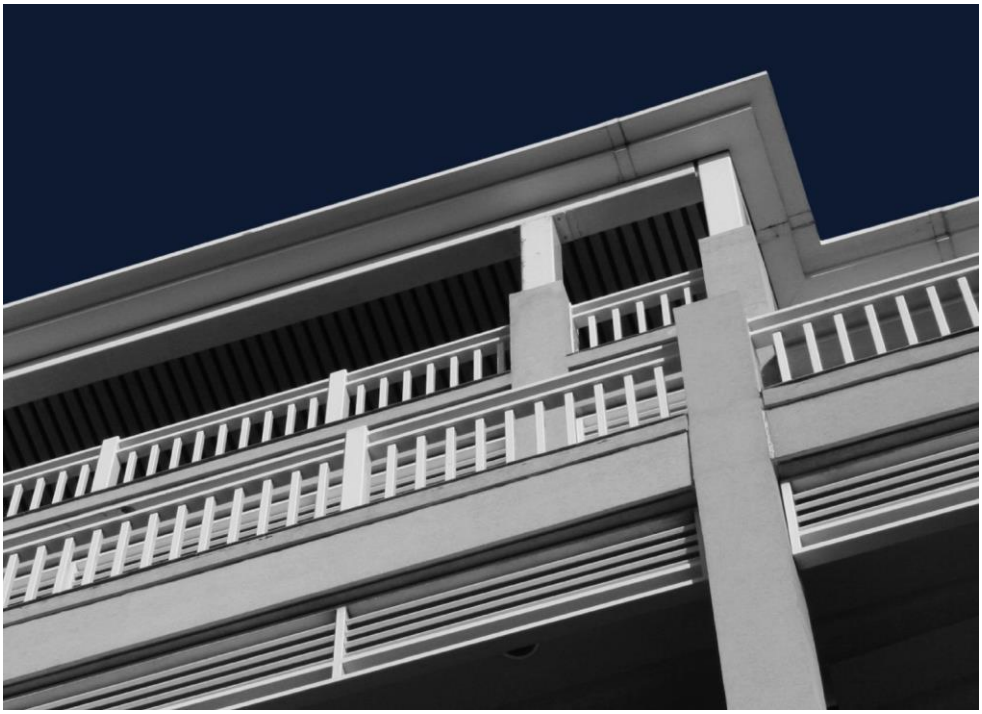
BMA
BERMUDA MONETARY AUTHORITY



CYBER REPORT 2018

Table of Contents

1. Introduction

Technology risk including, information security, cybersecurity and data privacy are all key enterprise risks affecting (re)insurers regulated by the Bermuda Monetary Authority (BMA or the Authority). These risks continue to feature prominently in global headlines as both the frequency and severity of data breaches increase. Global regulatory and local legislative initiatives, including the EU's General Data Protection Regulations (GDPR) and Bermuda's Personal Information Protection Act (PIPA) are focused on addressing some of these issues.

The Authority continues to apply a pragmatic, risk-based approach to regulating Bermuda's continuously evolving financial services sector including banks, (re)insurance companies, trust companies, investment businesses, investment funds, fund administrators, money service businesses, corporate service providers and most recently digital asset businesses.

On 12 February 2018, the Authority issued a notice entitled "Cybersecurity" outlining some expectations of licensed entities regarding the management and reporting of cybersecurity risks and incidents. In that notice, the Authority stated:

"As with any material risk, all licensed undertakings are required to have robust policies, procedures and controls in place to identify, assess and manage cybersecurity risks on an on-going basis consistent with the prudent business minimum licensing criterion."

While there are numerous standards and methodologies that can be applied to assess an entity's posture, the Authority believes there is merit in adopting a cybersecurity framework. The Authority has adopted the NIST Cybersecurity Framework (CSF), authored by the National Institute of Standard and Technology in the United States[1].

The Authority's assessment process is grounded in the NIST CSF and focuses on several areas including, but not limited to: governance, policies and procedures, ongoing training, critical/sensitive asset identification, protective measures, detection of anomalous activity, documented incident response plans, and effective business recovery processes.

The Authority recognises that there is no "one size fits all" approach to addressing these risks, as specific business circumstances may vary greatly from entity to entity. Each entity must assess its risks, create prudent policies and procedures to mitigate known risks, and ensure that the organisation is properly trained and equipped.

The Authority expects that the Board of Directors (the Board) of all licensed entities will have evaluated the risks associated with technology risk including information security, cybersecurity and data privacy; will have incorporated these factors in the overall enterprise risk management process; and ensured that prudent policies and procedures are in place and followed by the entity.

[1] https://www.nist.gov/cyberframework

In 2017, the Authority included questions in the 2017 year-end Commercial Insurer[2] Capital and Solvency Return (CSR) filing designed to assess information security, cybersecurity and data privacy preparedness of (re)insurers. This information request has been enhanced in the 2018 filing to include all financial services sector players in Bermuda, which will allow broader market information and thematic assessment of the technology risk posture of licensed entities. The Authority is issuing this communication to provide some feedback on the information obtained in the 2017 year-end filing and provide context for the 2018 year-end information requests.

Recognising that the global cyber (re)insurance market is rapidly expanding, and this being a new line of business, the Authority also requested Bermuda Commercial Insurers to provide cyber underwriting data as part of their 2017 year-end CSR filing. The information requested through that data call included: (i) underwriting data for cyber policies; (ii) confirmation of inclusion of cyber exclusion clause per line of business; and (iii) claims reported during the year, including the largest claim. Commercial Insurers were also required to provide cyber risk data, including their estimated aggregate exposure and description of their own cyber underwriting worst-case annual aggregate loss scenarios, and the underlying assumptions. This report also seeks to share a summary of the market data and the risks discerned from the information submitted.

2. Technology Risk Resiliency

From information provided in the 2017 year-end cyber resiliency questionnaire and feedback from the Authority's on-site reviews covering cyber, it is apparent that technology risk awareness and cybersecurity in particular has grown. Most (re)insurers have made efforts to enhance technology risk resiliency, however, much work remains to be done before the BMA can achieve a level of assurance that the possibility of large-scale cyber-attacks and financial and reputational loss is effectively mitigated. The following areas have been identified as still needing significant enhancements across the Bermuda Commercial Insurer market:

1) ***Board approval of technology risk strategy*** - The technology risk strategy and policies for a number of Commercial Insurers are approved by the Board, and cyber security is a standing item for the board meetings, but this practice needs to be more consistently implemented across the broader market.
2) ***Appointment of Chief Information Security (CISO) and/or data privacy officers*** - While a number of (re)insurers have a designated Chief Information Security Officer (CISO) or a data privacy officer, there are others that have not filled these positions and, in certain cases, it is unclear whether other individuals in the organisation are performing this role.
3) ***Third party cybersecurity risk assessments*** – Just over half of the Commercial Insurers commission third party cybersecurity risk assessments. It is also important to ensure that contracts with suppliers and third-party partners are structured in a manner that is consistent with the (re)insurer's cybersecurity policies.
4) ***Ongoing cybersecurity and data privacy training*** – The vast majority of Commercial Insurers indicated that staff are provided with ongoing cybersecurity and data privacy training; however, the effectiveness of the training, including social engineering and penetration testing, and tracking, was assessed as generally being inadequate.

[2] In this report, the term "insurer" includes "reinsurer", and (unless explicitly distinguished) "insurance" includes "reinsurance". Commercial Insurer includes Classes C, D, E, 3A, 3B and 4.

5) ***Incident response plans*** - Incident response and recovery plans, and procedures to ensure timely restoration of systems and assets affected by cybersecurity events were generally not present or not updated and tested regularly. A number of Commercial Insurers also do not have formal incident response communication plans.
6) ***Cybersecurity standards*** - A wide range of globally recognised cyber security standards or practices have been adopted by a number of Commercial Insurers, but a fit for purpose framework needs to be more broadly adopted by the wider market, for example NIST or Cobit.
7) ***Review of the cyber security programme by the third line of defence*** – While the majority of Commercial Insurers ensure that the cyber security programme is subject to internal audit review, this practice needs to become more common across the market.

To obtain evidence that the above deficiencies are being sufficiently addressed, the Authority will continue to closely monitor and ensure that cyber risk assessments are a key feature of its regulatory reporting framework and Onsite reviews.

Other observations included, whilst a number of (re)insurers buy cyber-specific insurance, the limits reported had a wide range even for similar sized (re)insurers in particular instances. Additionally, a significant number of (re)insurers budgeted a specific amount for cyber security and this was through various forms with the most common being: i) a percentage of the Insurer's IT budget, ii) consolidated budget for cybersecurity at Group level, and iii) a stated amount for cybersecurity.

Figure 1. Bermuda Insurers with Positive Responses to 2017 Year-end Cyber Questions

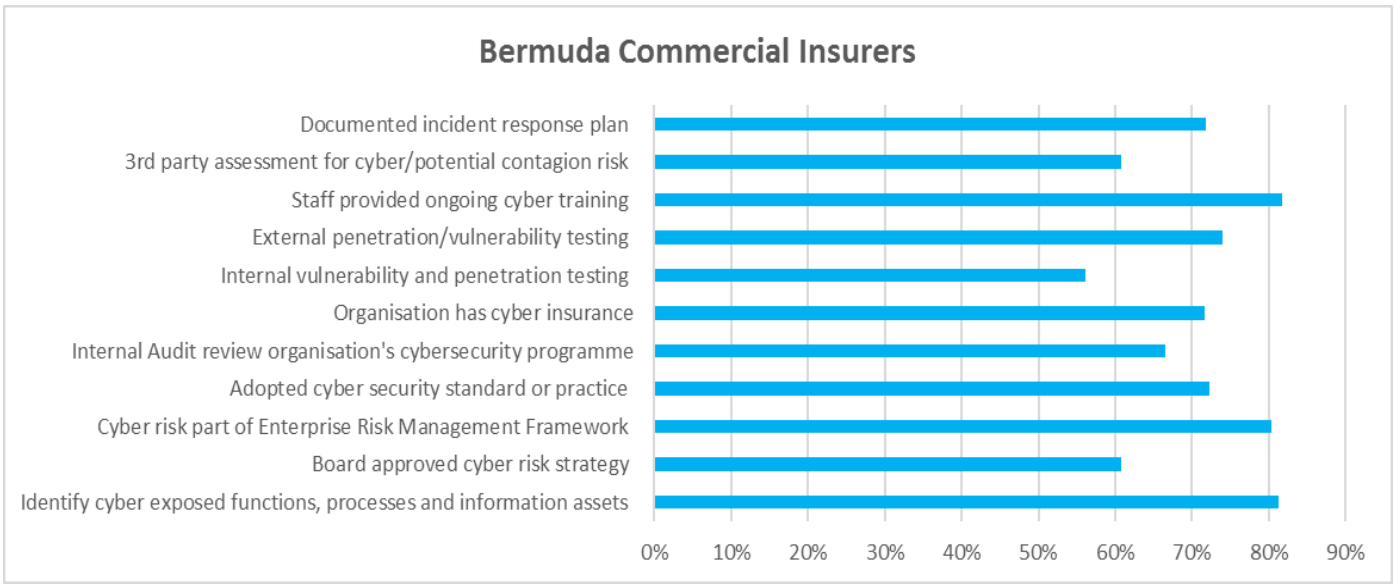


Figure 1. discloses averages for the Bermuda Commercial Insurer market. It was observed in the underlying data that the averages for Large Commercial Insurers[3] were higher than those for Small Commercial Insurers[4].

[3] For the purposes of this report, Large Commercial Insurers include Classes D, E, 3B and 4.
[4] For the purposes of this report, Small Commercial Insurers include Classes C and 3A.

The Authority recognises that appropriate prudent governance, internal controls and defensive resilience capabilities, including emphasis on both technology and people, go a long way to enhancing capabilities of (re)insurers to withstand cyber-attacks and other technology risks.

3. Cyber Underwriting

The last few years have seen cyber insurance becoming a significant area of growth for (re)insurers against a background of softening rates in other lines of business, an increasingly competitive market and increasing use of technology in all spheres. According to data captured in the 2017 year-end filings, 37 Bermuda Commercial Insurers and 15 Groups indicated that they are writing affirmative (direct) cyber insurance.

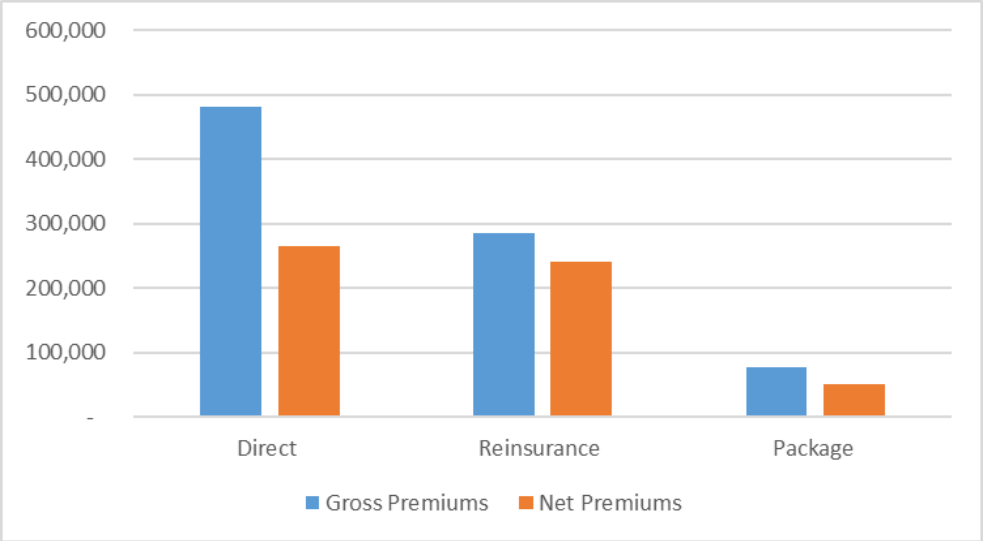
The objective of this section is to share the Authority's general observations from key data aggregated from Commercial Insurers' regulatory submissions. This being the first year that such information was sought, there were variances in terms of interpretation of what was required; enhancements and additional guidance has been included in the cyber risk reporting requirements for 2018 year-end CSR filings.

The questionnaire requested information on both affirmative cyber insurance and cyber exposure on other liability insurance policies where cyber is not explicitly excluded (silent cyber). Of the filings submitted, over 85% of the non-affirmative cyber policies do not contain an explicit cyber exclusion clause.

The Authority expects as part of prudent management of both affirmative and silent cyber risk, (re)insurers need to have relevant skills, clear strategies and Board approved risk appetites. (Re)insurers need to be quite clear on covered limits and sufficiently manage aggregation risk across industries, geography etc.

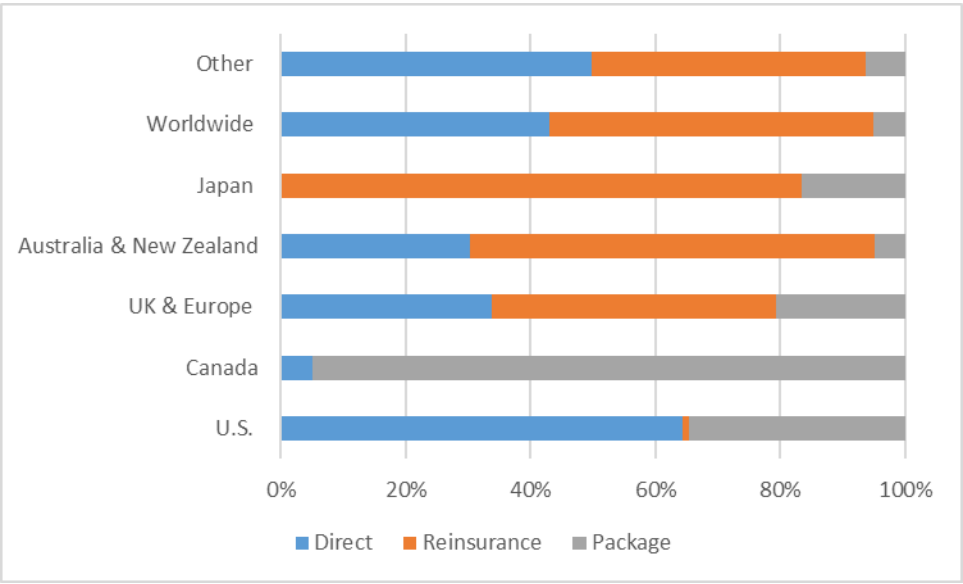
4. Key Statistics for 2017 Year-end [5]

Figure 2. Gross vs Net Premiums



Bermuda Commercial Insurers reported cyber risk Gross Written Premium of approximately $845 million and Net Written Premium of approximately $557 million from over 31,000 policies. On a cyber risk retention basis, 55% Direct, 84% Reinsurance and 68% Package were retained by Bermuda Commercial Insurers.

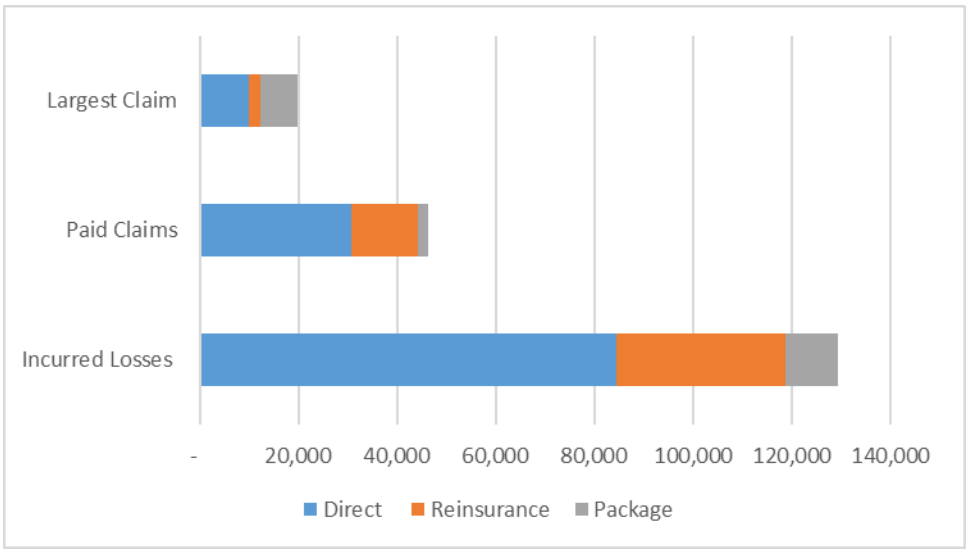
Figure 3. Policy Distribution by Geography



[5] Underwriting statistics quoted are from Insurance Company Statutory Returns.

The majority of the Commercial Insurer policies written were for the United States of America, accounting for 56% of the total policies, followed by Worldwide (26%) and Canada (14%). The rest are spread out among Japan, Australia & New Zealand, the United Kingdom and the European Union.

Figure 4. Claims Data



- Cyber claims paid by Commercial Insurers were approximately $46 million for over 6,600 claims. Direct policies accounted for 54% of the total claims, with Reinsurance accounting for 45% and Packages 1%.
- The largest claim per underwriting category for Commercial Insurers was approximately $10 million for Direct, $2.2 million for Reinsurance and $7.5 million for Package policies.
- Aggregated incurred losses for Commercial Insurers for the year were approximately $140 million.

5. Cyber Stress Scenarios

Commercial Insurers were required to provide cyber risk coverage data, including estimated aggregate exposure, and own cyber risk worst-case annual aggregate loss scenarios, and the underlying assumptions. The data showed that Bermuda Commercial Insurers' own worst-case scenarios from affirmative cyber risk coverage would not have significant impact on their statutory capital and surplus. The average gross and net impacts were 5.0% and 4.0% respectively. The Authority's general view is that much larger losses could arise from silent cyber contracts.