IAIS International Association of Insurance Supervisors

Global Insurance Market Report (GIMAR)

SPECIAL TOPIC EDITION

Cyber

April 2023

About the IAIS

The International Association of Insurance Supervisors (IAIS) is a voluntary membership organisation of insurance supervisors and regulators from more than 200 jurisdictions. The mission of the IAIS is to promote effective and globally consistent supervision of the insurance industry in order to develop and maintain fair, safe and stable insurance markets for the benefit and protection of policyholders, and to contribute to global financial stability.

Established in 1994, the IAIS is the international standard-setting body responsible for developing principles, standards and other supporting material for the supervision of the insurance sector and assisting in their implementation. The IAIS also provides a forum for members to share their experiences and understanding of insurance supervision and insurance markets.

The IAIS coordinates its work with other international financial policymakers and associations of supervisors or regulators, and assists in shaping financial systems globally. In particular, the IAIS is a member of the Financial Stability Board (FSB), a member of the Standards Advisory Council of the International Accounting Standards Board (IASB), and a partner in the Access to Insurance Initiative (A2ii). In recognition of its collective expertise, the IAIS also is routinely called upon by the G20 leaders and other international standard-setting bodies for input on insurance issues as well as on issues related to the regulation and supervision of the global financial sector.

For more information, please visit www.iaisweb.org
Follow us on LinkedIn: IAIS – International Association of Insurance Supervisors.

About this report

This is the special topic edition of the Global Insurance Market Report (GIMAR). The regular GIMAR presents the outcomes of the IAIS' Global Monitoring Exercise (GME), which is the IAIS' framework for monitoring risks and trends in the global insurance sector and assessing the possible build-up of systemic risk. Special topic editions of the GIMAR delve deeper into relevant topics stemming from each year's GME. This document was prepared by IAIS members (Carin Hamnell, Jemima Hall and Romain Labaune (PRA), Andrew Shaw (Federal Insurance Office, U.S. Department of The Treasury), Frank van Steen (NBB), Basani Mabaso (South African Reserve Bank), Cheng Wei Ng and Jessie Yee (MAS), Diana Vieira and Eugenio Avisoa (EIOPA), Francesco Ficarola (IVASS), John Hopman (National Association of Insurance Commissioners), Martin Schembri and Michael Lingham (BMA) and Sibel Kocatepe (BAFIN)), supported by the IAIS Secretariat (Fabian Garavito and Inwook Hwang) in consultation with the IAIS Macroprudential Monitoring Working Group (MMWG).

This document is available on the IAIS website (www.iaisweb.org).

Acronyms and abbreviations

AI	Artificial intelligence
AMRAE	Association pour le Management des Risques et des Assurances de l'Entreprise
CISO	Chief information security officer
CTP	Critical Third Party
DORA	Digital Operational Resilience Act
DOS	Denial of service
ENISA	European Union Agency for Cyber Security
ESA	European Supervisory Authorities
ESRB	European Systemic Risk Board
FMI	Financial Market Infrastructure
FSB	Financial Stability Board
GIMAR	Global Insurance Market Report
GME	Global Monitoring Exercise
GWP	Gross written premiums
ICT	Information and communications technology
ICP	Insurance Core Principle
IIM	Individual insurer monitoring
ILS	Insurance-linked securities
IORP	Institutions for Occupational Retirement Provisions
IT	Information technology
ITS	Implementing Technical Standard
ML	Machine learning
NatCat	Natural catastrophe
NCA	National Competent Authorities
ORSA	Own Risk and Solvency Assessment
ORTF	Operational Resilience Task Force
P&C	Property and casualty
RDP	Remote Desktop Protocols
RDS	Realistic disaster scenario
SDLC	Systems development life cycle
SWM	Sector wide monitoring
VPN	Virtual private network

Contents

Executive summary

This Global Insurance Market Report (GIMAR) special topic edition focuses on the cyber insurance market and the cyber resilience of the global insurance sector. The report covers the trends and key aspects of the global cyber insurance market, the cyber resilience of the insurance sector and the implications for financial stability. The report is based on data that the IAIS collected about cyber underwriting activities and cyber resilience through its 2022 Global Monitoring Exercise (GME), covering year-end 2021 data.

CYBER INSURANCE MARKET

Gross written premiums (GWP) for standalone cyber insurance are reported to have grown in 2021. This was likely driven by both risk-adjusted rate change and organic growth.[1] Increasing demand for cyber insurance is attributed to growing awareness of the expanding cyber attack surface area, growing dependencies on technology, and the complex cyber threat landscape. The cyber insurance market has also seen substantive changes in underwriting controls, including tighter terms and conditions and stricter risk selection and underwriting standards. As a result, clients not reaching minimum cyber hygiene standards found it harder to secure coverage in 2022. These market dynamics reflect market hardening following an increase in ransomware claims in recent years.[2]

As written premiums grew and the underwriting changes compounded, profitability seems to have improved for the sample in 2021 compared to 2020. Unsurprisingly, given that cyber insurance is still a comparatively new line of business, most of the premiums and claims reported were concentrated in a small number of carriers (and jurisdictions).[3]

About 40% of all global cyber premiums flowed to the reinsurance market.[4] This compares to 25% of non-life premiums ceded to reinsurers across the sample. This high level of ceded premiums is not unexpected for a new class, as new entrants seek to partner with a reinsurer to better understand the risks, diversify exposure, gain experience and collect data. While there was activity related to cyber risk transfer in the insurance-linked securities (ILS) market in 2021, volumes were low, and capital availability was limited.

---

1 Risk-adjusted rate change is a measure of the underlying change in price allowing for the change in exposure. It is a relative measurement, which can only be calculated on renewal business. For more information, see Lloyd's, Performance Management data return (2016).

2 See Gallagher Re, CY-Fi The Future of Cyber (Re)Insurance (2022).

3 The first cyber insurance policies were sold in 1997 – see J Wolff, Cyberinsurance Policy (2022).

4 See www.theinsurer.com/viewpoint/cyber-risk-evolution

A considerable degree of uncertainty remains around cyber catastrophe risk and what a cyber tail event would look like – more so than for other perils. One loss estimate for a 1-in-250-year event affecting the US standalone affirmative market is in the region of $30 billion. The largest cyber event to date was NotPetya in 2017, which resulted in an estimated $10 billion in losses, of which $3 billion has been covered by the insurance sector to date (both affirmatively and non-affirmatively).[5] To put this into context, an average Atlantic hurricane season has 14 named storms, seven hurricanes and three major hurricanes (Category 3, 4 or 5 on the Saffir-Simpson Hurricane Wind Scale), causing, on average, $20.5 billion in losses per event in the last 40 years.[6]

Insurers in the sample are addressing non-affirmative coverage in various ways, including: exclusion of some cyber risks from all-risk property and casualty (P&C) policies, affirmatively covering other cyber risks by endorsement (often for an additional premium), and/or offering standalone cyber insurance policies. Some insurers claimed to have dealt with this issue in 95% of their business at renewal. However, it is important to recognise that newly introduced exclusionary language may not have been tested in courts. It is also critical to note that this assessment of non-affirmative coverage applies only to the subset of insurers that took part in the IAIS data collection.

Finally, various reports indicated that cyber insurance only covered a small proportion of the potential economic loss resulting from cyber events. The cyber protection gap appears to be widening, with important differences across jurisdictions.[7]

Growing awareness of the expanding cyber attack surface area, growing dependencies on technology and the complex cyber threat landscape have led to increasing demand for cyber insurance.

CYBER RESILIENCE OF THE INSURANCE SECTOR

In line with the broader trend, insurers' exposure to cyber risk continues to grow. For instance, insurance operations continue to be digitalised to achieve economies of scale and enhance customer experience. Greater digitalisation adds complexity to information technology (IT) systems and increases the cyber attack surface for insurers.

Most insurers in the sample reported that they have cyber security frameworks, risk assessment processes and incident response plans in place. Additionally, these insurers reported that they have implemented essential risk controls. However, the data that were collected were not sufficient to assess the effectiveness of these cyber security frameworks, risk assessment processes, response plans and risk controls. Furthermore, the set of insurers is not representative of the entire population of insurance and reinsurers worldwide, and the responses to these questions are self-assessed.

---

5 See pcs.iso.com/globalnews/pcs_covid_informational_bulletin_4.pdf.

6 NOAA's Office for Coastal Management estimate.

7 For instance, the cyber protection gap of small and medium-sized enterprises appears to be considerable for companies in France. See Association pour le Management des Risques et des Assurances de l'Entreprise (AMRAE), Lumière sur la cyberassurance (2022).

Hence, any conclusions must be taken with caution and should not be extrapolated to the whole population.

The insurance industry has also been affected by the shortage of cyber security professionals. Insurers in the sample reported that it takes longer to fill security positions, the recruitment process has become more expensive, compensation packages have increased, and employers have to offer greater flexibility. This shortage of talent could lead to a greater reliance on third parties, or employee burnout when resources are overstretched.

Most insurers in the sample reported to follow cyber security standards. However, it was not clear whether this led to a certification, and hence, it was not possible to assess how closely these standards were followed. Certifications can help supervisors assess the level of cyber hygiene of a company, but overreliance on certification could also lead to complacency. Standards chosen by a firm should fit their business needs and their cyber security risk appetite.

Supervisors have also been actively developing and implementing macroprudential supervision frameworks and tools for cyber risk, such as including cyber scenarios in stress tests and collecting data on common vulnerabilities. Additionally, supervisors have been working on initiatives to develop a common taxonomy, standards and guidelines essential for effective supervision at the micro and macro levels.

FINANCIAL STABILITY

From an insurance risk perspective, the cyber underwriting activities of insurers in the sample were not assessed as posing a threat to financial stability. The affirmative coverage market was still small and the sector would have been able to absorb large losses. Because of data limitations and differences in how non-affirmative coverage was mitigated across jurisdictions and insurers, it was not possible to fully assess the risk this type of exposure poses to financial stability.

Cyber operational risks with potential systemic implications are most likely to be external risks (eg supply chain, critical infrastructure) and could be amplified through various transmission channels, such as loss of confidence (eg due to lengthy outages and compromised data integrity), interconnectedness (eg within the financial system and across technologies) and substitutability (eg critical infrastructure, key service providers).[8]

The cyber operational risk management practices of insurers in the sample did not appear to incorporate systemic risk considerations, such as the ecosystem's exposure to single points of failure. On the supervisory side, collecting firm-level cyber resilience data for microprudential purposes could help identify macroprudential risks. However, this approach is hampered by a lack of common definitions, taxonomy and reporting standards, which have created barriers to consolidating microprudential information for macroprudential purposes.

Important data gaps limit the assessment of the systemic implications of non-affirmative coverage.

[8] See International Monetary Fund, Cyber Risk and Financial Stability: It's a Small World After All, December 2020.

1. Introduction

GIMAR special topic editions focus on specific insurance sector issues and their impact on financial stability. This special topic edition contributes to the IAIS' strategic work on cyber risk, which is a key theme of the IAIS' five-year strategic plan for 2020–2024.[9]

Cyber risk is a key concern for supervisors, regulators and the insurance industry alike. According to the 2021 GIMAR, supervisors were increasingly concerned about the rising frequency and severity of these cyber attacks.[10] Similarly, the Allianz Risk Barometer 2022 ranked cyber risk as the most important global business risk for 2022, pointing to the increased frequency of ransomware attacks, remote working policies and a larger cyber attack surface.[11] These concerns have been heightened by the current geopolitical backdrop.

This report presents an analysis of the current risks and trends associated with cyber insurance coverage, cyber resilience in the insurance sector and the impact these risks may pose to financial stability. Based on data collected through the IAIS GME from insurers and jurisdictions (see section 3.1), the report presents:

- Information on cyber insurance premiums, claims, coverage and exposures, as well as a summary of the different risk-mitigation strategies adopted by insurers and their impact on protection levels;
- Analysis of the level of cyber resilience in the insurance sector based on information provided on security frameworks, risk assessment, response plans and risk-controls implementation, as well as a summary of the supervisory assessment of these risks and key supervisory initiatives in different jurisdictions.

This analysis is complemented by feedback provided during external stakeholder events in 2022, such as the IAIS' Chief Risk Officer Roundtable, Global Seminar and Annual Conference.[12,13,14]

Despite being one of the top risks across jurisdictions, there are important data gaps for supervisors. This edition of the GIMAR special topic series should be viewed as an initial attempt to collect data at the global level on the cyber insurance market, underwriting risks and the operational resilience of insurers. Despite the biases and limitations of the sample, the granularity of the data also allows for a bottom-up approach to assess systemic risks. The jurisdictional data provide a

9 See IAIS, IAIS Strategic Plan 2020–2024 (June 2019).
10 See IAIS, GIMAR 2021 (November 2021).
11 See www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2022-press-de.html.
12 See IAIS July 2022 newsletter.
13 See 2022 IAIS Global Seminar.
14 See 2022 IAIS Annual Conference.

broad view of the issues, while insurer-level data provide enough granularity to add nuance to the analysis.

The report also provides potential data templates for jurisdictions that are beginning to collect data on cyber risks.[15] Lastly, this analysis provides information on potential emerging risks that should help inform the need for future work. By publishing this report, the IAIS aims to contribute to the debate on the impact of cyber risk on the insurance sector, cyber protection gaps, cyber risks posed to financial stability, and the associated supervisory responses.

1.1 SCOPE AND CONTEXT

This report covers a general overview of trends and key aspects of the cyber insurance market and the cyber resilience of insurers from a supervisory perspective. It is not intended to be a technical analysis of the various actuarial and operational issues covered by the overview. For instance, while this analysis briefly covers data issues, it does not provide a rigorous analysis on data availability and suitability. Moreover, data limitations also constrain the depth of the analysis. Due to the lack of data, the report does not quantitatively assess the risks posed by cyber insurance exposures. While the assessment of the cyber resilience of the insurance sector focuses on security threats and third-party risks, it does not cover other issues, such as internal threats, systems failures and human error.

This report builds on previous IAIS work on this topic. In 2016, the IAIS published an issues paper that aimed to raise awareness about the challenges presented by cyber risk for insurers and supervisors.[16,17] It recommended the IAIS develop and publish an application paper to further explore cyber risk, cyber security and cyber resilience and propose supervisory practices for the insurance sector. An Application Paper on Supervision of Insurer Cyber Security was published in 2018. While these earlier papers focused on cyber resilience, the IAIS published an additional paper in 2020 focused on the cyber underwriting market.[20] Cyber risk was also a macroprudential theme of the 2021 GIMAR.[21] Most recently, in October 2022, the IAIS' Operational Resilience Task Force (ORTF) published for consultation a draft Issues Paper on Insurance Sector Operational Resilience, which included the topic of cyber resilience.[22]

1.2 STRUCTURE

The rest of this report is structured as follows:

- Section 2 describes the data collection process, the samples and the data limitations.
- Section 3 presents a general overview of key aspects and trends in the cyber insurance market, analyses the risks posed by affirmative and non-affirmative coverage and the different mitigation strategies adopted, considers the likely impact current trends may have on the cyber insurance protection gap and discusses the supervisory assessment.
- Section 4 analyses the risk-management strategies and cyber security posture of insurers in the sample, discusses limitations of this evaluation and presents the supervisory assessment.
- Section 5 evaluates how the cyber insurance market and the resilience of insurers could pose a threat to financial stability.
- Section 6 concludes the discussion and presents recommendations.

---

15 For a copy of the technical specifications of the data collection and the data templates, see GIMAR 2022 Annex 4.

16 IAIS Issues Papers provide background on particular topics, describe current practices, actual examples or case studies pertaining to a particular topic and/or identify related regulatory and supervisory issues and challenges.

17 See IAIS, Cyber Risk to the Insurance Sector (August 2016).

18 IAIS Application Papers provide supporting material related to specific IAIS supervisory material.

19 See IAIS, Supervision of Insurer Cybersecurity (November 2018).

20 See IAIS, Cyber Risk Underwriting Identified Challenges and Supervisory Considerations for Sustainable Market Development (December 2020).

21 See IAIS, GIMAR 2021 (November 2021).

22 See IAIS, Insurance Sector Operational Resilience (October 2022).

2. Data

2.1 SAMPLE SELECTION AND DATA COLLECTION

The IAIS collected data on cyber underwriting activities and cyber resilience through the 2022 GME data collections covering year-end 2021 data.[23] This data collection was split into two modules as follows.

The first module collected data from individual insurers that met the GME insurer pool qualifying criteria.[24] This insurer pool included about 60 of the largest international insurers from 18 jurisdictions. The cyber underwriting component of this data collection from individual insurers had a quantitative section that captured data on key aspects of the participating insurers' cyber underwriting activities, such as premiums, claims, exposures and coverage. It also had a qualitative section on cyber insurance practices (eg risk mitigation strategies for affirmative and non-affirmative coverage) and cyber operational resilience (eg cyber security frameworks, risk assessments, response plans and risk controls).

The second module of the data collection was sent to IAIS member jurisdictions that met the GME criteria (27 jurisdictions) and jurisdictions that did not meet the criteria but that volunteered the information (18 jurisdictions).[25,26] In total, these jurisdictions covered over 90% of global GWP.[27] This 2022 data collection from supervisors also included cyber qualitative and quantitative components. The quantitative information collected was on cyber insurance market data (eg premiums, claims, exposures and reinsurance activity). The qualitative section focused on approaches used to supervise the cyber insurance market and the cyber resilience of insurers. All questions allowed respondents to add comments or explanations, which provided further insights.

From the insurer pool, 25 insurers reported their cyber underwriting activity for 2021, and 50 sent in their information on cyber resilience. From jurisdictions, 19 reported on cyber underwriting activity in their market and 27 sent data related to the supervision of cyber resilience.

---

23 The GME is the IAIS' framework for monitoring risks and trends in the global insurance sector and assessing the possible build-up of systemic risk.

24 This data collection is referred to as individual insurer monitoring (IIM) in the GIMAR.

25 See IAIS, IAIS Holistic Framework for Systemic Risk in the Insurance Sector: GME (November 2019).

26 This data collection is referred to as sector wide monitoring (SWM) in the GIMAR.

27 See GIMAR 2022.

In this report, all data (from jurisdictions, insurers and external sources) are analysed and summarised by variable of interest (eg net claims). Unless otherwise stated and where applicable, aggregate jurisdictional data (broader scope) are presented and summarised first. These are followed by the aggregate insurer-level data (higher level of granularity) for each variable. This is complemented, where possible, with data from external sources to provide insights on changes across time.

2.2 DATA LIMITATIONS

Since the criteria for the inclusion in the insurer pool are based on the size of total assets of insurance groups, this set tends to be biased towards the life sector. Hence, this sample misses important carriers in the cyber underwriting market. The results must be read with caution, as they may not extrapolate to the whole industry. Additionally, the data coverage of some variables is not large enough to draw statistical inferences, and the voluntary nature of this exercise introduces selection bias.

The number of questions was kept to a minimum to reduce the burden on participating insurers and jurisdictions. Therefore, no data were collected for years before 2021, so it is difficult to assess the evolution of this market and the cyber resilience of the insurers across time. It is also difficult to evaluate changes in the supervisory assessments of and responses to these issues.

Therefore, as stated earlier, data collected are complemented with information from reputable external sources. It is up to the reader to evaluate the quality of their information and reports. Any issues with data from external sources may impact the conclusions reached in this report.

Comparing variables across jurisdictions and insurers is difficult, as some of their definitions vary considerably. Hence, the aggregation of variables (eg premiums) needs to be taken with caution. In some instances, proxies are constructed to derive insights into a particular variable of interest (eg loss ratios = claims/premiums). However, these proxies are noisy by construction, so any conclusion must be caveated, taken with care and not extrapolated.

Despite these biases, this novel dataset provides new insights into how cyber risk is underwritten, monitored and managed. The granularity of the data collected from individual insurers and the broad coverage of the data from jurisdictions provide a unique perspective into the cyber underwriting market and the cyber resilience of the industry in 2021.

The novel dataset used in this report provides new insights into how cyber risk is underwritten, monitored and managed.

3 . Trends and key aspects of the global cyber insurance market

3.1 BACKGROUND TO DATA IN CYBER INSURANCE

Cyber insurance policies date back to the late 1990s, when they were tailored to risks from internet-based activities such as e-commerce.[28] Since then, the market has experienced substantial growth, driven by demand for cyber risk management tools. The underlying risk has also evolved and grown over time as digitalisation continues to play a more important role in all aspects of life. Although data that are useful in underwriting cyber insurance have increased in quantity and quality since the market's inception, important data gaps remain, particularly about catastrophe events. Furthermore, there are complex issues around the capturing and sharing of data on cyber incidents.[29]

Across jurisdictions, different data-reporting requirements apply to cyber incidents, which causes challenges when analysing these data. To that end, standard-setting bodies such as the Financial Stability Board (FSB) are developing common definitions and standards for cyber incident reporting.[30] The insurance industry has also been leading efforts to collect data, provide analysis and intelligence and develop voluntary standards for cyber underwriting data.[31] Data vendors have also been developing data lakes (with proxies that track variables of interest), along with forward-looking indicators to circumvent stale data issues.[32]

This section summarises the information that was gathered through the IAIS data collection on cyber underwriting risk. Summary statistics for quantitative data collected from insurers and jurisdictions can be found in Table 1 and Table 2, respectively. The sample pool of insurers contains both reinsurers and direct insurers. Both are referred to as insurers unless there is a need for differentiation. Data from insurers are provided at the group level. Hence, data from insurers are not necessarily indicative of the cyber insurance market where the insurers are headquartered. All figures are presented in US$ millions unless otherwise stated.[33] For a complete definition of each variable, please see the GME technical specifications.[34]

---

28 For a discussion on issues and a historical perspective, please see J Wolff, (2022) Cyberinsurance Policy (2022).
29 See Gallagher Re, Evaluating Cyber Models (2022).
30 See FSB, Achieving Greater Convergence in Cyber Incident Reporting (October 2022).
31 See cyberacuview.com.
32 See P H Meland et al, A Systematic Mapping Study on Cyber Security Indicator Data, Electronics (October 2021).
33 To convert monetary amounts into United States dollars, the process set out in the GME was followed.
34 See GIMAR 2022 Annex 4.

TABLE 1: Summary statistics – GME 2022 insurer pool ($ millions)

		Sum	Average	Standard deviation	Minimum	First	Median	Third	Maximum	Insurers	Number of zeroes	Missing values
CYBER	Direct premiums written for cyber risk coverage	$6,658.42	$277.43	$531.98	$0.09	$8.55	$74.87	$289.11	$2,498.13	25	0	1
	Assumed premiums for cyber risk coverage	$2,584.35	$112.36	$206.64	–	$0.01	$33.00	$83.43	$806.58	25	6	2
	Net technical provisions (cyber related only)	$1,942.24	$129.48	$279.92	–	$0.15	$12.53	$112.89	$1,053.81	25	2	10
	Net incurred claims (cyber related only)	$2,508.05	$125.40	$206.19	–	$0.71	$46.81	$136.62	$819.82	25	2	5
	Premiums ceded to reinsurance (total in reporting currency, cyber related only)	$2,536.98	$120.81	$183.60	–	$1.02	$30.81	$148.81	$649.51	25	1	4
	Highest cyber coverage limit underwritten		$50.69	$41.23	$2.45	$23.07	$34.54	$93.56	$122.02	25	0	5
	Average cyber coverage limit underwritten		$3.29	$3.02	$0.29	$1.15	$2.43	$4.03	$11.14	25	0	5
ALL ACTIVITIES	Total assets	$10,520,521.57	$420,820.86	$414,678.80	$62,982.35	$127,715.44	$244,025.99	$596,112.00	$1,553,859.80	25	0	0
	Net incurred claims (non-life only)	$422,651.99	$19,211.45	$13,199.01	$2,891.26	$9,011.85	$17,059.62	$26,511.94	$49,964.00	25	0	3
	Common equity	$1,511,145.12	$65,701.96	$136,555.79	–	$11,607.94	$28,629.00	$58,548.06	$663,961.00	25	1	2
	Total GWP (non-life or health business)	$784,644.98	$35,665.68	$20,331.97	$4,729.93	$16,801.86	$35,983.88	$48,966.36	$74,207.59	25	0	3
	Premiums ceded	$143,500.07	$5,740.00	$4,452.04	$465.78	$2,285.00	$4,146.79	$8,986.55	$15,094.45	25	0	0
	ROE: Return on equity (%)		9%	4%	0%	6%	9%	13%	17%	25	1	0
	Net incurred claims/Net earned premium (%), non-life only		65%	8%	41%	63%	66%	70%	79%	25	0	3

Source: GME 2022 insurer pool

TABLE 2: Summary statistics – GME 2022 jurisdiction pool ($ millions)

		Sum	Average	Standard deviation	Minimum	First	Median	Third	Maximum	Insurers	Number of zeroes	Missing values
INSURANCE (CYBER)	Gross written premium	$13,696.80	$760.93	$1,546.61	$0.05	$17.70	$38.55	$376.07	$4,927.00	27	0	9
	Technical provisions	$5,658.62	$471.55	$1,178.43	–	$1.62	$8.56	$168.77	$4,095.30	27	1	15
	Net incurred claims	$4,211.80	$280.79	$523.90	–	$0.28	$2.54	$217.11	$1,597.00	27	1	12
	Premiums ceded to reinsurance	$1,990.64	$180.97	$461.94	$0.04	$9.29	$16.02	$56.56	$1,555.86	27	0	16
	Number of written contracts	3,008,804	188,050.23	444,475.55	3	2,623	13,036	100,215	1,537,579	27	0	11
	Number of paid claims	7,202	514.41	970.21	–	10	19	157	2,725	27	1	13
	Loss ratio		45%	35%	0%	15%	45%	65%	112%	27	1	9
REINSURANCE (CYBER)	Total gross reinsurance premiums assumed (or premiums written)	$4,843.02	$484.30	$1,205.02	–	$6.60	$11.95	$323.84	$3,874.49	27	2	17
	Technical provisions (affirmative)	$1,370.95	$195.85	$326.39	–	$1.58	$11.75	$307.83	$740.38	27	2	20
	Net incurred claims	$1,168.61	$146.08	$216.82	–	$0.44	$6.19	$266.88	$563.55	27	2	19
	Number of paid claims	13,004,677	2,167,446	5,308,613	0	12.75	52.5	737.0	13,003,608	27	2	21
	Loss ratio		75%	92%	0%	5%	44%	87%	278%	27	2	18
ALL ACTIVITIES	Total assets (in non-life sector)	$7,928,011.96	$293,630.07	$598,545.37	$1,565.61	$17,559.83	$119,597.07	$317,135.07	$2,907,088.00	27	0	0
	Total net technical provisions of which are non-life or health business	$2,955,451.47	$113,671.21	$201,798.50	$819.69	$7,237.49	$35,709.42	$104,297.88	$807,145.00	27	0	1
	Total revenues (in non-life sector, in reporting period)	$1,523,709.64	$89,629.98	$184,887.86	$3,403.90	$8,241.87	$29,903.50	$88,346.71	$777,266.00	27	0	10

Source: GME 2022 jurisdiction pool

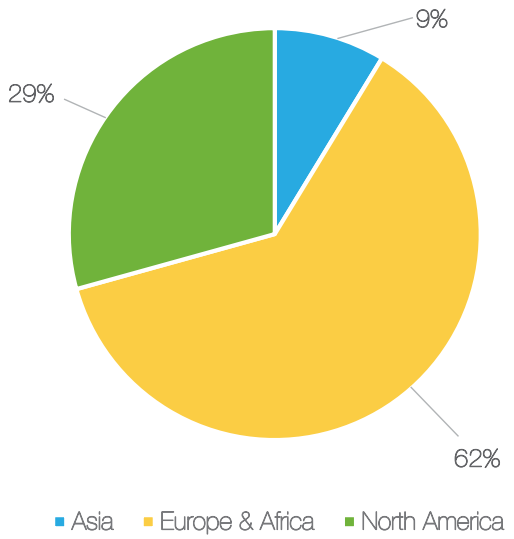
3.2 PREMIUMS

Nineteen jurisdictions reported a total of $13.7 billion in GWP in 2021 for cyber coverage, which compares to $6 billion of cyber GWP reported by 13 jurisdictions in 2020. As per Table 3, 71% of the premiums were underwritten in the Americas, 29% in Europe and Africa, and less than 1% in Asia and Oceania.

In 2021, insurers in the sample reported a total of $6.7 billion in direct written premiums for cyber risk coverage.[35] This amounted to less than 1% of the non-life GWP for these insurers. There was substantial variation in the level of premiums reported. For instance, the average of direct written premiums reported was $277.43 million, while the median was $74.87 million. Most premiums were concentrated in a small number of insurers – six insurers accounted for over 80% of all written reported premiums in the sample. As Figure 1 shows, over two thirds of the cyber insurance premiums reported were underwritten by insurers headquartered in Europe and Africa.

Global cyber insurance premiums have grown considerably in the last five years. According to

FIGURE 1: Direct premiums written by insurers' pool, 2021



Source: GME 2022 insurer pool

TABLE 3: Cyber GWP by region, 2021 ($ millions)

	Total GWP	Percentage of total	Countries	Missing data
Americas	$9,693.41	71%	5	0
Asia & Oceania	$55.72	<1%	3	0
Europe & Africa	$3,947.67	29%	11	1
Total	$13,696.80	100%	19	1

Source: GME 2022 jurisdiction pool

[35] For a definition of cyber coverage, please see GIMAR 2022 Annex 4.

Munich Re, global cyber insurance premiums have almost doubled from 2018 to 2021.[36] Marsh reports a full-year 2021 rate increase of 79%.[37] For Q2 2022, the Council of Insurance Agents and Brokers estimated that cyber premiums had increased 26% on average.[38] This level of growth is expected to remain high in the near term. For instance, Munich Re estimates that global premiums will reach $22 billion by the end of 2025 and Fortune Business Insights estimates that the global cyber insurance market will grow to $63 billion by 2029.[39,40] The higher frequency and severity of cyber attacks, a greater cyber attack surface as a result of digitalisation and remote working policies, and a riskier cyber landscape are expected to continue to push demand for cyber coverage to record levels.

3.3 NET CLAIMS AND PROFITABILITY

Net claims for cyber insurance reported by jurisdictions were $4.2 billion (from 15 respondents). Nearly two thirds of net claims originated in the Americas and about one third came from Europe and Africa (see Table 4). When the sample is limited to jurisdictions that report more than $1 million in premiums, the average loss ratio reported was 48% (from 16 respondents), where half the sample reported loss ratios lower than 53% (see Table 5). The average net claims to GWP for all non-life business in these jurisdictions was close to 38%. While these two metrics are not directly comparable, they seem to point to a lower profitability of cyber insurance compared to the overall non-life business in this sample.

TABLE 4: Net cyber insurance claims by region ($ millions)

	Net claims	Percentage of total	Countries	Missing data
Americas	$2,677.01	63%	5	0
Asia & Oceania	$4.35	0%	3	0
Europe & Africa	$1,575.93	37%	11	4

Source: GME 2022 jurisdiction pool

TABLE 5: Profitability for P&C and cyber

	Average	Standard deviation	Min	1st quartile	Median	3rd quartile	Max	N	Zeroes	Missing
Claims/GWP (P&C)	38%	10%	20%	34%	36%	40%	58%	16	0	0
Loss ratio	48%	32%	3%	27%	53%	65%	112%	16	0	1

Source: GME 2022 jurisdiction pool

36 See Cyber Insurance: Risks and Trends (2022).
37 See www.theinsurer.com/viewpoint/cyber-risk-evolution/.
38 See the Commercial Property/Casualty Market Index.
39 See Munich Re, Munich Re Global Cyber Risk and Insurance Survey 2022.
40 See www.fortunebusinessinsights.com/cyber-insurance-market-106287.

The total of cyber-related net incurred claims reported by insurers in the sample was $2.5 billion (15 respondents). This amounted to less than 1% of their total non-life net claims ($299 billion). Although not all the insurers active in the cyber insurance market reported net claims, their distribution was similar to that of direct written premiums, where the bulk of all net claims was concentrated in a few participants. This can be seen in the difference between the average ($125.40 million) and median ($46.81 million) net claims, where a few large outliers drove the average. One third of these net claims were reported by insurers and the remaining two thirds by reinsurers (see Table 6).

TABLE 6: Net incurred claims by business type

	Percentage
Insurance	35%
Reinsurance	65%

Source: GME 2022 insurer pool

The profitability of cyber insurance activity in the sample of insurers tended to be lower than that of their overall non-life business. To illustrate this point, Table 7 presents the distribution of a proxy for profitability (the ratio between claims and premiums). When the sample is restricted to companies that reported premiums over $1 million, the ratio of total net claims to total direct premiums is 68% for cyber insurance, compared to 55% for their overall non-life and health business (see Figure 2).[41] While these two ratios are not directly comparable (eg cyber is part of the non-life business), they do provide some insights into the differences in profitability of cyber insurance and overall non-life business. For example, the distribution of this profitability proxy for individual companies shows that for half of the insurers, their cyber business profit was better than their non-life profit (median cyber = 32.95%, median non-life = 57.80%). However, for the other half of insurers it was substantially worse (cyber third quartile = 87%, non-life third quartile = 60%). Evidently, the overall profitability of cyber was driven by a handful of outliers with large loss ratios. Hence, looking at the average of this ratio for cyber underwriting alone could be misleading because of the presence of a large outlier that is a small player in this market.

The total of cyber-related net incurred claims reported by insurers in the sample was $2.5 billion. This amounted to less than 1% of their total non-life net claims.

TABLE 7: Claims to premiums ratio

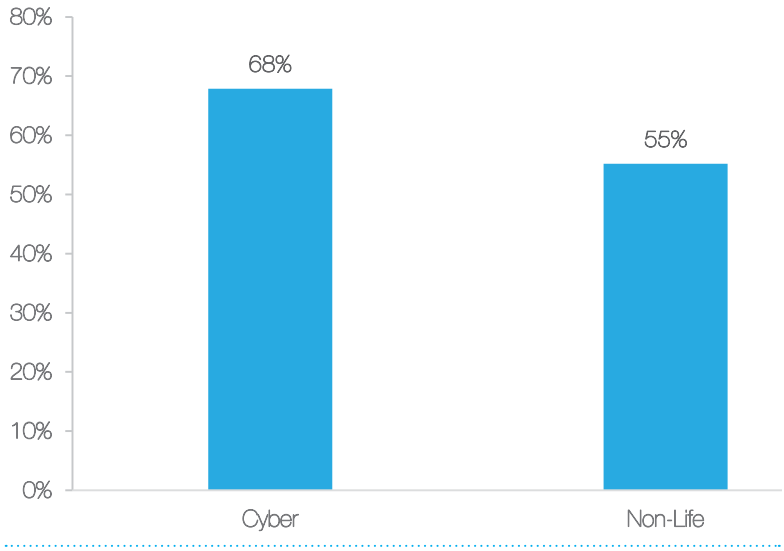
	Average	Standard deviation	Min	1st quartile	Median	3rd quartile	Max	N
Claims/premiums cyber	99%	186%	0%	13%	33%	87%	732%	15
Claims/premiums non-life	55%	8%	42%	47%	58%	60%	70%	15

Source: GME 2022 insurer pool

[41] This ratio is calculated by dividing the aggregate net claims reported by the aggregate premiums reported.

Data from external sources validate the findings for insurers presented above. Pre-2020, loss ratios in the US were below 50%.[42] However, these ratios increased to above 70% in 2020, with some major insurers exceeding 100%, mainly driven by ransomware claims.[43] Similar to the calculations above, Fitch ratings reports that the industry loss ratio was 65% in 2021, down from 72% in 2020.[44] The decline in this loss ratio was attributed to higher premiums but also to lower losses (reflecting fewer ransomware claims) and the implementing of various underwriting controls.

FIGURE 2: Ratio of aggregate claims to aggregate premiums



Source: GME 2022 insurer pool

The ratio of total net claims to total direct premiums is 68% for cyber insurance, compared to 55% for their overall non-life and health business.

3.4 NUMBER OF CLAIMS AND CONTRACTS

Participating jurisdictions reported data on the number of paid claims and written contracts (including standalone or affirmative cyber) in 2021. Table 8 shows the ratio of total net paid claims to the number of all paid claims in each jurisdiction. Table 8 also shows the ratio of total GWP to the number of all contracts for each jurisdiction. The ratio of net paid claims to the number of paid claims has an average of $630,000, with a median of $140,000. The ratio of GWP to the number of contracts is on average $20,000, with a median of $10,000.

TABLE 8: Dollars per claim and contract ($ millions)

	Average	Standard deviation	Median	Max	N
$/claim	$0.63	$1.11	$0.14	$3.64	10
$/contract	$0.02	$0.04	$0.01	$0.14	13

Source: GME 2022 insurer pool

42 See Aon, 2021 US Cyber Market Update, US Cyber Insurance Profits and Performance (2021).
43 See NAIC, Cybersecurity Insurance Market 2020 (2021).
44 See Fitch Ratings, US Cyber Insurance Sees Rapid Premium Growth, Declining Loss Ratios (2022).

3.5 COVERAGE LIMITS

In terms of coverage, insurers reported their maximum and average cyber cover offered in 2021. The highest coverage limit offered by insurers was on average $50 million, with a range between $2.45 million and $122 million and a median of $30.56 million. In terms of the average cyber coverage limit, the amount reported ranged from $0.29 million to $11.14 million, with an overall average of $3.59 million and a median of $3.08 million. Some insurers commented that limits are likely to be lower for new business and that higher limits are offered via consortiums.

3.6 ASSUMED AND CEDED PREMIUMS

Participating jurisdictions reported ceded premiums close to $2 billion (11 respondents). When the sample is restricted to jurisdictions that reported premiums over $1 million (nine respondents), 54% of the cyber premiums were ceded to reinsurers on average, whereas for overall non-life lines of business the figure was about 29% (see Table 9). On aggregate, the ratios of ceded to GWP were 38% and 22% for cyber and overall P&C lines of business, respectively, for these 16 jurisdictions.

Aggregate assumed and ceded premiums reported by insurers in the sample were $2.5 billion. Almost all the insurers in the sample reinsured cyber risk (see Table 10). Table 11 shows that for these insurers, on average 37% of the cyber direct premiums were ceded, compared to 12% of their overall non-life premiums. Guy Carpenter has estimated that about 40% of all cyber premiums flow to the reinsurance sector, consistent with the figures collected from both jurisdictions and individual insurers.[45] This could be driven by new entrants to the cyber market seeking to partner with a reinsurer – a common way to enter a new line of business to gain data and insight into the class.

TABLE 10: Is cyber risk exposure reinsured?

Answer	Percentage
Yes	88%
No	4%
No data	8%

Source: GME 2022 insurer pool

TABLE 9: Ceded premiums

	Min	Average	Median	Max
Ceded (cyber)	25%	54%	53%	89%
Ceded (non-life)	17%	29%	25%	58%

Source: GME 2022 jurisdiction pool

[45] See www.theinsurer.com/viewpoint/cyber-risk-evolution/.

TABLE 11: Proportion of premiums ceded

	Average	Standard deviation	Min	1st quartile	Median	3rd quartile	Max	N	Missing
Ceded (non-life)	12%	9%	3%	5%	11%	20%	27%	15	1
Ceded (cyber)	37%	22%	3%	20%	37%	56%	65%	15	0

Source: GME 2022 insurer pool

3.7 REINSURANCE

The data collected on reinsurance through the GME data collection were not representative, as the information was only provided by a handful of jurisdictions. However, the data have been summarised for completeness. Jurisdictions reported a total of $4.8 billion gross reinsurance premiums (10 jurisdictions) and technical provisions of $1.3 billion (seven jurisdictions) in 2021. Total net claims reported amounted to $1.17 billion (from eight jurisdictions). The average loss ratio reported (by nine jurisdictions) was 75%, with a median of 44%. The difference between the average and the median loss ratio can be attributed to a large outlier in the sample. Additionally, as of 2021, no national competent authority has reported being aware of any capital market activity with the purpose of transferring risk (eg insurance-linked securities, industry loss warranties). That said, it may be important to note that there have been cyber-related insurance-linked securities trades in 2023.[46,47]

3.8 EXPOSURES

While data on exposures were not representative, with only 12 jurisdictions providing information on technical provisions, the data still provided interesting insights. These jurisdictions reported total technical provisions for affirmative coverage for cyber exposures of $5.5 billion. As with other variables, the data were very skewed – a small number of jurisdictions accounted for most of the technical provisions reported.

Only 15 insurers submitted data on technical provisions for cyber policies. These insurers reported a total of $1.9 billion in technical provisions due to cyber policies in 2021. Some participating insurers indicated that they did not disaggregate technical provisions for their cyber line of business. Data on exposures arising from non-affirmative cover were not reported, exacerbating monitoring and supervisory issues.

To derive an estimate of potential cyber catastrophe exposure, CyberCube modelled the impact of non-cat (eg isolated data breaches, targeted ransomware) and cat (eg widespread cloud outages or widespread untargeted ransomware) cyber risks on the loss distribution for standalone affirmative coverage in the US.[48] The model incorporates their rate estimates for 2023. As shown in Figure 3, for a typical breakeven loss ratio, most of the losses would come from non-cat (local and scalable) losses. However, in the tail, a 1-in-250-year event could trigger insurance losses of about $30 billion.[49]

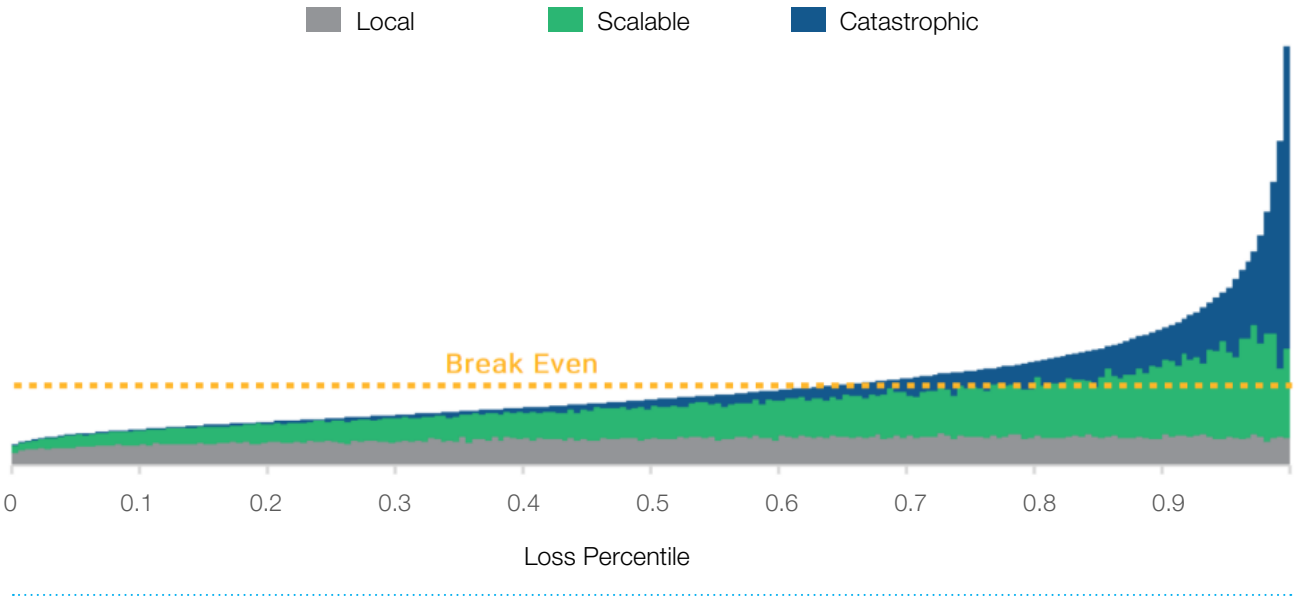
[46] First fully tradeable cyber cat bond under Rule 144A of the US Securities and Exchange Commission; for more information, see www.artemis.bm/deal-directory/beazley-cyber-cat-bond-2023-1/.

[47] First transfer of cyber risks to the capital markets through a proportional or quota share structure; for more information, see www.insuranceerm.com/news-comment/hannover-re-pioneers-$100m-cyber-retro-deal-with-stone-ridge.html.

[48] CyberCube is a provider of cyber risk analytics for the insurance industry. See www.cybcube.com.

[49] For illustrative purposes, a breakeven point is assumed to be 70% in Figure 3.

FIGURE 3: Representative loss ratio distribution



Source: CyberCube

It is also important to highlight that the frequency of these cyber tail events appears to be lower than that of natural catastrophe (NatCat) events such as category 5 and 4 hurricanes. To put these figures into context, Munich Re reports that NatCats were responsible for $270 billion of economic losses worldwide in 2022, of which $120 billion were insurance losses.[50] Hurricane Ian (category 4) alone was responsible for $100 billion and $60 billion in economic and insurance losses respectively in 2022. The largest cyber event to date (NotPetya in 2017) caused economic losses of $10 billion, of which about $3 billion was due to insurance losses (affirmatively and non-affirmatively).[51]

3.9 CYBER RISKS AND AFFIRMATIVE COVERAGE

Most insurers active in the cyber underwriting market covered (via affirmative coverage) data confidentiality, breaches and liability, network security, communication and media liability, cyber extortion and business interruption risks. The types of risk coverage least mentioned by insurers were technology disruptions, cyber fraud and theft and contingent business interruption (see Table 12).

According to participating insurers, the cyber threats with the highest potential underwriting losses were ransomware and mass vulnerability attacks, followed by cloud outages, data breaches and vulnerabilities stemming from third-party service providers (see Annex 1 Tables 41–47). Other threats reported were privacy breaches, business interruptions and social engineering attacks (see Figure 4). This aligns with Marsh and Microsoft's 2022 cyber risk survey, where ransomware was reportedly the top cyber threat, and 75% of participants were impacted by a cyber attack.[52]

[50] See www.reinsurancene.ws/munich-re-pegs-global-insured-nat-cat-losses-at-120bn-in-2022/.
[51] See pcs.iso.com/globalnews/pcs_covid_informational_bulletin_4.pdf.
[52] See Marsh and Microsoft, The State of Cyber Resilience (2022).

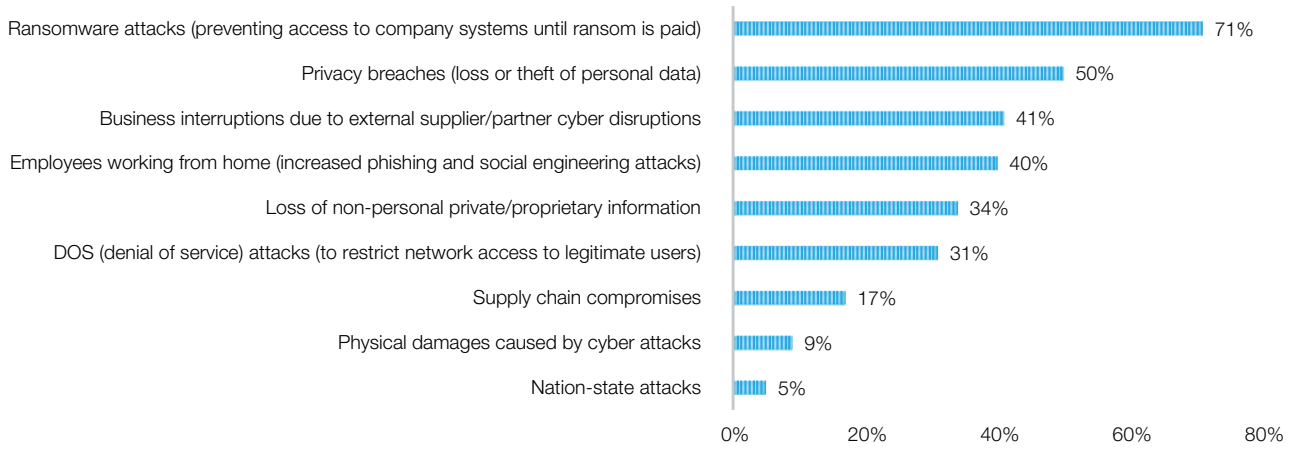
TABLE 12: Types of risk covered (select all that apply)

Answer	Percentage
Data confidentiality	88%
Liability	88%
Breaches	88%
Network security	84%
Business interruption	84%
Cyber extortion	84%
Communication and media liability	84%
Technology disruptions	68%
Cyber fraud and theft	68%
Contingent business interruption	52%
Other	12%

Source: GME 2022 insurer pool

According to insurers, the cyber threats with the highest potential underwriting losses were ransomware and mass vulnerability attacks, followed by cloud outage, data breaches and vulnerabilities stemming from third-party service providers.

FIGURE 4: Top cyber threats



Source: Marsh and Microsoft 2022.

3.10 RISK MONITORING AND MITIGATION STRATEGIES

3.10.1 Affirmative coverage

Affirmative coverage risk mitigation strategies (see Table 13) employed by insurers in the sample included reducing policy limits (84%), increasing deductibles (64%), making terms and conditions contingent on IT risk controls such as multi-factor authentication (48%) or on specific industry sectors (44%), and using reinsurance (36%). Insurers reported that the adoption of mitigation measures could depend on product type and the market. Others indicated that they were creating awareness and clarity as well as implementing pool solutions to mitigate these risks.

One way in which insurers can help prevent a peril – and minimise losses should the peril occur – is to offer ex ante and ex post services. An added benefit of these services is the increased awareness and better security posture of policyholders. About 64% of insurers active in cyber underwriting also provided cyber advisory services, either as part of the policy or as an add-on (see Table 14). The availability of these services varied across regions and cyber risks, and included pre-breach services, education tools and virtual chief information security officer (CISO) services (ex ante) and legal, forensic and consulting services (ex post).

Such services are not limited to insurers. Half of the reinsurers in the sample also offered cyber advisory services to their cedants, either as a standard policy benefit or as an add-on.

TABLE 13: What type of mitigation measures are in place to limit the impact of affirmative cyber risk? (Select all that apply)

Answer	Percentage
Reducing policy limits	84%
Increasing deductibles	64%
Terms and conditions contingent on IT risk controls (eg multi-factor authentication)	48%
Terms and conditions contingent on specific industry sectors	44%
Increasing co-insurance	36%
Assessment of ICT risk management of policyholders	36%
Requesting more data from insurers (eg more comprehensive/technical cyber insurance applications)	36%
Terms and conditions contingent on IT suppliers/vendors	28%
Introducing sub-limits for specific covers (eg business interruption)	24%
Exit business	24%
Pooling data with other insurers/third parties	12%
Decreasing underwriting	4%

Source: GME 2022 insurer pool

TABLE 14: Do you provide cyber advisory services to clients?

Answer	Percentage
Yes, as add-on service	32%
Yes, included in policy	28%
No	24%
No data	16%

Source: GME 2022 insurer pool

Most insurers in the sample applied some mitigating measures to limit the impact of non-affirmative cyber coverage.

TABLE 15: Is cyber risk explicitly excluded from the following policies?

Answer	Percentage
Property	64%
Business interruption	60%
Contingent business interruption	60%
Liability	56%
Kidnap and ransom	48%
Crime and fidelity	36%

Source: GME 2022 insurer pool

3.10.2 Non-affirmative coverage

Insurance groups in the sample have implemented several strategies to assess their exposure to non-affirmative cyber coverage. This seems to be split into three main phases: review of current policies; assessment; and accumulation modelling. In the review phase, carriers analyse whether their existing products could expose them to cyber risk even if this risk is not affirmatively covered. In some cases this is done by asking underwriters how realistic disaster scenarios (RDS) would impact current policies, or by scoring policies based on predetermined criteria that help identify non-affirmative exposures. In the assessment phase, insurers quantify potential losses for each policy. In the modelling phase, companies model accumulation risk and integrate these exposures into their internal risk models. This also allows insurers to perform stress and scenario tests.

Most insurers in the sample applied some type of mitigating measures to limit the impact of non-affirmative cyber coverage. Seventy-six per cent (76%) of insurers indicated that these measures usually comprised adjusting terms and conditions of the insurance policies potentially subject to non-affirmative cyber coverage, such as adding exclusions or adjusting policy wording (44%), adjusting or introducing limits or sub-limits to the insurance coverage and/or using reinsurance (28%). Explicit exclusion of cyber risk (see Table 15) was most common in property policies (64%), followed by business interruption (60%), contingent business interruption (60%) and liability (56%) policies. Several insurers have also explicitly excluded cyber risk from crime/fidelity and kidnap and ransom policies. Some clarified that exclusions typically apply to non-physical cyber events. However, consequential damage from cyber events was usually covered by property insurance (eg if a cyber event led to a fire, the insured asset damaged by the fire would be covered). It is important to note that newly introduced exclusionary language may not have been tested in courts. Other measures to mitigate the impact of non-affirmative coverage included developing guidelines, training and underwriting controls.

3.11 PROTECTION GAP

There are several aspects to consider in respect of a potential cyber risk protection gap, including geographic or sectoral differences in insurance penetration and the overall balance in global supply and demand. For example:

- As seen in Table 3 and Figure 1, GWP in Asia were less than 1% of the total GWP reported by jurisdictions and 9% of direct premiums reported by participating insurers headquartered in Asia;[53]
- The 2021 LUCY report from AMRAE documents that while 84% of large companies in their sample had cyber insurance cover, only 9% of mid-size companies did.[54] For small to micro companies, the cover rate was 0.2%.

3.12 SUPERVISORY ASSESSMENT

Supervisors in over half (58%) of the participating jurisdictions reported that cyber underwriting risks were increasing (see Table 16). One jurisdiction indicated that the risk was decreasing due to greater awareness of underwriters with respect to cyber risk, a tidying of the portfolio for non-affirmative cyber coverage, and more strict requirements in terms of the cyber hygiene of accepted policyholders. Of the respondents, 90% also stated that cyber risks were sometimes or always excluded from non-cyber policies (see Table 17), which largely aligned with what insurers have reported.

TABLE 16: Cyber underwriting risk (Increasing/Decreasing)

Answer	Percentage
Increasing	58%
Stable	11%
Decreasing	5%
No data	26%

Source: GME 2022 jurisdiction pool

TABLE 17: Is cyber risk explicitly excluded from non-cyber policies offered within your jurisdiction?

Answer	Percentage
Sometimes	79%
Always	11%
Never	5%
No data	5%

Source: GME 2022 jurisdiction pool

Half of the jurisdictions reported that they collect data on cyber underwriting activities (see Table 18), and most of the jurisdictions that did not collect these data indicated that they would soon start. For example, from 2023, EU jurisdictions are introducing a dedicated template to collect cyber underwriting data for Solvency II reporting.[55]

[53] Some jurisdictions are actively addressing this issue in the region. For instance, Singapore's Cyber Security Agency introduced the Cybersecurity Certification Scheme to promote cyber hygiene measures with a view to partnering with the insurance industry to encourage the adoption of cyber insurance.

[54] See AMRAE, Lumière sur la cyberassurance (2022).

[55] See EIOPA, Draft Amended Implementing Technical Standards (ITS) on Supervisory Reporting and Disclosure (2022).

The top concerns listed by supervisors were accumulation risk, increasing claims frequency, and the rapidly evolving cyber threat landscape. Other elements of elevated concern were non-affirmative cyber coverage, pricing difficulties caused by the lack of data, underwriting and exposure management, and the concentration risk resulting from the limited number of IT service providers.

In terms of monitoring, the most periodically assessed or monitored variable was market size, followed by accumulation risk (affirmative coverage) and market concentration (see Table 19). Of the respondents, 42% indicated that they have also implemented frameworks to monitor systemic cyber risks (see Table 20), and 32% indicated that they carried out stress tests focused on cyber risk (see Table 21). Some stated that within the stress test, insurers could choose whether to incorporate a cyber scenario, while others specified that insurers were expected to develop such stress tests within their Own Risk and Solvency Assessment (ORSA).

TABLE 19: Do you periodically assess/ monitor the following in your jurisdiction (cyber underwriting market)?

Answer	Percentage
Size of market	63%
Total risk accumulation (affirmative coverage)	58%
Market concentration	47%
Total risk accumulation (non-affirmative coverage)	42%
Protection gap	5%

Source: GME 2022 jurisdiction pool

TABLE 18: Do you collect data on cyber underwriting activities (total value of written premiums, exposures, etc) on a regular basis (eg via regulatory returns)?

Answer	Percentage
Yes	53%
No	47%

Source: GME 2022 jurisdiction pool

TABLE 20: Do you assess and monitor potential systemic cyber risks (eg due to concentration, substitutability, critical infrastructure/service providers, etc)?

Answer	Percentage
Yes	42%
No	58%

Source: GME 2022 jurisdiction pool

Supervisors in over half of the participating jurisdictions reported that cyber underwriting risks are increasing.

TABLE 21: Does your jurisdiction carry out an insurance stress test on a regular basis – and if so, do they contain a cyber scenario?

Answer	Percentage
No	63%
Yes	32%
No data	5%

Source: GME 2022 jurisdiction pool

Supervisors listed cyber attacks on critical infrastructure, ransomware attacks, unavailability of cloud services and data exfiltration as the scenarios that could cause the largest underwriting losses (see Table 22). The main concerns of supervisors regarding cyber underwriting activities were lack of data availability, model maturity, accumulation risk, inadequate management of exposures (such as non-affirmative cyber exposures) and catastrophic or systemic losses.

For a list of supervisory initiatives, please see Annex 2.

TABLE 22 Please list the top three cyber scenarios that would cause the highest underwriting losses to insurers in your jurisdiction

Answer	Percentage
Cyber attacks on critical infrastructure	58%
Ransomware	48%
Cloud outage	37%
Data breach	32%
Business blackout	6%
Inadequate terms and conditions	6%
Legal disputes	6%

Source: GME 2022 jurisdiction pool

Supervisors listed cyber attacks on critical infrastructure, ransomware attacks, unavailability of cloud services and data exfiltration as the scenarios that could cause the largest underwriting losses.

4. Cyber resilience of the insurance sector

The FSB has defined cyber resilience as "the ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents".[56] As such, cyber resilience is not only the quantifying of risks and the strategies to address them, but also the ability to recover from shocks when risk management practices have not been effective. This ability to adapt and recover is key, as the probability of a cyber attack is high. Indeed, 75% of the organisations in the 2022 Marsh and Microsoft survey reported that they had experienced cyber attacks.[57]

As outlined in this section, the IAIS collected information on the cyber resilience of the insurance sector to try to find risks that could pose a threat to financial stability. Due to its macroprudential focus, this report is not intended to cover all aspects of cyber resilience in great depth.[58] It covers some topics with potential macroprudential implications, such as risk management practices, response plans to cyber threats, and a non-exhaustive set of cyber risk controls. Furthermore, the self-reporting nature of the survey and the lack of data granularity do not support an in-depth analysis. For instance, the maturity, effectiveness and completeness of the cyber risk controls reported by insurers could not be gauged. In terms of self-selection bias, respondents with good cyber controls tend to answer self-reporting surveys more readily than others. As mentioned previously, this section should also be seen as an initial attempt to collect global data on cyber resilience in the insurance sector.

4.1 CYBER RISKS TO THE INSURANCE INDUSTRY

4.1.1 Cyber threats

Responding jurisdictions were asked to rank the top cyber operational risks to their insurers. Out of the possible answer options provided, ransomware was most frequently ranked first, followed by social engineering and third-party supply chain attacks. Malware, inadequate patch management, endpoint attacks and Internet of Things attacks were the options least often ranked first (see Tables 54–60 in Annex 1).

Responding jurisdictions most frequently reported ransomware as the top cyber operational risk to insurers in their jurisdiction.

[56] See FSB, Cyber Lexicon (November 2018).
[57] See Marsh and Microsoft, The State of Cyber Resilience (2022).
[58] For a more comprehensive treatment of cyber resilience, please refer to IAIS, Issues Paper on Insurance Sector Operational Resilience (2022).

4.1.1.1 Ransomware

The main driver of cyber claims in 2021 was ransomware attacks.[59] According to SonicWall, the number of ransomware attacks increased 232% from 2019 to 2021.[60] While a ransomware attack usually involves hackers demanding money in exchange for decryption keys, it could trigger other types of insurance losses, such as business interruption, data recovery, investigations and fines. However, after a peak in 2021, ransomware attacks were reported by some sources to have slowly decreased. SonicWall reported that ransomware attacks were down 23% (236.1 million ransomware attempts) in H1 2022 due to strong control implementation, increased government response and the geopolitical landscape. Coveware reported that the median ransom payment had decreased to $36,360 in Q2 2022 (–51% from Q1 2022).[61,62]

Some jurisdictions (around 80%) asked firms questions about their preparedness or ability to recover from ransomware incidents (see Annex 1 Table 49). Only 19% of jurisdictions in the sample did not ask their regulated firms about their preparedness or ability to recover from ransomware incidents. However, these jurisdictions considered the ransomware threat as part of a more general incident risk framework.

Table 50 (Annex 1) shows that, within the last year, 42% of participating national competent authorities had been notified of ransomware incidents before they were resolved. Four per cent of the incidents had severe consequences leading to a data breach.

In terms of ransomware risk to insurers, about one quarter (27%) of the sample (see Annex 1 Table 51) stated that the risk of ransomware over the past three years remained unchanged. Some added that this was because the requirement to report was set up recently. Forty-six per cent indicated that ransomware attacks have increased over the past three years.

In terms of overall ransomware risks, none of the national competent authorities in the sample reported a decrease in the number of ransomware attacks (see Annex 1 Table 52) in their jurisdictions, while 58% reported an increase and 19% indicated that the number of attacks remained the same.

Only 4% of responding jurisdictions noted a decrease in the severity of ransomware attacks (see Annex 1 Table 53) while at the same time noting an increase in the number of attacks. However, the responses seemed to point to a positive correlation between the frequency and severity of ransomware attacks in the sample.

4.1.1.2 Social engineering[63]

Although various forms of fraud via social engineering have always existed, social engineering has significantly evolved with the increased use of information and communications technologies (ICT). Recent examples of social engineering include phishing, pretexting, baiting, quid pro quo and tailgating.[64]

---

59 See Panaseer, Cyber Insurance Market Trends Report (2022).

60 See SonicWall, Cyber Threat Report (2022).

61 See www.coveware.com/blog/2022/7/27/fewer-ransomware-victims-pay-as-medium-ransom-falls-in-q2-2022.

62 In view of the increasing threat of ransomware attacks, some governments are exploring a coordinated response to tackle the issue, with calls for a global approach to counter ransomware. For more information, please refer to Singapore's Counter Ransomware Task Force report.

63 Section based on the definition by and recommendations from the ENISA, What is "Social Engineering"? www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering.

64 Social engineering terms:

- Phishing: Persuading potential victims to divulge sensitive information via spam mail, malicious websites, email messages or instant messages by appearing to be from a legitimate source;
- Pretexting: False justifications, where the attacker uses a pretext to gain trust and trick the target;
- Baiting: Luring the target to perform a specific task, such as plugging in an infected USB drive by labelling it "my private pics" or "confidential information";
- Quid pro quo: Requesting information under a false pretext in exchange for compensation/money;
- Tailgating: Following an authorised person into a restricted area or system.

In the context of IT, social engineering can be assessed from two different angles:

- Psychological manipulation to get further access to an IT system (to gain access to/infect computer systems);
- Using IT technologies supporting psychological manipulation techniques to obtain objectives outside the IT realm (information, credentials, money).

As the use of IT technologies has increased, so has the use of social engineering techniques, and most current cyber attacks include some form of social engineering. The European Union Agency for Cyber Security (ENISA) recommends frequent awareness campaigns: posters, presentations, emails, information notes, staff training and penetration tests to assess susceptibility and reduce the threat from social engineering attacks.

4.1.1.3 Third-party risk

Insurers' reliance on a limited number of third parties, particularly with regards to the provision of services, hardware and software could give rise to concentration risk. More specifically, a cyber incident that leads to a failure or outage at a third party could have macroprudential implications. Large companies are increasingly incorporated into large data ecosystems where they need to manage cyber and privacy risks around connections to suppliers and third parties.[65] Any contractor or outside business party on which a firm is reliant is a third party, which could potentially give rise to cyber security risks to the firm unless the firm's own security infrastructure is sufficiently strong.[66] As a reflection of the changing risk landscape, several regulators have published supervisory statements and guidelines around third-party risk management.[67] Depending upon the level of reliance and the interconnectedness of the ecosystem, these risks could become systemic.

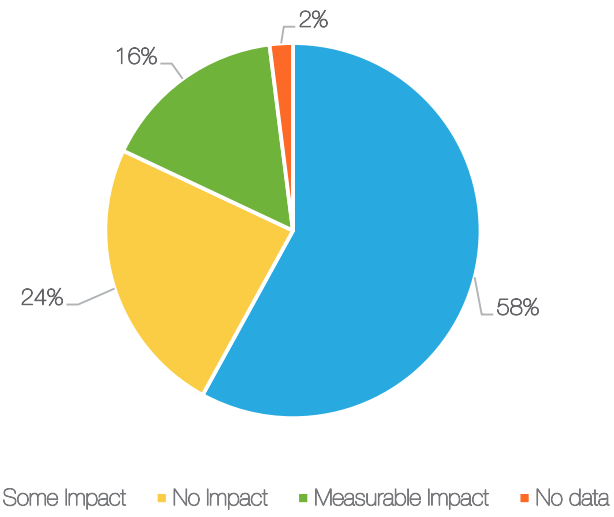
4.1.1.4 Talent shortage

The talent shortage poses a risk to the cyber resilience of the insurance sector. Most firms indicated that the global talent shortage was having a negative impact on their operations (see Figure 5). As a result, critical cyber security positions were open longer. Firms for whom the global cyber talent shortage had "some impact" on their operations also indicated that there was a limited availability of experts, which forced them to change their approach to recruiting (eg offer greater flexibility than might otherwise have been their practice). They furthermore stated that they were incurring greater recruitment costs and experiencing longer recruiting times to fill these positions than was previously the case. Firms for whom the talent shortage had a "measurable impact" indicated that there was a larger than usual number of positions open, which had caused significant gaps between workload and capacity. Some had to rely on external parties.

Insurers reported that it takes longer to fill cyber security positions, the recruitment process has become more expensive, compensation packages have increased, and employers have to offer greater flexibility.

[65] See PwC, Mapping and Managing Cyber Risks from Third Parties and Beyond.
[66] See Cyber Management Alliance, What Is Third-Party Cyber Risk Management & Why Is It Important? (2022).
[67] For an example, see Bank of England, SS2/21 Outsourcing and Third-Party Risk Management (2021).

FIGURE 5: Has the global talent shortage within cyber security affected your organisation?



Source: GME 2022 insurer pool

To put this into context, Cybersecurity Ventures reported that the annual number of unfilled cyber security jobs worldwide grew 350% between 2013 and 2021, which put the number of unfilled positions in 2021 at 3.5 million.[68] Job turnover was also high. For instance, 24% of Fortune 500 CISOs had been working in their roles for less than one year on average.[69]

The global shortage of talent is a problem with no obvious short-term solutions. It is likely to increase the reliance on third parties and contractors and to push firms to offer better compensation packages. It could also drive some firms to try new approaches to cyber security based on artificial intelligence (AI) or machine learning (ML), something that is already being used by many hackers to increase the effectiveness and scale of their attacks.[70,71] In an evolving cyber security landscape, it is unclear how these approaches, which rely heavily on vast amounts of data, would cope with new types of threats for which data are low or inexistent. Acquiring sufficient-sized data sets (even when available) would also be time-intensive and require investments, whereas an absence of huge volumes of data and events can lead AI systems to generate incorrect results and/or false positives.[72]

4.2 RISK ASSESSMENT AND RESPONSE OF INSURERS' POOL AND JURISDICTIONS

Insurers employ several tools and approaches to assess, measure and communicate cyber risks across the organisation. This document is not intended to be a comprehensive and in-depth analysis of how insurers assess these risks. Rather, it sets out to use the survey responses to cover some aspects that could have macroprudential implications, and to summarise and analyse the information collected from the insurers in the sample.

4.2.1 Third-party register

As noted above, third-party supply chain attacks are a significant source of cyber operational risk. As a part of third-party risk management, a frequently updated register may enable firms to better understand potential risks and to enhance their engagement with third parties.

From a macroprudential perspective, the information contained in insurers' third-party registers may be of interest to supervisory authorities. Such registers may enable the authority to identify, monitor and manage systemic concentration risk. They help the supervisor to understand the potential systemic disruption of a cyber attack at a commonly used third-party provider.

68 See Cybersecurity Ventures, 2022 Official Cybercrime Report (2022).
69 See cybersecurityventures.com/24-percent-of-fortune-500-cisos-on-the-job-for-just-one-year.
70 See cybersecurityventures.com/dont-get-obfuscated-use-ai-to-stop-attacks.
71 See McKinsey, Cybersecurity Trends: Looking over the Horizon (2022).
72 See G Belani, The Use of Artificial Intelligence in Cybersecurity, IEEE Computer Society.

TABLE 23: Do you have a register of your third parties and the services they provide, and are you engaged with them to understand mutual risks and recovery planning?

Answer	Percentage
Both	68%
Register of third parties with services provided	24%
Engaged with third parties to understand mutual risks and recovery planning	8%

Source: GME 2022 insurer pool

Of the insurers in our sample, 92% of all respondents reported having a register of third parties and/or engaging with them to understand mutual risk and recovery planning (see Table 23), which compared favourably with a recent Ponemon study, in which 57% of organisations (across industries) did not have any register of all third parties with whom information was shared.[73]

However, qualitative responses indicated that the frequency and depth in how third-party risks in the insurer pool were tracked and assessed varied significantly. Whereas some firms reported only initial assessments, others reported continuous monitoring and emergency drills with key third parties. A few respondents indicated that the monitoring and managing of this risk depended on whether a service was critical or not, with recovery planning and drills for more critical third parties.

Notably, without a common definition of "critical" or "important", third-party comparability across firms and jurisdictions has been difficult. The FSB's ongoing development of a toolkit to, among other objectives, develop "common definitions and terminologies" on third-party risk management and outsourcing may provide further clarity on definitions and facilitate future comparisons.[74]

4.2.2 Cyber security standards and frameworks

Sixteen participating insurers provided a list of their deployed or followed cyber security frameworks, standards, certifications, and directives. About half of the submitted list included cyber resilience supporting materials from domestic sources. The most cited international standards were NIST and the ISO27000s (See Table 24) – with 76% of the respondents having implemented one or both.

TABLE 24: Please indicate any national or international cyber security framework, certification or directive you employ or follow

Answer	Percentage
NIST	44%
ISO27000s	32%
FISC	8%
ISF	8%
FFIEC	6%
CIS	6%

Source: GME 2022 insurer pool

[73] See Ponemon Survey Report Webinar: CyberGRX, The Cost of Third-Party Cybersecurity Risk Management.
[74] See FSB Work Programme for 2022 (2022).

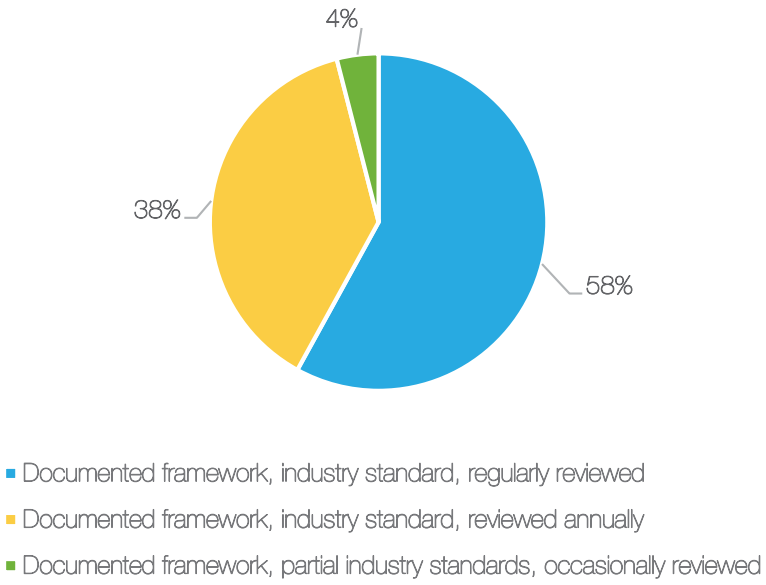
4.2.3 Implementation of cyber security frameworks and industry standards

The majority of insurers (96% of respondents) indicated that they had documented frameworks to maintain their security posture and to deliver their cyber security strategy, which were reviewed regularly (see Figure 6). However, there were differences in how these frameworks were implemented. For instance, some firms only referred to "group cyber policies" without further detail on any industry standards incorporated into an overall inhouse framework. Other firms went into significant detail with regards to board approval of policies, frequency of reviews and audit reports. Some firms referred to alignment to various industry standards, but no firm in the sample mentioned any external certification of cyber security frameworks.

Irrespective of the industry frameworks chosen, it is important that companies tailor and apply them to effectively fulfil their specific needs. In that regard, some firms may create their own internal standards based on features of different industry standards. The challenge for supervisors is to assess whether a firm has in place an effective cyber security framework (with effective standards and successful implementation). Industry certifications may help firms and supervisors in this regard. However, compliance with industry certifications should not replace firms' or supervisors' judgement.

From a supervisory point of view, it is also important to know if the standards chosen by a firm are appropriate for the business needs, whether the risk choices made are acceptable and whether internal auditing has verified the implementation.

FIGURE 6: Does a formally documented framework (including policies, standards and delivery programme) exist to maintain your security posture and to deliver the cyber security strategy, including recovery tolerances?



Source: GME 2022 insurer pool

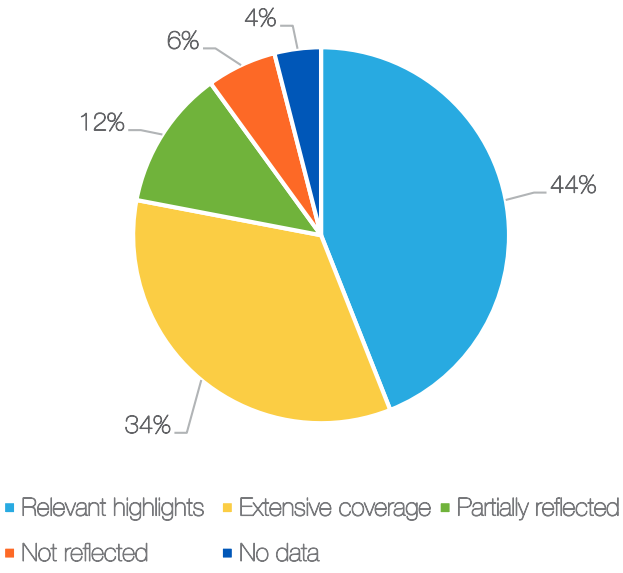
From a supervisory point of view, it is important to know whether the standards chosen by a firm are appropriate for the business needs, the risk choices made are acceptable, and an internal audit has verified the implementation.

4.2.4 Cyber risk and the ORSA

Most supervisors said that cyber is a key risk that must be assessed for all firms. Although the ORSA needs to be aligned with senior management's view of risk, different jurisdictions could have different requirements as to what extent the ORSA should reflect all relevant risks.

In the sample, over 75% of the respondents (see Figure 7) indicated that cyber risks were reflected in their ORSA. However, cyber security coverage in these assessments varied in terms of the layout and to the extent to which cyber risk was covered. For some firms, this risk was partially covered in their operational risk assessment, while for others it was covered in a separate section of the ORSA. If cyber risks are not covered in sufficient depth in the ORSA, supervisors should make sure that they have alternative channels to find this information.

FIGURE 7: Is the cyber security framework clearly reflected in the ORSA and embedded in the operational risk framework outlined in the ORSA report?



Source: GME 2022 insurer pool

4.2.5 Hardware and software monitoring

Most of the insurers in the sample (see Table 25) said that they proactively identified hardware and software vulnerabilities. Respondents described having in place comprehensive group guidelines and policies for risk assessment that were aligned to industry standards and other best-practice frameworks. Some also indicated that policies and procedures were integrated within global governance. Additionally, insurers reported that hardware and software vulnerabilities were regularly monitored using a variety of appropriate tools, and that technical controls were mature and effective. One respondent provided additional detail on practical controls in place, with systems development life cycle (SDLC) in preparation.

TABLE 25: Are hardware and software vulnerabilities proactively identified and documented with the risk assessment, and is there a documented process for secure software development life cycle (including proactive identification and management of vulnerabilities and end-of-life management)?

Answer	Percentage
Yes, identified and documented	32%
Yes, documented process for secure software development life cycle	2%
All of the above	66%

Source: GME 2022 insurer pool

Penetration testing assesses the firms' susceptibility to cyber attacks, including social engineering, and can also help firms to better understand weaknesses and vulnerabilities and to take remedial actions.[75,76]

4.2.6 Scanning and penetration testing

Most companies in the sample (See Table 26) indicated that they frequently conducted scanning and penetration testing.[77] Most of the additional comments received were to distinguish between penetration testing and vulnerability scanning as being different processes undertaken at different intervals. Penetration testing was mostly conducted annually or semi-annually, with additional tests before software application rollout or after major system changes. Vulnerability scanning was conducted at a much higher frequency, from continuously to daily or weekly. Scanning and testing activities were commensurate with the risk and criticality of assets. A range of tools was deployed to protect, detect and continuously monitor networks, systems and data at various levels (defence in depth). Respondents also stated that these tests were carried out internally by specialist third parties, red teams and bug bounty programmes. It is important to note that several supervisory initiatives were in place to develop frameworks that delivered intelligence-led cyber security tests (eg TIBER, CBEST).[78]

TABLE 26: How frequently do you undertake vulnerability scanning and penetration testing and ensure that security controls are effective?

Answer	Percentage
More than three times a year	68%
Once a year	20%
Twice a year	8%
Three times a year	4%

Source: GME 2022 insurer pool

75 See Bank of England, CBEST Threat Intelligence-Led Assessments (2022).
76 See ENISA, What is "Social Engineering"?
77 For more on supervisory initiatives, see IAIS, Issues Paper on Insurance Sector Operational Resilience (October 2022).
78 See IAIS, Issues Paper on Insurance Sector Operational Resilience (October 2022).

4.2.7 Quantification of cyber as a business risk

About 82% of the respondents (see Table 27) stated they had a process in place to define and quantify their business-risk tolerance relative to cyber security and ensure that it was consistent with their business strategy and risk appetite. However, it is possible that the question was not interpreted consistently by respondents. The quantification of cyber risk is important, as it helps communicate the potential impact of these risks across the enterprise and with supervisors.

4.2.8 Cyber security training

Training is a common tool for raising cyber security awareness and can reduce the threat of social engineering attacks.[79] Table 28 shows that 98% of the respondents conducted cyber security awareness (such as phishing simulation), with 76% providing training to all users, including board members and executives, and 22% reporting that their training excluded board members.

Training is a very common tool for raising cyber security awareness and can reduce the threat of social engineering attacks.

TABLE 27: Does the organisation have a process to define and quantify business-risk tolerance relative to cyber security and ensure that it is consistent with the business strategy and risk appetite?

Answer	Percentage
Yes	82%
No	14%
No data	4%

Source: GME 2022 insurer pool

TABLE 28: Do you conduct (cyber) security awareness training to maintain a high level of awareness among all users, including the board and executives? (eg phishing simulation)

Answer	Percentage
Yes, all users (including board members and executives)	76%
Yes, all users (excluding board members and executives)	22%
Yes, some users	2%

Source: GME 2022 insurer pool

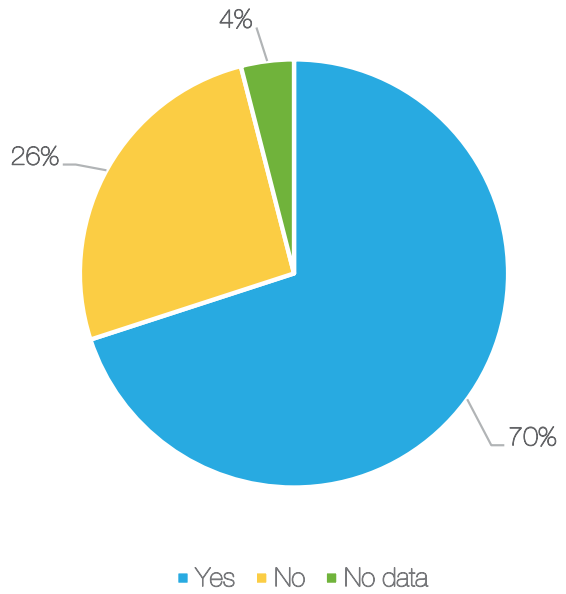
[79] See ENISA, What is "Social Engineering"?

4.2.9 Cyber insurance as a risk management tool

Over half of the participating insurers in the data collection set used insurance as a tool to manage cyber risk. Figure 8 shows that approximately 70% of the respondents bought cyber insurance, while 26% did not. This rate of purchase of cyber insurance was similar for all types of insurers (life, non-life, composite) in the sample.

For cyber insurance to be effective, a thorough assessment of the insured IT infrastructure, cyber posture and business requirements should be carried out. However, it was not possible to confirm whether these assessments had been carried out based on the information provided.

FIGURE 8: Do you buy cyber risk insurance? (From other insurers)



Source: GME 2022 insurer pool

4.2.10 Cyber incident response plans

Most insurers in the sample (96% – see Table 29) had documented (and regularly tested) response plans for business continuity, disaster recovery and cyber incident response. Comparatively less attention was given to data recovery, where 76% of respondents indicated a response plan. Most plans seemed to be regularly updated and tested. Most respondents indicated that business continuity plans were reviewed annually.

TABLE 29: Do you have a documented and regularly tested response plan (business continuity, disaster recovery and/or cyber incident response, data recovery)? Please choose all relevant options

Answer	Percentage
Business continuity	96%
Disaster recovery	96%
Cyber incidence response	94%
Data recovery	76%

Source: GME 2022 jurisdiction pool

4.2.11 Supervisory response

As a response to the increasing cyber threat, regulators have been increasing their guidance of corporate cyber security capabilities.[80] Financial supervisory authorities across jurisdictions have been working on establishing and implementing frameworks for cyber risk supervision (see Annex 2: Supervisory initiatives), although some debate remains about the optimal level of prescriptiveness (ie using a principle-based approach versus a more prescriptive framework).[81,82] Notably, this also creates challenges for firms, especially considering the talent shortage (described earlier), more stringent compliance requirements, evolving supervisory guidelines, and a significant number of cross-border data flow regulations.[83]

[80] See McKinsey, Cybersecurity trends: Looking over the horizon (2022).
[81] See International Monetary Fund: Monetary and Capital Markets Department, Cybersecurity Risk Supervision (2019).
[82] See European Commission, Document 52020PC0595: Proposal for a Regulation of the European Parliament and of the Council on Digital Operational Resilience for the Financial Sector and Amending Regulations. (EUR-Lex, 2020).
[83] See JC Crisanto & J Prenio, Regulatory Approaches to Enhance Banks' Cyber Security Frameworks, FSI Insights (August 2017).

Joint efforts are being made in specific areas across several international initiatives to improve the resilience of the financial sector and increase alignment with regards to standards and taxonomy. This would not only support jurisdictional best practice but also help international firms navigate the regulatory landscape.

The section below provides further insights into the supervisory approaches to executive accountability and cyber information gathering, analysing and sharing in the sample jurisdictions.

Table 30 shows that 61% of participating jurisdictions had requirements for a senior executive (board level) to be accountable for the delivery of the cyber security framework. This was corroborated by information collected by the IAIS' ORTF, where members stated that "many supervisory authorities seek assurance that insurers have sound governance frameworks and adequate board and senior management oversight over resilience measures, as well as strategies to mitigate risks associated with operational disruption."[84]

Timely and accurate information on cyber incidents is crucial for effective incident response and recovery and for promoting financial stability.[85] The majority of responding jurisdictions (73% – see Table 31) had a process for gathering, analysing and sharing information on cyber threats. Additional comments indicated that this could take place at multiple levels within a jurisdiction.

However, due to a lack of common standards for how cyber incidents are reported and of a common terminology around cyber incidents, it has been harder to assess and share information about incidents. Recognising the importance of timely and accurate information, the FSB had a public consultation, which set out recommendations to achieve greater convergence in cyber incident reporting, advance work to develop common terminologies around cyber, and propose the development of a format for incident reporting exchange (FIRE).[86]

For a list of supervisory initiatives, please see Annex 2.

TABLE 30: Does your regulatory framework require a senior executive (board level) to be appointed, who is accountable for the delivery of the cyber security framework within the organisation?

Answer	Percentage
No requirement	35%
Senior executive required to head cyber security	23%
Executive required to head cyber security	19%
Executive to head cyber security is encouraged	19%
No data	4%

Source: GME 2022 jurisdiction pool

TABLE 31: Is there a process for gathering, analysing and sharing information on cyber threats?

Answer	Percentage
Yes	73%
No	27%

Source: GME 2022 jurisdiction pool

[84] See IAIS, Insurance Sector Operational Resilience (October 2022).
[85] See FSB, Achieving Greater Convergence in Cyber Incident Reporting – consultative document (October 2022).
[86] See FSB, Achieving Greater Convergence in Cyber Incident Reporting – consultative document (October 2022).

4.3 CYBER RISK CONTROLS

Most insurers in the sample (98% – see Table 32) kept an inventory of physical devices, information systems and data within the organisation. Some participants in the data collection set indicated that they maintained an asset inventory or configuration management database (CMDB). The amount of information captured in the CMDB varied from hardware (physical devices), software and data (databases), to deployment tools, baseline configurations, asset ownership and relationships between assets. Some (but not all) organisations maintained asset inventory details in their CMDB for test systems. These respondents also indicated that asset inventory information was regularly reviewed and updated.

TABLE 32: Asset management – are physical devices, information systems and data within the organisation inventoried?

Answer	Percentage
Yes	98%
No	2%

Source: GME 2022 insurer pool

Over 90% (see Table 33) of the sample indicated that their organisations documented and enforced security configuration standards of all network devices. About a quarter of the groups in the sample provided additional information. Most had a documented configuration management process to establish, verify and monitor configurations for systems, applications and devices. Most comments exemplified baseline standards based on industry security-hardening techniques. Some indicated that compliance to security standards was periodically reviewed and enforced. Additionally, some stated that their configuration management processes were integrated within or applied in conjunction with wider change management processes.

TABLE 33: Does the organisation document and enforce security configuration standards of all network devices?

Answer	Percentage
Yes	94%
No	4%
No data	2%

Source: GME 2022 insurer pool

Most organisations (86% – see Table 34) stated that they have a segregated network environment made by multiple and separate trust zones (eg intranet, DMZ network, Wi-Fi, extranet, etc) managed by firewalls or other types of network and security appliances. One organisation was also addressing their security segregation towards the new concept of “Zero Trust”. About 12% of the sample reported having no segregated network environment, considering this a temporarily acceptable risk as they migrated towards more secure solutions.

TABLE 34: Has the organisation segregated the enterprise network into multiple, separate trust zones?

Answer	Percentage
Yes	86%
No	12%
No data	2%

Source: GME 2022 insurer pool

Ninety-eight per cent (see Table 35) of the groups in the sample performed an assessment of compliance against data protection regulatory requirements. Some of them performed several local assessments, as they had various branches worldwide. Organisations located in Europe were subject to the General Data Protection Regulation (GDPR), and one organisation asserted that its data protection had been enhanced through a GDPR compliance project.

TABLE 35: Has the organisation performed an assessment of compliance against data protection regulatory requirements?

Answer	Percentage
Yes	98%
No	2%

Source: GME 2022 insurer pool

Almost all insurers in the sample (96% – see Table 36) affirmed performing tests on their business continuity and IT disaster recovery plans during the preceding 12 months. However, some indicated that they conducted such tests annually and considered past years' tests as a reference because of the Covid-19 pandemic.

TABLE 36: Has a test of the Business Continuity and IT Disaster Recovery plans been performed during the past 12 months?

Answer	Percentage
Yes	96%
No	2%
No data	2%

Source: GME 2022 insurer pool

Most insurers in the sample (92% – Table 37) indicated that they had an internal cyber security incident response team (CSIRT), complemented by external experts in instances where specialised services were required, such as digital forensic expertise. External experts could also be retained to support incident-response capabilities. Some of these services were provided as part of their cyber insurance cover.

TABLE 37: In the event of a major incident, is the organisation contracted to a "4th-line" IT security expert service? (For example, a Managed Security Services Provider)

Answer	Percentage
Yes	92%
No	6%
No data	2%

Source: GME 2022 insurer pool

In terms of data security, 84% of the sample (see Table 38) indicated that data in transit and at rest were encrypted based on data protection standards and that a risk-based approach was applied in this regard. Others highlighted areas where data had not been encrypted – exceptions were managed through their operational risk management processes. Fourteen per cent of the respondents indicated that the data were only encrypted at rest or in transit, but not both. Some were still classifying data to determine which data would require encryption.

TABLE 38: Are data that are classified as critical encrypted in transit and at rest?

Answer	Percentage
Yes	84%
No	16%

Source: GME 2022 insurer pool

Most companies in the sample (94% – see Table 39) indicated that they had a logical access management standard that defined how systems access was verified, managed, revoked and audited. Some indicated that the process was managed automatically throughout the user life cycle, while others still used manual methods. Others indicated that separate standards had been established for managing general-user and privileged access.

TABLE 39: Is there a Logical Access Management Standard defining how systems access is verified, managed, revoked and audited?

Answer	Percentage
Yes	94%
No	6%

Source: GME 2022 insurer pool

The vast majority of participating individual insurers (98%) responded that they had a dedicated cyber security team and a CISO in their organisation (see Table 40). A few indicated that their group lacked a dedicated CISO and that someone else assumed the position's duties.

TABLE 40: Do you have a dedicated cyber security team (and CISO) in your organisation?

Answer	Percentage
Yes	98%
No	2%

Source: GME 2022 insurer pool

5. Financial stability

Like financial risks, cyber incidents could impact financial stability through the loss of confidence (eg due to lengthy outages and compromised data integrity), interconnectedness (eg within the financial system and across technologies) and substitutability (eg critical infrastructure, key service providers). [87]

However, important differences also exist. One distinguishing factor is that shocks may spread through a web of technologies and common dependencies rather than common financial links. This often involves layers of shared technologies and service providers that are not captured in traditional measures of counterparty risk. Other differences that set this risk apart are the antagonistic nature of cyber attacks and their speed and scalability.[88] Additionally, while capital and liquidity requirements are effective at minimising prudential risks by providing a cushion for financial losses, they are not as effective at speeding up the recovery process.[89]

While information collected by supervisors is on firm-level cyber resilience, which is important for microprudential supervision, it could also shed light on macroprudential concerns. For instance, most insurers in the sample have documented cyber security frameworks and cyber incident response plans, and they include cyber risk in their ORSAs. Additionally, many insurers conduct penetration testing and vulnerability scanning. Longitudinal analysis of this microprudential information could uncover important system-wide vulnerabilities. As an example, a sample-wide consideration of cyber incident response plans could show common sector reliance on one or more service providers (eg backup services), which might create capacity issues and bottlenecks. The appropriateness of a response plan should be evaluated considering micro- and macroprudential concerns.

Unfortunately, the lack of a common taxonomy, definitions and reporting standards makes the comparison and aggregation of these microprudential data challenging. Supervisory initiatives, such as the development of frameworks to deliver intelligence-led cyber security tests, should make it easier for supervisors to use microprudential information for macroprudential purposes. Additionally, work is underway at the international level to promote harmonisation and convergence, but it is important that smaller jurisdictions not be left behind.[90]

---

87 See International Monetary Fund, Cyber Risk and Financial Stability: It's a Small World After All, (December 2020).
88 See L Elestedt, U Nilsson & C-J Rosenvinge, A Cyber Attack Can Affect Financial Stability, Sveriges Riksbank (May 2021).
89 See D Brando et al, Implications of Cyber Risk for Financial Stability, FED Notes (May 2022).
90 See International Monetary Fund, Cyber Risk and Financial Stability: It's a Small World After All, (December 2020).

The information collected shows that the cyber operational risk management of insurers in the sample has been focused on idiosyncratic risks. Systemic risk considerations, such as concentration risk or the ecosystem's exposure to single points of failure, did not seem to receive sufficient attention, especially given their interconnectedness in terms of shared technologies and service providers. Supervisors, on the other hand, have been actively incorporating systemic risk considerations into their monitoring and supervisory activities. For instance, some jurisdictions have incorporated cyber underwriting and resilience scenarios in their stress-testing frameworks, and some have been collecting information on exposure to critical infrastructure.

To better understand how cyber underwriting activities and the cyber resilience of the insurance sector could pose risks to financial stability, the systemic risk taxonomy proposed in Insurance Core Principle (ICP) 24 (Macroprudential Supervision) is followed in the analysis below.[91] We also focus on three transmission channels: loss of confidence (impacting affected and unaffected parties); operational (eg cross-border technical services); and financial (through losses as a direct consequence of an attack, or indirect losses due to, for instance, loss of confidence).

5.1 INWARD RISKS

"Inward risks" arise from a response to a shock by one or many insurers. This is a second-round effect, where the collective actions of a set of insurers could have implications for the overall system.

The insurance sector is exposed to inward risks like those faced by other financial institutions, such as exposure to critical infrastructure, a small set of service providers, common single points of failure and third-party risks. This suggests that financial institutions are exposed to a common set of cyber-related risks and vulnerabilities. If one of these risks materialises, it may have systemic implications for the financial industry and could be a threat to financial stability. For instance, a widespread cyber event could disrupt essential services such as payment, settlement or clearing systems. This kind of disruption would not only impact insurers but also counterparties and/or policyholders and could trigger a reaction with systemic implications (eg cash hoarding). Exposure to these vulnerabilities and the reaction to a shock could also increase uncertainty, bring about lack of confidence due to reputational issues, and increase legal risk at a time of crisis. Moreover, operational issues that bring insurance operations to a halt could impact sectors of the economy that rely on insurance coverage for their normal functioning (eg international commerce, maritime insurance).

Information collected by supervisors for microprudential supervision could also shed light on macroprudential concerns.

[91] See IAIS, ICP and ComFrame Online Tool.

A sufficiently large cyber event could render cyber underwriting unattractive and/or unprofitable. This could lead to a severe contraction in the cyber underwriting market, which would reduce or eliminate an important risk management tool for companies. The widening protection gap could incentivise economic agents to choose higher levels of self-insurance, funded by higher levels of precautionary savings. This, in turn, could have an impact on the real economy as less resources are allocated to productive investments or consumption. Such a contraction could also eliminate any positive externalities that a cyber insurance product might have to improve the overall cyber security posture. However, it is important to put this risk into perspective. The level of coverage offered is low relative to the economic losses sustained by economic agents as a result of cyber events each year.

5.2 OUTWARD RISKS

"Outward risks" refer to the build-up of systemic risk at the individual insurer level or in the sector as a whole. This first-round effect would be proportional to the size and interconnectedness of the insurer/sector.

From a cyber underwriting perspective, potential transmission channels are asset liquidation, loss of confidence and the transfer of losses to other participants (eg reinsurers).[92] From an affirmative coverage perspective, the size of the market was too small relative to the overall insurance sector, and tail losses arising from affirmative coverage would have been absorbed with the level of coverage being offered. Regarding non-affirmative coverage, if strategies to minimise exposure to non-affirmative coverage were effective (with no additional legal risk), then non-affirmative cyber exposures were unlikely to be a source of systemic risk for this set of insurers. Having said that, there are important differences in the adoption and implementation of these risk mitigation strategies across firms and jurisdictions. Due to these differences, and with the limitations of the data collected, it is impossible to assess with an appropriate level of certainty whether non-affirmative coverage represents a threat to financial stability.

Cyber shocks may spread through a web of technologies and common dependencies. The antagonistic nature of cyber attacks, as well as their speed and scalability, sets this risk apart from financial risks.

[92] For transmission channels to financial market and real economy, see IAIS, Holistic Framework.

6. Conclusions and recommendations

Cyber risk is a unique, growing and evolving risk that impacts businesses and broader society. For the insurance sector, however, cyber is not only an operational risk but a commercial one too. This dual risk could create synergies for some insurers, such as using cyber security skills developed on the operational side to better understand business risks on the insurance side (and vice versa). On the other hand, cyber risks on the operational side might compromise the effectiveness of cyber insurance as a product; should insurers be exposed to the same cyber threat as policyholders, their ability to process claims and offer ex post services could be impaired (eg data recovery services) when most needed.

Cyber insurance could also be a tool to reduce the operational impact of cyber events. As described above, regulatory capital and liquidity requirements may not mitigate the effect of a cyber event in the same way they can mitigate financial losses because they cannot speed up the recovery of systems or data. Insurers not only cover financial losses but also offer recovery services to help policyholders minimise insured losses (eg business continuity, liability, etc). The unintended result is that the provision of these ex post services could also contribute to enhancing the cyber resilience of policyholders and the system.

Cyber insurance may incentivise investment in cyber security, as insurers have been more selective in their risk selection (eg only covering those that meet certain cyber security standards). Similarly, insurers can (and some do) help improve the security posture of policyholders by providing ex ante services, such as pre-breach and virtual CISO services. However, insurers' ability to incentivise good behaviour and stimulate investment in cyber security has its limits.[93] Public policy aimed at enhancing the cyber security of economic agents should factor in these limitations.

While there are many initiatives to collect data on insurance-level cyber resilience and the cyber insurance market, important data gaps remain. In terms of cyber insurance, it is difficult to collect data on cyber exposures. On the affirmative side, some insurers do not disaggregate technical reserves for cyber exposures, as these may come from non-standalone policies. On the non-affirmative side, the exposures are not easy to estimate. Regarding cyber resilience, assessing the effectiveness of risk management strategies and cyber risk controls at the firm level is challenging, expensive and time-consuming. At the system level, not much data are available on digital interdependencies, concentration and bottlenecks. The lack of a standard taxonomy, common reporting standards or common language compound these difficulties.

[93] See KS Abraham and D Schwarcz, The Limits of Regulation by Insurance, Indiana Law Journal 98(1) (July 2022).

This report underscores the importance of understanding, monitoring and actively supervising cyber risks in the insurance sector, both from an underwriting and operational perspective. As the cyber insurance market grows and the risk landscape evolves, effective macroprudential supervision of these risks will continue to grow in importance. Based on the findings of this report, the recommendations below can inform future international work.

CYBER UNDERWRITING RISK

- Continue to gather information on cyber insurance underwriting risk at the jurisdictional level within the GME, and explore where some data fields could be better defined or harmonised. This would improve the ability of the IAIS to continue to monitor factors such as the global growth of cyber insurance and the relative reliance of these insurers on reinsurance.

- Speak to jurisdictions about affirmative versus non-affirmative cyber risk to assess the possible macroprudential impact of remaining latent exposure under non-affirmative covers and whether existing regulatory and insurer efforts effectively mitigate this risk. Consider including the potential impact on standalone and add-on policies.

- Continue to monitor the cyber protection gap. Cyber could be a valuable addition to the scope of the IAIS Protection Gap Task Force.[94]

CYBER OPERATIONAL RESILIENCE

- Continue to support efforts to harmonise cyber security standards applicable to insurers so that comparisons can be made within and across jurisdictions. Such harmonisation would help insurers' micro- and macroprudential supervision and reduce the regulatory burden on insurers, especially those that are internationally active. Regulators may also refer to the IAIS Application Paper on Insurer Cyber Security for useful advice.[95]

- Macroprudential supervision of cyber risk is still in its infancy. More work needs to be done to understand the macroprudential ramifications of cyber risk in the insurance sector. Ideally, this work should promote the development of frameworks to monitor and supervise system-level vulnerabilities and research in this space.[96] Given the uniqueness of this risk, it would be useful to review the Holistic Framework, the Application Paper on Macroprudential Supervision and the IAIS macroprudential framework (ICP 24 (Macroprudential Supervision)) to ensure it is suitable to monitor, assess and supervise this risk.

This report underscores the importance of understanding, monitoring and actively supervising cyber risks in the insurance sector, both from an underwriting and operational perspective.

[94] See the IAIS Roadmap 2023–2024.
[95] See IAIS, Supervision of Insurer Cybersecurity (November 2018).
[96] See G Falco et al, A Research Agenda for Cyber Risk and Cyber Insurance (2019).

Annex 1: Tables

TABLE 41: (Highest threat) Please rank the following cyber threats in terms of potential underwriting losses (1 = Highest, 7 = Lowest) for affirmative and non-affirmative coverage

Answer	Percentage
Ransomware	28%
Mass vulnerability attack	24%
Business blackout	16%
Cloud outage	16%
Data breach	4%
No data	12%

Source: GME 2022 insurer pool

TABLE 42: (Second-highest threat) Please rank the following cyber threats in terms of potential underwriting losses (1 = Highest, 7 = Lowest) for affirmative and non-affirmative coverage

Answer	Percentage
Mass vulnerability attack	20%
Ransomware	20%
Data breach	12%
Business blackout	12%
Cloud outage	8%
Third-party vendor outage	8%
Other	4%
No data	16%

Source: GME 2022 insurer pool

TABLE 43: (Third-highest threat)
Please rank the following cyber threats in terms of potential underwriting losses (1 = Highest, 7 = Lowest) for affirmative and non-affirmative coverage

Answer	Percentage
Cloud outage	28%
Mass vulnerability attack	20%
Data breach	16%
Business blackout	12%
Third-party vendor outage	4%
No data	20%

Source: GME 2022 insurer pool

TABLE 44: (Fourth-highest threat)
Please rank the following cyber threats in terms of potential underwriting losses (1 = Highest, 7 = Lowest) for affirmative and non-affirmative coverage

Answer	Percentage
Data breach	24%
Third-party vendor outage	20%
Cloud outage	16%
Ransomware	12%
Mass vulnerability attack	4%
No data	24%

Source: GME 2022 jurisdiction pool

TABLE 45: (Fifth-highest threat)
Please rank the following cyber threats in terms of potential underwriting losses (1 = Highest, 7 = Lowest) for affirmative and non-affirmative coverage

Answer	Percentage
Third-party vendor outage	28%
Ransomware	16%
Business blackout	12%
Data breach	12%
Mass vulnerability attack	4%
Cloud outage	4%
No data	24%

Source: GME 2022 insurer pool

TABLE 46: (Sixth-highest threat)
Please rank the following cyber threats in terms of potential underwriting losses (1 = Highest, 7 = Lowest) for affirmative and non-affirmative coverage

Answer	Percentage
Answer	Percentage
Business blackout	20%
Third-party vendor outage	16%
Data breach	16%
Ransomware	8%
Cloud outage	4%
Mass vulnerability attack	4%
Other	4%
No data	28%

Source: GME 2022 insurer pool

TABLE 47: (Seventh-highest threat) Please rank the following cyber threats in terms of potential underwriting losses (1 = Highest, 7 = Lowest) for affirmative and non-affirmative coverage

Answer	Percentage
Other	48%
Business blackout	4%
Mass vulnerability attack	4%
No data	44%

Source: GME 2022 jurisdiction pool

TABLE 48: Are insurers in your jurisdiction expected to report ransomware incidents (and recovery actions, root cause analysis, etc) to you?

Answer	Percentage
Yes	85%
No	15%

Source: GME 2022 jurisdiction pool

TABLE 49: Do you ask firms questions about their preparedness for or ability to recover from ransomware incidents?

Answer	Percentage
Yes	81%
No	19%

Source: GME 2022 jurisdiction pool

TABLE 50: Were you ever notified of a ransomware incident before it was resolved in the last year?

Answer	Percentage
No	54%
Yes	42%
No data	4%

Source: GME 2022 jurisdiction pool

TABLE 51: Looking at the reported number of ransomware incidents to insurers within your jurisdiction over the past three years, has the risk of ransomware attacks...

Answer	Percentage
Increased	46%
Remained unchanged	27%
No data	27%

Source: GME 2022 jurisdiction pool

TABLE 52: Looking at the number of ransomware attacks that you are aware of in your jurisdiction, would you say that over the past three years the number has...

Answer	Percentage
Increased	58%
Remained unchanged	19%
No data	23%

Source: GME 2022 jurisdiction pool

TABLE 53: Looking at the number of ransomware attacks that you are aware of in your jurisdiction, would you say that over the past three years the severity has...

Answer	Percentage
Increased	42%
Remained unchanged	23%
Decreased	4%
No data	31%

Source: GME 2022 jurisdiction pool

TABLE 54: Ransomware threat ranking

Answer	Percentage
1	38%
2	15%
3	15%
4	9%
5	8%
No data	15%

Source: GME 2022 jurisdiction pool

TABLE 55: Social engineering attacks (phishing, vishing, smishing) ranking

Answer	Percentage
2	27%
1	19%
3	15%
6	12%
4	8%
5	4%
No data	15%

Source: GME 2022 jurisdiction pool

TABLE 56: Malware ranking

Answer	Percentage
3	27%
4	23%
2	16%
5	15%
1	4%
No data	15%

Source: GME 2022 jurisdiction pool

TABLE 57: Third-party supply chain attacks (single point of failure) ranking

Answer	Percentage
4	27%
5	23%
1	12%
2	11%
3	8%
6	4%
No data	15%

Source: GME 2022 jurisdiction pool

TABLE 58: Endpoint attacks ranking

Answer	Percentage
6	38%
5	15%
3	8%
4	8%
7	8%
No data	23%

Source: GME 2022 jurisdiction pool

TABLE 59: Internet of Things attacks ranking

Answer	Percentage
7	65%
1	4%
3	4%
5	4%
No data	23%

Source: GME 2022 jurisdiction pool

TABLE 60: Inadequate patch management ranking

Answer	Percentage
2	15%
4	15%
6	15%
3	12%
1	8%
5	8%
7	4%
No data	23%

Source: GME 2022 jurisdiction pool

Annex 2: Supervisory Initiatives

Jurisdiction	Authority	Initiative	Description
Belgium	National Bank of Belgium (NBB)	NBB Insurance Stress Test 2022	NBB insurance stress test on cyber underwriting.
Bermuda	Bermuda Monetary Authority (BMA)	Insurance Act 1978	Statutory responsibility for principal representatives and companies to report events is now embedded at the Insurance Act level.
Bermuda	BMA	Insurance Sector Operational Cyber Risk Management Code of Conduct	Insurance sector cyber code of conduct has been in force since 1 January 2022.
Bermuda	BMA	Annual Bermuda Solvency Capital Requirement (BSCR) filing	Cyber-specific questions on governance and controls in insurer's annual BSCR filing. In 2022, the BMA added a cyber-specific stress test in the insurer's annual BSCR filing.
Bermuda	BMA	Bermuda Insurance Sector Operational Cyber Risk Management – 2021 Report	The report is based on the analysis of BSCR filing data and is published annually.
Bermuda	BMA	ORSA submissions	Requirement for commercial insurers to explicitly incorporate both cyber underwriting and operational cyber risks in their yearly ORSA submissions. For policies incepting 1 January 2024, the BMA requires that commercial insurers' non-cyber policies must provide clarity as to whether cyber coverage is provided, and to document their exposure assessment and efforts on this exercise in their 2023 ORSA submissions to the BMA.
Bermuda	BMA	Bermuda Cyber Underwriting Report	Bermuda Cyber Underwriting Report
EU	European Insurance and Occupational Pensions Authority (EIOPA)	Financial Stability Report	Regular assessments on cyber risks are included in EIOPA's Financial Stability Reports.

Jurisdiction	Authority	Initiative	Description
EU	EIOPA	Risk dashboard	Inclusion of digitalisation and cyber risks in the EIOPA risk dashboard.
EU	EIOPA	Discussion Paper on Methodologies of Insurance Stress Testing – Cyber component	Development of insurance stress-testing methodological principles, with focus on cyber risk.
EU	EIOPA	Digitalisation Market Monitoring Survey	Development of a Digitalisation Market Monitoring Survey to monitor innovations in the insurance sector. The survey includes a dedicated section on cyber risks.
EU	EIOPA	Amendments to reporting Implementing Technical Standards (ITSs) under Solvency 2 Directive to introduce a regular reporting template on cyber risk	Proposal for draft amendments to reporting ITSs under Solvency 2 Directive to introduce a regular reporting template on cyber risk.
EU	EIOPA	Survey on access to cyber risk insurance for small and medium enterprises	Launch of a survey to collect information on access to cyber coverage for small and medium enterprises.
EU	EIOPA	Digital operational resilience for the financial sector in "A Europe fit for the digital age", Digital finance: Digital Operational Resilience Act (DORA)	As part of the EU Digital Finance Strategy, the co-legislators have adopted DORA to strengthen resilience in the financial sector by laying down requirements concerning the security of network and information systems supporting the business processes of financial entities. This regulation will apply from 17 January 2025. The European Supervisory Authorities (ESAs), including EIOPA, National Competent Authorities (NCAs) and other relevant authorities are currently working on the development of a wide variety of technical standards that further specify the obligations as stated in DORA. This work is coordinated via the Joint Committee of the ESAs.
EU	EIOPA	EIOPA supervisory statements on non-affirmative risk and potential exclusions	EIOPA published two supervisory statements on exclusions related to systemic events and the management of non-affirmative cyber exposures.
EU	EIOPA	Guidelines on information and communication technology security and governance	EIOPA guidelines on information and communication technology security and governance.
EU	EIOPA	Guidelines on outsourcing to cloud service providers	EIOPA guidelines on outsourcing to cloud service providers.

Jurisdiction	Authority	Initiative	Description
EU	EIOPA	Guidelines on system of governance	EIOPA guidelines on system of governance.
EU	EIOPA	Opinion on the supervision of the management of operational risks faced by Institutions for Occupational Retirement Provisions (IORPs)	EIOPA opinion on the supervision of the management of operational risks faced by IORPs.
EU	European Systemic Risk Board (ESRB)	Recommendation of the contribution to the development within the ESRB of 2 December 2021 on a pan-European systemic cyber incident coordination framework for relevant authorities (EU-SCICFESRB/2021/17)	The ESAs, including EIOPA, contribute to the development of a pan-European systemic cyber incident coordination framework for relevant authorities (EU-SCICF), in compliance with the ESRB recommendation.
Italy	Institute for the Supervision of Insurance (IVASS)	Regolamento n. 38, reference article n. 16 (Sistemi informatici e cyber security)	1) Proportionality: ICT systems must be suitable in terms of nature and complexity of the undertaking. 2) a. Company must have a strategic plan on ICT, including cyber security, to guarantee the maintenance of a complex architecture, suitable with its requirements and based on national and international standards. b. Related to cyber security, undertakings must define the following: i. Roles and responsibilities; ii. Risk assessment on all stakeholders; iii. Incident monitoring; iv. Incident response; v. Remediation and recovery; vi. Communication; and vii. Threats update. c. Access management: Access to all ICT systems must be regulated and controlled. d. ICT Procurement: Purchase of software and hardware assets must be formalised. e. Disaster recovery and business continuity. 3) Integration plan of ICT systems in case of takeover or division. 4) Incident reporting to IVASS: Undertakings must report serious cyber security incidents.

Jurisdiction	Authority	Initiative	Description
Singapore	Monetary Authority of Singapore (MAS)	Cyber Security Regulations and Guidance	a) Notice on cyber hygiene for insurers and insurance agents: Sets out cyber security requirements on securing administrative accounts, applying security patching, establishing baseline security standards, deploying network security devices, implementing anti-malware measures and strengthening user authentication. b) Notice on technology risk management for insurers: Sets out requirements for the identification of critical systems and for insurers to maintain high availability and recovery time objectives for critical systems. Insurers are also required to notify MAS of relevant incidents according to the prescribed timeline and format. Insurers must also implement IT controls to protect customer information from unauthorised access or disclosure. c) Guidelines on technology risk management: Set out risk management principles and best practices to guide financial institutions to establish sound and robust technology risk governance and oversight, as well as maintain IT and cyber resilience.
Singapore	MAS	Advisory on Addressing the Technology and Cyber Security Risks Associated with Public Cloud Adoption	Risk management principles and best practice standards to guide financial institutions in managing the technology and cyber security risks of public cloud adoption.
Singapore	MAS	MAS Cyber Security Advisory Panel (CSAP)	The panel advises on strategies for MAS and financial institutions in Singapore to sustain cyber resilience and trust in our financial system.
UK	Prudential Regulation Authority (PRA)	Insurance stress test 2022	An external environment of high volatility and uncertainty, stress and scenario testing will become an even more important tool for firms to assess their own resilience, and for the PRA in pursuing a forward-looking, proportionate, and judgement-based approach to supervision.

Jurisdiction	Authority	Initiative	Description
UK	PRA	Cyber resilience tools – CBEST and CQUEST	CBEST provides a framework for regulators to work with firms using a simulated cyber attack, enabling firms to explore how an attack on the people, processes and technology of their cyber security controls may be disrupted. CQUEST forms part of the Bank of England and PRA/Financial Conduct Authority (FCA)'s supervisory toolkit to gauge the cyber risk and resilience capabilities of the financial sector. CQUEST can also be used by other firm(s) as a self-assessment tool to consider their own cyber risk and resilience maturity. The CQUEST questionnaire comprises 50 questions with multiple-choice answers across six domains: Governance and Leadership, Identify, Protect, Detect, Respond and Recover.
UK	PRA	Critical Third Parties (CTPs)	Another tool that the supervisory authorities could use to test certain CTPs is cyber resilience testing. Cyber resilience testing of firms and Financial Market Infrastructures (FMIs) is a well-established tool in the UK. Following the 2021 Financial Policy Committee (FPC) comments, HM Treasury has been working with the Bank of England, including the PRA and FCA, to understand what "direct regulatory oversight" of critical third-party services might involve, and to come up with a framework that enables the management of risks to financial stability and their statutory objectives.

Jurisdiction	Authority	Initiative	Description
UK	PRA	Cyber coordination groups	Malicious cyber actors targeting internet-facing systems such as email servers and virtual private networks (VPNs) with newly disclosed vulnerabilities; ransomware attacks using Remote Desktop Protocols (RDP) and unpatched devices; denial of service attacks; and inadequate supply chain oversight leading to supply chain compromise. The Covid-19 pandemic continued to impact the sector in 2021, with challenges posed by remote and hybrid ways of working. Emerging trends in cyber security risks include supply chain compromise and exploitation of zero-day vulnerabilities. The importance of board engagement in setting the organisational cyber risk appetite extends to board support in measuring the effectiveness of cyber security postures and board assurance that supply chain partners effectively protect the information shared with them. Several common good practices can be used for implementing security in the early stages of the software development cycle (also known as DevSecOps). This includes empowering rather than mandating security practices and giving the development teams access to security tools.

International Association of Insurance Supervisors
c/o Bank for International Settlements
Centralbahnplatz 2
CH-4002 Basel
Switzerland

Tel: +41 61 280 80 90
E-mail: iais@bis.org
Web: www.iaisweb.org