 2022, compared to $89.8 billion in 2021, and **$146.8 billion** on a net basis, compared to $32 billion in 2021.

Comparably, commercial insurers reported aggregate modelled CWCS gross and net losses of $14.1 billion (2021: $7.3 billion) and $9.6 billion (2021: $5.1 billion). The applicable policy limits for these CWCSs reported to the Authority are estimated to be an aggregate of $295.2 billion and $178.3 billion on a gross and net basis, respectively.

To put these numbers into perspective, the current year aggregate policy limits for both groups and commercial insurers pertaining to CWCS exceed the ten-year average industry loss of $134 billion for natural catastrophes reported in 2023, according to Swiss Re.

Applying the modelled CWCS losses indicated above to the Bermuda market's aggregate statutory capital and surplus, the Bermuda market is still expected to meet its Enhanced Capital Requirement (ECR), although mean and median ECRs post-CWCS levels have been reduced to 81.3% gross (92.2% net) and 91.2% gross (95.4% net), respectively.

On an individual basis, however, the Authority noted a number of commercial insurers that had minimal capital buffers and are expected to fall below their ECR post-CWCS level. On average, insurers reported a delta ranging between **1% to 57% of the ECR levels** after applying the estimated losses under CWCS to their pre-CWCS levels. These insurers have been notified by their respective supervisory teams and will be required to submit a detailed mitigation plan to the Authority as part of their ongoing supervisory engagement.

A major limitation to this exercise, however, is that a large portion of groups and commercial insurers did not submit their own stress test result in their filing. The Authority will continue engaging with the industry to understand the reasons for this and will subsequently revisit the approach and requirements accordingly.

4.2 BMA-prescribed Cyber Worst-Case Scenarios

To enhance its market analysis on the impact of extreme cyber events, the Authority designed its own prescribed cyber stress scenarios in 2022 in consultation with the industry. The goal was to complement the companies' stress testing frameworks to assess, measure and mitigate their cyber risk exposures.

The BMA prescribed three cyber worst-case scenarios to test, namely:

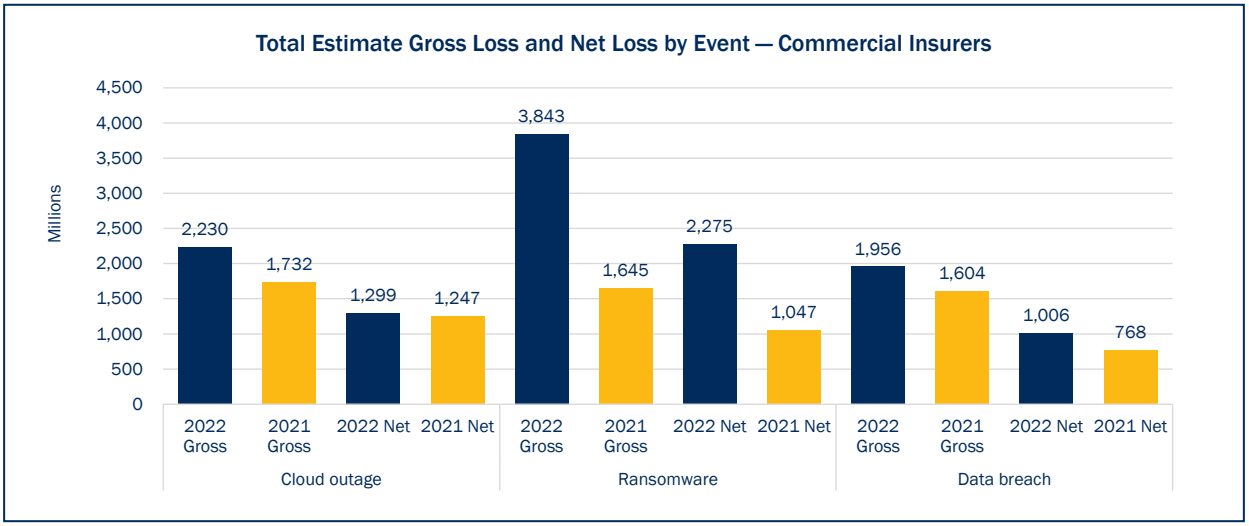
1. A major cloud outage of the policyholders' cloud hosting services that causes significant disruption and loss of availability of critical services;

4.2 BMA-Prescribed Cyber Worst-Case Scenarios (Continued)

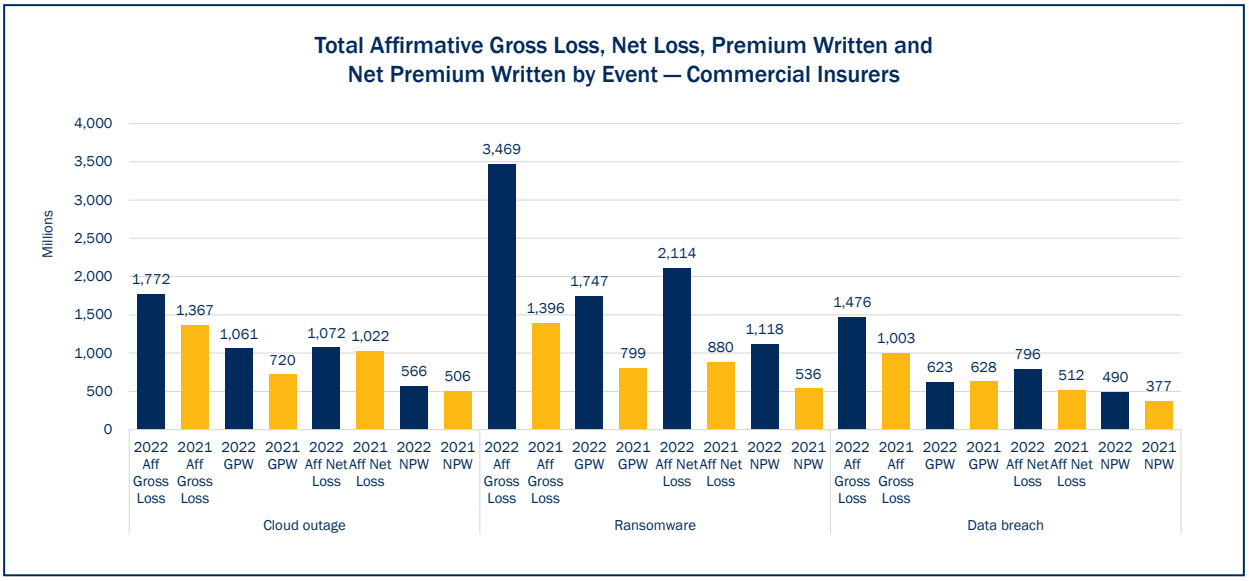
2. A widespread malicious software attack that infects many of the policyholders' operations and disrupts critical operations for 72 hours; and

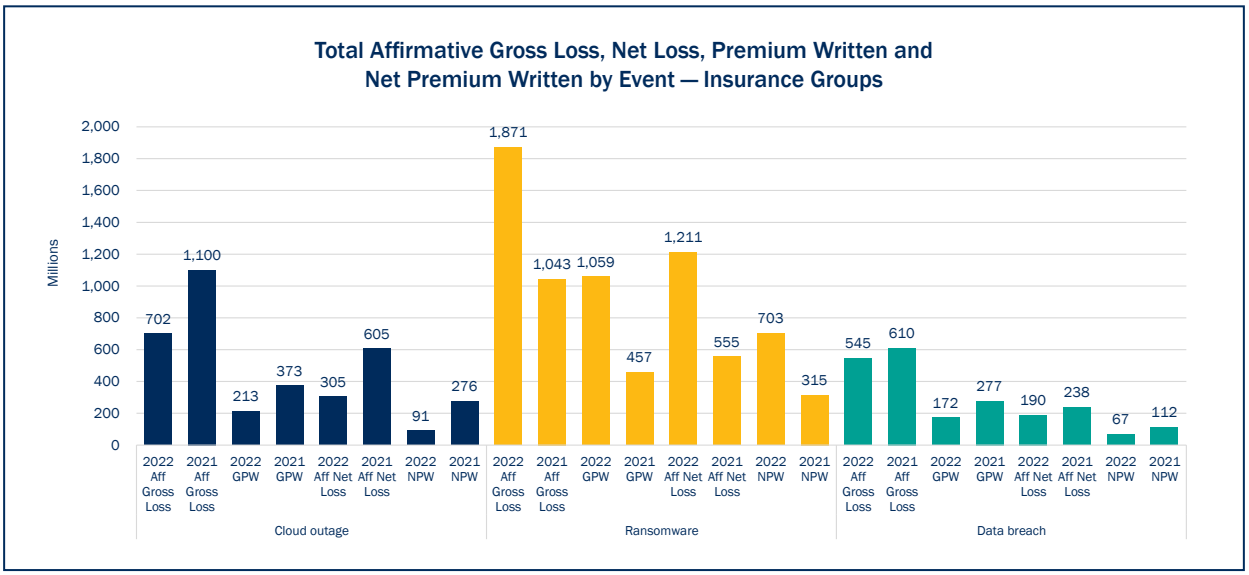
3. A large-scale data breach exposing sensitive and confidential client information forces the insurers to face severe contractual damages and regulatory fines, in addition to suffering business interruption for critical operations.

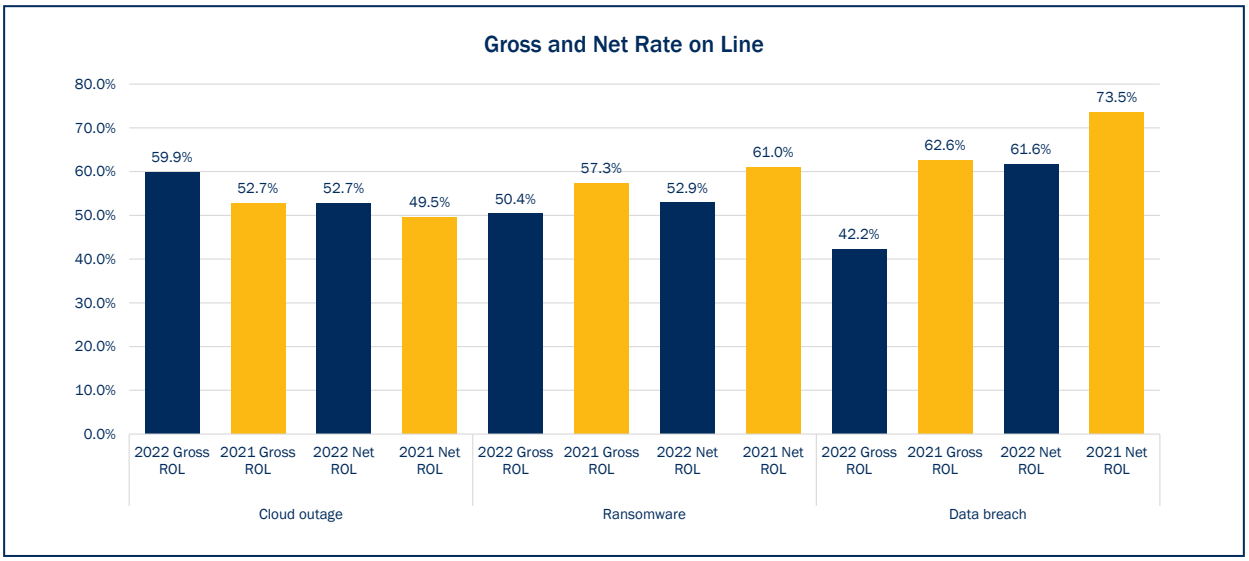
The following charts outline the aggregated results of the companies that performed the BMA-prescribed CWCS:



Accordingly, gross and net reported losses for each scenario have increased yearly, with ransomware returning the highest increase in 2022. The Authority also required the industry to estimate gross and net loss exposures for each of the three prescribed stress scenarios, differentiating between affirmative and non-affirmative exposures. Premiums corresponding to each stress scenario were also required to estimate premium adequacy in relation to the estimated losses or policy limits. The charts below outline the results.

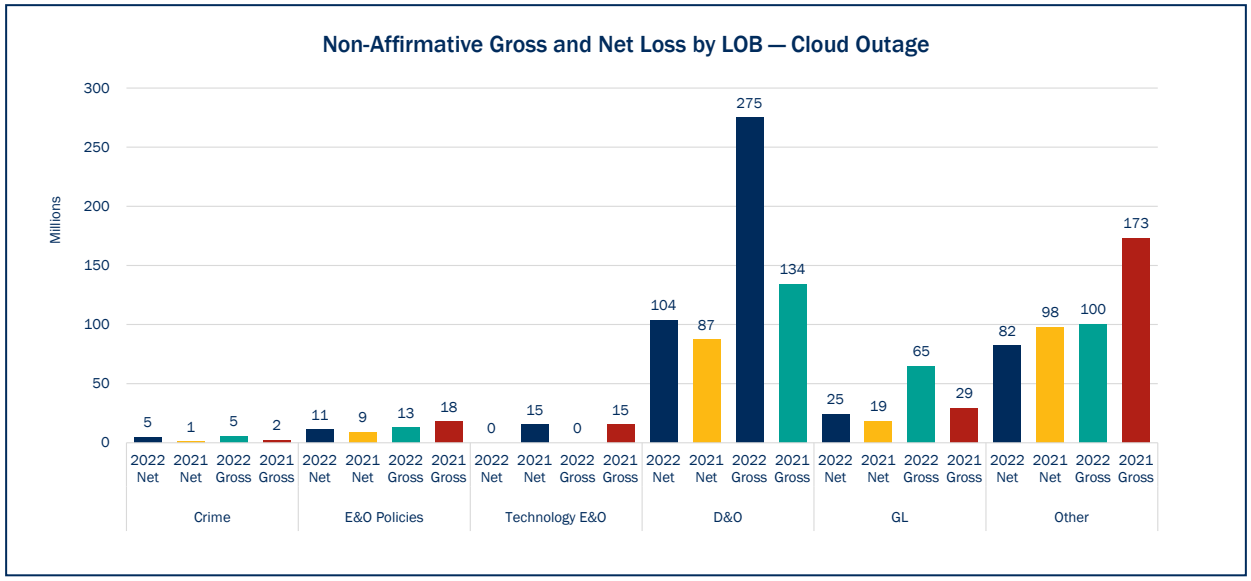


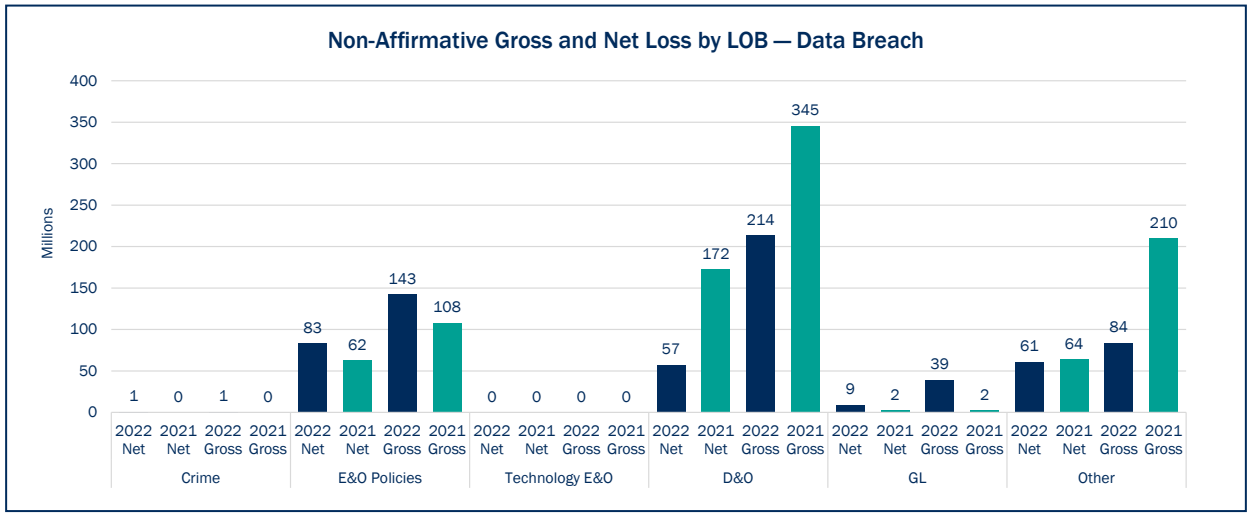


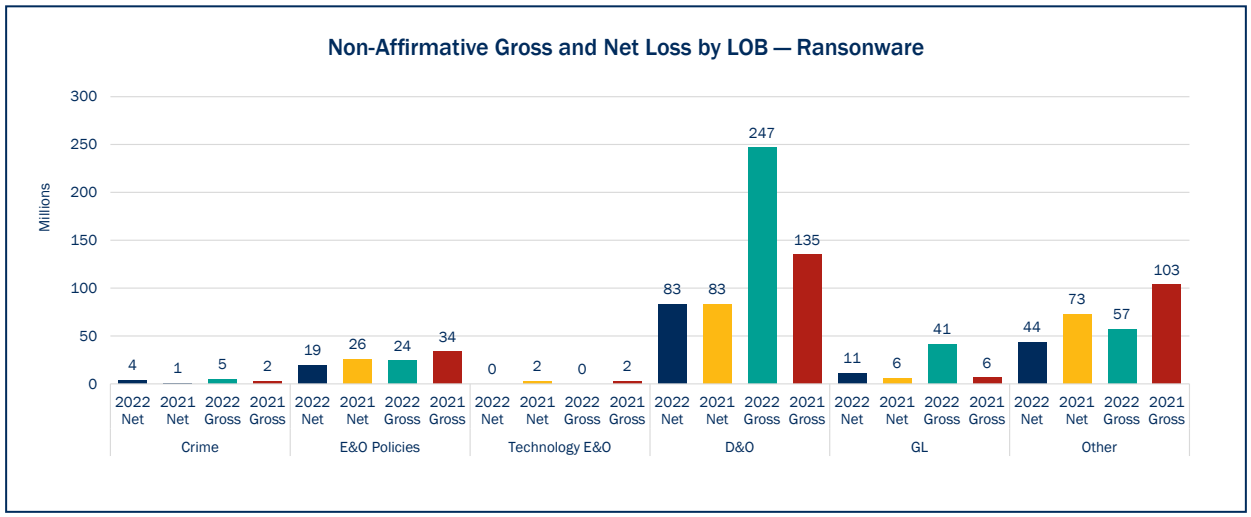


Consistent with 2022, the premium for the estimated worse-case loss ratio ranged between 42% to 62% of the reported exposure (2020: 49% to 74%), which is still relatively higher than other lines of business.

The charts below provide additional information and analysis on the impact of non-affirmative exposure for each stress scenario. They also reveal 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.


Non-Affirmative Gross and Net Loss by LOB — Cloud Outage
Millions
300
250
200
150
100
50
0
5 1 5 2 11 9 13 18 0 15 0 15 104 87 275 134 25 19 65 29 82 98 100 173
2022 Net 2021 Net 2022 Gross 2021 Gross
Crime
E&O Policies
Technology E&O
D&O
GL
Other

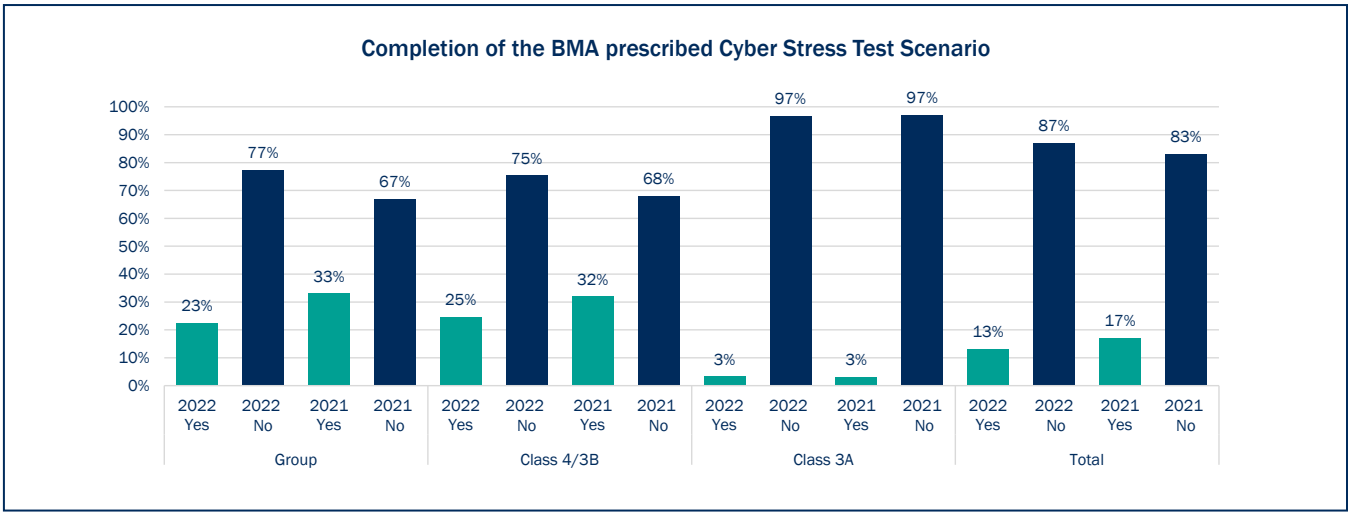

Non-Affirmative Gross and Net Loss by LOB — Data Breach
Millions
400
350
300
250
200
150
100
50
0
1 0 1 0 83 62 143 108 0 0 0 0 57 172 214 345 9 2 39 2 61 64 84 210
2022 Net 2021 Net 2022 Gross 2021 Gross
Crime
E&O Policies
Technology E&O
D&O
GL
Other


Non-Affirmative Gross and Net Loss by LOB — Ransonware
Millions
300
250
200
150
100
50
0
4 1 5 2 19 26 24 34 0 2 0 2 83 83 247 135 11 6 41 6 44 73 57 103
2022 Net 2021 Net 2022 Gross 2021 Gross
Crime
E&O Policies
Technology E&O
D&O
GL
Other

D&O policies still represent the highest estimated exposure in response to cyber events among the different lines of business, followed closely by the 'Other' category. To obtain more information and improve future analysis, the Authority will require a more detailed breakdown of this category for the subsequent YE filing.

In general, 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. They ranged between a one to three basis points reduction from their pre-stress ECR levels. This aligns with the Authority's observations about the results compiled from the companies' own worst-case scenarios, as described in Section 4.

Similarly, it is important to bear in mind that the above insights may not accurately reflect the actual state of the Bermuda market. This is because a large portion of the companies did not complete the BMA-prescribed stress test scenario. The following chart shows the number of companies who completed the test by license class.



Key Action Item for Bermuda Groups and Commercial Insurers

Last year, when the BMA-prescribed CWCS was released, the market was allowed to complete this section on a voluntary and best-effort basis. A materiality threshold was also provided in the second year to guide companies on whether or not they would be required to complete this section. Given the importance of this exercise in assessing the Bermuda market's resilience against systemic and large-scale cyber-attacks, **completion of this section will now be mandatory starting with the 2024 YE filing, regardless of insurer's size and regardless of whether or not a company writes affirmative cyber insurance policies.** This will allow the BMA to have a more accurate and consistent assessment of the industry's resilience under extreme but plausible cyber events and assist the market in enhancing its own cyber risk management framework across all companies.

4.3 Non-affirmative (Silent) Cyber Exposure

In the last four years, the Authority has also required companies to indicate on each non-cyber statutory line of business in their year-end filings whether or not they generally have appropriate explicit exclusion clauses for cyber risks in place. Correspondingly, **37% of the groups and commercial insurers** in 2023 continued to have no explicit cyber risk exclusions in their portfolios, which is an improvement from 42% in 2022. Nonetheless, the imperfect nature of this metric, coupled with the quality of the CISSA/GSSA disclosures observed by the Authority from this year's filing, still raise concerns regarding how companies manage their cyber exposures.

Effective January 2024, Bermuda insurers were guided to add clear and contract-certain language within their non-cyber policies, to clarify whether or not the policy covers cyber triggers. The overarching goal of this guideline is to ensure that policyholders are given clarity on coverage for cyber exposure by reducing contract ambiguity where possible.

While including exclusionary language in the policies is a logical first step to managing non-affirmative cyber risk exposures, the Authority also recognises that newly introduced exclusionary languages have not been tested yet in courts across many jurisdictions. Furthermore, there remains some level of uncertainty as to the effectiveness of such an approach in managing silent cyber risks. The BMA also acknowledges that changing the policy language may not be possible in certain circumstances, such as in compliance with some local statutory laws. Further, the BMA's interaction with the industry revealed that certain types of insurance policies, such as D&O policies or follow-form excess of loss contracts, have already established mature and widely-accepted policy wordings and structures where cyber coverage is already provided for (and expected) and understood by the insureds.

In such cases, the insurer's **intent** is therefore critical in determining whether or not the general guideline of putting more explicit and contract-certain wording into the policies should apply. For example, if the insurer intends to cover losses for a peril such as damages from wrongful acts, even if a cyber event did not cause it within a D&O policy, an express affirmation may not be necessary. However, if the insurer intends not to cover cyber losses for these kinds of non-cyber policies, insurers have an obligation to clarify this in the contract using the current policy wording. The BMA encourages the industry to contribute to the global effort to reduce ambiguity and ensure contract certainty for policyholders rather than leaving the final determination of coverage with the courts. The aim is to enhance policyholder protection and a clear understanding of the coverage.

In cases where the ability to meet regulatory reporting requirements is not possible or will significantly threaten the insurer's business viability, the **BMA's minimum requirement is for the insurer to clearly outline to the BMA why it cannot comply with this requirement in its CISSA/GSSA filings, and articulate their exposure management strategy and plans for silent cyber mitigation**. In addition, the BMA acknowledges that it will take time for insurers to fully comply with this guideline. Therefore, it would be acceptable for insurers to share their progress in this area to the Authority in their CISSA/GSSA filing.

In this regard, the Authority will continue to engage with the market to monitor progress. The BMA will also require the industry to adequately monitor and manage any residual non-affirmative cyber risk exposures within its overall risk management frameworks.

Impact of Generative AI on Cyber Insurance Policies

The rapid rise of advanced technologies, particularly Generative AI (GenAI), also has the potential to add another layer to the complexity of managing silent cyber risk. GenAI introduces several novel risks that may

manifest as silent cyber exposures if not properly addressed in insurance policies. GenAI may lead to operational disruptions that are indirectly related to cyber events (e.g., AI errors in supply chains, manufacturing, or service delivery), leading to claims that may not be explicitly covered under cyber or general policies. As generative AI introduces new risks, insurers may find existing policy wordings inadequate, causing claims under traditional policies that were never intended to cover such events. Insurers, therefore, need to closely monitor these developments and consider updating their policies to explicitly address the potential impacts of GenAI. For this reason, the Authority will continue to monitor progress in this area.

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

Upon review of this year's filings, some groups and commercial insurers lacked appropriate and adequate disclosures on their CISSA/GSSA reports. The Authority would like to provide further clarification and guidance on these required disclosures:

1. Cyber underwriting (affirmative and non-affirmative)

   Companies should provide a comprehensive outline of their cyber underwriting process, both for affirmative covers (if the company writes affirmative policies) and risk management process to address non-affirmative/silent cyber covers. The disclosures should include the company's current cyber underwriting framework, policies and procedures, overall portfolio exposure estimation, model governance and a description of how the insurer will ultimately link these various components into its current and planned capitalisation levels.

   In addition, companies should indicate current and planned efforts to enhance policy language and structure to provide greater clarity for their policyholders regarding cyber coverages for non-cyber policies, addressing the points raised in Section 4. Companies should estimate their gross and net exposures to silent cyber, demonstrate how this aligns with their risk tolerance and evaluate their capacity to absorb such losses.

2. Stress/scenario testing results

   As the cyber threat landscape continues to expand each year, the BMA requires companies to perform their own tests in addition to the BMA's prescribed cyber stress scenarios. Companies must provide sufficient details of the results in their CISSA/GSSA report. Details about the impact on the companies' affirmative cyber portfolio must be disclosed, as well as an estimation of the potential impact of such events on non-cyber policies for each event. Companies must also provide appropriate information on the assumptions and methodologies used to calculate the estimates for both sets of stress tests performed. Subsequently, the stress testing results must be applied to the companies' current capital and ECR levels to arrive at post-stress ECR levels. Finally, companies must provide their planned management actions and risk mitigation strategies for each stress test scenario.

3. Accumulation risk management

   In addition to the disclosures required in points one and two, companies must consider the potential accumulation risk of cyber. This involves identifying catastrophic events and potential accumulation points impacting their book of business. These points could include common technologies, service providers or critical infrastructure dependencies within the insurer's business environment. The company must disclose its risk assessment process, methodologies and governance used to oversee the accumulation of risk, including information that uses proprietary or third-party tools and models to quantify the risk. The results

of its assessment must then be reviewed alongside its liquidity and capitalisation levels, indicating any contingent capital access or alternative risk transfer strategies and tools that the company will use as necessary to mitigate accumulation risk. Moreover, **model validation and back testing** must be performed regularly, or at least once a year for any models the company uses to manage risk accumulation and cyber risk in general.

Overall, a company's CISSA/GSSA report must provide the Authority with a clear picture of its cyber risk management framework to review the self-solvency assessment process. The insights from these disclosures, coupled with the qualitative data collected from the year-end filings, will help the BMA assess the state of the market at a macro level and identify any systemic or market-wide risks and considerations that will need to be factored in for future regulatory enhancements in this area.

6. A Growing Cyber ILS Sector

As with the natural catastrophe line, the Authority recognises that third-party capital can complement traditional market capacity to address the large protection gap in cyber insurance risk. This insurance coverage gap is currently estimated to be $900 billion annually, second only to pensions ($1 trillion), but exceeds all other perils, such as natural catastrophes ($139 billion) and healthcare ($800 billion), according to a GFIA report released in 2023.

While the cyber ILS market is still in its infancy, the growth potential is significant as the industry seeks additional capacity to meet the rising demand for cyber insurance. Advances in the sophistication of cyber models, coupled with the rise of parametric technologies, will likely promote and facilitate the increased use of ILS vehicles to complement traditional capacity.

In 2023, Bermuda insurers issued a number of cyber-specific ILS, providing a total coverage of $**670 million**, which is quite significant for its first year of issuance. The development of this market is crucial for providing adequate coverage against increasingly sophisticated and more frequent cyber threats. The BMA will, therefore, continue to monitor this growing sub-sector to enhance its oversight of the ILS space while facilitating further innovation and speed to market. Another important goal for the BMA is to offer clear and valuable information to policyholders and investors.

6.1 Operational Cyber Risk Management

As the cyber threat landscape continues to grow, 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 Insurance Sector Operational Cyber Code of Conduct (Code), which came into force in 2022, to ensure that they abide by best practices.

Further, Insurers should review the *Bermuda Insurance Sector Operational Cyber Risk Management 2023 Report* issued earlier this year. It provides further guidance on how their companies have fared against the requirements and best practices set out in the Code and against their peers, especially in areas where control deficiencies are identified in the report. The Authority will continue engaging and coordinating with these companies through its insurance and cyber supervisory teams.

7. Conclusion

The BMA's review of the companies' YE filings provided important insights that validated the need to continue its supervisory focus and attention on cyber risk, both as a peril that could potentially impact all lines of business and as major component of the Bermuda insurance market's overall resilience.

While the market has generally improved its cyber underwriting practices, standards and overall risk management, several areas for improvement were noted by the Authority, particularly in the areas of stress and scenario testing, silent cyber risk and accumulation risk management and CISSA/GSSA disclosure, as outlined in the previous sections. At the same time, technologies such as Generative AI are continuously and rapidly advancing and being adopted across all industries, presenting both risks and opportunities for the market . It is, therefore critical that both the industry and the BMA stay abreast of these developments to promote and maintain a robust and sustainable cyber insurance market based on the results of this report and the proliferation of new technologies.

The BMA also recognizes Bermuda's role in the global cyber insurance market. Out of the total $13.5 billion cyber GWP written globally in 2022, as reported by Insurance Business Magazine, $7.5 billion was written by and/or consolidated into Bermuda groups and commercial insurers. Another $172 million was written by the captive sector in Bermuda. Together, these two sectors constituted approximately 57% of the global cyber GPW written in 2022. In addition, the ILS sector provided a complementary capacity of $670 million in coverage through cyber-specific ILS issuances in 2023. Furthermore, the BMA's innovative framework has encouraged and facilitated innovation in the market. This framework has resulted in creating and enhancing new cyber insurance products that address current and emerging threats across industries.

Collectively, these trends highlight the Bermuda market's critical role in addressing the growing cyber protection gap. According to a recent report issued by the Global Federation of Insurance Associations (GFIA), this insurance coverage gap currently stands at $900 billion. This makes it one of the largest and most pressing insurance gaps globally and comparable to the existing protection gaps in natural catastrophes, healthcare and pensions.

Therefore, the BMA deems it important to continue its supervisory focus on cyber risk. In summary, the following enhancements and steps will be implemented by the Authority for the 2024 YE filing:

1. **Mandatory completion of stress/scenario testing exercises:** As outlined in Section 4, the materiality threshold will be removed and all groups and commercial insurers will be required to complete the BMA-prescribed stress tests starting with their 2024 YE filing. The BMA also reiterates its requirement for companies to perform and submit their stress testing results every year-end;

2. **CISSA and GSSA reviews:** As outlined in Section 5, a significant portion of the Bermuda market continues to require significant improvement in the quality of their CISSA and GSSA submissions. Supervisors will review the quality of next year's submissions and continue to engage with the companies to monitor progress; and,

3. **Issuance of a Guidance Note on cyber underwriting:** The BMA will aim to consolidate all the cyber risk management guidelines articulated in this report and in previous publications into a draft Guidance Note. The Authority will consult with the industry before publishing a final version.

Finally, the Authority will continue to enhance and build upon its existing regulatory and supervisory frameworks as the cyber threat landscape evolves. The Authority will also continue with its consultative approach to policymaking and regularly engage with relevant industry stakeholders such as Industry

associations (e.g., the Association of Bermuda Insurers and Reinsurers Cyber Working Group and Bermuda Captive Network), cybersecurity firms, modelling firms and rating agencies. Further, the BMA will continue participating in international discussions and forums by sharing information, best practices and insights on cyber risk supervision with its peer regulators. Collectively, this approach will assist the Authority in building and maintaining a robust regulatory and supervisory framework, with the overall goal of promoting a stable and resilient 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