



eiopa

EUROPEAN INSURANCE
AND OCCUPATIONAL PENSIONS AUTHORITY

Understanding Cyber Insurance – A Structured Dialogue with Insurance Companies

Neither EIOPA nor any person acting on behalf of EIOPA is responsible for the use that might be made of the following information.

Luxembourg: Publications Office of the European Union, 2018

Print ISBN 978-92-9473-047-3 doi:10.2854/223306 EI-01-18-761-EN-C
PDF ISBN 978-92-9473-046-6 doi:10.2854/33407 EI-01-18-761-EN-N

© EIOPA, 2018

Photos: © EIOPA

Reuse is authorised provided the source is acknowledged.

For any use or reproduction of photos or other material that is not under the EIOPA copyright, permission must be sought directly from the copyright holders.

Contents

1. Executive summary	2
2. Products and Services	6
2.1. Supply of products and services	7
2.1.1 Provision of Coverages	7
2.1.2 Tailoring products	8
2.2 Demand for products and services	10
2.2.1 Higher demand, low conversion rates	11
2.3 Balancing supply and demand	12
3. Cyber Insurance Underwriting and Risk Management	14
3.1 Factors considered in pricing cyber insurance	15
3.2 Non-affirmative risks	16
3.3 Cyber exposures and Accumulation Risks	17
3.4 The use of stress test scenarios	18
4. Cyber Insurance, Market Developments and Regulation	20
4.1 Market Developments	21
4.1.1 New market entrants are new opportunities	21
4.1.2 Need for a deeper understanding of cyber risk is a core challenge	21
4.2 Regulatory practices	24
4.2.1 Moderate regulation is welcomed	24
4.2.2 Government intervention might be needed in case of extreme events; market should be fully in action otherwise	25
5. Conclusions	26
6. References	30
7. Appendix	32

1. Executive summary



Cyber risk¹ is a growing concern for institutions, individuals, and financial markets. In less than five years, it has surged to the top positions in the list of global risks for business. Additionally, large-scale cyber-attacks rank sixth in the list of risks most likely to occur in the next 10 years.² The increasing number of cyber incidents, the continued digital transformation and new regulatory initiatives in the European Union are all expected to raise awareness and boost the demand for cyber insurance.

It is estimated that approximately 90% of the stand-alone cyber insurance market is located in the United States (PwC, 2016; Marsh 2016) and only approximately 5% to 9% is based in Europe, which amounts to between USD 150 million and 400 million.³ Given this asymmetry, the majority of the reports and surveys focus on the global or the US insurance market. Consequently, so far very little attention has been paid exclusively to the European market.

This fact might be intrinsically related to one of the key findings of this report (see box): the need for a deeper understanding of cyber risk is the core challenge for the European cyber insurance industry. It generates or fosters other challenges, such as improper treatment of non-affirmative risks and difficulties to quantify risks, among others.

Key findings

- There is a clear need for a deeper understanding of cyber risk, both on the supply and demand side, in order for the European cyber insurance industry to develop further. This relates not only to the assessment and treatment of risks in new cyber insurance propositions, but also to the understanding of clients' own needs.
- In terms of products and services, coverage is mainly focused on commercial business. However, interest in providing cyber insurance for individuals is increasing as technology such as the Internet of Things (IoT) develops and consumers are increasingly exposed to infringement of digital services.
- The cyber insurance industry expects a gradual increase in the demand for cyber insurance, mainly driven by new regulations, increased awareness of risks and by a higher frequency of cyber events. The relevance and importance of cyber coverage in the overall functioning of the economy is expected to increase significantly.
- Qualitative models are more frequently used than quantitative models to estimate pricing, risk exposures and risk accumulations. Lack of data is a relevant obstacle in the context of most models. Such limitations may not allow the proper estimation and pricing of risks.
- Non-affirmative exposures are identified as a key concern regarding the proper estimation of accumulation of risks.
- Lack of specialised underwriters, data and quantitative tools are key obstacles to the development of the industry and the provision of proper coverage to the economy.
- Regulation may be welcomed by the industry in a moderate fashion, as it could help to address some of the identified challenges notwithstanding the need for compliance with the Solvency II-Directive (2009/138/EU).

This survey is the first attempt by EIOPA to fill this gap. In line with EIOPA's mandate to safeguard financial stability and identify at an early stage trends, potential risks and vulnerabilities at a micro- and macroprudential level, this survey aims at getting a better understanding

¹ According to IAIS (2016), cyber risk can be defined as any type of risk emanating from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks. It also encompasses physical damage that can be caused by cybersecurity incidents, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity and confidentiality of electronic information – being related to individuals, companies, or governments.

² The Global Risks Report 2017, 12th Edition. World Economic Forum. Available at: http://www3.weforum.org/docs/GRR17_Report_web.pdf

³ Please see OECD (2017), Thomas and Finkle (2014); Marsh (2016) and Wong (2017) for references. It should be noted that London is a major cyber insurance centre, with approximately 25% of Global GWP being written through Lloyd's syndicates in 2017.

of the latest European cyber insurance developments. It covers a range of topics such as supply and demand of cyber products, cyber underwriting strategies, and potential build-up of risks. As it focuses on topics related to underwriting, it does not address cybersecurity practices of insurance companies.⁴

This report is based on responses of 13 (re)insurance groups based in Switzerland, France, Italy, Germany and UK to a set of 14 qualitative questions. The sample was selected based on expertise and current exposures in cyber insurance and consists of eight insurers and five reinsurers.

The survey was conducted through three-party telephone interviews (EIOPA, national supervisory authorities and participating (re) insurance group). The questions were sent in advance and companies had the option to send the answers in advance.

Overall, the outcome of this structured dialogue with the industry provides useful insights on the functioning, growth potential, challenges and risks of cyber insurance in Europe, notwithstanding the qualitative nature of the survey and the relatively limited sample.

The expected growing importance of cyber insurance in the portfolios of (re)insurers as well as the functioning of the real economy, necessitates further work on the topic. In that context, EIOPA included a combination of qualitative and quantitative questions on cyber risk in the 2018 Insurance Stress Test.

4 EIOPA will also work on common supervisory expectations on insurance undertakings' practices on cybersecurity and explore efficient ways to perform a cyber-attack test. See EIOPA Supervisory Convergence Plan 2018/2019 available at: <https://eiopa.europa.eu/Publications/Reports/Supervisory%20Convergence%20Plan%202018-2019.pdf>.



2. Products and Services

2.1. Supply of products and services

This chapter is dedicated to presenting the products and services and the main practices of the cyber insurance market based on the conducted survey. It first provides an overview of the supply side of the European cyber insurance market, maps the main coverage reported in the responses, assesses the appetite of the companies for specific products and elaborates on tailored coverages. It is then complemented by an analysis of the demand side of the market.

2.1.1 Provision of Coverages

This section provides a high level mapping of different type of coverages reported by the undertakings. A summary of the types of coverage offered is presented in Tables 1a and 1b.

One widely recognised difficulty for the cyber industry is the lack of commonality in risk assessment language, which becomes evident in various aspects – from coverage to underwriting questionnaires (ENISA, 2017). In order to mitigate this issue in this report, the tables were constructed and adapted based on the coverage type taxonomy proposed by the European Union Agency for Network and Information Security (ENISA) (2017).⁵

Cyber insurance can be offered as a stand-alone product and as an add-on coverage to traditional lines of business. It can include coverage for both first party and third party liabilities. Most undertakings provide tailor-made solutions as well and some undertakings also offer their products through partnerships with other insurance undertakings.

All groups in the sample offer coverage for first and third party liabilities and/or a combination of both. The most common types of coverage offered are business interruption (BI) and data restoration. Cyber extortion coverage and legal support are also provided by the majority of the insurance undertakings, although to a lesser extent.

Five undertakings in the sample also offer coverage for reputational issues. Typically, this type of coverage contains loss of net profit directly related to a cyber-attack, similar to a business interruption cover, but also provides additional support for the cost of hiring public relations consultants to help manage the insured's public perception following a cyber incident.

Regarding data breaches, there are ongoing concerns regarding the accuracy in quantifying its impact, as the consequences of such events might involve financial losses and other implications on future revenues. Another challenge is to identify whether the loss is permanent or temporary, and determining the precise impact on the brand image. In most cases, decrease in share prices was observed following data breaches (mainly based on the US experience). Overall, the market for covering reputational damage is not considered mature yet.

Additionally, three undertakings also offer coverage for individuals. They mainly include protection against conflicts arising from the use of the internet and social media or small sub limits to customers' personal area such as identity theft and payment card theft. Four companies are either developing or considering cyber insurance products with coverage for individuals. The demand for this type of coverage is perceived as promising, as discussed in the section 2.2.

Finally, there seems to be no appetite to offer potential coverage related to transactions involving cryptocurrencies at the moment, as the risks involved are currently not fully understood.

⁵ According to ENISA (2017), when it comes to language commonality with respect to cyber insurance coverage, harmonization refers to the extent that different carriers define the scope of the aforementioned coverage types in the same way.

With respect to reinsurance, it was reported that stand-alone affirmative cyber risk cover⁶ is preferably reinsured on a proportional basis with annual aggregate limitations. Furthermore, affirmative cyber extensions and endorsements are still widely attached to traditional lines. Those are reinsured depending on whether the extensions are separately flagged, have separate sub-limits and/or have specifically assigned premiums.

Reinsurers claimed to have a careful approach towards their coverage. As shown in section 4.1.2, receiving transparent and accurate information is still a challenge. Therefore, there is a strong preference to work with undertakings that can provide transparency via comprehensive underwriting information on the original coverage.

All groups directly writing cyber insurance also offer ancillary services such as advisory, legal and crisis management services. Besides the services reported in Table 1b, some undertakings also provide prevention programs such as trainings for employees to increase awareness, as well as penetration testing and scanning of systems. Furthermore, most undertakings arrange ancillary services with external providers for clients. A considerable amount of these services are offered optionally. In reinsurance contracts, costs for some ancillary services can be reinsured.

2.1.2 Tailoring products

The vast majority of the (re)insurers surveyed adopt a focused approach to cyber insurance and tailor products according to the client companies' size and needs.⁷

⁶ Affirmative cyber cover refers to insurance policies where the coverage and the perils are explicitly defined in the policy contract.

⁷ Only one insurance company claimed that the coverages are offered in the same format across industry sectors and to all sizes.

Table 1a - Coverage reported by the participant companies - Adapted from ENISA (2017)

First Part Loss - direct loss incurred by the insured	1	2	3	4	5	6	7	8	9	10	11	12	13
Network Interruption													
Loss of business income due to cyber incident			Yes	Yes		Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Business interruption	Yes	Yes			Yes	Yes	Yes	Yes	Yes			Yes	Yes
Damage to intangible assets	Yes			Yes			Yes						
Damage to tangible assets (products liability)	Yes												
Network Interruption OSP													
Loss due to outside provider security or system failure	Yes					Yes							
Network Interruption: System Failure													
Loss due to system failure or human error	Yes					Yes			Yes				
Cyber Extortion													
Cost of ransom payment	Yes	Yes				Yes			Yes			Yes	
Cyber specialist	Yes		Yes					Yes	Yes			Yes	
Electronic Data Incident													
Loss due to accidental damage of computer system													
Cyber theft													
Financial loss from fraudulent electronic transfer of funds						Yes			Yes				
Data restoration	Yes			Yes	Yes	Yes		Yes	Yes			Yes	Yes
Extra expense	Yes					Yes							
System clean-up costs													Yes
Administrative investigation and penalties													

Note: The classification should be read with caution and as a general guideline, as the undertakings were not asked to strictly classify their coverage according to this taxonomy. The table includes the responses from reinsurers, considering the underlying business being covered. Furthermore, the meaning of the blank cells is limited to the fact that the correspondent coverage was not mentioned. Therefore, they should not be interpreted as exclusions, which are listed afterwards in this section.

**Table 1b - Coverage reported by the participant companies -
Adapted from ENISA (2017)**

Third Party Loss - liability coverage / losses to others	1	2	3	4	5	6	7	8	9	10	11	12	13
Data Protection and Cyber Liability													
Liability claims	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Fines		Yes				Yes							
Media liability		Yes				Yes							Yes
Wrongful collection of information													
Media content infringement/defamatory content						Yes							
Violation of notification obligations													
Other benefits - costs and services	1	2	3	4	5	6	7	8	9	10	11	12	13
First Response													
Crisis management / IT experts	Yes		Yes		Yes	Yes					Yes	Yes	Yes
Breach-related Legal advice	Yes		Yes	Yes		Yes	Yes		Yes	Yes		Yes	Yes
Forensic investigation costs	Yes									Yes			
Call center / Hotline	Yes			Yes									
Event Management													
Legal/PR		Yes	Yes	Yes					Yes	Yes		Yes	
Technical forensic		Yes	Yes						Yes	Yes			Yes
Incident notification	Yes	Yes			Yes					Yes			
Communication costs													
Following damage to reputation		Yes				Yes	Yes	Yes					Yes
Credit / identity monitoring									Yes				
Criminal Reward Fund		Yes											

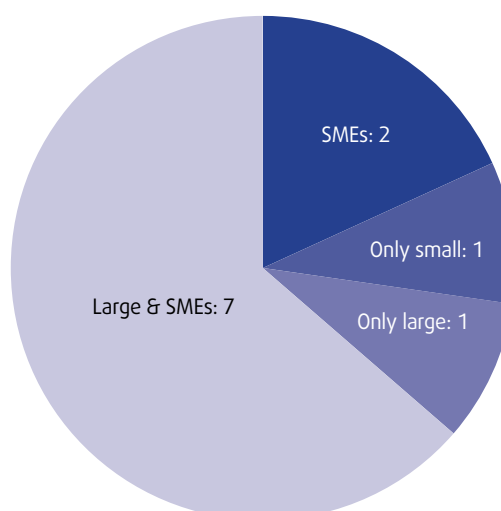
Note: The classification should be read with caution and as a general guideline, as the undertakings were not asked to strictly classify their coverage according to this taxonomy. The table includes the responses from reinsurers, considering the underlying business being covered. Furthermore, the meaning of the blank cells is limited to the fact that the correspondent coverage was not mentioned. Therefore, they should not be interpreted as exclusions, which are listed afterwards in this section.

Figure 2 shows the responses regarding the market target based on clients' size. The majority provides coverage for all sizes but adjusts the products for each case.

In general, specific products are offered to large corporations and individually underwritten with higher limits and more coverage than standard products in the market. Large companies typically invest more in their information technology (IT) security management in-house, while small companies often outsource IT facilities and security to a significant degree. The insufficient level of understanding of the risks faced by the customers is one of the key challenges for the cyber insurance market. On that front, the reputation of the potential client company plays a role in the underwriters' assessment, in particular when there is a lack

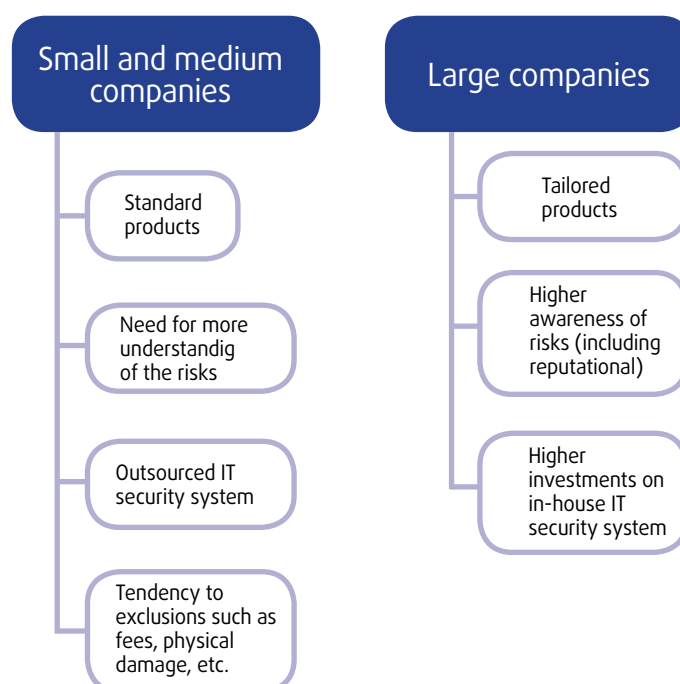
of quantitative data. An overview of the main features distinguishing SMEs from large companies can be seen in Figure 3.

Figure 2 - Cyber insurance target market by size of company



Note: SMEs stand for small and medium enterprises. The Figure incorporates answers from 11 undertakings as two participants did not respond to this question given they do not offer their own products as reinsurers.

Figure 3 – Cyber insurance related characteristics by the size of the company



The distinction of products by sector is only made by a few undertakings. While the market recognises the difference of exposures in this context, the main criteria to discern their products remains the size of the client company.

2.2 Demand for products and services

All surveyed undertakings reported a substantial increase in the demand for cyber insurance recently. Upcoming regulation and increased awareness following a number of incidents⁸ that made media headlines, such as NotPetya⁹ and Wannacry¹⁰ attacks are key reasons pointed out by the undertakings.

⁸ Some examples of major recent cyber attacks are Petya, NotPetya, Wannacry.

⁹ NotPetya is similar to ransomware incidents, but among other things, it causes severe damages to the hard drives and systems.

¹⁰ Wannacry was also similar to many ransomware incidents, but with worm tactics. The connected LANs and WANs were scanned and subsequent infections occurred automatically without user interaction. It is estimated to have infected 300,000 computer systems in four days.

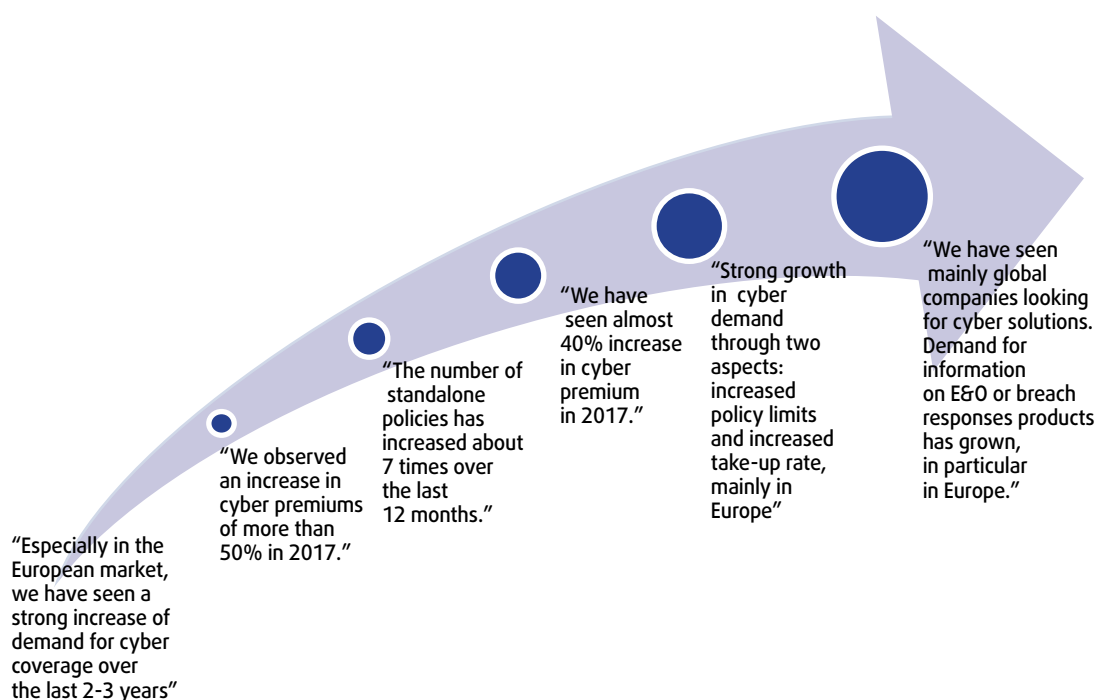
Figure 4 shows some extracts of the dialogues with different undertakings in which they report trends and some numbers related to the recent demand.

Considering the demand for new cyber insurance products, it was clearly reported that the market is expanding as more clients demand cyber risk coverage policies resulting in more tailor-made products being developed.

Along these lines, anecdotal evidence suggests that both global and mid-market customers are shifting their areas of interest away from traditional privacy liability towards business interruption policies. The focus is on coverage for commercial, small and medium sized enterprises (SMEs) and potentially retail customers. Additionally, an increasing demand for reputational damages and penalties has been witnessed in all markets.

The development of personal lines in Europe is also seen positively, as individuals are more and more exposed to cyber risks through, for instance, the Internet of Things (IoT), payment card theft and

Figure 4 – Increasing demand as reported in the survey



identity theft. Insurers are looking to fill this insurance gap for individuals, but properly understanding customer needs and adequate pricing remains a challenge.

Finally, it was also reported that reinsurance treaties are still used on a very low basis, but demand is expected to grow.

2.2.1 Higher demand, low conversion rates

Despite the observed increase in the demand, some (re)insurers highlighted that one should be careful in distinguishing actual demand and demand for information. The majority of undertakings mentioned that the conversion rates¹¹ are still low. Two companies reported an average conversion rate on the SMEs cyber packages of around 10%.

Potential explanations for the observed low conversion rates provided by the undertakings were:

- Uncertainty on scope of coverage and price level;
- Relatively high prices from the customer point of view;
- Insufficient level of understanding of the products being offered;
- Lack of clarity on the needs of the companies, in particular for SMEs;
- Many customers do not believe they are at sufficient risk to warrant the purchase of additional protection;
- Individual customers often do not fully perceive cyber as a risk and they do not understand the benefits of the insurance policy unless IT assistance is provided (hard problem or data issues).¹²

Despite the remarks above, it was also mentioned that there was improvement in the conversion rate over time, with the quote/speed of conversion in one case dropping from about 3 years in 2003 to between 1 and 6 months now.

¹¹ The conversion rate mentioned in this report represents the proportion of customers that purchase a product after showing an interest in it.

¹² One company also mentioned that it explains why demand from retail is increasing slower, with low level of interest.

Box 1: The impact of the General Data Protection Regulation (GDPR) on the demand for cyber insurance: gradual increase or a turning point?

There is a widespread expectation in the market that the enforcement of the GDPR on 25 May 2018 – at which time those organisations in non-compliance with the new regulation may face heavy fines¹³ – will stimulate a considerable increase in the demand for cyber insurance.

The predominant view of the respondents is that the expected increase in demand in this context will be more gradual rather than abrupt. Reasons for this are that it is yet unclear whether GDPR fines and fees will be insurable and the fact that the new regulation is very extensive, with most companies focusing on compliance for now. Overall, however, it is expected that GDPR will ultimately increase awareness of cyber risk and stimulate demand for cyber insurance.

While the role of regulation in increasing the demand is widely recognised,¹⁴ respondents also reported that other factors such as the potential increasing number of international cyber incidents and increased awareness are equally important and should not be necessarily considered less relevant than GDPR.

One of the key challenges for the insurance sector will be to adjust to the increase in demand following the new regulation and the changing customer needs and risk profiles.

2.3 Balancing supply and demand

Considering that most undertakings observed an increase in demand for cyber insurance coverage, while at the same time still being confronted with low conversion rates, it seems that the market for cyber insurance is not perfectly balanced.

While many undertakings observe a significant potential for growth, they still prefer to adopt a careful approach in light of the uncertainties surrounding cyber risk, ranging from difficulties in risk modelling to adequate pricing to assessing exposures. The majority of undertakings believe that supply is currently lagging behind demand, with a lack of expertise cited as the main reason for this.

However, some undertakings also indicated that the mismatch is caused by an insufficient level of understanding of cyber insurance products and their relevance by customers on the demand side. Considering that demand for cyber insurance is expected to increase significantly, this may aggravate the imbalance on the cyber insurance market in the near future in case the industry does not prepare itself properly.

¹³ The Directive requires that the Data Controller will be under a legal obligation to notify the supervisory authority about a data breach within 72 hours. Individuals have to be notified if an adverse impact is determined. The scope of the EU data protection law is also extended to all foreign companies processing data of EU residents.

¹⁴ Many companies make comparisons with the impact of regulation in increasing the demand in US cyber insurance in particular around beginning 2000's. Some makes a more cautious comparison by highlighting the differences in both markets.



3. Cyber Insurance Underwriting and Risk Management

3.1 Factors considered in pricing cyber insurance

All companies writing direct insurance business reported the use of some model for pricing purposes. However, given the lack of data and specialised tools to estimate benchmark prices in case of cyber losses, the majority of companies are making use of qualitative models for pricing (Figure 5). In general, robust pricing solutions are still under development by the market.

The level of complexity of the models varies across the participants, which might reflect a potential discrepancy in the accuracy of the pricing outcomes. Indeed, risk of underpricing was one of the concerns reported by the participants, as shown in the section 4.1.2. The main differences between the models are the methodology, the type and number of parameters included, the complexity of the model and the degree of specialisation of such models for cyber, i.e. taking into account particularities that are not entirely captured by standard models. Figure 6 provides an overview of the models the factors considered for pricing.

Some (re)insurers also reported efforts to improve such models while databases

Figure 5 – Use of qualitative and quantitative models for pricing as reported by companies



are being created or purchased from external providers in some cases. Difficulties are observed in the implementation of advanced systems as there is still a lack of sufficient amounts of claims data and even so, it is hard to measure the relevance to the current or the future cyber landscape because of the rapid technological advances. The qualitative models are often based on a rating approach, with its fundamentals grounded on questionnaires.

Figure 6 – Overview of pricing tools and factors considered in the estimations

Qualitative	<ul style="list-style-type: none"> • Pricing tool based on risk assumptions of exposure • Rating approach, based on questionnaires/web scanner • Expert judgement
Quantitative	<ul style="list-style-type: none"> • Actuarial pricing rating tools • Interconnected models covering different parameters
Key factors considered	<ul style="list-style-type: none"> • Size • Industry classification • Customers' behaviour • Loss experience/historical • Coverage provided - Jurisdiction - Level of encryption - IT processes - Expected level of impairment - Policy limits

Finally, given the large tail risks and uncertainties around cyber risk, cyber insurance is currently relatively expensive compared to other types of insurance coverage, with estimations that cyber insurance coverage can be three times more expensive than general liability coverage and six times more expensive than property insurance.¹⁵

3.2 Non-affirmative risks

This section assesses “non-affirmative” or “silent” risks. This risk refers to instances where cyber exposure is neither explicitly included nor excluded within an insurance policy.¹⁶ This is considered one of the key concerns of the industry (see section 4.1.2).

Non-affirmative risks can result in accumulation of losses within other policies triggered by a cyber event. That can be alarming as the potential for losses exists but there are difficulties in estimating the potential exposure. As technology develops and the access to devices that offer

facilities and services highly dependent on the web increases, quantifying such exposures becomes even more challenging, as mentioned several times in the survey.

Overall, there are generalised efforts from the industry to address the challenges they are facing. Some participants declared that it remains difficult to separate aggregated risks from individual risks, the latter being the ones current policies are assumed to cover. Others see the main challenge in detecting the non-affirmative exposure in traditional lines of business and to quantify and estimate it properly.

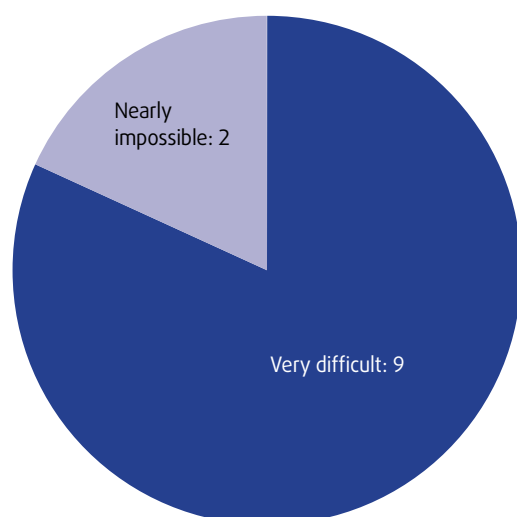
In principle, nearly everything included in property and casualty could eventually be exposed to non-affirmative risks. However, there are currently few examples of cyber-attacks that have materialised as physical damage, as cyber manifests in more intangible losses, and not so much in physical damages.

A common approach to assess non-affirmative exposures is to build scenarios and stress test existing portfolios. Assumptions about potential loss penetration and claim volumes by line of business are often implemented. The general process might involve identifying the type of cyber threats, the dimension of the cyber-attack, the assessment of the silent part and the transmission. Potential cyber-attacks on electricity power infrastructure facilities are considered as the key scenario for non-affirmative risks.

Some (re)insurers are also building up a framework that looks at the fundamental coverage given for each line of business and write specific exclusions for cyber risk. The intention is to form risk assessment guidelines, a framework based on the exposure of the underlying risk for all lines of business.

In some cases, exclusions might not be practical, and instead the coverage language should be made clearer such that it becomes affirmatively covered, and included in pricing calculations. In this

Figure 7 – Is it possible to quantify non-affirmative risks?



¹⁵ PwC (2015) and Z/Yen Group (2015).

¹⁶ Silent or non-affirmative risks can be illustrated as a malware infecting a GPS, which might cause aviation, marine or car accidents; or as cyber incident causing fire for example through a device connected to houses.

Figure 8 – Initiatives to address non-affirmative risks



regard, it was mentioned that ultimately customers will be better served by buying a dedicated specific cyber product, although the market is not yet mature to the point of being very detailed and specific in this context. In that respect, according to the Organisation for Economic Co-operation and Development (OECD) (2017), the potential for silent coverage to be found in traditional policies could also be impeding the willingness of insurance companies to expand the coverage they provide for cyber risk.

3.3 Cyber exposures and Accumulation Risks

This section provides a description of the exclusions (Figure 9) and the main insights related to cyber exposures and accumulation of risk reported by the respondents. As is the case with non-affirmative risks, the industry is also making considerable efforts to assess accumulation risks.

Despite the fact that (re)insurers can make a better assessment of the affirmative cyber exposures, the degree of uncertainty when estimating accumulation risk could be high in that case. The lack of stochastic models at the moment is seen as a limitation for the risk assessments. Instead, there is a prevalence of deterministic processes that are used.

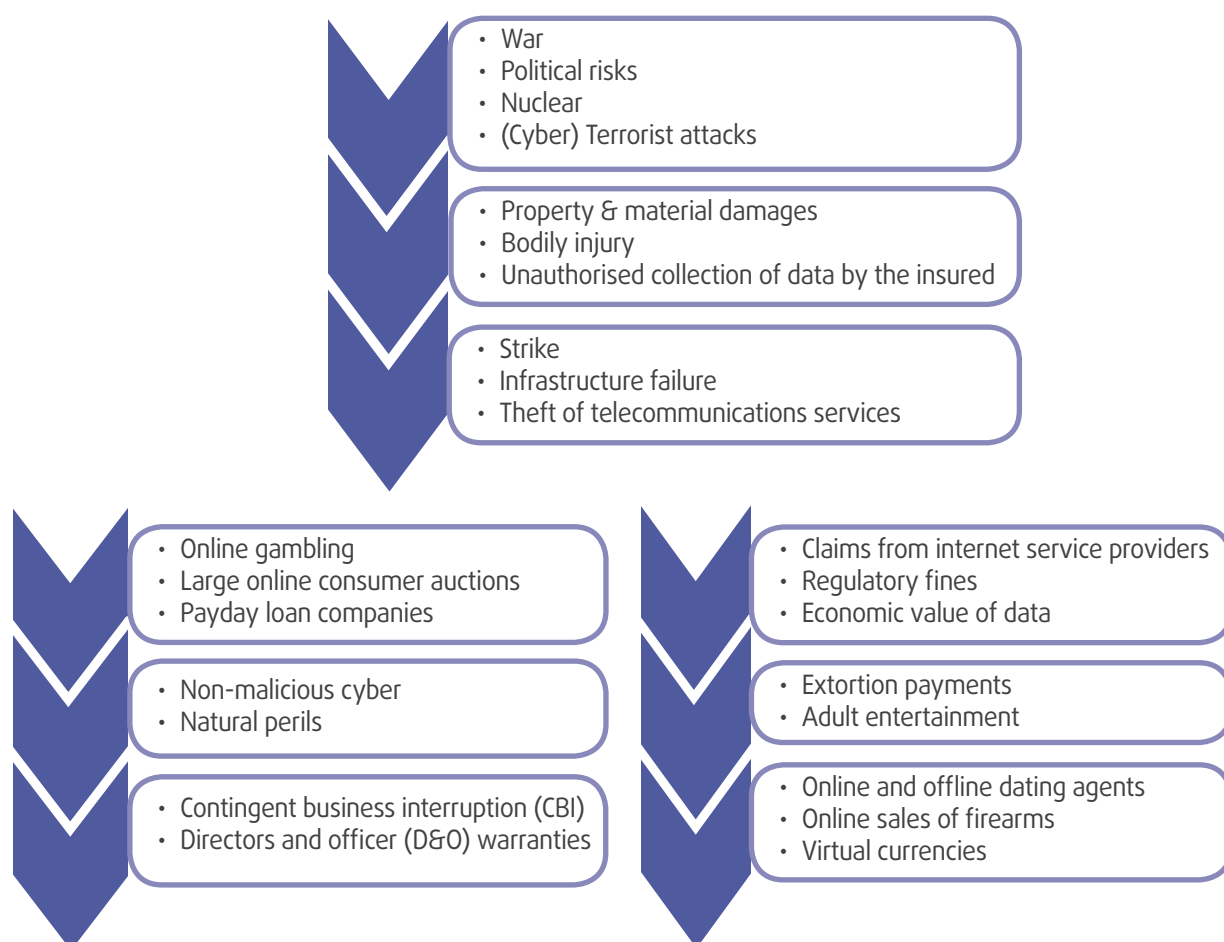
In order to understand exposures and to identify common aggregation paths, (re)insurers rely on multiple scenarios. Those are often calculated in a similar approach as handling natural catastrophes aiming at identifying limits and which level of cyber threat will lead to an accumulation of risks. In addition, external cyber risk models are often fully implemented or incorporated for complementary purposes. Some cyber scenarios include aspects like cloud service provider failure, theft from a data aggregator, ransomware and physical damage scenarios.

Some participants also mentioned practices of classifying affirmative cyber cover in internal underwriting systems by making use of codes. Furthermore, the development of databases to enable the assessment of aggregation across multiple dimensions including industry, company size, geography and common providers were also reported, although still less common.

In order to access accumulation risk, realistic disaster scenarios try to estimate the impact of losses arising from the same cause/event in products across the whole portfolio, including assumptions about relative losses. This can be applied in the context of both affirmative and non-affirmative risks.

Figure 9 - Exclusions reported by the participant companies

18



Some undertakings reported that accumulation risk is taken into account by adding the loss estimates to their external business and (depending on the scenario) operating entities with the largest impact of the respective scenario. Therefore full dependency of the losses of those carriers is assumed.

The development of a cyber escalation threshold was also reported. The idea is that scenarios that exceed certain pre-defined threshold levels are escalated internally for review and discussion.

3.4 The use of stress test scenarios

Most respondents reported the use of stress test scenarios for assessing cyber risk exposures. The few companies that did not use stress tests justified this

mainly based on the limited size of their current cyber risk exposure.

There is a generalised effort to implement quantitative components in the models as much as possible. Lack of data and specialised stochastic models are considered as key limitations. Some reported joint work with CAT modellers to model eventualities for example involving Malware and Wannacry events. Others also license data from third parties that incorporate the explicit IT and non-IT dependencies across counterparties.

Another approach mentioned was the estimation based on an internal research of various cyber “nodes of aggregation.” As an example, a ‘Linux Data Theft scenario’ considers the potential for all Linux users to be subject to the same event based on an exploited flaw in source code. While there is an effort to explicitly

identify companies that use Linux, this approach is supplemented by simulation running.

The key parameters included in scenarios and models mentioned by the participants are listed in Figure 10.

Some of the scenarios shared with EIOPA include power blackouts, attacks on service providers, cyber-crime events such as a virus attack that would affect a wide range of insured individuals and companies, data breaches of a key provider, mass distribution of a commodity ransomware strain and reverse stress testing.¹⁷

Figure 10 – Key parameters included in the stress test scenarios

Key Parameters	
	Attack rates
	Attack vectors
	Assets compromised
	Assets impacted
	Number of policies affected by the same event.
	Coverage costs
	Number of contracts
	Anticipated period of outage
	Exposure to the expected peril
	Extent of the impact and recovery of business
	Range of area/number of customers affected (by scenario and by product lines)
	Exposure to the expected peril
	Interaction with reinsurers
	Limit and geographical profiles

¹⁷ The reverse stress testing starts with a presumption that the (re) insurer is no longer viable to continue and capital eroded, building the analysis backwards to achieve a conclusion whether the company would be prepared for such an event and is taking mitigating action.



4. Cyber Insurance, Market Developments and Regulation

4.1 Market Developments

The digital transformation and technological innovation progresses at a fast pace, bringing new business opportunities and entrants. As a consequence, consumers have more alternatives for insurance while the insurance sector faces stronger competition. This section focuses on participants' general views about new market practices, the implied challenges, and its impact on the cyber insurance market.

4.1.1 New market entrants are new opportunities

All participants see new entrants such as InsurTech start-ups as potential partners and an opportunity to innovate and improve products rather than a threat. Competition is seen as a positive and important element that incentivises further developments on the market. It is widely recognised that there is substantial capacity in the market at the moment. Business collaboration with new entrants is already a reality and intentions to develop it were expressed as a possibility by several participants.

In this respect, it was mentioned that although there are many new ideas in the market, it is very hard to assess which will ultimately succeed. It is therefore important to understand that it can take a considerable amount of time and risk to identify which companies and start-ups would be worth collaborating with.

The predominant view is that new players acting in the market result in higher risk awareness, efficiency, and more innovative products, while improvement of cyber education was also mentioned as an important outcome. The education of brokers and buyers in both mature and emerging markets plays an important role in ensuring that clients' risks are addressed by the products provided because a need for a deeper understanding and knowledge from both sides is currently the key limitation towards the cyber insurance market. Especially, brokers should learn to assess the risk from the aggrega-

tion perspective and through commercial insurance products.¹⁸

In this regard, the survey indicates that a more competitive environment could create an opportunity to underwrite cyber insurance more accurately. That would apply not only in terms of enhanced underwriting expertise, but also with respect to the overall improvement of the clarity of insurance wordings across all lines of business, addressing silent risks. In particular, a more holistic view of cyber would improve the buying pattern of insured clients and should help to address difficulties to differentiate terrorism, IT security failures and different forms of cyber-attacks.

The importance of new technologies to evaluate clients' vulnerabilities and propose preventive solutions was in general also considered a key benefit of new technologies. There are many aspects to be learned for instance from internet traffic and the use of social media, which could provide a better view of the risks. The potential partnerships using advanced technology such as cloud services could lead to a more efficient distribution of cyber insurance as well.

4.1.2 Need for a deeper understanding of cyber risk is a core challenge

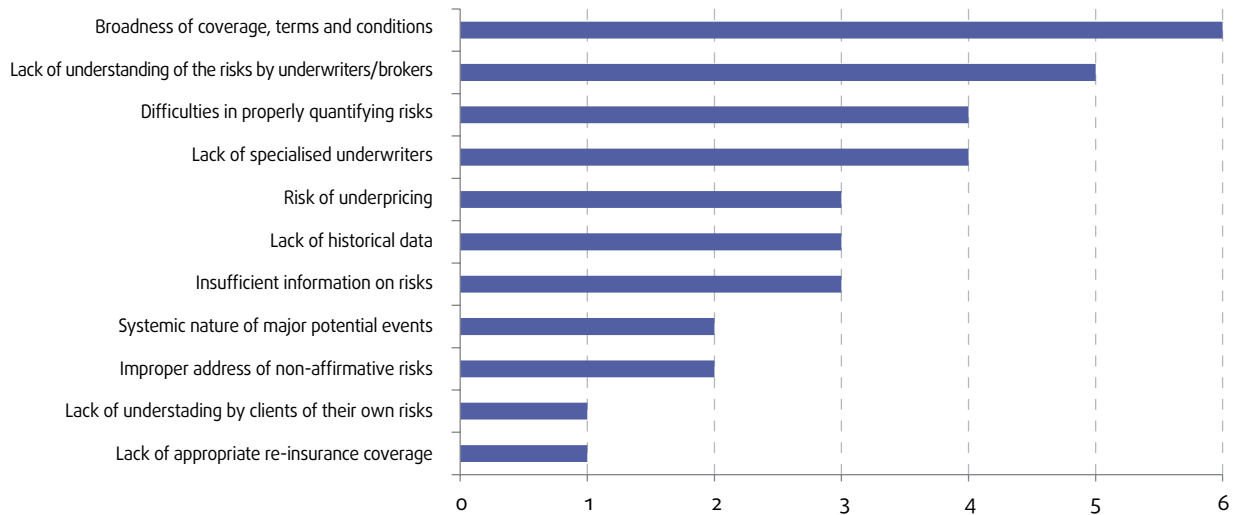
Considering the need to identify aspects to be monitored and further analysed, the survey addressed the main concerns of (re)insurers regarding the current cyber insurance market practices.

Figure 11 shows all concerns mentioned. It is important to highlight that this topic was addressed as an open question, meaning that the concerns were not restricted to a pre-defined list and participants were free to mention anything they would acknowledge as relevant.

Overall, the key concerns are clearly interconnected (Figure 12). In this sense,

¹⁸ Please see also the report (The Geneva Association, Ten Key Questions on Cyber Risk and Cyber Risk Insurance, 2016).

Figure 11 - Market concerns (by number of responses)



although it is the second most mentioned challenge in the survey, it is possible to identify the **need for a deeper understanding of cyber risk** as the **core challenge** for the industry, as it either fosters or directly causes other risks and challenges. Furthermore, if it could be removed or lessened, that would substantially mitigate the overall level of concern of the market regarding risks.

The need for a deeper understanding of cyber risk is not only from the industry's perspective, as participating groups also mentioned that the same challenge exists from the clients' point of view. Many clients do not understand the products or their own needs. In particular, this can be observed in small and medium size companies.

The lack of specialised expertise and players in the market is another intrinsic challenge for the industry. However, as cyber insurance is a new line of business for many entities and there is a willingness to rapidly expand this business, demand for talents is expected to grow significantly, bringing new expertise to the market.¹⁹ On the other hand, given its fast evolving nature, it is somehow a risk with new layers of complexity, which on its own, is not yet fully understood.

The core challenge is fomented by **external challenges**, which are those that cannot be fully addressed either indefinitely or in the short/medium-term given its nature or given the current stage of maturity of the market. The challenges identified as such are lack of historical data and systemic nature of major potential events.

Lack of data is a primary obstacle to a detailed understanding of fundamental aspects of cyber risk. It is challenging to build adequate models to assure accuracy in the risk management if the availability of data is limited. That might not only reinforce the fact that there is a need for a deeper understanding of cyber risks, but also foment the insufficient level of risk information in the market. This challenge was particularly reported as relevant by reinsurers, which raised the issue of receiving submissions with insufficient risk information without an adequate level of control. From their perspective, it represents substantial underwriting risk. On the other hand, a lack of appropriate re-insurance coverage for cyber risks is also reported as a main concern for insurance companies. Overall, survey participants expressed efforts to mitigate insufficient level of information by, for example, requiring at least a minimum level of necessary information.

Insufficient information on the associated risks can therefore be designated as one of the obstacles to a deeper understand-

¹⁹ The industry is also trying to address the lack of specialized knowledge by for example offering trainings to improve expertise in cyber underwriting.

ing of cyber risk, but it can also be a result of it, as with improper assessment of the risks, it is not possible to share adequate information. Another aspect that was not directly mentioned by the participants in this respect but still cannot be left outside of the analysis is the reputational implications that some companies fear in sharing information under a full transparency and non-anonymised approach. This is an additional obstacle to address the information collection challenge.

The systemic nature of major potential events is another type of external challenge which makes it very difficult to understand the dimension and the accumulated risks for the market as whole.

All the remaining challenges are somehow a consequence of the core challenge and its reinforcing factors, being therefore **outcome challenges**. The most frequently mentioned concern regarding current cyber insurance market practices was the tendency of broadening coverage, terms and conditions.

Most of the respondents attributed intermediaries such as brokers as being the key drivers of this behaviour, but start-ups and insurance companies were also seen as adopting a more flexible approach to-

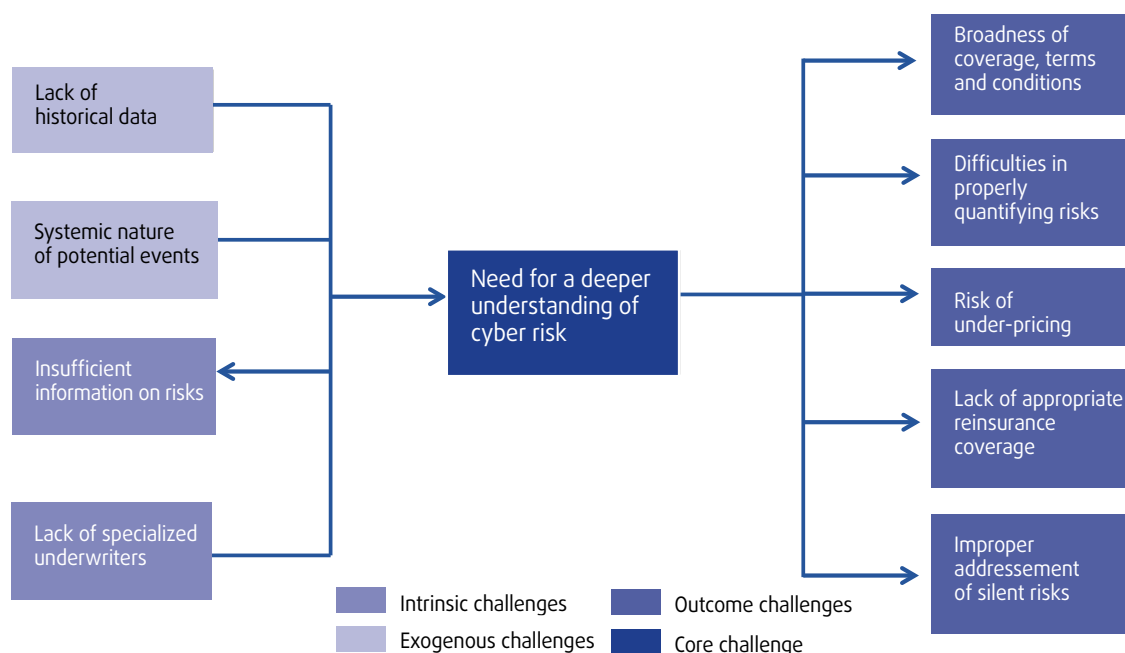
wards contracts. The fact that there are seemingly few big managing general agents holding a significant share of the market was also highlighted.

The key explanations provided for this behaviour were the increasing competition and, again, that a deeper understanding of the risks is still missing. Coverage may include items that are highly demanded by policyholders, but that are less well understood from a frequency and aggregation point of view, such as systems failures (for example operation IT risk) and contingent business interruption.

Difficulties in properly quantifying risks were mentioned by several undertakings as a main concern. It was stated that cover limits are driven by price rather than by the assessment of the likely indemnity required to recover the business from a cyber event. Along these lines, there are concerns that some insurers may be moving towards writing cyber risk on the least possible amount of information without using intellectually property from external cyber risk modelling providers. As a result, there is a risk that covers are under-priced.

The treatment of contingent business interruption and the potential aggregation risk were also mentioned as concerns from

Figure 12 - Framework of the key concerns raised by the companies



an insurance perspective. The increase in connectivity of destructive attacks in combination with the centralisation of IT services, for instance cloud services, will make it very challenging for the market to properly quantify and fund this risk. This concern includes misevaluation of accumulation risk as a result of the lack of industrialised market standards and tools for accumulation control and risk assessment. The growing interest in stop-loss reinsurance to address the silent exposure was also mentioned.

4.2 Regulatory practices

This section provides an overview on how the participants perceive cyber regulation and the potential role of governments on addressing cyber risk. While the majority does not see any regulatory obstacles that could ultimately restrain the growth of the cyber insurance market in the present, all companies do see the need of regulation to some extent in the future.

A potential intervention of governments was mentioned as necessary, in particular in the case of extreme events, although this view was not fully aligned among all participants.

4.2.1 Moderate regulation is welcomed

When asked whether there would be any obstacles in the current supervisory framework²⁰ that could ultimately restrain the growth of the cyber insurance market, the vast majority of the companies answered in a forward-looking fashion: after promptly excluding negative regulatory externalities at the present, most under-

takings proactively suggested issues that regulation could tackle in the near future.²¹

The relative eagerness to welcome regulatory measures was accompanied by a clear urge of moderation regarding such measures in order to avoid the imposition of overly stringent requirements to the market. Some participants also raised the importance of harmonisation of a potential supervisory framework across countries. In that context, an additional area for follow-up work for EIOPA would be to investigate the possibility of introducing (a) new line-of-business code(s) in Solvency II, which could help provide more insights into the quantitative dimension of cyber insurance.

In general, regulation is viewed as a mitigating measure for the main concerns mentioned in the previous section. Figure 13 provides a list of possible contributions that regulators could make to improve the functioning of the cyber insurance market from the point of view of the participants.

The most mentioned potential contribution that regulation could make was to ensure appropriate pricing and monitoring of the risks, including aggregation risks. Secondly, it was highlighted that regulation should allow sharing of data, such as breach information.²² Legal conditions should be created to allow companies within different industries to share common interest and information with the sole purpose of addressing cyber threats and the mitigation measures. They advocated for an anonymous, centralised system that could enable information sharing.

Thirdly, it was stated that regulatory practices should help to enhance the level of

²⁰ There are several EU initiatives aiming at targeting cyber risk at the EU level, such as the cyber security package in the context of the Digital Single Market strategy, the NIS Directive, the General Data Protection Regulation and the Contractual Public-Private Partnership (cPPP) on cybersecurity, signed by the European Commission and the European Cyber Security Organisation (ECSO). For more details, please refer to Box 1 of the EIOPA Financial Stability Report of December 2017, available at: https://eiopa.europa.eu/Publications/Reports/Financial_Stability_Report_December2017.pdf

²¹ One participant exceptionally reported that excessive and strict regulation in its jurisdiction to insure ransomware might be hampering this type of business.

²² In this regard, a common taxonomy across industries is essential for better analysis and benchmarking. The CRO Forum developed a common categorisation methodology for cyber events that might fill the existing gap of unavailability of digital event/cyber loss data. For more information please see article available at: https://www.thecroforum.org/wp-content/uploads/2018/02/201802_CROF_Capture_and_sharing_of_digital_event_data.pdf

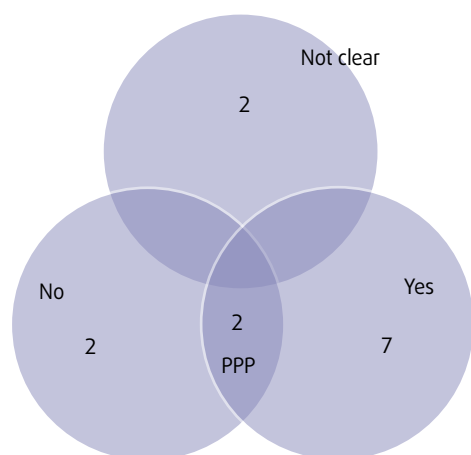
Figure 13 – Potential contributions of regulation – by number of companies



understanding of risks, which was identified as a core concern in the section 4.1.2. However, no further details on which measures and the extent of feasibility to achieve this purpose were provided.

The other suggested contributions concern the need of introducing minimum information security and IT standards, the enhancement of prudence of new entrants, adequate capital requirements against underwriting risks, measures to avoid contagion in case of bigger scale events and ensuring both a greater clarity about coverages and adequate estimation of value for money measures in order to ensure a better risk assessment in case of periods of higher losses. The latter should consider factors such as risk distribution volatility and average loss experience.

Figure 14 – The need of a potential intervention of the government



4.2.2 Government intervention might be needed in case of extreme events; market should be fully in action otherwise

Given the potential for significant accumulation of losses and the difficulties in estimating the extent of major cyber incidents, the government is often seen as a potential last resort of the system. A strong majority has confirmed that governments should play that role in particular when massive incidents might take place. Examples of such events included scenarios where critical infrastructure is interrupted for a period long enough to impact the economy.

Among those in favour of a clear role of the government in the cyber context, there were diverging views on the urgency and the extent of government intervention. While some participants expressed concerns about the capacity of the insurance sector to handle accumulation risk in case of (a series of) extreme, highly severe events and on capital capacity; it was also reiterated that some parts of cyber risk are even certainly uninsurable. The “borderless” nature of cyber events was mentioned by three groups, enhancing the need of a potential cross-country cooperation in this sense.

Furthermore, some (re) insurers highlighted the importance of considering public-private partnerships (PPP). An overview of the results is provided in Figure 14.

5. Conclusions



The European cyber insurance industry is growing. However, risks are still not fully understood. That holds both for the industry as for the clients. New regulations, as well as new technological developments and further materialisation of incidents are expected to raise awareness and foster demand for cyber insurance in the upcoming years. The industry is currently still small in relative size, and is perceived to have a great potential to develop further.

This report is the first attempt by EIOPA to enhance the level of understanding of cyber risk underwriting with a focus on the European market. As the industry faces several challenges to meet the expected increasing demand and satisfy clients' needs, further work will also be required from the supervisory side, in particular on the quantitative side.

In this respect, EIOPA has included a questionnaire related to cyber risk in the 2018 Insurance Stress Test exercise. As the Stress Test will encompass close to 78% of the total EU-wide market,²³ the conclusions are expected to reflect the overall European cyber insurance market. Furthermore, by including more detailed questions regarding assessment and quantification of risks requiring estimations and numbers, EIOPA will be able to identify further aspects in more detail. In addition, EIOPA will investigate the possibility of introducing (a) new line-of-business code(s) in the Solvency II framework to enhance understanding of the quantitative dimension on a more structural basis.

As for the insurance industry, the key challenges are observed in developing expertise and implementing more advanced systems, as there is still a lack of sufficient amounts of claims data - and even so, it is hard to measure the relevance to the current or the future

cyber landscape because of the rapid technological advances. Therefore, it is not only scarcity of data that makes the development and application of quantitative tools difficult, but also the evolving and dynamic nature of the incidents.

Non-affirmative exposures are another concern for the industry. Although no major related event has materialised yet, the industry should continue to invest in solutions to address it. The above-mentioned initiative on cyber risk in the 2018 Insurance Stress Test will also include a more detailed assessment of non-affirmative risks.

This survey, although based on a limited sample, allows for some interesting key findings:

- There is a clear need for a deeper understanding of cyber risk. This relates not only to the assessment and treatment of risks in new cyber insurance propositions, but also to the understanding of clients' own needs.
- Coverage is mainly focused on commercial business so far, but interest in providing cyber insurance for individuals is increasing as technology such as the Internet of Things (IoT) develops and consumers are increasingly exposed to infringement of digital services.
- The cyber insurance industry expects a gradual increase in the demand for cyber insurance, mainly driven by new regulations, increased awareness of risks and by a higher frequency of cyber events. The relevance and importance of cyber coverage in the overall functioning of the economy is expected to increase significantly.
- At the moment, qualitative models are more frequently used than quantitative models to estimate pricing, risk exposures and risk accumulations. Lack of data is a relevant obstacle in the context of most models. Furthermore, non-affirmative exposures are identified as a key concern regarding the proper estimation of

²³ The target sample encompasses 42 insurance groups based on total consolidated group assets in the Solvency II reporting.

accumulation of risks. In that regard, lack of specialised underwriters, data and quantitative tools are key obstacles for the development of the industry and the provision of proper coverage to the economy.

- Finally, regulation may be welcomed by the industry in a moderate fashion, as it could help to address some of the identified challenges.

6. References

The background of the slide is a dark blue image. On the left, there is a white diagonal line. To the right of the line, there is a large, dark blue flag with a white grid pattern on the left side and a white star on the right side. The flag is waving. In the background, there is a large, white, dome-shaped structure with a grid pattern, possibly a stadium or a large building.

- EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA), 2017. Commonality of risk assessment language in cyber insurance Recommendations on Cyber Insurance. ISBN 978-92-9204-228-8, DOI 10.2824/691163.
- MARSH (2016). Continental European Cyber Risk Survey: 2016 Report, Marsh LLC, October.
- PwC (2015), Insurance 2020 & beyond: Reaping the dividends of cyber resilience, PwC.
- PwC (2016). Moving forward with cybersecurity and privacy: Key findings from The Global State of Information Security® Survey 2017, PwC
- IAIS (2016). Issues Paper On Cyber Risk to the Insurance Sector. IAIS publication.
- OECD (2017), Enhancing the Role of Insurance in Cyber Risk Management, OECD Publishing, Paris. <http://dx.doi.org/10.1787/9789264282148-en>
- THOMAS, L. and J. FINKLE (2014), "Insurers struggle to get grip on burgeoning cyber risk market", Reuters Technology News, 14 July, www.reuters.com/article/us-insurance/cybersecurity-idUSKBN0FJ0B820140714.
- WONG, S. (2017), "Cyber Risk Insurance", Presented at NAIC-OIC-OECD Roundtable on Insurance and Retirement Savings in Asia, 20-21 September, Bangkok, www.oecd.org/daf/fin/insurance/oecd-insurance-retirement-asia-2017.htm.
- Z/YEN GROUP (2015), Promoting UK Cyber Prosperity: Public-Private Cyber- Catastrophe Reinsurance, Long Finance.

7. Appendix



Questions sent in advance to the companies

Products and services

1. What type(s) of cyber insurance coverage does the company offer? Does it also offer coverage for third party liability in this context? Are there any exclusions regarding some types of cyber risks?
2. Are there different products offered based on type of sectors, i.e. to financial and non-financial sectors or based on size (large, small and medium-sized enterprises, retail business)? If yes, could you please provide more details on the major differences?
3. Has the company been noticing an increase in the demand for cyber insurance products in the last 2 years? Do you have any estimate on the increase (based for example on number of contracts, amount of insured capital, etc) and type of products?
4. Does the company offer provision of ancillary services to customers, such as advisory, pre and post breach risk analysis or data remediation after attacks?
5. How does the company perceive the future perspectives for the cyber insurance market? Do you notice or expect an increase of demand for cyber products due to the implementation of General Data Protection Regulation (GDPR) in 2018? What are the main challenges?
6. In your opinion, are there any obstacles in the current supervisory framework that could ultimately restrain the growth of the cyber insurance market?
7. In general, what is the geographical scope and what are the typical events and risks insured (business interruption, reputational damage, protection against loss of sensitive data, etc.)?

Cyber Insurance Underwriting and Risk Management

8. Does the company use a quantitative model for assessing cyber insurance? What are the factors considered in pricing cyber insurance?
9. How prevention measures and internal policies by the customer are taken into account into pricing and how is the treatment of the residual risk?
10. Cyber exposure – How do you estimate the accumulation of risk in the portfolio? Please elaborate on affirmative vs non-affirmative risk.
11. How is non-affirmative risk assessed and how does the company mitigate such risks? Which lines of business could be concerned by non-affirmative cyber risk? How do you classify your current affirmative covers?
12. How do you manage cyber exposure risk in your portfolio? Is cyber exposure part of your risk appetite?
13. Do you incorporate a cyber scenario within your stress testing framework? What are the main parameters? How do you consider the dependency of cyber insurance contracts to the same cyber-event?
14. What are your main concerns on the current market practices related to cyber coverage? For example, is there any concern related to intermediaries or startups acting in the market?

