CYBER RISK FOR INSURERS– CHALLENGES AND OPPORTUNITIES

https://eiopa.europa.eu/

eiopa

European Insurance and
Occupational Pensions Authority

PDF	ISBN 978-92-9473-213-2	doi:10.2854/305969	EI-03-19-498-EN-N
Print	ISBN 978-92-9473-214-9	doi:10.2854/158469	EI-03-19-498-EN-C

Luxembourg: Publications Office of the European Union, 2019

CYBER RISK FOR INSURERS– CHALLENGES AND OPPORTUNITIES

CONTENTS

EXECUTIVE SUMMARY

In August 2018, EIOPA published the report "Understanding Cyber Insurance - A Structured Dialogue with Insurance Groups". The key finding was that the need for a deeper understanding of cyber risk presents the core challenge for the European cyber insurance industry.

In line with these findings and with EIOPA's mandate to safeguard financial stability, this report aims at further enhancing our understanding of cyber risks for the insurance sector. While the first report was based on a qualitative survey focusing on cyber underwriting only, this report covers both cybersecurity challenges and cyber underwriting practices of insurers.

As cyber threats have become more prominent in recent years, they are increasingly considered as a top global risk for the financial sector and the economy as a whole. The increasing frequency and sophistication of cyber attacks, the fast digital transformation and the increased use of big data and cloud computing make insurers increasingly susceptible to cyber threats. Insurance groups also form a natural target for cyber attacks, as they possess substantial amounts of confidential policyholder information. On the other hand, the digital economy and the advance of technology also offer opportunities to cyber underwriters. A well-developed cyber insurance market can play a key role in enabling the transformation to the digital economy, by raising awareness of cyber risks, sharing knowledge on good cyber risk management practices and facilitating responses to and recovery from cyber attacks.

Overall, this report provides new information about cyber risk for the European insurance sector, both from an operational risk management perspective and an underwriting perspective, based on the responses of 41 large (re)insurance groups across 12 European countries representing a market coverage of around 75% of total consolidated assets. The findings reflect the need for a sound cyber resilience framework for insurers as well as the challenges faced by the cyber underwriters. The main conclusions can be summarized as follows:

Cyber risk as an element of the insurer's own operational risk profile

- Having clear, comprehensive and common requirements on governance of cybersecurity as part of operational resilience would help ensure the safe provision of insurance services. This includes a consistent set of definitions and terminology on cyber risks to enable a more structured and focused dialogue between the industry, supervisors and policymakers, which could further enhance the cyber resilience of the insurance sector.
- The most common cyber incidents affecting insurers are phishing mail, malware infections (ransomware), data exfiltration and denial of service attacks. The main consequences suffered by insurers following these cyber incidents are business interruption and material costs for policyholders and third parties.

- Overall, the results indicate that the industry is aware of the potential cyber threats and have incorporated cyber risk explicitly in their risk management frameworks.
- Further actions to strengthen the resilience of the insurance sector against cyber vulnerabilities are essential, in particular considering the dynamic nature of cyber threats. This would include streamlining of the cyber incident reporting frameworks across the insurance and financial sector, to avoid inconsistencies in the reported information and ultimately enhance operational resilience.

Cyber insurance market

- Although still small in size, the European cyber insurance industry is growing rapidly, with an increase of 72% in 2018 in terms of gross written premium for the insurers in the sample, amounting to EUR 295 million in 2018 compared to EUR 172 million in 2017. The increasing frequency of cyber attacks, changes in regulation as well as continued technological developments are all expected to increase demand for cyber insurance in the near future.
- Non-affirmative cyber exposures remain a source of concern. While common efforts to assess and address non-affirmative cyber risks are under way, the lack of quantitative approaches, explicit cyber exclusions and action plans to address non-affirmative cyber exposures suggest insurers are currently not fully aware of the potential exposures to cyber risk.
- Some groups have adopted a 'wait-and-see' approach to address non-affirmative cyber risk, where the implementation of actions plans to address non-affirmative exposure depends on the materialization of future events. This approach in dealing with cyber risks can be particularly problematic, as insurers may suffer substantial unforeseen losses in traditional polices if a cyber incident materializes.
- The lack of transparency in non-affirmative exposures also creates uncertainty for policyholders, as it is often not clear whether their cyber claims would be covered within their insurance polices. Further effort is therefore needed to properly tackle non-affirmative cyber exposures to address the issue of potential accumulation risk and provide clarity to policyholders.
- It is essential for the industry to further improve its assessments and data collection, so that cyber risks can be adequately measured, monitored and managed. Ultimately, having common and harmonized standards for both cyber risk measurement and reporting purposes could greatly facilitate the understanding of cyber risk underwriting. To this end, creating a European-wide cyber incident reporting database, based on a common taxonomy, could be considered as well.

1. INTRODUCTION

Cyber risks have been on the rise for quite some time, as digitalization and interconnectivity are transforming business and the global economy at an unprecedented pace. While technology has expanded the scope of opportunities beyond geographical limits and has markedly changed the way companies conduct business, the intense use of technology also opens doors to vulnerabilities.

In line with EIOPA's mandate to safeguard financial stability, EIOPA has been taking several initiatives[1] to monitor cyber risks in the context of the insurance sector.

This report aims at further enhancing the understanding of both the vulnerabilities of the European insurance sector towards cyber risk as well as challenges facing cyber insurers in the European cyber insurance market. To this end, the report provides an overview of cyber risk as part of the risk profile of insurers from the operational risk perspective as well as the challenges and opportunities for the European cyber insurance market. As such, it builds on the EIOPA report "Understanding Cyber Insurance - A Structured Dialogue with Insurance Groups" published in August 2018.

This report is divided in 5 chapters. Following this introduction, Chapter 2 describes the data coverage and the sample. Chapter 3 elaborates on cyber risk as an element of the insurer's own operational risk profile, focusing on the vulnerabilities of insurers towards cyber threats. Chapter 4 focuses on cyber insurance, covering the main challenges regarding affirmative and non-affirmative cyber risk exposures. Chapter 5 concludes.

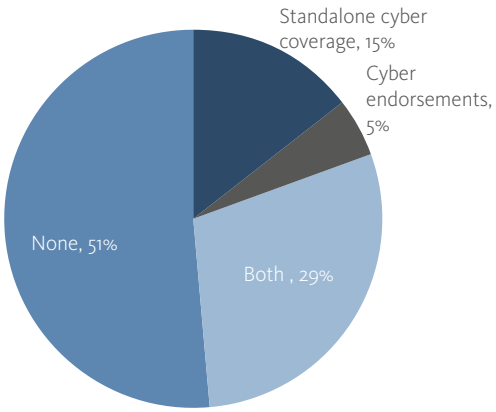
1 See for example, a summary of the EIOPA Cyber Insurance Workshop available at https://eiopa.europa.eu/Pages/EIOPA-Cyber-Insurance-Workshop.aspx. In addition, since June 2016, analyses and assessments on cyber risks are included in EIOPA's Financial Stability Report, available at: https://eiopa.europa.eu/Pages/Financial-stability-and-crisis-prevention/Financial-Stability-Report-June-2016.aspx. Finally, EIOPA has also, together with EBA and ESMA, issued Joint Advices on ICT Risk Management and cybersecurity to the European Commission, available at https://eiopa.europa.eu/Pages/News/ESAs-publish-Joint-Advice-on-Information-and-Communication-Technology-risk-management-and-cybersecurity-.aspx

2. DATA AND SAMPLE

The data used in this report is based on the responses from 41 large (re)insurance groups across 12 European countries to a EIOPA questionnaire on cyber risk.[2] The questionnaire contained both qualitative and quantitative questions and was split in two main parts: the first part collected information on the vulnerabilities of the insurance groups to cyber risks as part of their own operational risk profile. Therefore, it was filled in by all groups in the sample. The second part was aimed at assessing cyber risk as part of underwriting risk and this part was only filled in by the participating insurance groups that provide cyber insurance.

The sample under consideration is very similar to the one from the EIOPA Insurance Stress Test 2018, representing a market coverage of around 75% of total consolidated assets.[3] The only difference is the non-participation of 1 group included in the sample for the Stress Test 2018 exercise.[4] Due to the cross-border activities of the participating groups, this exercise focuses on group-level information. Therefore, no country results are provided in the report.

Figure 1 – Type of cyber insurance offered



A total of 20 insurance groups included in the sample offer some type of affirmative cyber insurance, which accounts for 49% of the sample. The majority (12 groups, 29% of the sample) offers both standalone and cyber endorsements. Six groups (15% of the sample) offer only standalone cyber coverage while only two (5% of the sample) offer cyber endorsements alone (see Figure 1).

Therefore, while the majority of the statistics and conclusions provided in the report is based on the responses of the full sample of 41 groups, the part dedicated to cyber insurance underwriting (Chapter 4) is restricted to the 20 groups that provide cyber insurance.

Extensive verifications have been performed on the data submitted to provide sufficient data quality assurance. This included both a national validation by the relevant group supervisors and a central validation by EIOPA. When necessary, insurers were required to resubmit their responses to the questionnaire and/or provide clarifications. In some cases, the data was not available for some insurers, which is indicated in the report by adding this information in footnotes.

2 The participating countries are: Austria, Belgium, Denmark, Finland, France, Germany, Italy, Netherlands, Norway, Spain, Sweden and United Kingdom.

3 The Stress Test 2018 sample was selected among the biggest (re) insurance groups supervised in the European Economic Area (EEA) to represent the European insurance sector. The groups participating in this ST exercise were selected by EIOPA in coordination with the NCAs based on their size, EU-wide market coverage, business lines (life and non-life business) and the involvement of a sufficient number of local jurisdictions. The local market coverage was also taken into account in a second stage.

4 The list of the participants is provided in the appendix. COVEA did not provide the answers to the questionnaire.

3. CYBER RISK AS AN ELEMENT OF THE GROUP'S OWN OPERATIONAL RISK PROFILE

Cyber risk has been gaining increasing relevance as one of the main sources of operational risk faced by organisations, being considered the top risk in many countries.[5] The increasing frequency and sophistication of cyber attacks and the digital transformation make insurers increasingly susceptible to cyber threats, as more and more insurance groups are embracing new technologies and make use of big data.

Insurance groups are a natural target for cyber attacks as well, as they possess substantial amounts of confidential policyholder information. In contrast to other sectors, which hold mainly sensitive financial data, insurers typically also collect a large amount of protected personal sensitive information. Once obtained, this information could be used for different criminal purposes, such as financial gains through identity theft. Besides the direct financial consequences, cyber incidents could also result in severe and mainly long-lasting issues for the insurance groups involved. The reputational damage might be substantial or even irreversible, while malicious cyber incidents may also cause business interruptions, which could affect all policyholders.

This chapter aims at assessing the vulnerabilities of the insurance sector to cyber risk as part of their own operational risk profile. The first section provides an overview regarding cyber risk definitions used, followed by a more detailed overview of types of cyber risk management.

3.1 DEFINING AND UNDERSTANDING CYBER RISKS

Cyber risk is a broadly used term with several definitions. In order to enhance a common understanding of the concept of cyber risk, participating insurance groups were asked to provide their own internal definition of cyber risk, whereby the definition from the Financial Stability Board (FSB) Cyber Lexicon was provided as a reference.[6]

Based on the responses, half of the participating groups seems to be aligned with the FSB definition of cyber risk to some extent. While some groups use an identical definition, others use similar ones with additional specificities, resulting in a narrower definition. Many groups declared that they use the IAIS definition.[7]

However, some definitions were substantially different from the FSB Cyber Lexicon. In some cases, the definition of cyber risk was very close to the FSB definition of a cyber incident[8], where groups define cyber risks as an ex-post event which implies harmful outcomes. One group defined cyber risks as the risk of non-compliance with regulatory and legal requirements due to inadequate cyber protection. Finally, a few groups do not have a specific definition for cyber risks at all, although they declared to be working on establishing a clear definition. In these cases, cyber risk is typically a part of Information Security Risk.

5 See the results of the qualitative risk assessment based on the bottom-up survey among national competent authorities published in Chapter 5 of the EIOPA Financial Stability Report available at: https://eiopa.europa.eu/financial-stability-crisis-prevention/financial-stability/financial-stability-reports. Furthermore, see e.g. Allianz Risk Barometer-Top Business Risks for 2018. Available at: https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2018.pdf

6 See question 1.1. of the questionnaire. The FSB Lexicon defines cyber risk as "the combination of the probability of cyber incidents occurring and their impact". The FSB Lexicon is available at the following link: https://www.fsb.org/2018/11/cyber-lexicon/

7 According to IAIS, the definition of cyber risks is "Any risks that emanate 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 – be it related to individuals, groups, or governments." See IAIS (2018) Draft Application Paper on Supervision of Insurer Cybersecurity. Available at: https://www.iaisweb.org/file/75304/draft-application-paper-on-supervision-of-insurer-cybersecurity

8 See definition in box 1, Section 3.3.

Overall, it seems that the insurance sector is not fully aligned yet when it comes to conceptually defining cyber risks. Having a clear, comprehensive and common set of definitions on cyber risks would enable a more structured and focused dialogue between the industry, supervisors and policymakers, which could facilitate the development of sound solutions to cybersecurity challenges.

3.2 ASSESSING CYBER RISKS

Overall, the responses indicate that insurance groups are aware of cyber threats. With the exception of one group that does not make specific quantitative assessments of cyber risk, all other groups provided their own assessment of cyber threats. According to the data, 28% of the participating groups evaluate their current own risk as a target of cyber threats as high, 63% as medium and 10% as low (Figure 2). Furthermore, all groups established self-assessment processes to identify cyber risk (Figure 3).

Self-assessments can be in the form of qualitative risk assessments based on expert judgements using internal data and, to a lesser extent, on quantitative models. Typically, a broad range of potential cyber events are considered in order to assess, manage and control cyber risks. However, the complexity and the number of selected events vary through groups. While some insurance groups provided a detailed list of the cyber events considered to assess cyber risks, others focus on the most common types of events such as malware, website defacements, data breaching or denial of service. Past cyber events are also used as an input to track the progress of the resilience of the security system. In some cases, Basel II operational risk event types[9] are used to categorize cyber risks.

Most of the groups also try to identify cyber risks by collecting data on cyber events. Some groups have been collecting data for more than 10 years, while others have implemented this practice quite recently in the last 3 or 4 years, or are still in the consolidation phase. The data collection is often used as input for regular analysis and in some cases the most relevant information is reported to Senior Management and Board levels. Another common type of process used to assess cyber risks is third parties assessments. These practices may involve internal and external security audits including assurance exercises. Other processes consist of gap and scenario analysis, inputs from the government and the industry and use of consultants and external experts for a cyber defence review and other types of services to find weakness in their processes and systems.

Figure 2 - Own assessment of cyber threats

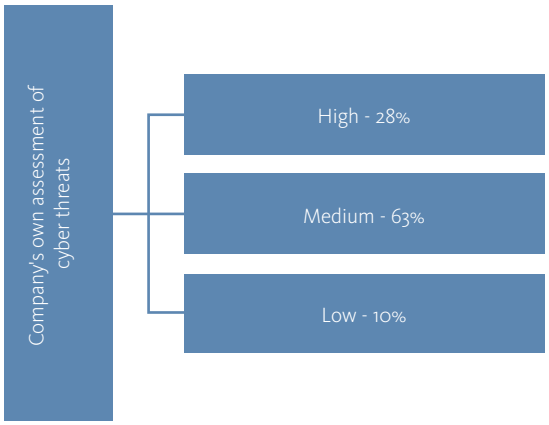
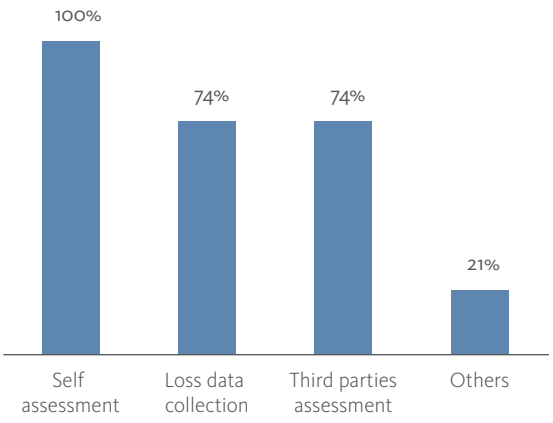


Figure 3 – Identification of cyber risks



Note: Responses based on a sample of 40 groups.

9 The seven categories of Basel II event types are: 1) internal fraud, 2) external fraud, 3) employment, 4) practices and workplace safety, 5) clients, products, and business practices, 6) damage to physical assets, business disruptions and system failures and 7) execution, delivery, and process management.

3.3 VULNERABILITIES TOWARDS CYBER EVENTS AND CYBER INCIDENTS

In order to make a harmonised, solid and consistent analysis on vulnerabilities of the participating insurers, the questionnaire required the participating insurance groups to use the correspondent definitions from the FSB Cyber Lexicon whenever a question referred to cyber events and cyber incidents (Box 1).

BOX 1: CYBER EVENTS AND CYBER INCIDENTS

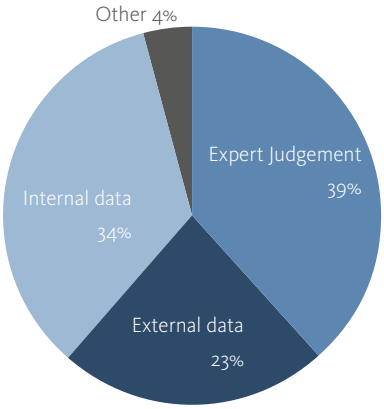
According to the FSB Cyber Lexicon, a **cyber event** is defined as: "*Any observable occurrence in an information system. Cyber events sometimes provide indication that a cyber incident is occurring.*"

A **cyber incident** is defined as a cyber event that: *"(i) jeopardizes the cyber security of an information system or the information the system processes, stores or transmits; or (ii) violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not."*

Based on these definitions, most of the groups in the sample keep track of both cyber incidents and cyber events, while some register only cyber incidents.[10] The risk analysis for cyber incidents is typically made based on a combination of expert judgement and inputs of internal and external data (Figure 4). Risk analyses might also be ultimately audited in some cases.

In contrast to tracking systems that capture and register an unlimited and broad range of cyber events, some systems identify a narrower spectrum of types of cyber events and only report them up to a limited number. Therefore, while approximately half of the groups reported the occurrence of cyber events between 0 to 100 in 2018, the remaining groups' estimates ranged between thousands and more than billions (Figure 5). The dispersion is more contained in the case of cyber incidents, as the range varies from 0 to 60567 in 2018 (Figure 6). Although the reported incidents affected groups in different levels and severities, they still count as harmful cyber incidents.

Figure 4- Means of conducting risk analysis for cyber incidents



On average, 10% of the cyber events become a cyber-incident, but this rate widely varies across groups. Some groups seem to have more resilient cyber security systems which constraint cyber incidents to close or equal to 0, while others have a higher rate of successful cyber attacks of around 50%. The reported average time between the occurrence of a cyber incident and its recognition by the group is less than 3 days, which can be considered as relatively short.

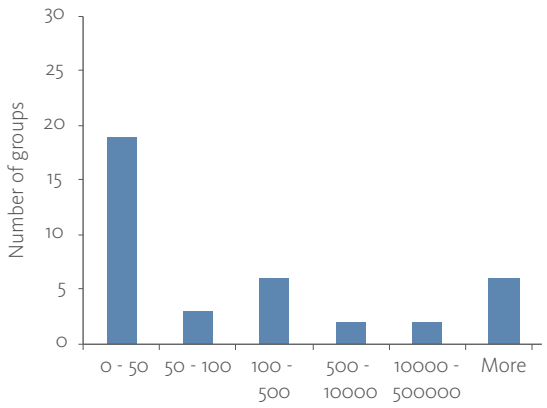
The dynamic and spreading nature of cyber events is also reflected in the growth rates of cyber events and cyber incidents in 2018 compared to 2017: an increase of respectively 300% and 43% was reported.

3.4 TYPES OF CYBER INCIDENTS

This section is dedicated to identifying which type of cyber incidents are more frequent and more costly for insurers. Furthermore, it also aims at revealing which type of damages insurers are more exposed to after having suffered a cyber incident. It should be noted, however, that the dynamic nature of cyber threats implies a quick occurrence of different types of cyber incidents, requiring continuous attention to cyber resilience to protect against new threats, also beyond the ones discussed here.

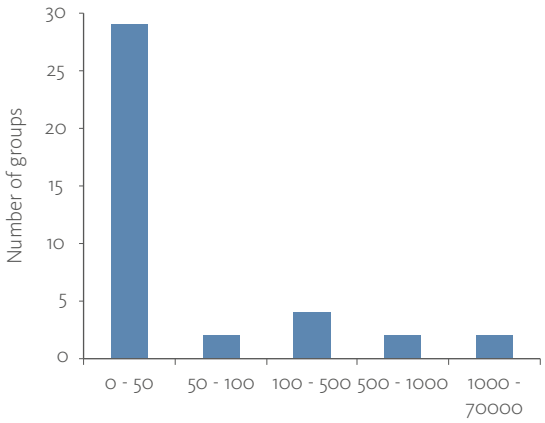
10 It should be noted that despite all efforts in the definitions provided, the results for some statistics on cyber events and cyber incidents are characterised by a high dispersion. That is given mainly by the different cybersecurity software and platform systems employed by the groups. The process of collecting this type of data is typically executed by a software that aggregates data generated throughout the organization's technology infrastructure, which enables the identification, categorization and analysis of incidents and events.

Figure 5- Distribution of cyber events



Note: Numbers reported for 2018.

Figure 6 – Distribution of cyber incidents



Note: Numbers reported for 2018.

Based on the responses, the most frequent types of cyber incidents against insurers are phishing mails, malware infections (ransomware), data exfiltrations and Distributed Denial of Service (DDoS). Business email compromise/CEO fraud was also mentioned but to a lesser extent. Typically, these cyber attacks aimed a financial gain, disruption or espionage. Figure 7 shows the three cyber incidents considered the most important in terms of frequency, costs, and effects. Malware infection, in particular ransomware, is considered the most costly cyber incident, although it was only reported as the second most frequent cyber incident.

Indeed, as financial gains is in the nature of ransomware incidents, it is not surprising that it can cause relatively higher financial losses than phishing mails. Data exfiltration and DDoS are listed together as the third most frequent cyber incident, but the latter was reported as more costly than the former. Other types of cyber incidents mentioned includes identity theft, steal of hardware, misuse of resources, failures of counterparties or suppliers, SQL injection, cryptojacking and cyber risk incidents within supply chain.

Furthermore, some insurers did not specify the type of malware infection according to the list provided, reporting general malware infection as a top costly and frequent incident instead. A non-exhaustive list of the different type of cyber incidents can be found in box 2.

Finally, the most frequent effect faced by insurers as a consequence of cyber incidents is business interruption, which is aligned with the expected consequences of the most frequent cyber incidents. Often, business interruption carries a high risk of severe revenue losses and of reputational damage. The second most frequent consequence of a cyber incident related to material costs for policyholders and third parties, which is directly linked mainly with phishing mail, malware infections (ransomware), data exfiltration and denial of service.

BOX 2: TYPES OF CYBER INCIDENTS

Having an overview of the most common cyber threats targeting the insurance sector is relevant to help insurers to identify actions and preventive measures in order to coordinate efforts to minimise, monitor and control the impact of those risks. EIOPA asked the groups to order in terms of frequency and costs the top cyber incidents within the list below:[11]

Data exfiltration: the loss of confidential data from companies to unauthorised people that breach the privacy of their customers, employees, clients, or counterparties.

Business Email Compromise/CEO fraud: In these attacks, a cyber criminal pretends to be a CEO or other senior executive from your organization. The criminals send an email to staff members like yourself that try to trick you into doing something you should not do.

Malware infection - Ransomware: A type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

Malware infection - Cryptojacking: Cryptojacking is defined as the secret use of an organization's computing device to mine cryptocurrency.

Distributed Denial of Service (DDoS): DDoS is a type of attack where multiple compromised systems, which are often infected with a Trojan, are used to target a single system causing a Denial of Service (DoS) attack.

SQL injection attack: SQL injection is a code injection technique, used to attack data-driven applications, in which SQL statements are inserted into an entry field for execution (e.g. to dump the critical database contents to the attacker).

Zero-day exploit: A zero day exploit is a cyber attack that occurs on the same day a weakness is discovered in software. At that point, it's exploited before a fix becomes available from its creator.

Financial transaction theft: unauthorised transfer of funds through trusted transaction networks to syphon money away and not be recoverable.

Failures of counterparties or suppliers: failures of third-party systems that companies rely on for their information technology services, such as software product providers, online service providers, cloud service providers, and others.

Phishing mail: this attack will typically direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has.

11 EIOPA provided the list and the respective definitions in the questionnaire. See questions 2.8 and 2.9, as well as the sheet "Information" of the template.

Figure 7- Top 3 types of cyber incidents by frequency, cost and effects

By frequency	By cost	By effect
• Phishing mail • Malware infection - Ramsonware • Data Exfiltration/DDoS (Denial of Service)	• Malware infection - Ramsonware • Phishing mail • DDoS (Denial of Service)	• Business interruption • Material costs for policyholders and third parties • Data destruction/ confidentiality breach

3.5 MANAGING CYBER RISKS

Managing cyber risks involves several processes including the identification, analysis and measurement of potential effects in the context of cyber incidents. Furthermore, implementing well-established preventive measures and action plans for potential cyber incidents is crucial to build a more resilient system. The participating insurance groups seem to be aware of the importance of these aspects. The results show that 100% of the groups include cyber risk in their Operational Risk Management (ORM), either implicitly (37%) or explicitly (63%) (Figure 8) and 80% of the groups include cyber risk in their Own Risk and Solvency Assessment (ORSA) (Figure 9).[12]

When analysing cyber incidents, 52% of the groups conduct stress tests, 23% worst case scenario analyses and 11% multiple scenario analysis (Figure 10). The remaining 14% prefer to perform other kind of risk assessments,

Figure 8- Cyber risks in ORM

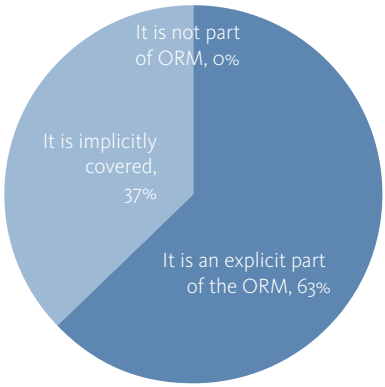
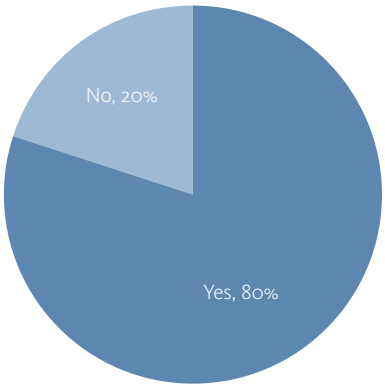


Figure 9- Cyber risks in ORSA



12 Article 45 of the Solvency II Directive requires every (re)insurance undertaking in Europe to conduct its Own Risk Solvency Assessment (ORSA), which is an internal process aiming at assessing the adequacy of its risk management and current and prospective solvency positions under normal and severe stress scenarios.

Figure 10 - Types of analysis conducted

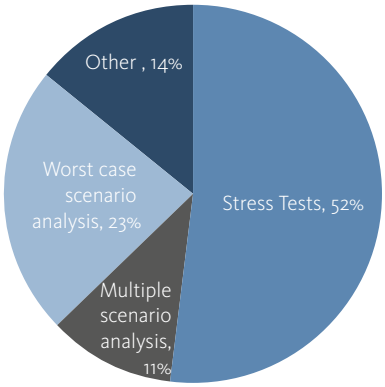
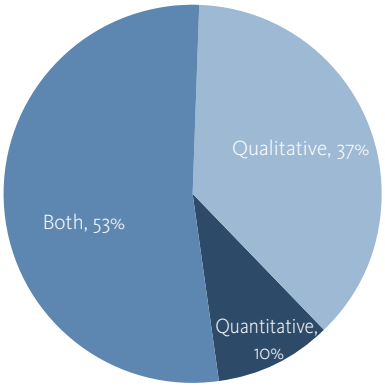


Figure 11- Nature of the analysis



such as heatmap, purple, red and blue teaming,[13] disaster recovery test, penetration testing, crisis tests and several types of simulations. The majority of the groups perform these analyses by combining quantitative and qualitative tools (Figure 11). However, when isolated, qualitative types of analysis are more common (37%) than quantitative ones (10%).

These analyses typically assess aspects related to the cybersecurity maturity of the insurance company, in order to verify the resilience capabilities of the cybersecurity system when faced by severe cyber events. Furthermore, these analyses also aim at evaluating the probability of different type of incidents, risk drivers and control adequacy.

Quantitative analysis typically includes estimations of costs related to crisis management, legal expenses, total operational and financial loss, as well as remediation and disaster recovery costs considering several types of cyber incidents. In some cases, the reputational impact is also considered. Some examples of tested scenarios are the assumption of complete IT system failure for a specific period or certain assumptions of lapses, business and data losses. In addition, 68% of the insurers have insurance covering their own cyber risk (38% have one insurer and 29% have more than one). The quantitative impact of cyber incidents on the balance sheets varies from EUR 0,2 to 430 million, which represents respectively 0.002% and 10% of the own funds of the correspondent groups that provided these estimates (see box 3).

The obtained results indicate a generalized engagement of the industry to increase the resilience against cyber incidents. However, evidence shows that less than one-in-five CEOs of insurance groups believes that their organisation is fully prepared for a cyber-event.[14] Therefore, further actions to strengthen the resilience of the insurance sector against cyber vulnerabilities are essential, in particular considering the dynamic nature of cyber threats. Clear, comprehensive and harmonized requirements on governance of cybersecurity as part of operational resilience would help ensure the safe provision of insurance services. To this aim, EIOPA plans to develop Guidelines further defining supervisors' expectations on cybersecurity as part of the governance and risk management framework during 2019.[15] Furthermore, streamlining of the cyber incident reporting frameworks across the insurance and financial sector could help to avoid inconsistencies in the reported information and ultimately enhance cyber resilience.

13 Red teaming is the practice of challenging plans, policies, systems and assumptions by adopting an adversarial approach. It can be performed by externals or internal staff. Blue team is a group of experts aiming at defending against both real attacks and simulations performed by the red teams, identifying security vulnerabilities and verifying the effectiveness of security measures. Finally, the purple teams are groups with the objective to ensure and maximize the effectiveness of the red and blue teams. Three groups reported to make use of this type of practice.

14 Estimation from a sample of 100 CEOs of insurance groups. See KPMG (2017) Facing the cyber threat in the insurance sector. Available at: https://assets.kpmg/content/dam/kpmg/au/pdf/2017/facing-the-cyber-threat.pdf

15 See the ESA Joint Advice ICT risk management requirements for more details: https://eiopa.europa.eu/Pages/News/ESAs-publish-Joint-Advice-on-Information-and-Communication-Technology-risk-management-and-cybersecurity-.aspx

BOX 3: QUANTITATIVE IMPACTS OF CYBER INCIDENTS

Assessing the overall quantitative impact of cyber incidents is difficult due to their complex nature and the assumptions considered in the calculations. For example, the impact on the balance sheet considering only ransomware attack in all workstations might reach EUR 16 million, while the impact can be around EUR 38 million when including both violation of IT system and breach of an outsource provider information system. One group attributed EUR 0,2 million losses in the balance sheet for a typical IT outage while the worst case hacker attack would represent losses of EUR 25 million (corresponding to respectively 0.002% and 0.22% of the own funds), another group reported estimated losses of approximately 0.12% of the balance sheet and 2.31% of the SCR when considering violation of IT system with loss of confidentiality of customers' personal data estimated losses.

In some cases, ranges were provided instead of an unique number. For example, data leakage and information system stoppage might have an impact on the balance sheet ranging approximately between EUR 100 million to EUR 450 million, which represents from 2% to 10% of the group's own funds. A minority of groups reported that the quantitative impact of cyber incidents in the balance sheets might not be material.

Estimative of impacts on SCR were even more challenging to be provided. Some groups reported that the SCR for operational risks is calculated based on the Solvency II Standard Formula and did not provide numbers. While some groups reported estimations of losses of approximately EUR 26 million in the SCR, others reported numbers such as EUR 190 million (representing 18% of the operational risk).

Several initiatives at the European level aiming at addressing cyber threats might also incentivize further measures to increase the resilience against cyber threats in the insurance sector. Among crisis management mechanisms applied to the digital context, proposals to establish institutional reforms to make products, services and processes safer and more harmonised across Europe in the cyber context have been developed. The implementation of the Directive on security of network and information systems (NIS Directive)[16] and General Data Protection Regulation (GDPR)[17] are one of the key initiatives in this regard.[18]

16 The NIS Directive requires companies in critical sectors (energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure) to adopt risk management practices and report major incidents to the National Authorities.

17 GDPR is a regulation that intends to strengthen and unify data protection for individuals within the European Union (EU). 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

18 For a more detailed review of the regulatory initiatives related to cyber risks and technological developments and how they might impact the insurance sector, please see the Box 1 on Chapter 1 (Key Developments) of the EIOPA Financial Stability Report published in December 2017. Available at: https://eiopa.europa.eu/Pages/Financial-stability-and-crisis-prevention/EIOPA-Financial-Stability-Report---December-2017-.aspx

4. CYBER RISK AS PART OF UNDERWRITING RISK

This chapter provides a broad overview of the main aspects of the European cyber insurance underwriting market from both quantitative and qualitative perspectives. It is divided into two sections. The first section is dedicated to affirmative cyber exposures, mapping the main coverage reported in the responses and providing information about the European cyber insurance market. The second part focuses on non-affirmative cyber exposures, especially on how insurers assess and deal with non-affirmative cyber risks.

4.1 AFFIRMATIVE EXPOSURES

In general, affirmative cyber insurance can be offered as standalone products specifically designed to cover cyber perils or as add-on coverage to traditional lines of business, known as cyber endorsements. It can include coverage for both first party and third party liabilities.

As described in Chapter 2, a total of 20 insurance groups included in the sample offer some type of affirmative cyber insurance, which accounts for 51% of the sample. The majority (12 groups) offer both standalone and cyber endorsements. Six groups offer only standalone cyber coverage while only two offer cyber endorsements alone (see Figure 1 in Chapter 3).

The majority of groups provide a relatively broad range of cyber insurance coverage. The most common coverages offered are data restoration and cyber theft (Table 1). Cyber extortion, administrative investigation and penalties, network interruption, first responses and extra expenses are examples of less commonly provided coverages.The cyber insurance market is growing rapidly in Europe and increased on average by 71% in 2018 in terms of gross written premium for the groups in the sample. Total gross written premiums account approximately for EUR 295 million in 2018, compared to EUR 172 million in 2017. This is aligned with previous estimates for the European cyber insurance market[19] and represents approximately 0.02% of the total gross written premiums in 2017 of the participating groups in the exercise. Most premiums are written for standalone products, which are approximately 5 times larger than for cyber endorsements.[20]

The upward trend in cyber insurance is not only due to the generalized increase of written contracts offered by each group, which has grown by 36% in 2018 in comparison with 2017, but also due to the fact that the number of insurers providing cyber insurance increases every year. The increasing frequency of cyber attacks, changing and stricter regulation regarding cybersecurity as well as continued technological developments are all expected to increase demand for cyber insurance in the near future. Furthermore, investments by businesses in their own cyber security may also lead to more demand for cyber insurance, as potential clients become more aware of the cyber risks involved, while a certain level of cyber maturity would facilitate the process of obtaining residual cyber insurance coverage (as it reduces potential moral hazard and information asymmetries between the insurer and the client).

19 The GWP refer to risks underwritten in Europe. The previous estimates were between USD 150 million and 400 million in gross written premiums - see e.g. OECD (2017), Thomas and Finkle (2014); Marsh (2016) and Wong (2017). 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.

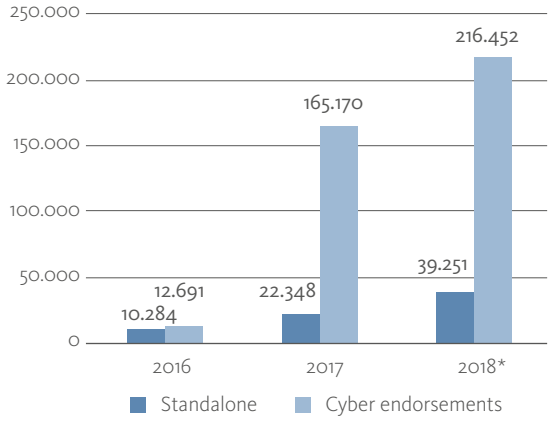
20 The difference might be slightly lower than the current numbers, as one group with an expressive participation in this market did not have the numbers available for 2018 yet. Therefore, the current value for 2018 is estimated using the underlying assumption that the Gross Written Premium for this specific company remains the same as for 2017.

Table 1 - Coverage reported by the participating groups

Coverages	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	Total	Share
Data restoration	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		19	95%
Cyber theft	X	X	X	X	X	X	X	X	X	X	X	X		X	X	X	X		X	X	18	90%
Third party loss	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				X		17	85%
System clean-up costs	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X		X			17	85%
Electronic Data Incident	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X					16	80%
Cyber Extortion	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X					16	80%
Administrative investigation and penalties	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X						15	75%
Network Interruption	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X					15	75%
First responses	X	X	X	X	X	X	X	X	X	X	X	X	X		X			X			15	75%
Extra expenses	X	X	X	X	X	X	X	X	X	X	X		X	X			X			X	14	70%
Others	X	X	X	X	X	X		X							X		X	X			11	55%

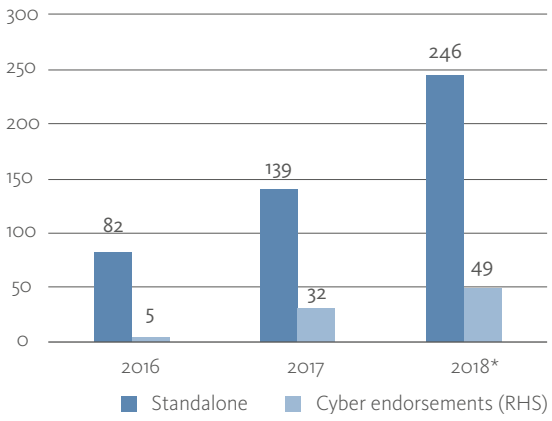
Note: Each column represents one participating group. The last two columns refer to the total number of groups and its relative share offering the coverage described in the first column.

Figure 12 – Number of written contracts



Note: The number of written contracts for cyber endorsements for 2018 is an estimate as one group with an expressive participation in this market did not have the numbers available for 2018 yet. The underlying assumption is that the Gross Written Premium for this specific group remains unchanged in 2018.

Figure 13 – Gross Written Premium (in millions of euros)



Note: Gross written premiums for cyber endorsements for 2018 is an estimate as one group with an expressive participation in this market did not have the numbers available for 2018 yet. The underlying assumption is that the Gross Written Premium for this specific group in 2018 remains the same as for 2017.

Based on the responses, the number of written contracts of standalone and cyber endorsements were approximately the same level in 2016 (Figure 12). However, written contracts for cyber endorsements increased by more than 10 times in 2017, while standalone contracts approximately doubled. Nevertheless, gross written premiums from standalone products are substantially higher than from cyber endorsements (Figure 13).

This difference may be explained by the complementary nature of cyber endorsements, which requires relatively less technical expertise in cyber risks than offering a standalone product, as adapting existing products is faster and simpler than creating a specialized cyber product. The cyber endorsement in traditional policies typically only relates to a small part of the total premiums as well. This might also reflect the fact that currently only few specialized underwriters operate in the market, which is currently considered one of the main challenges of the cyber insurance industry.[21] The standalone products of these specialized players are typically tailored to specific large clients and contain a larger breadth of coverage than endorsements. These products currently still dominate the market in terms of written premiums. Further work therefore seems needed to enhance the standardisation and transparency of cyber coverage to facilitate the use of cyber insurance by SMEs. This could also help improve the comparability of cyber insurance and foster further development of the European cyber insurance market.

Furthermore, the data indicates heterogeneity on how cyber insurance policies are sold. The most common way of selling policies are through a combination of tied agents, brokers and direct sells. The proportion of each channel in sales varies from group to group. However, the data shows that in general one of these channels account for more than 85% in purchasing new contracts.[22] Interestingly, no group has mentioned to use the internet as intermediation channel in the questionnaire. This could reflect the relatively complicated and non-standardized nature of cyber products, requiring more hands-on distributions channels.

An interesting aspect of the outcome of the questionnaire is the relatively low rate of responses received for other quantitative questions such as claims received, technical provisions or combined ratio for affirmative cyber insurance.[23] This suggests that the cyber insurance market is still very much in development and insurers are still working on disentangling their cyber specific business, which are typically included within traditional lines of business. Having common and harmonized standards for both cyber risk measurement and reporting purposes could facilitate our understanding of cyber risk underwriting. EIOPA is therefore currently also working on harmonized reporting on cyber insurance coverage in the context of the Solvency II Reporting Review, while a European-wide cyber incident reporting database, based on a common taxon-

21 See EIOPA (2018), Understanding Cyber Insurance – A Structured Dialogue with Insurance Companies

22 Measure estimated as a percentage of total gross written premium in terms of new contracts.

23 See question 3.1 of the questionnaire for more details about the information requested.

omy, could be considered to further support the development of the European cyber insurance market as well.

4.2 NON-AFFIRMATIVE EXPOSURES

Non-affirmative cyber risk refers to instances where cyber exposure is neither explicitly included nor excluded within an insurance policy. The latter type of cyber risk is also referred to as "silent" cyber risk.[24] Two main implications can result from non-affirmative cyber exposures: first, some insurers may pay claims for unforeseen cyber losses when they have not charged a premium for this risk in certain circumstances, and second, depending on the cyber incident, it can trigger accumulation of losses within other policies.

Unlike standard standalone cyber insurance policies or cyber endorsements, which clearly specify insurance cover concerning cyber risks, most of the traditional insurance policies have been designed without taking cyber exposures into consideration. The absence of cyber exclusion practices is reflected in the results of this report: only five insurance groups[25] claimed that cyber risks are explicitly excluded from the property and casualty policies offered.

Several reasons were attributed to explain the non-exclusions. Some groups consider that cyber exclusions from traditional policies might not be practical given the difficulty in linking certain coverages with potential cyber incidents, such as medical expenses, personal injury, or property and casualty insurance targeting household customers. Other groups do not even consider cyber exposure a relevant threat to their business in the present nor in the near future.

While it is indeed more straightforward to relate cyber risks with other lines of business (for instance traditional property, liability and/or casualty), as technology develops and the access to digital services increases, rethinking policies in the light of cyber events is becoming more and more necessary. Internet of Things (IoT)[26] is an example of how technology can increase the exposure of households towards cyber risks (see Box 4).

BOX 4: INTERNET OF THINGS (IOT)

The idea behind IoT is to connect everyday objects through internet devices which enables the user to have a remote control over different electronic equipment. While IoT can potentially increase prevention loss by for example detecting certain risks earlier (e.g. signs of fire), the big amount of data and its interconnectedness builds a powerful ecosystem that might become attractive to hackers interested in having access to sensitive and confidential data information.

Furthermore, cyber attacks might also materialize as physical damage, caused for example by devices programmed remotely (intentionally or not) to damage machines and devices. This logic can be extended to infrastructure, life and means of transport.

In some cases, the inaction in terms of exclusions was justified by a limited experience with non-affirmative cyber exposures, which so far demands no changes in how contracts are stipulated according to some groups. This indicates that some groups might consider more concrete actions to be taken only *ex-post*, i.e. once enough cases are registered and demand for a change. This approach in dealing with cyber exclusions can be problematic in particular if this type of losses would be triggered by a severe event with potential to affect several claims simultaneously.

Other limiting factors in the implementation of cyber risk exclusions are widely related to market dynamics. Some insurance groups mentioned that cyber is a relatively new risk and wording exclusion is not part of the current market practices, which could indicate that the current way of designing products is outdated. However, it was also mentioned that the "Institute Cyber Attack Exclusion

24 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. Another example can be a malware event that embeds into a computer system that impacts multiple sites that a firm operates from where a manufacturing process is interrupted, causing business interruption and a fire causing physical damage to property – triggering multiple types of commercial insurance policies at the same time.

25 In total, twenty-six groups provided an answer to this question.

26 The Internet of Things (IoT) has been defined as a global infrastructure [...], enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies. See http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx

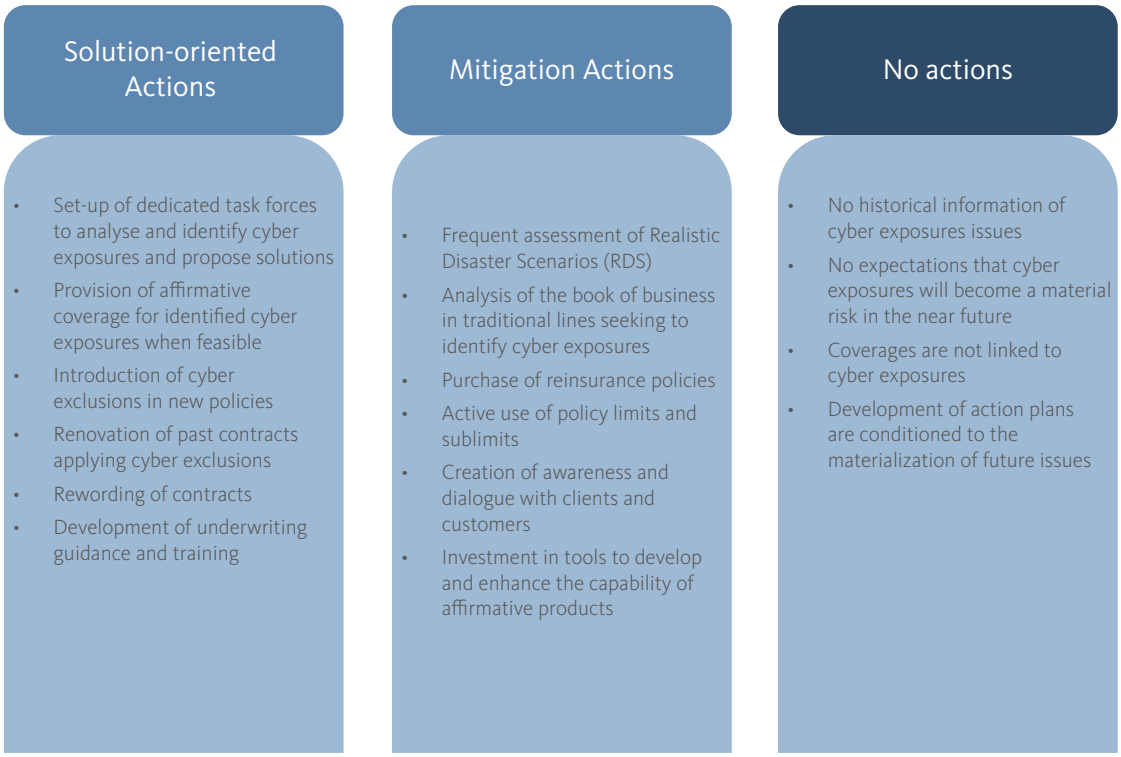
Clause" (CL 380)[27], which is mainly used in marine insurance, is sometimes incorporated into some contracts to exclude cyber risk.

Furthermore, competition and how the insurance group is positioned in the market also seem to play a role in cyber exclusions. One group mentioned it aims to offer the best coverage as possible in the market, so no exclusions are considered. Likewise, in contrast to "leading groups", if the group is a "following" (re)insurer, there are clear limitations in influencing the final wordings in contracts, given the small share of their market participation.

4.2.1 INITIATIVES TO ADDRESS AND MITIGATE NON-AFFIRMATIVE RISKS

Despite the obstacles and reasons mentioned in the previous section preventing explicit exclusions of cyber risks in traditional contracts, there are efforts from the industry to address challenges related to non-affirmative cyber exposures. However, still 41% of groups[28] replied that there is no action plan in place to review the portfolio in the context of cyber exposures and, if necessary, rewording the contracts. Figure 14 provides an overview of the initiatives reported to address and mitigate non-affirmative risks, as well as the reasons behind the inaction of some groups in developing action plans (third column).

Figure 14 – Initiatives to address and mitigate non-affirmative risks and the reason behind no actions



27 The Institute Cyber Attack Exclusion Clause (CL. 380) 10/11/2003 was set forth by the guidelines of the International Maritime Organization Institute. The first paragraph of Cl 380 states: "(...) in no case shall this insurance cover loss damage liability or expense directly or indirectly caused by or contributed to or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system."

28 Calculation considering a sample of 27 groups that provided an answer for the question 3.2.1.b: Is there any action plan in place to review the portfolio and if necessary rewording the contracts?

Solution-oriented actions encompass concrete changes in contracts, such as rewording and exclusions[29], as well as the set up of internal task forces, sometimes with help of external consultants, to enhance the expertise of the group in cyber exposures and propose solutions.

Mitigation actions also involve investments in technical expertise, but measures such as policy limits and purchase of reinsurance are more extensively used. Indeed, reinsurance plays an important role in the cyber insurance market. Most of the groups reported that cyber coverage is reinsured by one or more reinsurer. Furthermore, cyber coverage is preferably reinsured on a proportional basis with annual aggregate limitations. Quota share treaty was mentioned as the most common type of contract, followed by proportional facultative reinsurance.[30]

Despite indications from the industry of efforts to reduce the uncertainty related to cyber risk in the portfolio, the fact that many groups are conditioning mitigating actions to the materialization of future events is problematic, as non-affirmative risk is identified as a key concern regarding the proper estimation of accumulation of risks.[31] In other words, waiting to take actions until some event becomes concrete may be too late, as the occurrence of a single event generating a widespread impact on several policyholders at once could expose insurance groups to high financial losses. Box 5 provides some examples of the loss scenarios that could have an important impact for cyber risk policies, based on the responses of the participating groups.

Furthermore, the very low number of responses received for questions with a quantitative approach towards non-affirmative risks indicate that participating groups' quantitative assessments of non-affirmative risk are not yet fully developed. While it is important to take into consideration that some other relevant cyber insurers did not participate of the survey, it still the case that the large majority of groups that are active in the cyber market could not provide figures regarding the exposure cyber risk, such as part of the written premium related to cyber risk, claims received potentially related to cyber events or even total policy limit exposed to non-affirmative cyber risk.[32]

To summarize, while common initiatives in the market to address non-affirmative cyber risks are under way, further effort is needed to properly address the risks associated with silent cyber exposures. The lack of quantitative assessment of non-affirmative risks combined with a generalized absence of cyber exclusion practices and action plans suggest insurers are currently not fully aware of the potential exposures to cyber risk. Hence, it is essential to consider further actions to prevent non-affirmative risks and ultimately, cyber accumulation risk.

29 Typical exclusions are war, political risks, nuclear, cyber terrorist attacks, property and material damagers, among others. For a more detailed list of exclusions, please see EIOPA (2018) Understanding Cyber Insurance – A Structured Dialogue with Insurance Companies, Figure 9, page 18.

30 Proportional reinsurance is an agreement in which the reinsurer share a percentage of the losses.A quota share treaty is a pro rata contract in which the insurer and reinsurer share premiums and losses according to a fixed percentage. Facultative reinsurance is coverage purchased by a primary insurer to cover a single risk or several risks held in the primary insurer.

31 See EIOPA (2018), Understanding Cyber Insurance – A Structured Dialogue with Insurance Groups.

32 See question 3.2.3 of the questionnaire for more details about the information requested.

BOX 5. LOSS SCENARIOS FOR CYBER RISK POLICIES

Loss scenarios play an important role in keeping insurance groups attentive about how they would be affected should a cyber incident materialize. Scenarios can help to identify and assess risks and improve action plans to prepare for severe incidents.

Examples of scenarios for cyber risks that could trigger material losses mentioned in the survey are:

Data theft through cloud attack - commercial lines first party scenario: A security failure in one of the world top 4 cloud computing providers leading to confidential data leaks,data destruction and business interruption. This could trigger further insurance losses related to investigation, data restoration and notification costs. Some estimations provided showed that a cloud service provider failure of smaller scale might lead to losses of 1%-2% of cyber portfolio. Other scenarios involving data breach or data damage in banks and insurers are estimated to cause losses between EUR 3.5 million to EUR 30 million.

Generalized Denial of Service: Breakdown of a widely used software affecting a large number of clients. For example, a scenario involving Denial of Service on main DNS providers targeting money extortion by a botnet consisting of millions of malware infected internet-enabled devices in the context of Internet of Things (see Box 4) was estimated to cause gross losses of EUR 533 million.

Cyber attacks against infrastructure: A cyber incident causing a widespread power blackout in a metropolitan region could trigger significant insurance losses, with estimations of net losses ranging from approximately EUR 200 million to EUR 841 million, depending on the scope of the blackout.. Another potentially harmful scenario considered a cyber attack on a traffic light system in a tunnel generating severe accidents, which was estimated to cause netv losses of EUR 6 million.

5. CONCLUSIONS

Cyber security and cyber risk are at the forefront of the concerns of the financial sector, private companies and public authorities. Finding collective solutions to deal appropriately with cyber risk calls for an appropriate framework for cyber risk assessment, cyber resilience and cyber insurance coverage. Insurers play a key role in this: not only are insurers susceptible to cyber threats directly themselves, but they also offer coverage for cyber risk through their underwriting activities. This report has analysed cyber risk from both angles based on responses from 41 large (re)insurance groups across 12 European countries.

Cyber risk as an element of the insurer's own operational risk profile

The increasing frequency and sophistication of cyber attacks, the fast digital transformation and the increased use of big data and cloud computing make insurers increasingly susceptible to cyber threats. Insurance groups are a natural target for cyber attacks, as they possess substantial amounts of confidential policyholder information. This calls for a sound cyber resilience framework for insurers. Ultimately, harmonized general requirements on governance of cybersecurity as part of operational resilience would help ensure the safe provision of insurance services.

This report has analyzed the most common cyber threats faced by insurers and identified key challenges in collecting aggregated statistics related to cyber threats, which can be mainly attributed to different systems employed by insurance groups to capture and analyse cyber events and cyber incidents. As a result, a harmonized overview of cyber incidents across insurance groups is limited. Having a clear, comprehensive and common set of definitions and terminology on cyber risks would enable a more structured and focused dialogue between the industry, supervisors and policymakers, which could further enhance the cyber resilience of the insurance sector.

Furthermore, this report has found that the most common cyber incidents affecting insurers are phishing mail, malware infections (ransomware), data exfiltration and denial of service attacks. The main consequences suffered by insurers following these cyber incidents are business interruption and material costs for policyholders and third parties. Overall, the results indicate that the industry is aware of the potential cyber threats and has incorporated cyber risk explicitly in their risk management frameworks. However, further actions to strengthen the resilience of the insurance sector against cyber vulnerabilities are essential, in particular considering the dynamic nature of cyber threats. This would include streamlining of the cyber incident reporting frameworks across the insurance and financial sector, to avoid inconsistencies in the reported information and ultimately enhance operational resilience.

Cyber insurance market

A well-developed cyber insurance market can play a key role in enabling the transformation to the digital economy, by raising awareness of cyber risks, share knowledge on good cyber risk management practices and facilitate responses to and recovery from cyber attacks.

Although still small in size, the European cyber insurance industry is growing rapidly, with an increase of 72% in 2018 in terms of gross written premium for the insurers in the sample, amounting to 295 million in 2018 compared to EUR 172 million in 2017, which represents approximately 0.02% of the total gross written premiums of the participating groups. The majority of affirmative cyber insurance is written within standalone cyber products (EUR 246 mln), with the remainder being offered as cyber endorsement for traditional policies (EUR 49 mln). The increasing frequency and awareness of cyber attacks, changes in regulation as well as continued technological developments are all expected to increase demand for cyber insurance in the near future.

However, non-affirmative cyber exposures remain a source of concern for the European cyber insurance market. While common efforts to assess and address non-affirmative cyber risks are under way, the lack of quantitative approaches, explicit cyber exclusions and action plans to address non-affirmative cyber exposures

suggest insurers are currently not fully aware of the potential exposures to cyber risk. This report has found that some groups have adopted a 'wait-and-see' approach to address non-affirmative cyber risk, where the implementation of actions plans to address non-affirmative exposure depends on materialization of future events. This is partly being driven by standard market practices, market competition and a lack of data to assess cyber risk fully to price it into premiums. This approach in dealing with cyber risks can be particularly problematic, as insurers may suffer substantial unforeseen losses in traditional polices if a cyber incident materialize. Moreover, the lack of transparency in non-affirmative exposures also creates uncertainty for policyholders, as it is often not clear whether their cyber claims would be covered within their insurance polices. Further effort is therefore needed to properly tackle non-affirmative cyber exposures to address the issue of potential accumulation risk and provide clarity to policyholders.

Lastly, the low number of responses received for some questions with a quantitative approach towards both affirmative and non-affirmative risks indicate that insurers' quantitative assessments of cyber risk are not yet fully developed. Hence, it is essential for the industry to further improve its assessments and data collection, so that cyber risks can be adequately measured, monitored and managed. Ultimately, having common and harmonized standards for both cyber risk measurement and reporting purposes could greatly facilitate our understanding of cyber risk underwriting. To this end, creating a European-wide cyber incident reporting database, based on a common taxonomy, could be considered as well.

6. REFERENCES

Allianz (2018), *Risk Barometer 2018 -Top Business Risks for 2018*, available at: https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2018.pdf

EIOPA (2018), *Understanding Cyber Insurance – A Structured Dialogue with Insurance Companies*, available at: https://eiopa.europa.eu/Publications/Reports/EIOPA%20Understanding%20cyber%20insurance.pdf#search=understanding%20cyber%20insurance

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.

FSB (2018), *Cyber Lexicon*. Available at: https://www.fsb.org/2018/11/cyber-lexicon/

IAIS (2018), *Draft Application Paper on Supervision of Insurer Cybersecurity,* https://www.iaisweb.org/file/75304/draft-application-paper-on-supervision-of-insurer-cybersecurity

IAIS (2016), *Issues Paper On Cyber Risk to the Insurance Sector*. IAIS publication. Available at: https://www.iaisweb.org/page/supervisory-material/issues-papers

KPMG (2017), Facing the cyber threat in the insurance sector, https://assets.kpmg/content/dam/kpmg/au/pdf/2017/facing-the-cyber-threat.pdf

Marsh (2016). *Continental European Cyber Risk Survey: 2016 Report*, Marsh LLC, October

OECD (2017), *Enhancing the Role of Insurance in Cyber Risk Management*, OECD Publishing, Paris. Available at: 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, Available at: www.reuters.com/article/us-insurancecybersecurity-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.html

Z/Yen Group (2015), *Promoting UK Cyber Prosperity: Public-Private Cyber- Catastrophe Reinsurance*, Long Finance.

7. APPENDIX

Group	Country
Vienna Insurance Group AG Wiener Versicherung Gruppe	Austria
Ageas	Belgium
KBC Insurance Group	Belgium
PFA_PENSION	Denmark
Forsikringsselskabet Danica, skadeaktieforsikringsselskab	Denmark
Sampo plc	Finland
AXA	France
CNP Assurances	France
BNP Paribas Cardif	France
Crédit Agricole Assurances	France
GROUPAMA SA	France
GROUPE DES ASSURANCES DU CREDIT MUTUEL	France
Natixis Assurances	France
Sogecap	France
Münchener Rückversicherungs-Gesellschaft AG	Germany
Allianz SE	Germany
HUK-COBURG Versicherungsgruppe	Germany
HDI Haftpflichtverband der Deutschen Industrie VVaG	Germany
R+V Versicherung Aktiengesellschaft	Germany
Assicurazioni Generali S.p.A.	Italy
UNIPOL GRUPPO SPA	Italy
Poste Vita Group	Italy
Intesa Sanpaolo Vita S.p.A.	Italy
Aegon N.V.	Netherlands
NN Group N.V.	Netherlands
Achmea	Netherlands
Gjensidige Forsikring	Norway
Storebrand ASA	Norway
MAPFRE S.A.	Spain

Group	Country
VIDACAIXA S.A.U. DE SEGUROS Y REASEGUROS	Spain
Nordea Life Holding AB	Sweden
Livförsäkringsbolaget Skandia, ömsesidigt	Sweden
Aviva plc	United Kingdom
Legal & General Group Plc	United Kingdom
RSA Insurance Group plc	United Kingdom
Phoenix Group Holdings	United Kingdom
Prudential plc	United Kingdom
Standard Life Aberdeen plc	United Kingdom
The Royal London Mutual Insurance Society Limited	United Kingdom
Scottish Widows Group Limited	United Kingdom

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct Information Centres.

You can find the address of the centre nearest you at: http://europa.eu/contact

On the phone or by e-mail

Europe Direct is a service that answers your questions about the European Union.

You can contact this service

– by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

– at the following standard number: +32 22999696 or

– by electronic mail via: http://europa.eu/contact

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: http://europa.eu

EU Publications

You can download or order free and priced EU publications from EU Bookshop at: http://bookshop.europa.eu. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see http://europa.eu/contact)

EU law and related documents

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex at: http://eur-lex.europa.eu

Open data from the EU

The EU Open Data Portal (http://data.europa.eu/euodp/en/data) provides access to datasets from the EU. Data can be downloaded and reused for free, both for commercial and non-commercial purposes.

EI-03-19-498-EN-C

EUROPEAN INSURANCE AND OCCUPATIONAL PENSIONS AUTHORITY

Westhafenplatz 1,
60327 Frankfurt am Main, Germany

Publications Office
of the European Union