EUROPEAN UNION AGENCY
FOR CYBERSECURITY

DEMAND SIDE OF CYBER INSURANCE IN THE EU

Analysis of Challenges and Perspectives of OESs

FEBRUARY 2023

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

For contacting the authors please use team@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

Javier GOMEZ PRIETO, Athanasios DROUGKAS (ENISA),
Jelger GROENLAND, Alessandro LAZARI (Experts).

ACKNOWLEDGEMENTS

To all stakeholders who contributed to the elaboration of this report, including operators of essential services (OESs) who responded to the survey, interviewed experts and colleagues who provided feedback, especially colleagues of the European Insurance and Occupational Pensions Authority (EIOPA).

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN 978-92-9204-586-9, DOI: 10.2824/94949, Catalogue nr TP-04-22-095-EN-N

TABLE OF CONTENTS

TABLE OF FIGURES

EXECUTIVE SUMMARY

This report analyses current perspectives and challenges of Operator of Essential Services (OESs) related to the acquirement of cyber insurance services. Information and statistics are presented according to the selection, acquisition and use of cyber insurance as a mitigation tool in the context of their daily business' lifecycle. The collection of data and opinions were elaborated in relation to the category of OESs included in the network and information security (NIS) directive (Directive (EU) 2016/1148. Nonetheless, results and evidences would be also applicable to essential and important entities defined in the framework of the NIS2 Directive (EU) 2022/2555.

The report addresses exclusively the 'demand side' of cyber-insurance market, applicable to the particular case of OESs. The analysis and results have been conducted from a **methodological approach which integrates: desk-research, on-line survey, phone interviews, data analysis and recommendations for policymakers**. To the purpose, the analysis aims at addressing different segments of the cyber insurance contracting process, namely: risk management practices, cyber insurance coverage, claims processes and opinions from the respondents in key areas such as skills.

In terms of results, the analysis shows that a big proportion of operators of essential services consider cyber insurance less attractive due to increasing prices and decreasing coverage. This phenomenon is highly noted specially in small entities in a moment in which ransomware incidents are on the rise[1]. Data from both the survey and the semi-structured interviews support these findings. Other key findings of the analysis were:

- **third-party liabilities are the preferred additional coverage** that companies would like to have added in their cyber insurance coverage;
- **cyber-risk is being highly addressed on qualitative basis**. For a 77 % of operators of essential services there is a formalized process to identify cyber-risk. On the other hand, 64 % of OESs do not quantify cyber-risks;
- **other risk mitigation strategies** were often mentioned as more favourable than risk transfer due to coverage and costs.

Regarding recommendations, the report provides **advice to policymakers in EU and its Member States and also to the community of OESs**. The report focuses on the analysis of demand side of cyber insurance (particularly OESs), and accordingly related recommendations target policymakers and OESs. Accordingly, **key recommendations for policy makers** are:

- Implement guidance mechanisms to OESs focused on: **identification of assets, monitor key metrics, conduct periodic risk assessments, security controls identification and quantification of risks**.
- Promote the **creation of frameworks oriented to identify and exchange good practices among OESs**, particularly those related to identification, mitigation and quantification of risk exposure.
- Be aware of the **heterogeneity of OESs in terms of size, economic sector and strategic function.** Formulation of policy action should be coherent with specific needs and challenges of OESs without losing sight of differences among them, e.g. small entities vs large operators.

[1] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021/@@download/fullReport

- Address the **feasibility of more economically sustainable cyber-insurance policies** by working closer to cyber-insurance brokers.

Similarly, key recommendations to OES are:

- **Improve maturity of risk management practices**, especially those related to identification, mitigation and quantification of risk exposure.
- Consider to allocate or increase budgetary provisions to **implementing processes related to identification of assets, monitor key metrics, conduct periodic risk assessments**, **security controls identification and quantification of risks based on industry best practices**.
- Improve **knowledge transfer and sharing among OESs allowing to learn from good practices** when contracting and implementing cyber insurance to the benefit of these operators.

1. INTRODUCTION

Objective

The main objective of this analysis is to understand and identify current requirements and challenges faced by operators of essential services (OESs)[2] when contracting cyber insurance. Accordingly, the aim of the analysis is to provide recommendations to policymakers and OES on possible ways to face these challenges. The work is particularly focused on the analysis of OESs as acquirers of cyber insurance products and services.

Scope

The conducted work aims at shedding light on potential barriers that are preventing OESs from purchasing cyber insurance. The report addresses exclusively the 'demand side' of cyber-insurance market, applicable to the particular case of OESs. Therefore, considerations and analysis related to the supply side of the cyber-insurance sector (e.g. insurers, brokers) are out of the scope of this analysis.

The study has focused on challenges faced by 262 OESs distributed in 25 EU Member States, representing all strategic sectors defined by Directive (EU) 2016/1148, known as the NIS directive. The final outcome of the analysis is reflected in the main part of this report. The comprehensive set of questions and answers addressed in the survey are included in the annexes.

Background

Prior to the analysis presented in this report, ENISA had conducted deep-dives analysis on specific aspects of cyber insurance from a policy development point of view. Key outputs of this previous work were:

a) Cyber insurance: recent advances, good practices and challenges[3];
b) Commonalities of risk assessment language in cyber insurance - recommendations on cyber insurance [4].

The results from these reports, released between 2016 and 2017, provided solid evidence of the existence of good practices in the areas of both cyber insurance and risk management and on the existence of challenges that are yet to be tackled and that require further investigation into their respective causes and consequences.

At interinstitutional level, ENISA has developed strong synergies with several stakeholders including the European Insurance and Occupational Pensions Authority (EIOPA) in actions oriented to have a better understanding of the sector of cyber insurance from a two-fold perspective: cybersecurity and market development. These synergies have been materialised on close coordination activities to monitor cyber insurance developments, knowledge exchange and multidisciplinary collaboration.

[2] As defined in the Article 5(2) of the NIS Directive: the criteria for the identification of the operators of essential services are the following: (i) The entity provides a service which is essential for the maintenance of critical societal and/or economic activities. (ii) The provision of that service depends on network and information systems. (iii) An incident would have significant disruptive effects on the provision of that service.
[3] https://www.enisa.europa.eu/publications/cyber-insurance-recent-advances-good-practices-and-challenges
[4] https://www.enisa.europa.eu/publications/commonality-of-risk-assessment-language-in-cyber-insurance

Methodological approach

The study was conducted based on the following steps:

Desktop research: Focused on gathering information helping to understand the state of the art of the market, the requirements and challenges faced by OESs and the experiences around the use of cyber insurance as mitigation tool in different contexts. The knowledge base allowed the formulation of preliminary hypotheses which were used as input to create the survey and the interview guide.

Online survey: Consisted of obtaining data related to challenges and requirements of OESs in acquiring cyber insurance. The survey covered over sixty questions distributed in seven thematic blocks including: (i) information about the respondent, (ii) risk identification, quantification and prioritization, (iii) identification and selection phase, (iv) contractual phase, (v) coverage maintenance and support, (vi) claim procedure and (vii) skills. For a complete overview of the survey please refer to Annex B.

Semi-structured interviews: A series of 10 interviews were conducted to investigate the background and motivation of answers in the survey. This activity provided additional insights into the experiences of OESs in finding acquiring and managing cyber insurance as a tool for cyber risk mitigation. The respondent consisted of a diverse group of OESs in terms of size, geography and sector represented.

Data analysis and validation: A final step in the approach was to conduct an analysis of the survey and interview data. Challenges, issues and key insights derived from both the interviews and through analysis of the dataset were captured in the report.

Policy recommendations: As a result of previous methodological steps, the analysis concludes with a list of recommendations addressed to policymakers. These recommendations are elaborated on the basis of evidences, findings and data gathered mostly in first half of 2022. To this end, interested parties should keep in mind the constant and rapid evolution of the cyber insurance market, and should therefore consider the time in which related analysis took place.

2. THE DEMAND SIDE OF CYBER INSURANCE SECTOR

Based on the desk-research analysis[5], the following aspects provide a general overview of the cyber insurance sector. Existing literature has addressed cyber insurance from several angles, mostly from the perspective of the cyber insurance offer-side of the market, such as insurers or brokers.

- Cyber insurance is still in a development phase and it is challenging to capture how expectations on coverage may change over time and how emerging threats may change the expectations regarding coverage.
- The cyber insurance industry may expect a gradual increase in the demand for cyber insurance and the importance of cyber coverage is expected to increase significantly
- The cyber insurance processes follow three main pillars: risk identification, risk analysis and establishing a contract.
- The overall awareness and perceived probability of the cyber risks is high but expected impacts of a cyber-attack may yet be underestimated.
- Lack of incident-related data is a primary obstacle to a detailed understanding of fundamental aspects of cyber risk and to the provision of proper coverage to end users.
- Insurers may face challenges in collecting accurate information from end-users as they may be reluctant to provide complete answers in questionnaires or to provide access to information related to critical assets, internal procedures and security controls.
- End-users may be concerned about possible non-disclosure or incomplete information leading to claims being rejected. As a result, it is hard to determine how much risk to transfer and insurers may also face risks they may not have properly quantified.
- The lack of credible data and the potential for high aggregate losses may lead to cyber insurance policies with gaps in coverages and limits that are too low, which may lead to a lack of indemnification for cyber losses.
- Systems change continuously as new systems are added and obsolete ones are dismantled, leading to a continuous change of the risk profile.
- Statistics on cyber incidents are not completely reliable as victims do not always report incidents (e.g. to avoid reputational damage)
- It can take a very long time before a breach is noticed and depending on the policy conditions, such an event may be no longer covered.
- Guidelines for cyber insurance are available and can provide an initial framework for end-users to approach the selection and use of cyber insurance in their respective contexts[6].

In contrast, the desk research activity did not contribute to obtain data and information related to the demand side in cyber insurance market dynamics. Accordingly, the work presented in this report aims at analysing cyber insurance challenges and perspectives, targeting the particular group of entities called: operators of essential services (OESs), as defined in the NIS Directive. The following sections discuss in detail related analysis and obtained results. The sections are a reflect of typical cyber insurance lifecycle that includes: risk management practices (section 2.1), coverage (2.2), identification and selection of insurer (2.3), contracts (2.4), maintenance (2.5), claim procedures (2.6) and awareness and skills (2.7)

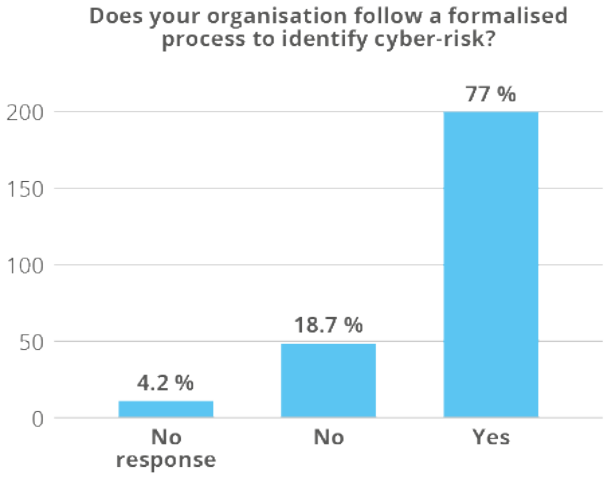
[5] A complete overview of the publications reviewed can be found in the Annex A.
[6] See: Information security management — Guidelines for cyber-insurance ISO/IEC 27102:2019

2.1 RISK-MANAGEMENT PRACTICES

Cyber insurance is a strategy to reduce risk and therefore is addressed in a context of risk management processes within an organisation. The risk management processes can also be a pre-requisite for cyber insurance. As risk transfer is preceded by the identification and quantification of risk exposure, it can be one option in a range of other risk management strategies (acceptance, termination of activities or risk mitigation through process controls). Therefore, respondents were asked about risk management processes, risk mitigation options and the quantification of cyber risks.

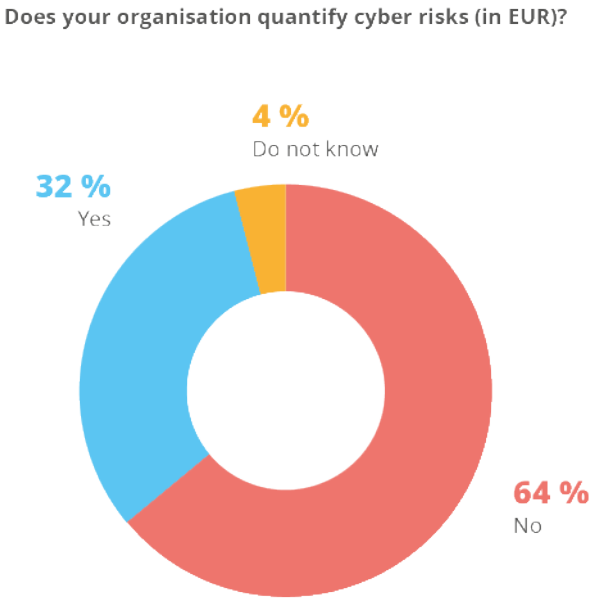
Of all the respondents, over 77 % indicated that they follow a formalised process to identify cyber risks. In contrast, the analysis also shows that 23 % are not using a formalised process or are unsure that there is one. This gap expands when respondents were queried regarding existing processes to make decisions on risk mitigation tools and controls. In 32 % of the cases, a process to determine risk mitigation tools and controls is not in place.

Figure 1: Formalised process to identify cyber-risk



This observation becomes even clearer when analysing the data on risk quantification. The results also demonstrate that only 32 % of respondents quantify cyber risk. The difference between these numbers could be explained by respondents only applying a qualitative risk assessment process (for the 67 % that have a formalised process to identify cyber risk). Respondents who have cyber insurance are more likely to quantify cyber risk as well. The research shows that 61 % of respondents with cyber insurance do, compared to the 22 % of respondents who do not have cyber insurance.

Figure 2: Formalised process to identify cyber risk



As risk quantification is a pre-requisite for risk transfer, the relative lack of risk quantification practices among OESs can be seen as an emergent challenge in the preliminary steps oriented to acquiring cyber insurance services. During the interviews, some respondents indicated that the risk quantification process was conducted by their insurance broker or agent.

All interviewed contributors indicated to have risk-management practices in place and a process to determine controls. Most of respondents did not quantify cyber risks themselves but worked with their broker or insurance company to quantify their exposure and determine coverage needs. In some cases, the coverage chosen was also a trade-off between coverage and costs, to keep the annual cyber insurance policy fee within the allowed budget.

Summing up, it can be stated that for a subset of OESs, the maturity of the risk-management processes can be improved. The obtained data suggests that as risk-management maturity improves, the coverage of cyber insurance will also increase. Other key findings of risk management practices in OESs are:

- Most respondents (77 %) follow a formalized process for qualitative risks assessments (N = 202). Additionally, 68 % follows a process for the selection of controls to mitigate risk (N = 177).
- Among all respondents, only 32 % (N = 84) quantifies cyber risk (N = 167 does not).
- Within respondents who already have cyber insurance, 22 % of them quantify cyber risk

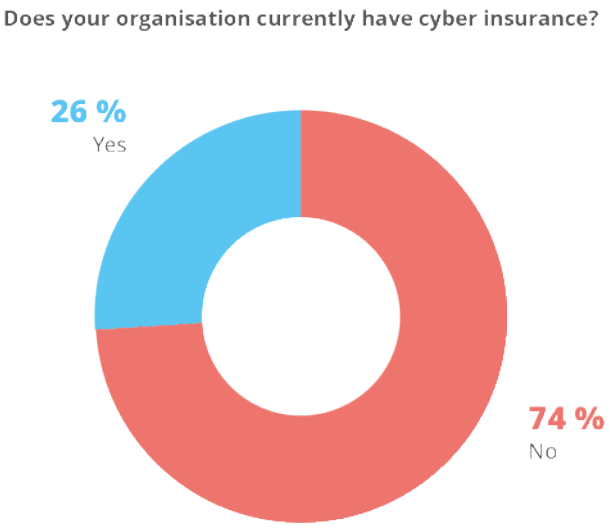
2.2 CYBER INSURANCE AND OTHER COVERAGE

A key aspect of the research was to understand the cyber coverage of OESs. In addition, coverage through other existing policies was investigated as well as the type of coverage, missing elements and failed attempts to get cyber insurance in the past. The motivations behind contracting cyber insurance and the major challenges were also analysed.

Current cyber coverage

The survey revealed that only 26 % of the respondents currently have cyber insurance and 74% do not. This indicates a slightly lower coverage than the NIS investment results of 2022, which report that 32 % of OESs/DSPs have cyber insurance (or the 30 % of OESs/DSPs with cyber insurance in 2021[7]). Although the reported coverage percentages from this cyber insurance survey are slightly lower than in NIS investment reports, it does show a declining trend over the last few years.

Figure 3: Cyber insurance uptake in OESs



From a territorial point of view, regional differences in cyber coverage appear. In western and northern Europe the cyber coverage appears to be the highest (45 %), followed by southern Europe (39 %) and lastly eastern Europe, with the lowest adoption of cyber insurance (12 %).

Table 1: Cyber insurance uptake across the EU

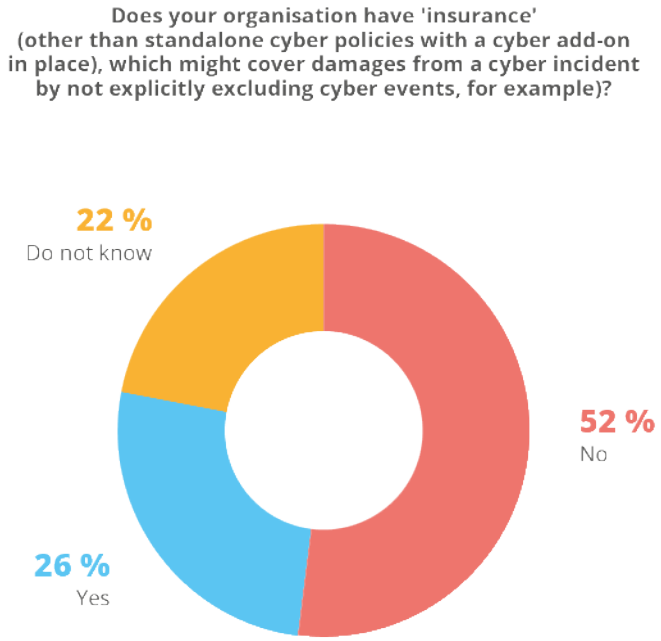
Cyber insurance	Western and northern Europe	Southern Europe	Eastern Europe
No	55 %	61 %	88 %
Yes	45 %	39 %	12 %

[7] NIS Investment report 2021: https://www.enisa.europa.eu/publications/nis-investments-2021

Other insurance coverage including cyber

In addition to specific cyber policies, other insurance policies might sometimes provide coverage for cyber incidents. This could be explicitly through a cyber add-on or more implicitly by not excluding any cyber incidents. Over half of the respondents indicated that they do not have this coverage, but 26 % (N = 64) indicated that they have some form of cyber coverage through their other policies.

Figure 4: Insurance, other than standalone cyber policies



What cyber insurance policies cover

The coverage of cyber insurance is quite broad and includes various damages and incidents. Coverage ranges from (Distributed) denial of service (DDoS) attacks, malware, ransomware attacks, stolen credentials (unauthorised access and use of data assets and computer systems), phishing attacks, network interruption and more.

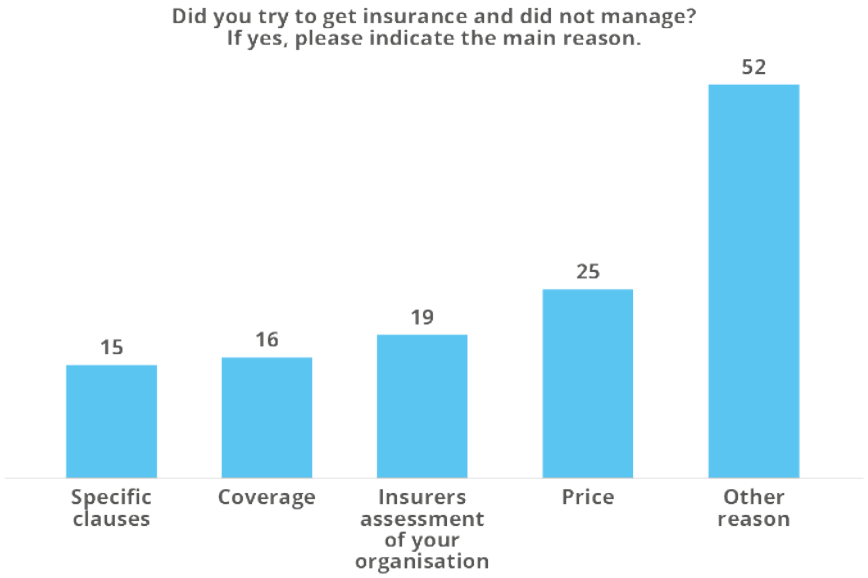
However, respondents to the interview expressed concern about the ease of renewing the policies and exclusions, limitations, and price of the prolongations. In particular, getting coverage for ransomware has become increasingly difficult in the last few years according to respondents.

Not able to get cyber insurance

The survey revealed also that companies have difficulties in getting cyber insurance mainly for three reasons:

- Coverage is not sufficient for their needs.
- Because of the way insurers assess the organisation.
- The price of the insurance policy or offer generally does not meet the expectations.

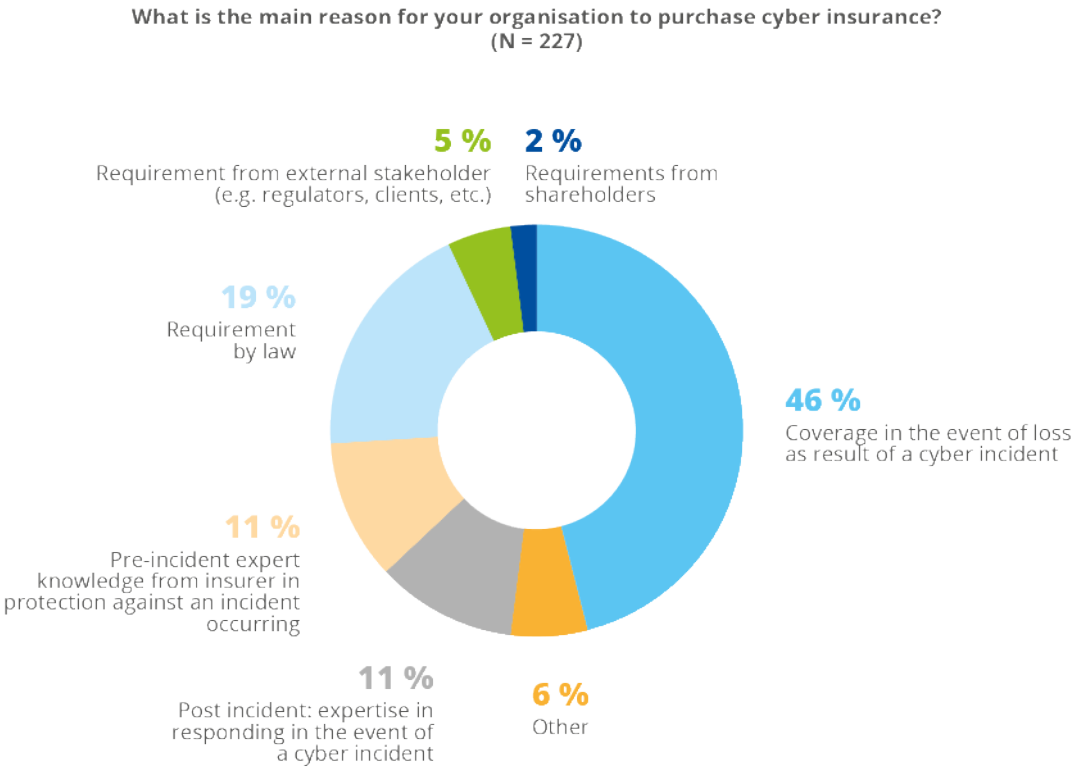
Figure 5: Reasons for not contracting cyber insurance



Reasons to purchase cyber insurance and preferred coverage

Coverage in case of incident is, for almost half of respondents, the driving reason to purchase cyber insurance. Requirements by law (19 %), pre-incident (11 %) and post-incident (11 %) coverage were in less degree important reasons. Respondents who did not have insurance indicated to be interested in various types of coverage including: business continuity, expert support during an incident and ransomware coverage.

Figure 6: Main reason to purchase cyber insurance



One of the respondents, a large OESs from western Europe, revealed that the organisation had decided against a cyber insurance policy due to costs and limitations in available coverage. The key decision in this case was to invest the budget in the Chief Information Security Officer (CISO) function instead, as this was seen as more effective.

Key findings

- For 26 % of respondents, other insurance policies would provide some cover in case of a cyber incident (N = 64). 53 % of respondents do not have this coverage (N = 131), other 22 % do not know (N = 54).
- Only 26 % of OESs has a cyber policy (N = 67), 74 % of the respondents does not have cyber insurance (N = 195).
- Third party liability coverage is the preferred additional coverage by the respondents (e.g. coverage of incidents at a supplier which would interrupt business for the insured).
- Regional differences show that western and northern Europe have the highest coverage (45 %), followed by Southern Europe (39 %). Eastern Europe has the lowest coverage with 12 %.
- Of all respondents 36% (N = 95) have not evaluated a cyber insurance offer before, against 38 % (N = 100) who have and 20 % who expects this in the future.
- Both market research and the interviews indicate cyber insurance policies are increasing in price and decrease in coverage.
- OESs increasingly looking at alternative risk mitigating strategies (e.g. risk treatment/risk reduction).
- 56 % of respondents stated they consider other risk mitigations tools to be more effective compared to cyber insurance (N = 147).
- Some respondents indicated to consider discontinuing current cyber insurance if pricing keeps on increasing.
- Combined data from this study and previous NIS Investment data shows a declining cyber insurance coverage trend.

2.3 IDENTIFICATION AND SELECTION OF CYBER INSURER

This section describes aspects related to the identification and selection phase of a cyber insurer as part of a cyber insurance contracting process. Similarly, the section addresses the perception of OESs to the acceptance by the insurance company.

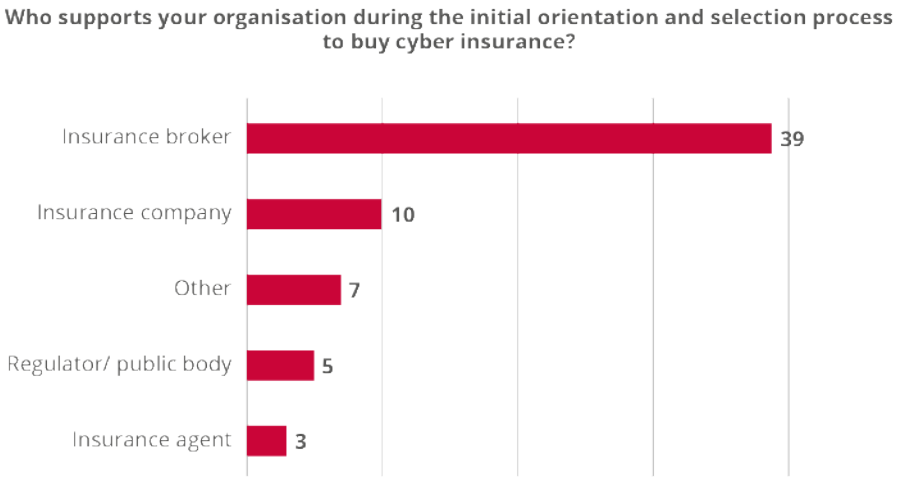
Orientation, identification, and selection

The data shows that 26 % of the respondents (N = 67) currently have cyber insurance and 74 % do not. However, 37 % of the respondents (N = 97) confirms that they have identified cyber insurance as a risk mitigation tool and 20 % states that they are considering acquiring it within one year (N = 28) or after two years (N = 25).

It is important to highlight that 56 % of the respondents (N = 157) reports that ‘other risk mitigation tools were considered more adequate’. This topic has been discussed in detail with the OESs during the interviews and the reason for this response it is often linked to the high

prices of available coverages. This trend explains why other mitigation strategies (like investment in cyber controls) are becoming a more feasible investment for some OESs.

Figure 7: Support during initial steps of cyber insurance

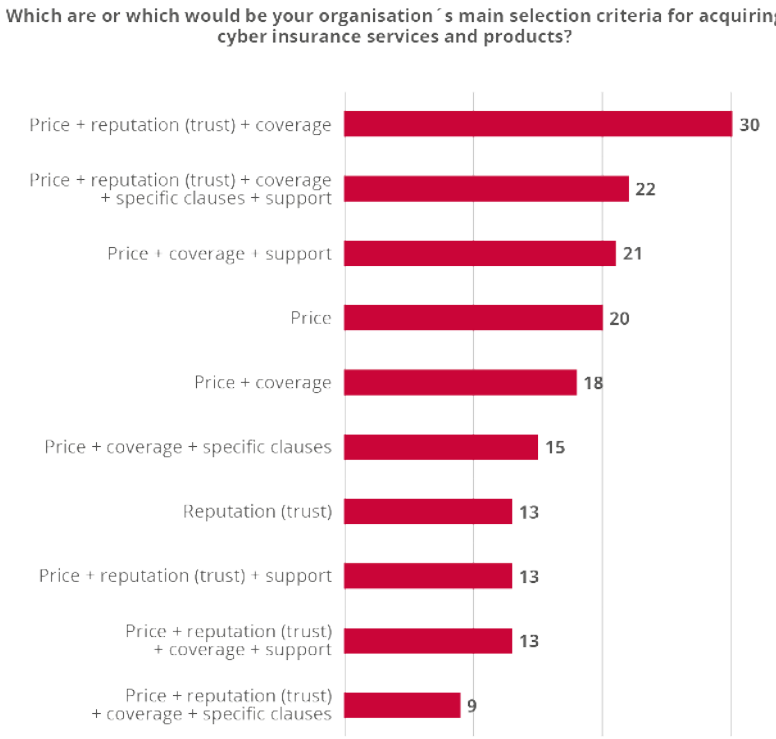


With reference to the selection process, most of the OESs that have insurance have pointed out that they rely on the insurance broker or on the insurance company to identify the right cyber insurance. In contrast, when asking the same question to OESs that have not yet acquired cyber insurance (out of 169 respondents), 57 % would rely on the insurance broker or on the insurance company and 24 % would rely on the regulator / public body.

Still on the selection process, out of 232 respondents, 54 % confirms knowing about cyber insurance offers through own research, 27 % have been contacted by an agent or a broker and 10 % have relied on other resources (e.g., information from other internal organisation departments, parent companies, shareholders). Finally, only 13 out of 232 OESs declare that they have acquired knowledge about cyber insurance offers through interactions with other OESs.

When asked about the selection criteria for acquiring cyber insurance, 174 respondents have provided the answers as shown in Figure 8.

Figure 8: Selection criteria for acquiring cyber insurance



It can be noted that 'price' appears on its own or in combination with other criteria in every possible combination. Therefore, price emerges as the most important criterion for acquiring cyber insurance. Immediately after the price, other criteria conditioning cyber insurance acquisition are:

- reputation of the insurance company,
- coverage,
- specific clauses,
- support.

Finally, out of 64 OESs entities that have cyber insurance, only 16 % of them declare that they are not satisfied with their insurance regarding their risk exposure, while the rest of them declare that they are satisfied (69 %) or very satisfied (16 %).

Many of the respondents indicated they worked with their broker to identify cyber insurance options. One respondent with a sizable insurance team indicated that the initiative came from their insurance responsible – later supported by the insurance broker.

Assessment and acceptance by the insurance company

On the matter of the intake assessment, the OESs have been asked to provide an answer based on the elements that apply to the procedure they have undergone. Their answers are shown in Table 2.

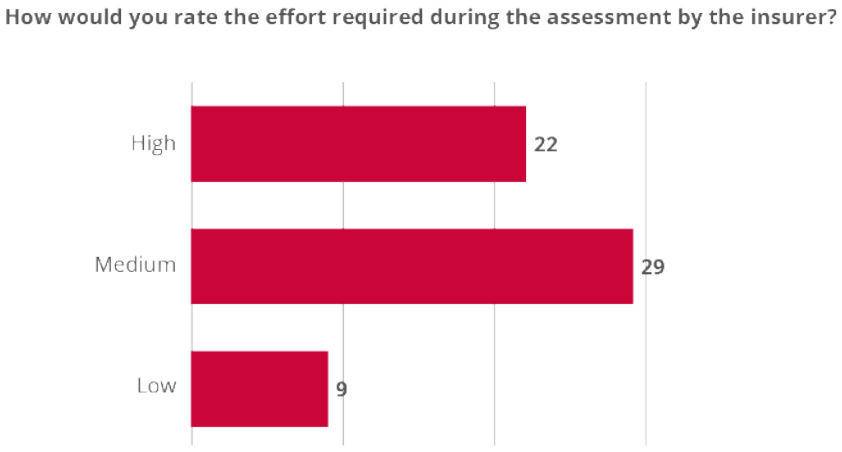
Table 2: Intake assessment conducted by insurers

How did the insurance company conduct the intake assessment?	Total
Questionnaire	14
Questionnaire + interviews	12
Questionnaire + interviews + request of documentation	11
Questionnaire + request of documentation	10
Other methods	3
Questionnaire + Interviews + request of documentation + third party assessment	3
Interviews + third-party assessment	2
Interviews + request of documentation	2
Interviews	1
Request of documentation	1
Questionnaire + third-party assessment	1
Questionnaire + other methods	1
Third-party assessment	1
Interviews + request of documentation + third-party assessment	1
Questionnaire + request of documentation + third-party assessment	1
Grand total	64

It can be noted that most of the assessments relied on questionnaires, interviews and requests for documentation. Also, third-party[8] assessments are among the assessments' methods, but they don't happen very often.

On the duration of the assessment, only 18 out of 61 respondents have reported that they consider it too long, while the vast majority (70 %) answered that the length of the assessment was 'about right' (N = 39) or 'short' (N = 4). In respect of the effort required during the assessment, 60 OESs have replied as follows:

Figure 9: Effort required during the assessment



Finally, on the matter of legal limitations (e.g. classified or internal documentation) potentially encountered during the assessment phase, the respondents reported that they had no limitations and, if existing, they could be adjusted to allow information sharing. Only one respondent out of 60 reported that these legal limitations couldn't be adjusted. It has to be noted that in 7 % of the cases (N = 4), legal limitations led to a rejection or modification of the offer by the insurer.

[8] In line with the ENISA report: 'Cyber Insurance: Recent Advances, Good Practices and Challenges', third party risks are risks that might initially affect someone other than the insured (first party) or insurer (second party), against which an insured would like to have coverage.

On the interviews several respondents indicated that time and effort to renew insurance was getting longer and more effort-intensive, especially in the last couple of years.

Key findings

- One in four OESs currently have cyber insurance in place. Moreover, 37 % of the respondents (N = 97) confirms that they have identified cyber insurance as a risk mitigation tool and 20 % state that they are considering acquiring cyber insurance within one year (N=28) or after two years (N = 25).
- Half of OESs confirms knowing about cyber insurance offers through own research, 27 % have been contacted by an agent or a broker and 10% have relied on other resources. Only 13 of OES declare that they have acquired knowledge about cyber insurance offers through interactions with other OESs.
- Within the criteria for acquiring cyber insurance, price appears to be the most important, followed by: reputation of the insurance company, coverage, specific clauses and support.
- Legal limitations at the time of sharing information with the broker do not normally trigger a problem. Yet, in 7 % of the cases, legal limitations led to a rejection or modification of the offer by the insurer.

2.4 CONTRACT AND PROCESS

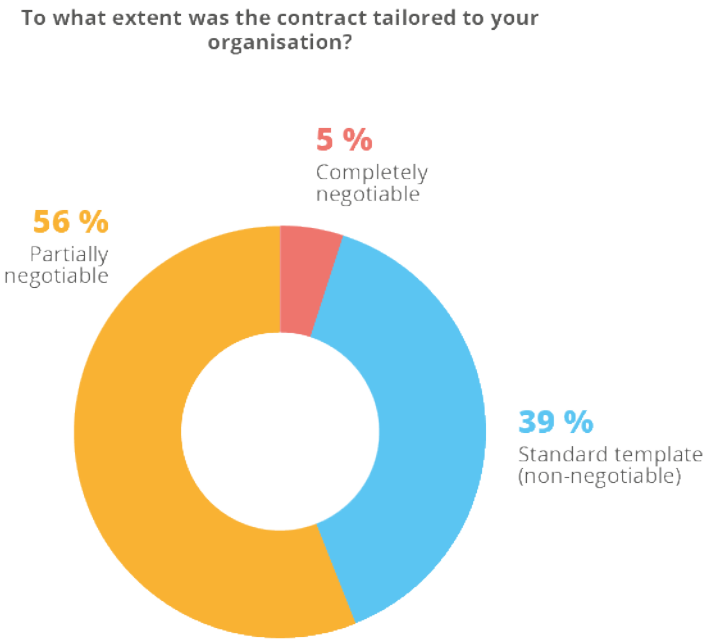
For 13 % of respondents, Chief Information Security Officer (CISO) or security team is responsible for procuring cyber insurance. The respondents who have cyber insurance are slightly more likely to have a dedicated insurance team involved in the procurement of cyber insurance. As shown in Table 3, in most of cases decision making regarding acquisition of insurance takes place outside the CISO function. Decisions regarding cyber insurance are more often taken by executives, a dedicated insurance team or the finance function.

Table 3: Responsible for cyber insurance in OESs

In case insurance coverage is identified as a mitigation measure, who is responsible for procuring cyber insurance in your organisation?	Total
No response	19
CFO or financial team	37
CISO or security team	34
Dedicated insurance manager or team	67
Executive manager	66
Other, please specify	39
Grand total (N)	262

For 39 % of the overall experiences show that the contract was not negotiable and based on standard templates, while most of the experiences show that the contract could be at least partially negotiable if not completely negotiable.

Figure 10: Cyber insurance contracts according to organisational needs



The data regarding the existence of certifications (e.g. ISO 27001) and their impact on the contractual agreement show that in 77 % of the cases this element led to the easing of the acceptance by the insurance company. Out of 40 OESs, 5 reported that the existence of certifications led to the reduction of the price and 4 declared that owning these features had an impact on the coverage limits. Still on the matter of coverage, only 7 OESs out of 58 reported that the assessment conducted by the insurer led to exclusions and sub-limits, while 44 % responded that no limitations were introduced.

With reference to the information received when purchasing cyber insurance, out of 60 respondents, 57 % reported that they have received clear information about any embedded exclusions and limitations of the coverage, including the cases of systemic events.

At the same time, only 32% of the OESs (N = 19) have confirmed that they have been presented with a list of examples of events that are excluded from the coverage. It should be noted that in the same two questions, almost one third of the participants replied that they do not know whether they have received clear information and a list of exclusions.

An insurance manager expressed his concerns about how to interpret certain clauses of the cyber insurance contract. He mentioned the lack of standardisation in the clauses and the lack of available precedents to understand how clauses would be explained in a loss scenario.

Key findings

- Decision making regarding acquisition of insurance, in most of cases, takes place outside the CISO function (only in 12 % of OESs).
- Only 3 % of OESs (2 out of 62) stated the contract and its annexes to be unclear.
- Of respondents with cyber insurance, 63 % of respondents found the contract clauses clear or somewhat clear.

- On the negotiability of the contract, 61 % was partially or completely negotiable (N = 61).
- A 57 % of OESs reported to have received clear information about any embedded exclusions and limitations of the cyber insurance coverage, including the cases of a systemic events.

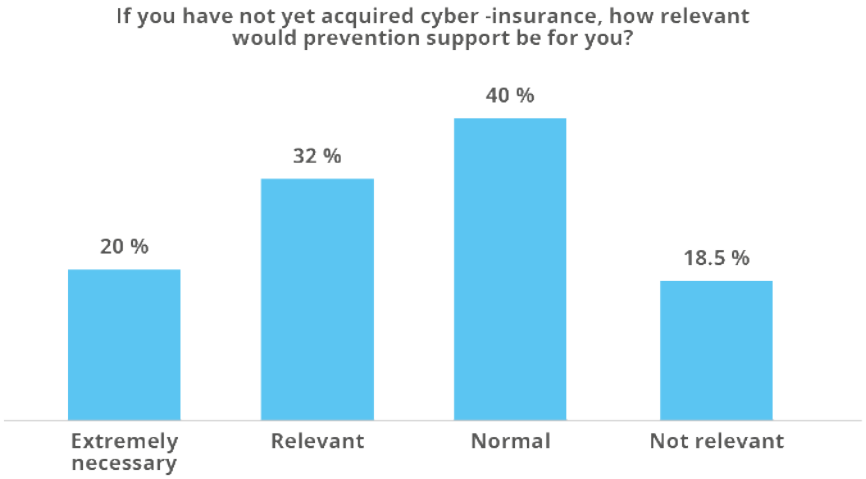
2.5 MAINTENANCE AND SUPPORT

When exploring the area regarding additional features or services embedded in the cybersecurity insurance acquired by the OESs, it can be noted that:

- 40 % of respondents (24 out of 60) declared that their insurance company provide support in prevention of cyber incidents;
- 68 % of respondents (40 out of 59) declared that their insurance company provide post-incident cyber support.

The question related to importance of 'prevention support' services has also been asked to the participants. Cyber insurance support appears to be not relevant for 18 % of OESs and relevant for the 32 %. Only 20 % of OESs consider it as extremely necessary.

Figure 11: Relevance of cyber insurance



In contrast, the insured OESs have been asked if a cyber incident has led to an increase of costs or denial of coverage. In this case only 10 % of the respondents has confirmed this possibility, while 50 % has declared that they haven't observed any incident. The rest of the respondents were equally divided between 'no' and 'does not know'.

A few respondents mentioned cyber-incident response to be a very valuable service. However, in many cases an existing relationship with a cyber-incident response party is already in place, making the insurance company a less likely candidate to offer this service.

Key findings:

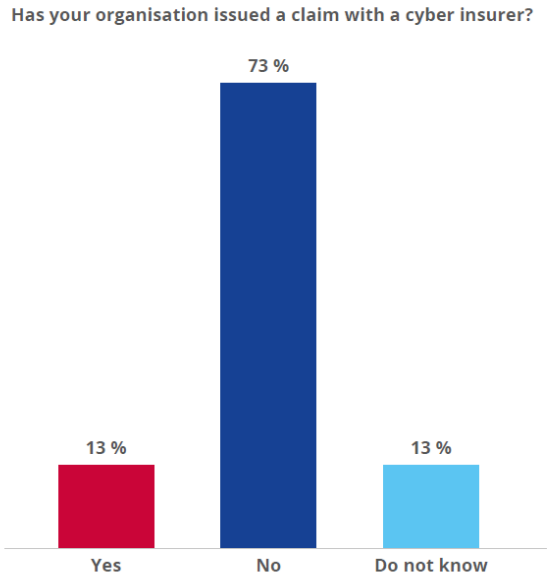
- For OESs, post-incident response services provided by cyber insurers are more prominent that pre-incident response services.
- For 20 % of non-insured OESs, maintenance and support from a cyber insurer provider would be extremely necessary.
- Half of insured OESs have not witnessed any cyber-incident, therefore they cannot assess how the increase of cyber insurance costs could be related

2.6 CLAIM PROCEDURE

The final section of the survey, dedicated to the gathering of data about the experiences of OESs that have acquired cyber insurance, has been focused on the 'claim procedure'.

To the question: has your organisation issued a claim with a cyber insurer? Almost 3 in four OESs (44 out of 60), have never issued a claim. Likewise, 13 % of the respondents (8 out of 60) have issued a claim and 13 % do not know.

Figure 12: Issuing a claim



Operators of essential services were also asked if they have ever issued a cyber claim with their insurer on a non-cyber policy. In this case 7 out of 8 responded that they have never done it, 1 did not know.

Determining the claim and proving all supporting evidence can be quite a complex step in the process. A respondent indicated that they hired a claims adjustment consultant due to the complexity of the case.

Key findings

- 13 % of the respondents (8 out of 60) have issued a claim with their cyber insurer.
- Of the 8 respondents, 6 confirmed their claim was approved and 2 confirmed that the reimbursement was enough to cover the actual damage.
- 3 out of 6 respondents also confirmed that the claim was processed in a timely manner (only 2 responded that it was not).
- On the clarity of the methodology for calculating the amount of the claim, 3 out of 6 confirmed that the methodology was clear (only 2 responded that it was not).
- Out of the 6 respondents, 5 reported that the claim did not lead to any legal dispute with the insurer, 1 did not know.

2.7 AWARENESS AND SKILLS

To increase awareness about cyber insurance, the top responses (in order of priority) were communication and dissemination, better coverage, ad-hoc collaborative networks and peer-learning. Interestingly, better coverage was mentioned, which could indicate that cyber insurance is perceived as a mitigation strategy with limited scope for the risk itself. Some respondents mentioned that they do not regard cyber insurance as a viable risk mitigation strategy at all. Informal learning and recommendations were suggested as a good way to improve strategy. Options mentioned less often were public support and research and scientific evidence.

To increase the purchase of cyber insurance, the top responses (in order of priority) were:

- better coverages,
- less exclusions,
- clearer policy wording,
- communication and dissemination.

These responses would be understood in line with higher expectations from organisations according to the offered cyber insurance services. This finding is coherent with outcomes of interviews where interviewees expressed their decreasing appetite for cyber insurance as a strategy to reduce risk.

In the interviews, interviewees expressed that cyber insurance policy fees have gone up significantly in recent years, while at the same time the policy terms have become less attractive (exclusions, sub-limits, etc.). The decreasing attractiveness of cyber insurance due to price and coverage was a recurring theme during the interviews. Investments in cyber controls (risk treatment instead of transfer) were generally seen as more effective in mitigating cyber risk.

Lastly, respondents were asked to indicate the relevant skills they believed to be necessary when purchasing cyber insurance. The top skills mentioned (in order) were risk assessment skills, knowledge about legislation, information management and functioning of the insurance market. As risk-management skills were indicated as the primary skill, it is notable to mention the maturity gap described in section 2.1 on risk-management practices.

Several respondents indicated that it was unclear how premiums are being calculated. They asked for more transparency – so as to be able to see the risk models - so to be able to make a better weighted decision on the level of coverage to buy. One respondent also

argued that it was unclear how investment in cyber controls would contribute to lower premiums (creating a better foundation for a business case).

Key findings

- Communication and dissemination, better coverage, ad-hoc collaborative networks and peer-learning are prominent areas to raise awareness on cyber insurance relevance.
- In the opinion of OESs, key aspects oriented to increase purchase of cyber insurance are: better coverages, less exclusions, clearer policy wording, communication and dissemination.
- From an awareness perspective, most of interviewees realised how cyber insurance policy fees have gone up significantly in recent years, while policy terms have become less attractive.
- In terms of skills, the top ones mentioned as relevant for cyber insurance sector are: risk assessment, knowledge about legislation, information management and functioning of the insurance market.

Table 4: Summary of key findings

Risk management practices	Coverage	Identification and selection of cyber insurer
Most respondents (77 %) follow a formalized process for qualitative risks assessments (N = 202). Additionally, 68 % follows a process for the selection of controls to mitigate risk (N = 177). Among all respondents, only 32 % (N = 84) quantifies cyber risk (N = 167 does not). Within respondents who already have cyber insurance, 22 % of them quantify cyber risk	For 26 % of respondents, other insurance policies would provide some cover in case of a cyber incident (N = 64). 53 % of respondents do not have this coverage (N = 131), other 22 % do not know (N = 54). Only 26 % of OESs has a cyber policy (N = 67), 74 % of the respondents does not have cyber insurance (N = 195). Third-party liability coverage is the preferred additional coverage by the respondents (e.g. coverage of incidents at a supplier which would interrupt business for the insured). Regional differences show that western and northern Europe have the highest coverage (45 %), followed by southern Europe (39 %). Eastern Europe has the lowest coverage with 12 %. Of all respondents 36 % (N = 95) have not evaluated a cyber insurance offer before, against 38 % (N = 100) who have and 20 % who expects this in the future. Both market research and the interviews indicate cyber insurance policies are increasing in price and decrease in coverage. OESs increasingly looking at alternative risk mitigating strategies (e.g. risk treatment/risk reduction). 56 % of respondents stated they consider other risk mitigations tools to be more effective compared to cyber insurance (N = 147). Some respondents indicated to consider discontinuing current cyber insurance if pricing keeps on increasing. Combined data from this study and previous NIS Investment data shows a declining cyber insurance coverage trend.	One in four OESs currently have cyber insurance in place. Moreover, 37 % of the respondents (N = 97) confirms that they have identified cyber insurance as a risk mitigation tool and 20 % state that they are considering acquiring cyber insurance within one year (N = 28) or after two years (N = 25). Half of OESs confirms knowing about cyber insurance offers through own research, 27 % have been contacted by an agent or a broker and 10 % have relied on other resources. Only 13 of OESs declare that they have acquired knowledge about cyber insurance offers through interactions with other OESs. Within the criteria for acquiring cyber insurance, price appears to be the most important, followed by: reputation of the insurance company, coverage, specific clauses and support. Legal limitations at the time of sharing information with the broker do not normally trigger a problem. Yet, in 7 % of the cases, legal limitations led to a rejection or modification of the offer by the insurer.

Contracts and process	Maintenance and support	Claim procedures	Awareness and skills
Decision making regarding acquisition of insurance, in most of cases, takes place outside the CISO function (only in 12 % of OESs). Only 3 % of OESs (2 out of 62) stated the contract and its annexes to be unclear. Of respondents with cyber insurance, 63 % of respondents found the contract clauses clear or somewhat clear. On the negotiability of the contract, 61 % was partially or completely negotiable (N = 61). A 57 % of OESs reported to have received clear information about any embedded exclusions and limitations of the cyber insurance coverage, including the cases of a systemic events.	For OESs, post-incident response services provided by cyber insurers are more prominent that pre-incident response services. For 20 % of non-insured OESs, maintenance and support from a cyber insurer provider would be extremely necessary. Half of insured OESs have not witnessed any cyber-incident, therefore they cannot assess how the increase of cyber insurance costs could be related	13 % of the respondents (8 out of 60) have issued a claim with their cyber insurer; Of the 8 respondents, 6 confirmed their claim was approved and 2 confirmed that the reimbursement was enough for covering the actual damage; 3 out of 6 respondents also confirmed that the claim was processed in a timely manner (only 2 responded that it was not) On the clarity of the methodology for calculating the amount of the claim, 3 out of 6 confirmed that the methodology was clear (only 2 responded that it was not); Out of the 6 respondents, 5 reported that the claim did not lead to any legal dispute with the insurer, 1 did not know.	Communication and dissemination, better coverage, ad-hoc collaborative networks and peer-learning are prominent areas to raise awareness on cyber insurance relevance. In the opinion of OESs, key aspects oriented to increase purchase of cyber insurance are: better coverages, less exclusions, clearer policy wording, communication and dissemination. From an awareness perspective, most of interviewees realised how cyber insurance policy fees have gone up significantly in recent years, while policy terms have become less attractive. In terms of skills, the top ones mentioned as relevant for cyber insurance sector are: risk assessment, knowledge about legislation, information management and functioning of the insurance market.

3. RECOMMENDATIONS

The following recommendations are provided aiming to mitigate challenges faced by OESs when addressing cyber security. The following set of recommendations are addressed primarily to policymakers and OESs in the EU and its Member States, dealing cyber insurance policy.

Recommendations to policymakers

- Implement guidance mechanisms aiming at improving maturity of risk management practices of OESs. Specific areas where guidance would be more helpful are: identification of assets, monitoring key metrics, frameworks for risk assessment and quantification, security controls identification and quantification of risks.

- Promote the creation of frameworks oriented to identify and exchange good practices among OESs, particularly those related to identification, mitigation and quantification of risk exposure. Also, facilitate exchange of experiences among OESs related to contracting and implementing cyber insurance in different contexts.

- Be aware of the heterogeneity of OESs in terms of size, economic sector and strategic function. Formulation of policy action should be coherent with specific needs and challenges of OESs as a whole, without losing sight of differences among them, e.g., small entities vs large operators.

- The study shows that OESs tend to prefer self-investment to risk transfer if prices of cyber insurance are high. Policymakers should address the feasibility of more economically sustainable cyber insurance policies by working closer to brokers.

- Address the link between the cyber-insurance and cyber security by making sure that procurement of products, services and processes certified in the European Union – or that have obtained a label associated with those schemes - obtain a higher score in the intake assessment performed by the insurance companies.

- Foster initiatives, including standardization and guidance development, to provide elements and assessment methodologies on the quantification of cyber risks, circumstance that would also improve the awareness and decision-making on specific areas in which cyber insurance would be the optimal mitigation tool.

- Steer multi-stakeholder dialogues oriented to improving clarity, understandability and comparability of policies by fostering the development of terminology of reference (taxonomy) for cyber insurance.

- Develop collaborative frameworks with public and private partners to enable skills frameworks and programmes for cyber insurance, particularly in areas such as risk assessment, legal aspects, information management and cyber insurance market dynamics.

Recommendations to OESs

- Improve maturity of risk management practices. The risk management practices related to identification, mitigation and quantification of risk exposure would contribute to clarify cyber insurance needs.
- Consider to allocate or increase budgetary provisions to implementing processes related to identification of assets, monitor key metrics, conduct periodic risk assessments, security controls identification and quantification of risks based on industry best practices.
- Improve knowledge transfer and sharing with other OESs allowing to learn from other good practices when contracting and implementing cyber insurance to the benefit of these operators. Also improve incident data sharing among sectors.
- Improve coverage all over digital supply chains, specifically covering 3rd party liability managed service providers. As supply chain are digitally connected, coverage for only a participant in the entire chain might not reduce risks sufficiently.

4. ANNEXES

4.1 ANNEX A. ABBREVIATIONS

CISO	Chief Information Security Officer
CFO	Chief Financial Officer
DSP	Digital Service Provider
EC	European Commission
EIOPA	European Insurance and Occupational Pensions Authority
EU	European Union
ISO	International Standardization Organisation
MS	Member State (of the European Union)
NIS	Network and Information Security (Directive)
N	Number of operators of essential services who responded to questions in the survey
OES	Operator of Essential Service

4.2 ANNEX B. BIBLIOGRAPHY

1. Cebula, J. J., Popeck, M. E. and Young, L. R., *A Taxonomy of Operational Cyber Security Risks Version 2*, Carnegie Mellon University, May 2014, https://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_91026.pdf

2. Chondrogiannis, N., Farao, A. and Bountakas, P., 'Security Economics service platform for smart security investments and cyber insurance pricing in the beyond 2020 networking era', 16 March 2021, https://secondo-h2020.eu/wp-content/uploads/2021/04/D5.1_Cyber_Insurance_Market_Attributes_and_Sources.pdf

3. CRO Forum, 'Cyber resilience – The cyber risk challenge and the role of insurance', December 2014 https://www.thecroforum.org/wp-content/uploads/2015/01/Cyber-Risk-Paper-version-24-1.pdf

4. CRO Forum, *Emerging Risks Initiative – Major trends and emerging risk radar – 2021 update,* 2021, https://www.thecroforum.org/wp-content/uploads/2021/06/ERI-Risk-Radar-2021.pdf

5. Cyber Innovative Technologies, 'Cyber insurance limits case study', https://cyberinnovativetech.com/wp-content/uploads/2020/03/Cyber-Insurance-Limits-Case-Study.pdf

6. Cyber underwriting small group, *Cyber Risk Underwriting – Identified challenges and supervisory considerations for sustainable market development*, International Association of Insurance Supervisors, December 2020

7. CyberArk, *Contain cyber insurance costs and accelerate readiness with CyberArk SaaS Identity Security solutions*, https://www.cyberark.com/resources/white-papers/contain-cyber-insurance-costs-and-accelerate-readiness-with-cyberark-saas-identity-security-solutions

8. De Smidt, G. and Botzen, W., 'Perceptions of corporate cyber risks and insurance decision-making', *The Geneva Papers on Risk and Insurance – Issues and Practice*, Vol 43, 2018, pp. 239–274

9. European Insurance and Occupational Pensions Authority, 'EIOPA Cyber Insurance Workshop', 1 April 2019

10. European Insurance and Occupational Pensions Authority, *Cyber Risk for Insurers – Challenges and opportunities*, Publications Office of the European Union, Luxembourg, 2019 https://www.eiopa.europa.eu/document-library/report/cyber-risk-insurers-challenges-and-opportunities_en

11. European Insurance and Occupational Pensions Authority, *EIOPA Strategy on Cyber Underwriting*, 2020, https://www.eiopa.europa.eu/document-library/strategy/cyber-underwriting-strategy_en

12. European Insurance and Occupational Pensions Authority, *Understanding Cyber Insurance – A structured dialogue with insurance companies*, Publications Office of the European Union, Luxembourg, 2019, https://www.eiopa.europa.eu/sites/default/files/publications/reports/eiopa_understanding_cyber_insurance.pdf

13. Farley, J., *Cyber Market Conditions*, Gallagher, January 2022 https://www.ajg.com/us/news-and-insights/2022/jan/2022-cyber-insurance-market-report/

14. Franke, U. and Meland, P. H., 'Demand side expectations of cyber-insurance', *2019 International Conference on Cyber Situational Awareness, Data Analytics And*

Assessment (Cyber SA), June 2019,
https://www.researchgate.net/publication/337504102_Demand_side_expectations_of_cyber_insurance
https://link.springer.com/article/10.1057/s41288-018-0082-7
https://www.eiopa.europa.eu/media/event/eiopa-cyber-insurance-workshop
https://www.iaisweb.org/uploads/2022/01/201229-Cyber-Risk-Underwriting_-Identified-Challenges-and-Supervisory-Considerations-for-Sustainable-Market-Development.pdf

15. Insurance Europe, 'Examples of cyber-resilience initiatives by national insurance associations', October 2019 https://www.insuranceeurope.eu/publications/2295/examples-of-cyber-resilience-initiatives-by-national-insurance-associations/download/National+examples %20A5.pdf

16. Insurance Europe, 'Response to FSB consultation on effective practices for cyber incident response and recovery', 17 July 2020 https://www.insuranceeurope.eu/mediaitem/3ae6ae30-2c79-43c2-b44d-5197419989ed/Response %20to %20FSB %20consultation %20on %20effective %20practises %20for %20cyber %20incident %20response %20and %20recovery.pdf

17. International Organisation for Standardization, *Information Security Management – Guidelines for cyber insurance*, ISO/IEC 27102:2019, August 2018, https://www.iso.org/standard/72436.html

18. International Telecommunication Union (ITU), telecommunication standardization sector of ITU, *Cyber insurance acquisition guidelines*, August 2021, https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1061-202108-I!!PDF-E&type=items

19. Johansmeyer, T., 'The cyber insurance market needs more money', *Harvard Business Review*, Harvard Business Publishing, 10 March 2022, https://hbr.org/2022/03/the-cyber-insurance-market-needs-more-money

20. Marsh, 'Cyber insurance market overview: Fourth quarter 2021', 12 July 2021, https://www.marsh.com/us/services/cyber-risk/insights/cyber-insurance-market-overview-q4-2021.html

21. Organisation for Economic Co-operation and Development, *Enhancing the Availability of Data for Cyber Insurance Underwriting – The role of public policy and regulation*, 2020, https://www.oecd.org/finance/insurance/Enhancing-the-Availability-of-Data-for-Cyber-Insurance-Underwriting.pdf

4.3 ANNEX C. SURVEY QUESTIONS

Section I. Information about the respondent

1. What is the name of your organisation?
2. Where is your organisation located?
3. What sector is your organisation active in?
4. Is your organisation officially designated as operator of essential services (OES) according to the NIS Directive (EU) 2016/1148? (answer to this question will be used for statistical purposes only and won't be disclosed)
5. What is the size of your organisation by number of employees?
6. If insurance coverage is identified as a mitigation measure, who is responsible for procuring cyber insurance in your organisation?

Section II. Risk identification, quantification, prioritisation

7. Does your organisation follow a formalised process to identify cyber-risk?
8. Does your organisation follow a formalised process to decide which tools should be used to mitigate cyber-risk?
9. Does your organisation quantify cyber risks (in EUR)?

Section III. Identification and selection phase

Orientation, identification, and selection

(Only presented if respondent has cyber insurance: presentation contingent on answer to question 10)

10. Does your organisation currently have cyber insurance?
11. Has your organisation identified cyber insurance as a risk mitigation tool?
12. Has your organisation evaluated a concrete cyber insurance offer before, or would your organisation consider it in the future?
13. Who supports your organisation during the initial orientation and selection process to buy cyber insurance?
14. Who would support your organisation during the initial orientation and selection process of buying cyber insurance?
15. How did your organisation come to know about cyber insurance offers?
16. How satisfied are you with the offered cyber insurance coverage with respect to your risk exposure?
17. Which are or which would be your organisation's main selection criteria for acquiring cyber insurance services and products by your organisation? (Please select that apply)

Assessment and acceptance by the insurance company

(Only presented if respondent has cyber insurance)

18. How did the insurance company conduct the intake assessment? (Please select what applies)
19. How would you rate the duration of the assessment by the insurer?
20. How would you rate the effort required during the assessment by the insurer?
21. Has your organisation encountered any legal limitation (e.g. classified or internal documentation) in sharing information with the insurer during the assessment phase?
22. Did legal limitations (e.g. classified or internal documentation) in sharing information with the insurer lead to a rejection or modification of the offer by the insurer?

Current situation and coverage

(Only presented if respondent has cyber insurance)

23. Does your organisation have 'insurance' (other than standalone cyber policies or policies with a cyber add-on in place), that might cover damages from a cyber incident, (i.e. by not explicitly excluding cyber events, for example)
24. If you have cyber insurance, what does it cover?
25. If you have cyber insurance, is there any additional risk you would like to cover which is not included in your current policy?
26. Did you try to get insurance and did not manage? If yes, please indicate the main reason
27. If your organisation does not have cyber insurance, what would you consider getting insurance coverage for?
28. What is the main reason for your organisation to purchase cyber insurance?
29. What do you see as a major challenge in your cyber insurance policy?

Section IV. Contractual phase

(Only presented if respondent has cyber insurance)

30. Are the contract and its annexes well written and easy to understand?
31. To what extent was the contract tailored to your organisation?
32. Did the existence of certifications (e.g., ISO 27001) have an impact on the contractual agreement?
33. Did the assessment conducted by the insurer result in any exclusions or sub-limits?
34. When purchasing cyber insurance were you clearly informed about any embedded exclusions and the limitations of the coverage, including for risks arising from a systemic event?
35. When purchasing cyber insurance were you presented with a list of examples of events that are excluded from the coverage?

Section V. Coverage maintenance and support

(Question only presented if respondent has cyber insurance)

Pre-incident support

36. Did your insurance company provide support in the prevention of cyber incidents?
37. If you have not yet acquired yet cyber insurance, how relevant would this support be for you?

Post-incident support

38. Does your cyber insurance company provide incident support?

Maintenance

39. Has a cyber incident led to an increase of costs or denial of coverage?

Claim procedure

(Question only presented if respondent has cyber insurance)

40. Has your organisation issued a claim with a cyber insurer?
41. Was the claim approved?
42. Was the reimbursement enough to cover the actual costs of the damage?
43. Was the claim processed in a timely manner according to contract?
44. Was the methodology to calculate the amount of claim clear?
45. Was the claim followed by a legal dispute because of a disagreement with the insurer?
46. Have you issued a claim with your general insurer due to damages resulting from a cyber incident not covered by cyber standalone policies or policies with cyber add-ons?
47. Was your claim approved? (Following previous question)

Closing questions

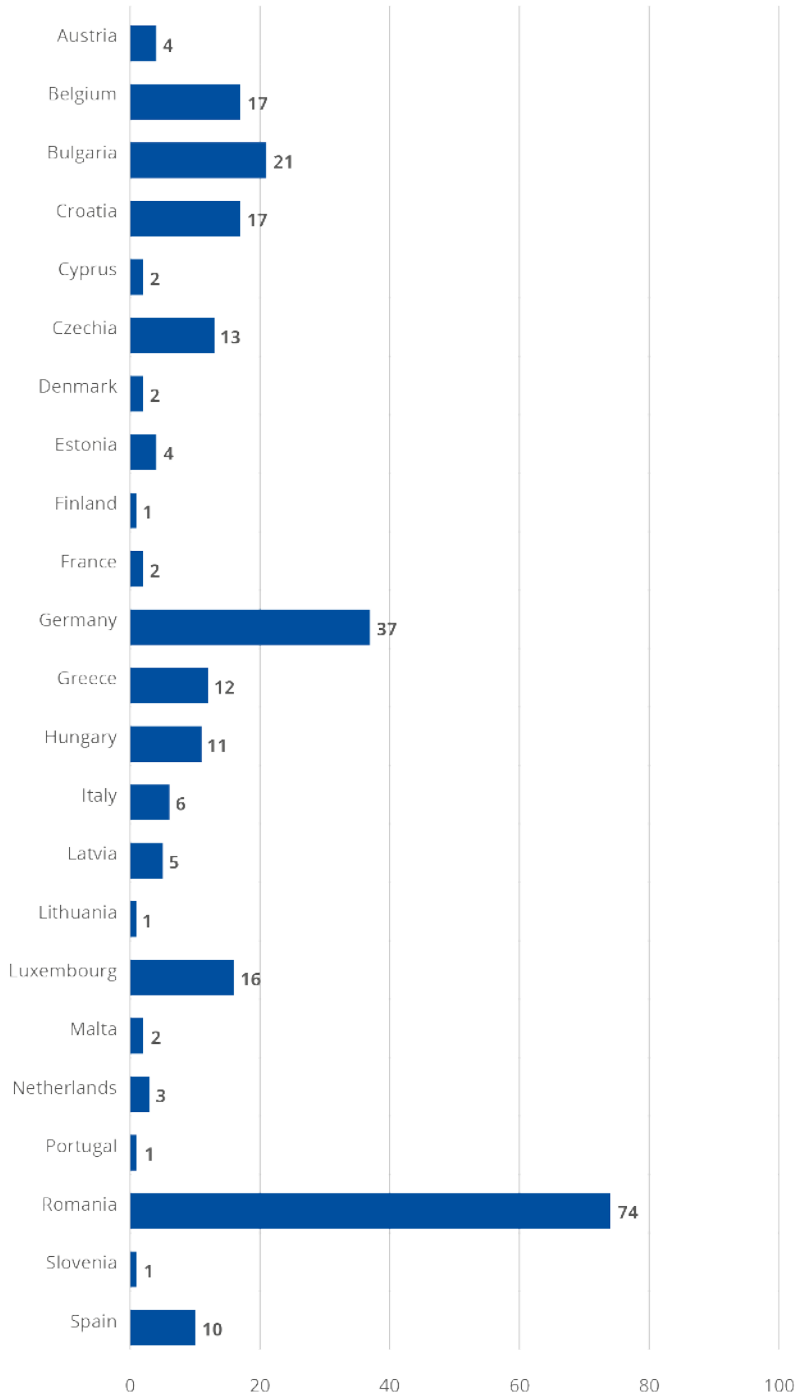
48. In your opinion what type of actions would lead to increased awareness of cyber insurance as a risk mitigation in OESs?
49. In your opinion what type of actions would lead to increased purchase of cyber insurance in OESs?
50. In your opinion, what are the most relevant skills needed in your organisation at the time of acquiring an adequate cyber insurance coverage?

4.4 ANNEX D. SURVEY RESULTS

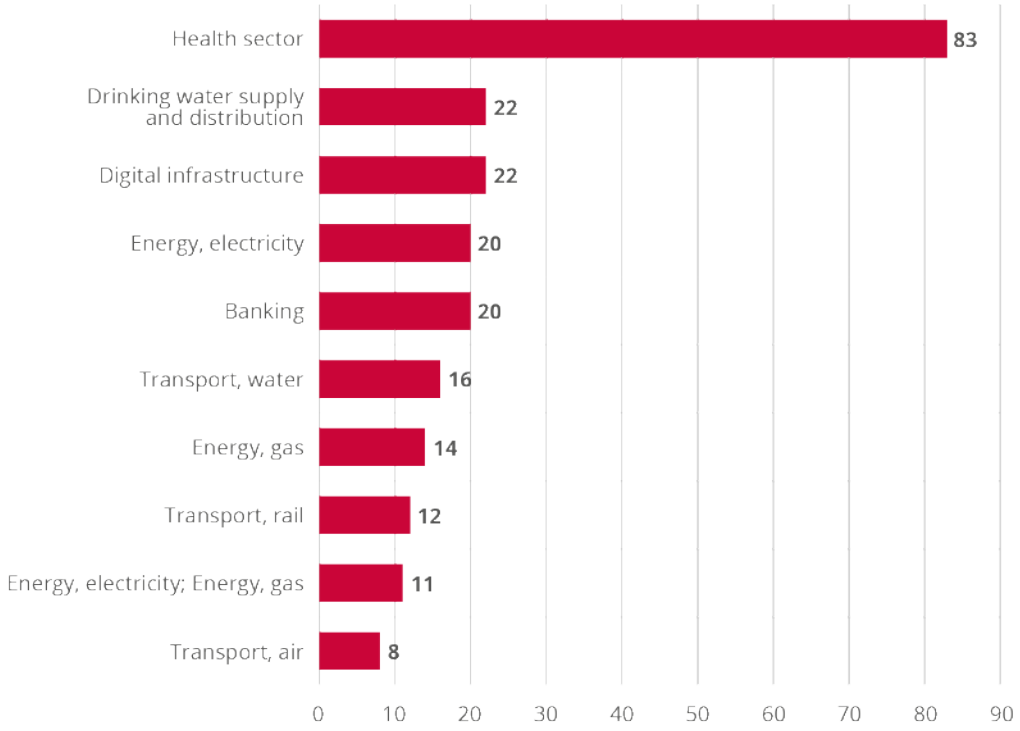
Section I. Information about the respondent

1. What is the name of your organisation?
In total 262 respondents completed the survey.

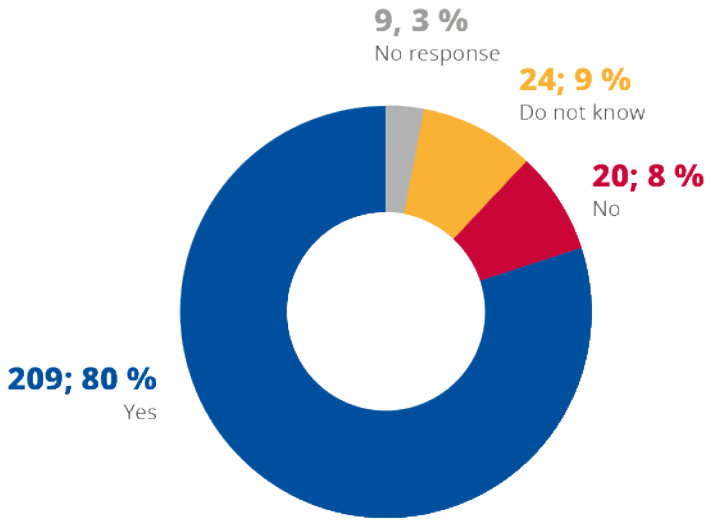
2. Where is your organisation located?



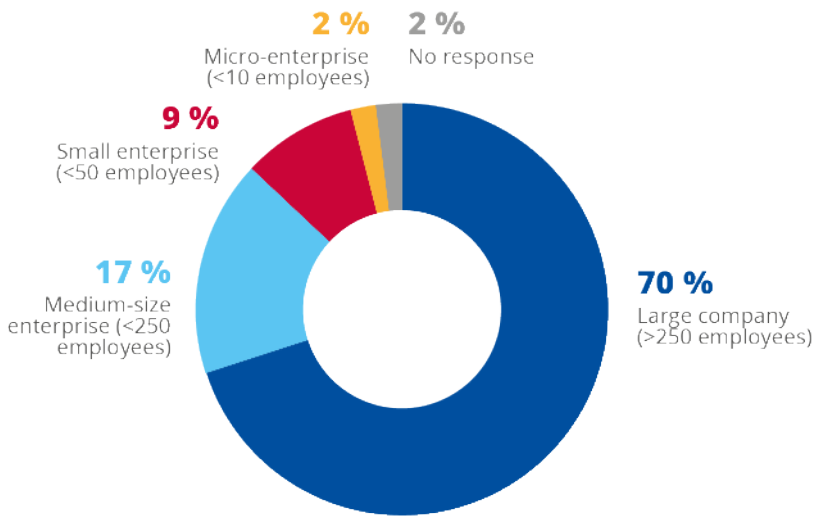
3. What sector is your organisation active in (top 10)?



4. Is your organisation officially designated as an OES according to Directive (EU) 2016/1148?

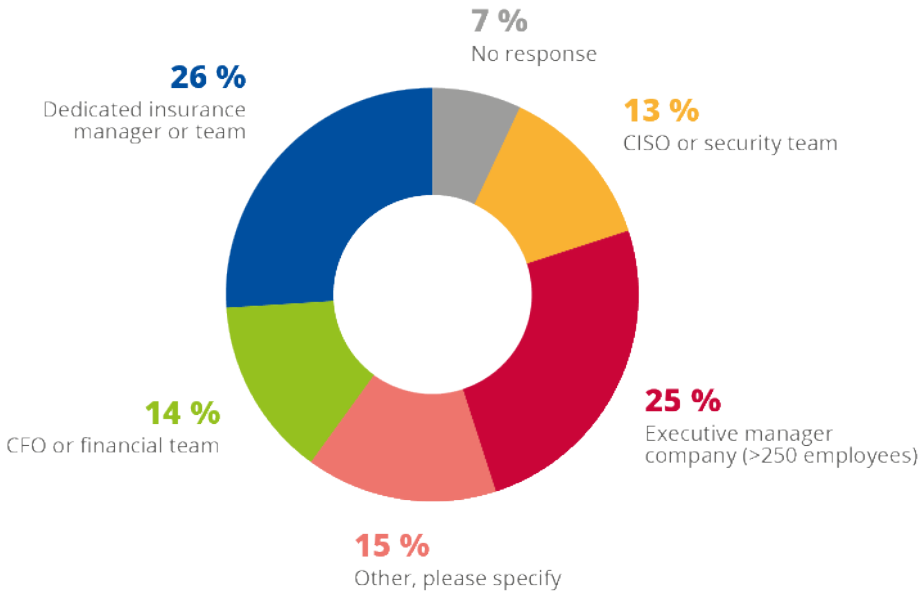


5. What is the size of your organisation by number of employees?



What is the size of your organisation by number of employees?	Total
No response	6
Large company (>250 employees)	183
Medium-size enterprise (<250 employees)	45
Micro-enterprise (<10 employees)	4
Small enterprise (<50 employees)	24
Grand total	262

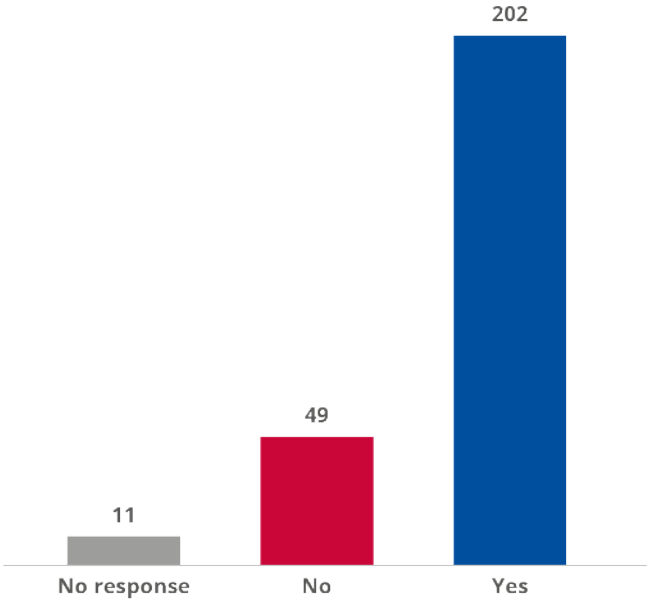
6. If insurance coverage is identified as a mitigation measure, who is responsible for procuring cyber insurance in your organisation?



If insurance coverage is identified as a mitigation measure, who is responsible for procuring cyber insurance in your organisation?	Total
No response	19
CFO or financial team	37
CISO or security team	34
Dedicated insurance manager or team	67
Executive manager	66
Other, please specify	39
Grand total	262

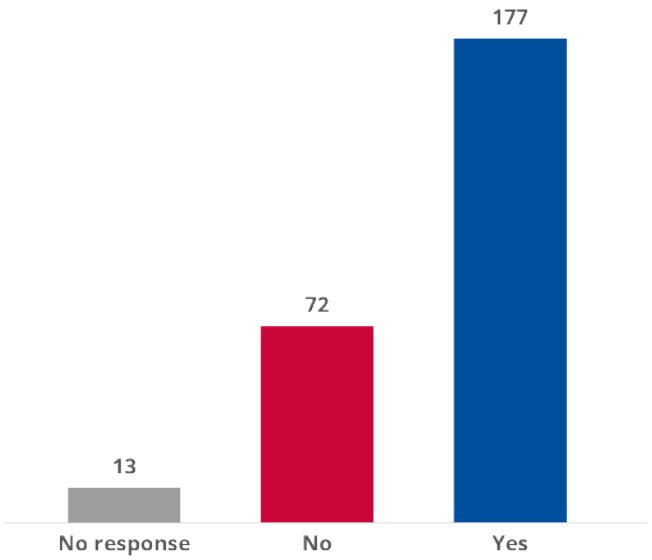
Section II. Risk identification, quantification, priorisation

7. Does your organisation follow a formalised process to identify cyber risk?



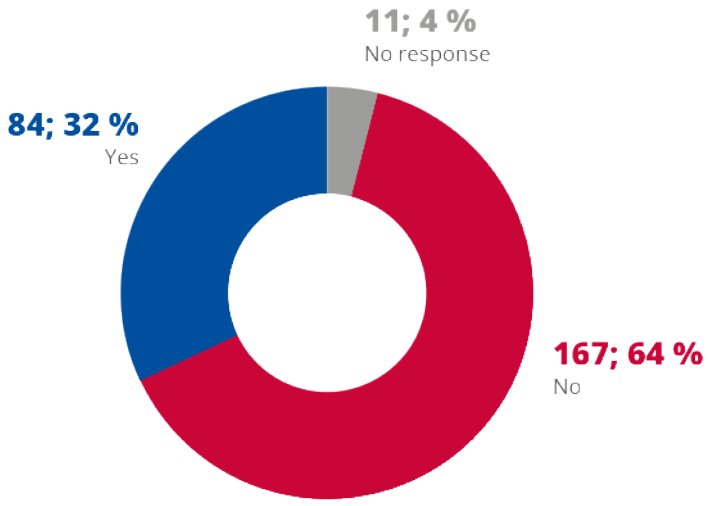
Does your organisation follow a formalised process to identify cyber risk?	Total	%
No response	11	4.2
No	49	18.7
Yes	202	77
Grand total	262	100

8. Does your organisation follow a formalised process to decide which tools should be used to mitigate cyber-risk?



Does your organisation follow a formalised process to decide which tools should be used to mitigate cyber risk?	Total
No response	13
No	72
Yes	177
Grand total	262

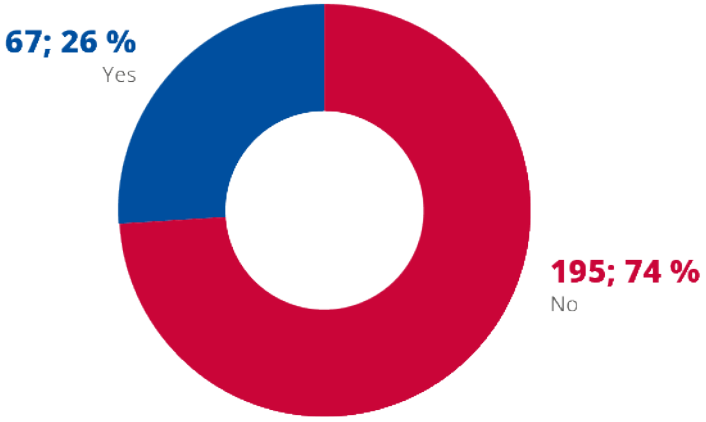
9. Does your organisation quantify cyber risks (in EUR)?



Section III. Identification and selection phase

Orientation, identification, and selection
(Only presented if respondent has cyber insurance: presentation contingent to answer question 10)

10. Does your organisation currently have cyber insurance?



Cyber insurance per region (Question 10 and 2 combined)

Western and northern Europe	Number	Percentage
No	45	55 %
Yes	37	45 %
Grand total	82	100 %

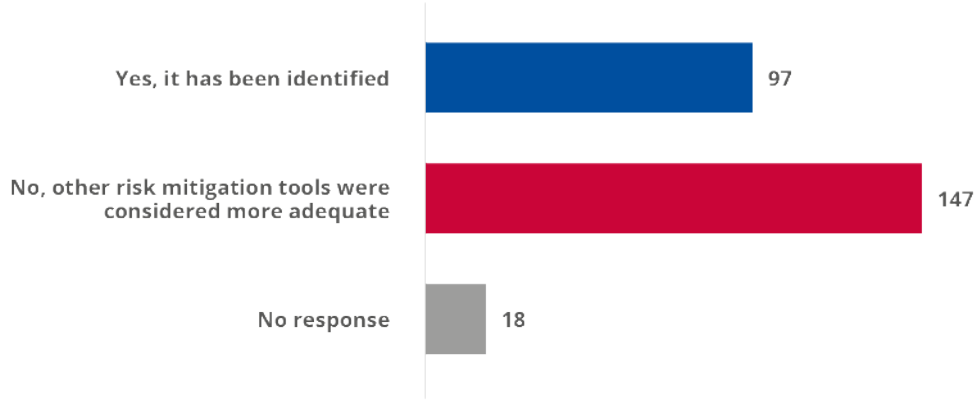
Eastern Europe	Number	Percentage
No	130	88 %
Yes	17	12 %
Grand total	147	100 %

Southern Europe	Number	Percentage
No	20	61 %
Yes	13	39 %
Grand total	33	100 %

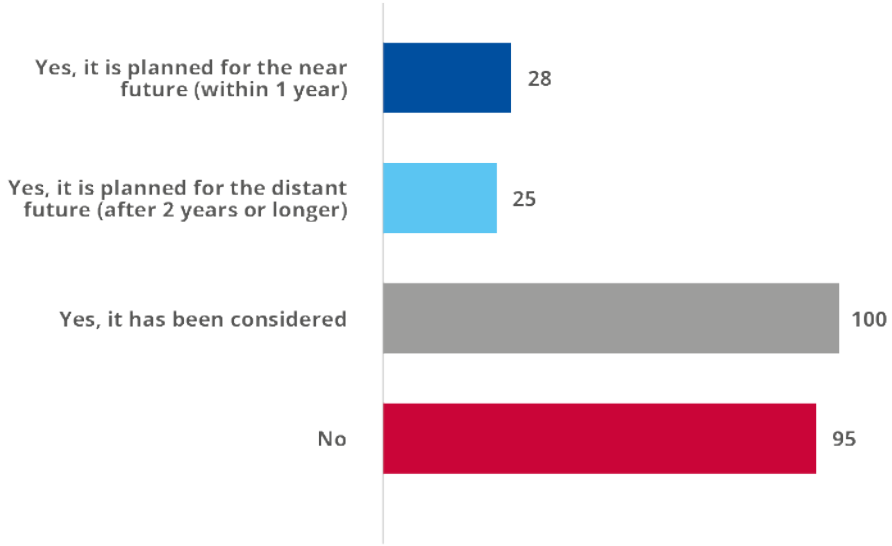
Cyber insurance and cyber risk quantification (Question 10 and 9 combined)

	Does your organisation currently have cyber insurance?		
Does your organisation quantify cyber risks (in EUR)?	No	Yes	Grand total
No response	9	2	11
No	143	24	167
Yes	43	41	84
Grand total	195	67	262

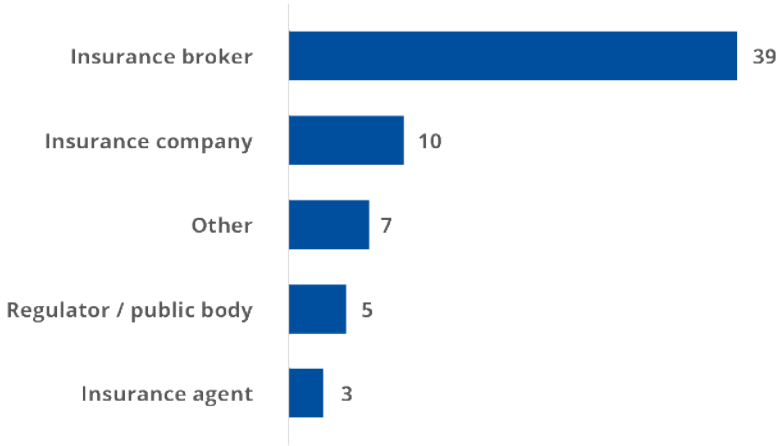
11. Has your organisation identified cyber insurance as a risk-mitigation tool?



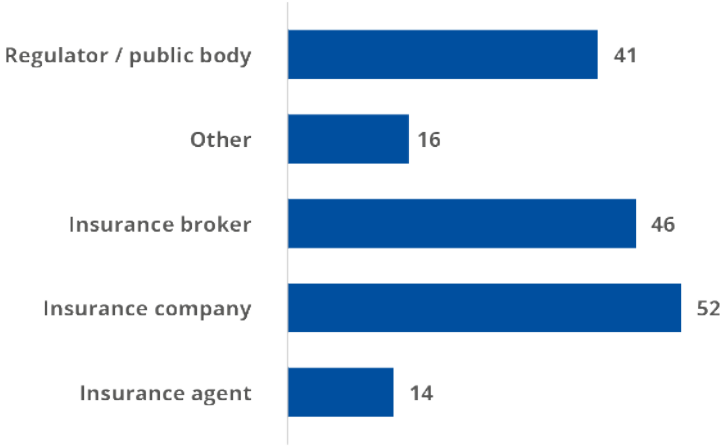
12. Has your organisation evaluated a concrete cyber insurance offer before, or would your organisation consider it in the future?



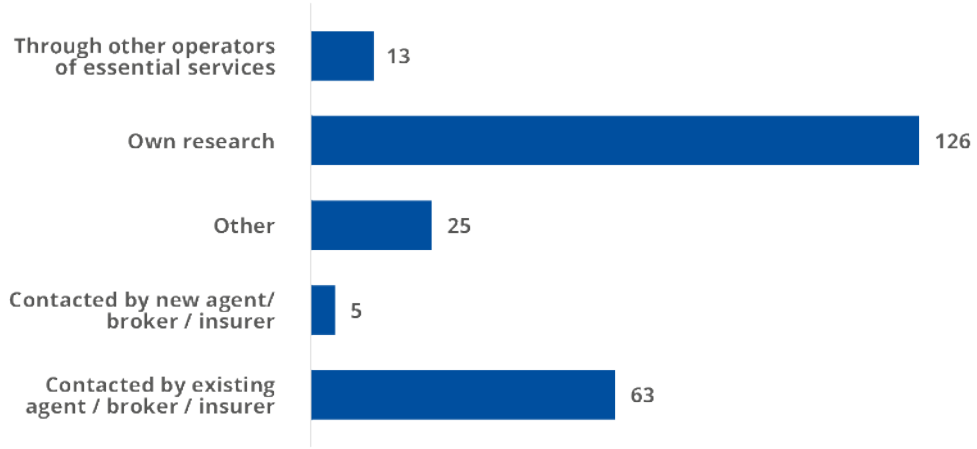
13. Who supports your organisation during the initial orientation and selection process to buy cyber insurance?



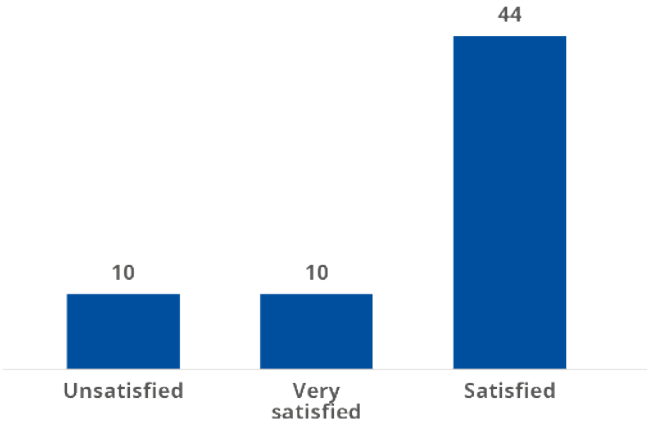
14. Who would support your organisation during the initial orientation and selection process to buy cyber insurance?



15. How did your organisation know about cyber insurance offers?

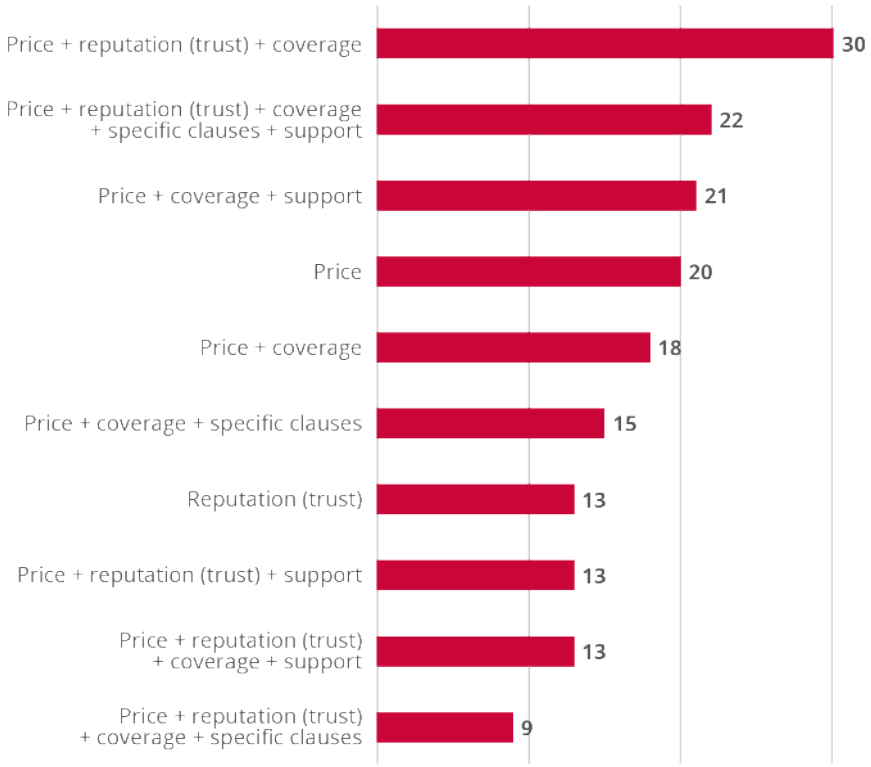


16. How satisfied are you with the offered cyber insurance coverage in respect to your risk exposure?



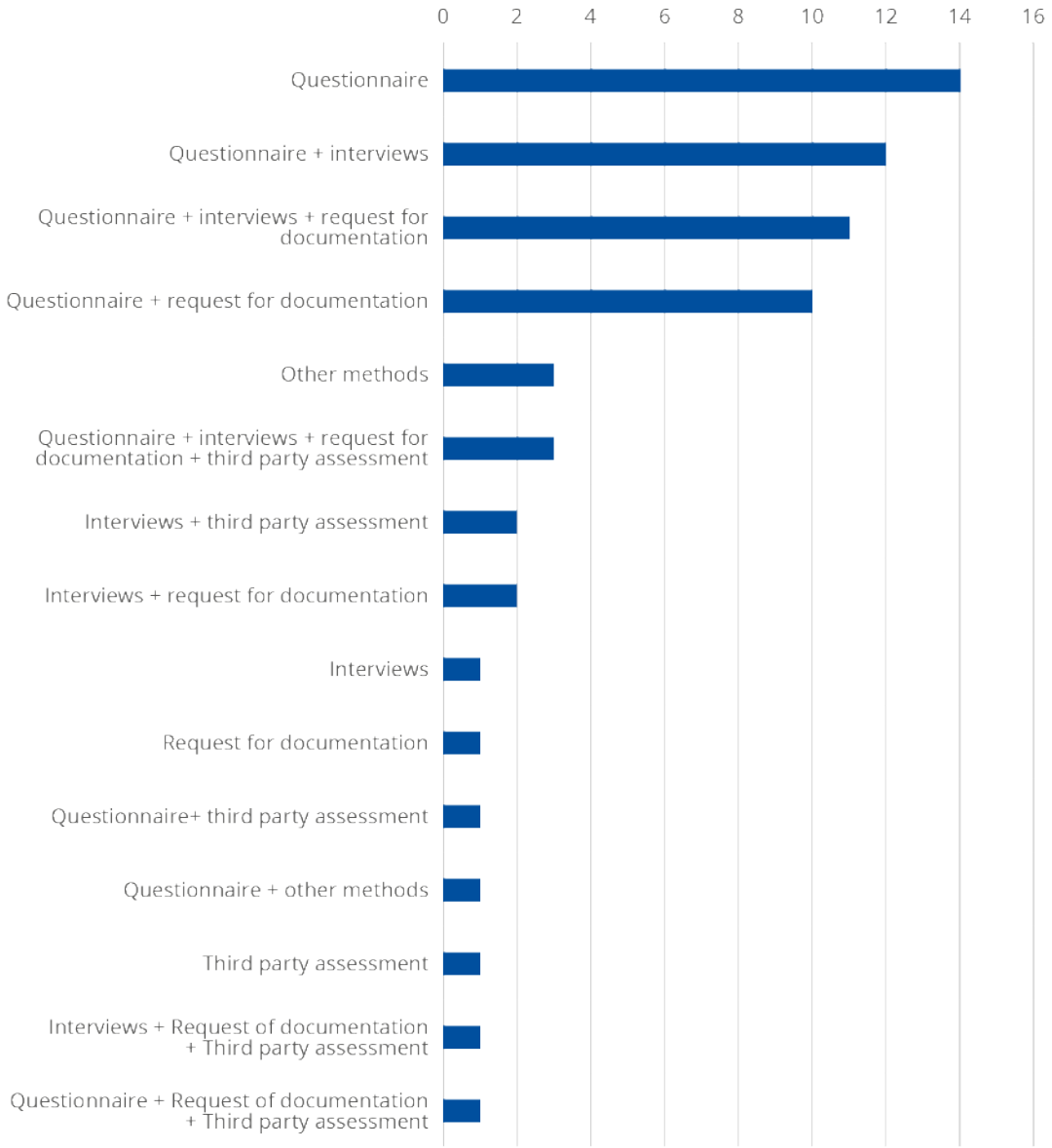
How satisfied are you with the offered cyber insurance coverage with respect to your risk exposure?	Total	percentage
Unsatisfied	10	16 %
Very satisfied	10	16 %
Satisfied	44	69 %
Grand total	64	100 %

17. Which are or which would be the main selection criteria for acquiring cyber insurance services and products by your organisation?

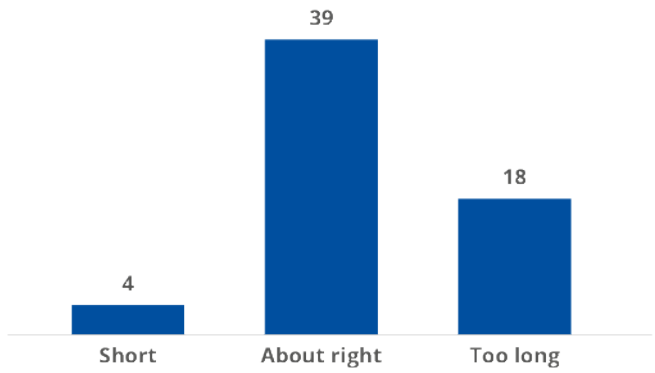


Assessment and acceptance by the insurance company
(Only presented if respondent has cyber insurance)

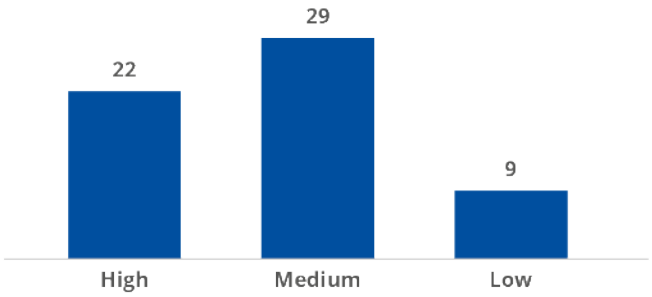
18. How did the insurance company conduct the intake assessment?



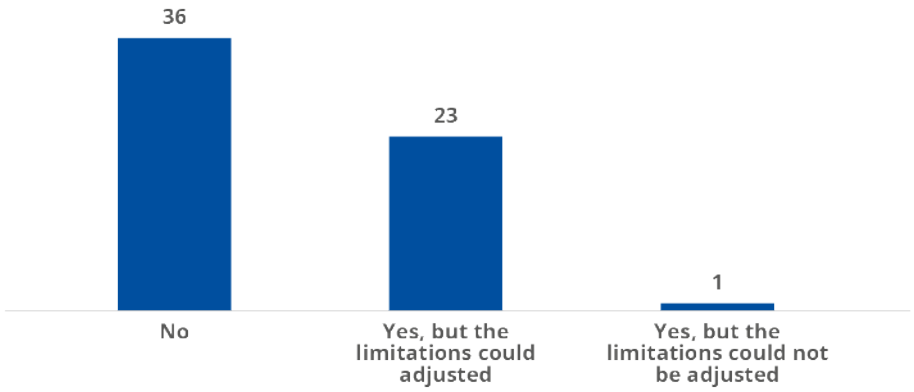
19. How would you rate the duration of the assessment by the insurer?



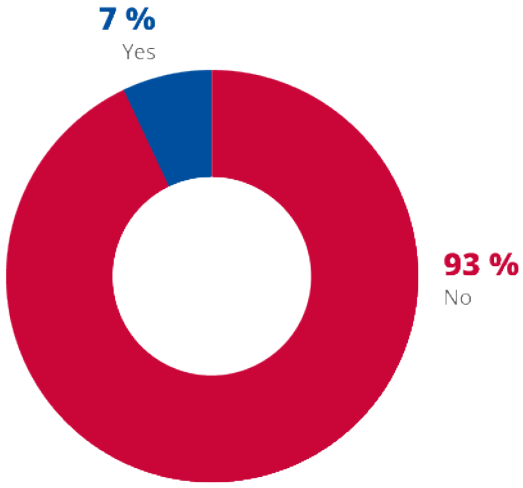
20. How would you rate the effort required during the assessment by the insurer?



21. Has your organisation encountered any legal limitation (e.g. classified or internal documentation) in sharing information with the insurer during the assessment phase?



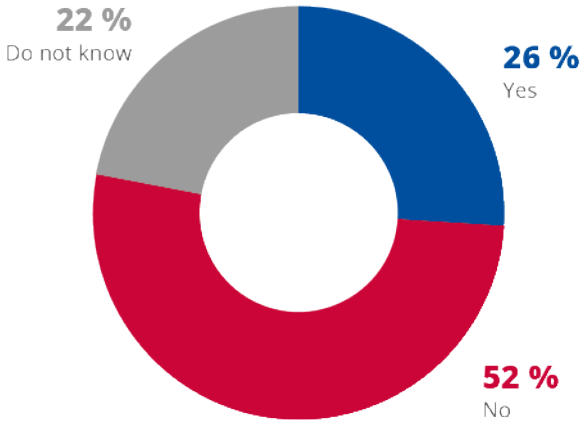
22. Did legal limitations (e.g. classified or internal documentation) in sharing information with the insurer lead to a rejection or modification of the offer by the insurer?



Did legal limitations (e.g. classified or internal documentation) in sharing information with the insurer lead to a rejection or modification of the offer by the insurer?	Total
No	56
Yes	4
Grand total	60

Current situation and coverage
(Only presented if respondent has cyber insurance)

23. Does your organisation have 'insurance' (other than standalone cyber policies or policies with a cyber add-on in place), which might cover damages from a cyber incident, (i.e. not explicitly excluding cyber events?)

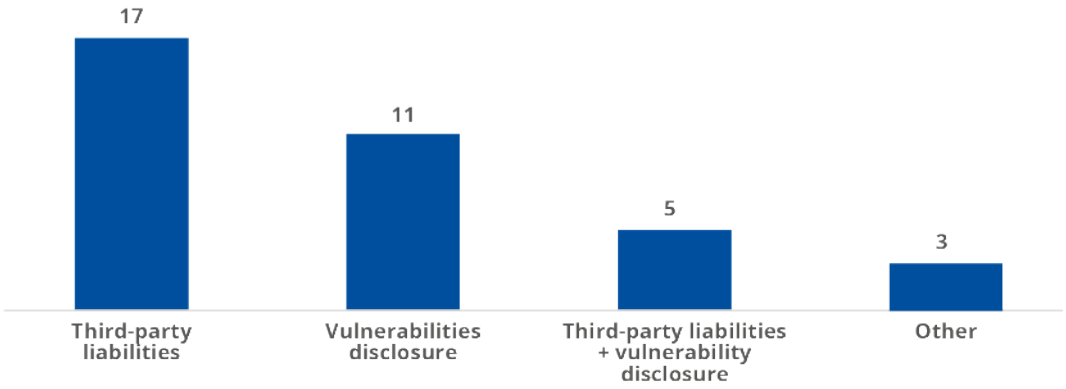


Does your organisation have 'insurance' (other than standalone cyber policies or policies with a cyber add-on in place), which might cover damages from a cyber incident, i.e. by not explicitly excluding cyber events, for example?	Total
Yes	64
No	131
Do not know	54
Grand Total	249

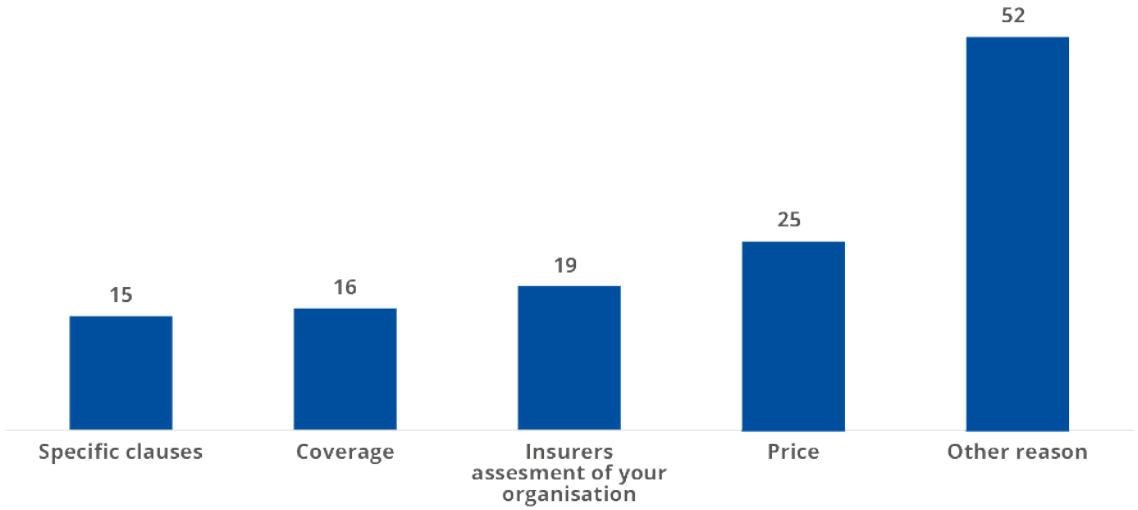
24. If you have cyber insurance, what does it cover?

If you have cyber insurance, what does it cover? (Top 5 responses, N = 57)	Total
(Distributed) denial of service (DDoS) attack; malware; zero-day attack; ransomware; stolen credentials – unauthorised access and use of data assets and computer systems; phishing; network interruption; network interruption OSP (Open Settlement Protocol); network interruption	18
(Distributed) denial of service (DDoS) attack; malware; ransomware; stolen credentials – unauthorised access and use of data assets and computer systems; phishing; network interruption; network interruption OSP (Open Settlement Protocol); network interruption	3
(Distributed) denial of service (DDoS) attack; malware; ransomware; stolen credentials – unauthorised access and use of data assets and computer systems; phishing; network interruption; network interruption: system failure; cyber extortion; data restoration; Extra	2
(Distributed) denial of service (DDoS) attack; malware; ransomware; network interruption; network interruption: system failure; cyber extortion; data restoration; extra expense; administrative investigation and penalties; data protection and cyber liability	2
(Distributed) denial of service (DDoS) attack; malware; zero-day attack; ransomware; stolen credentials – unauthorised access and use of data assets and computer systems; network interruption; network interruption OSP (Open Settlement Protocol); network interruption	2

25. If you have cyber insurance, is there any additional risk you would like to cover which is not included in your current policy?



26. Did you try to get insurance and did not manage? If yes, please indicate the main reason

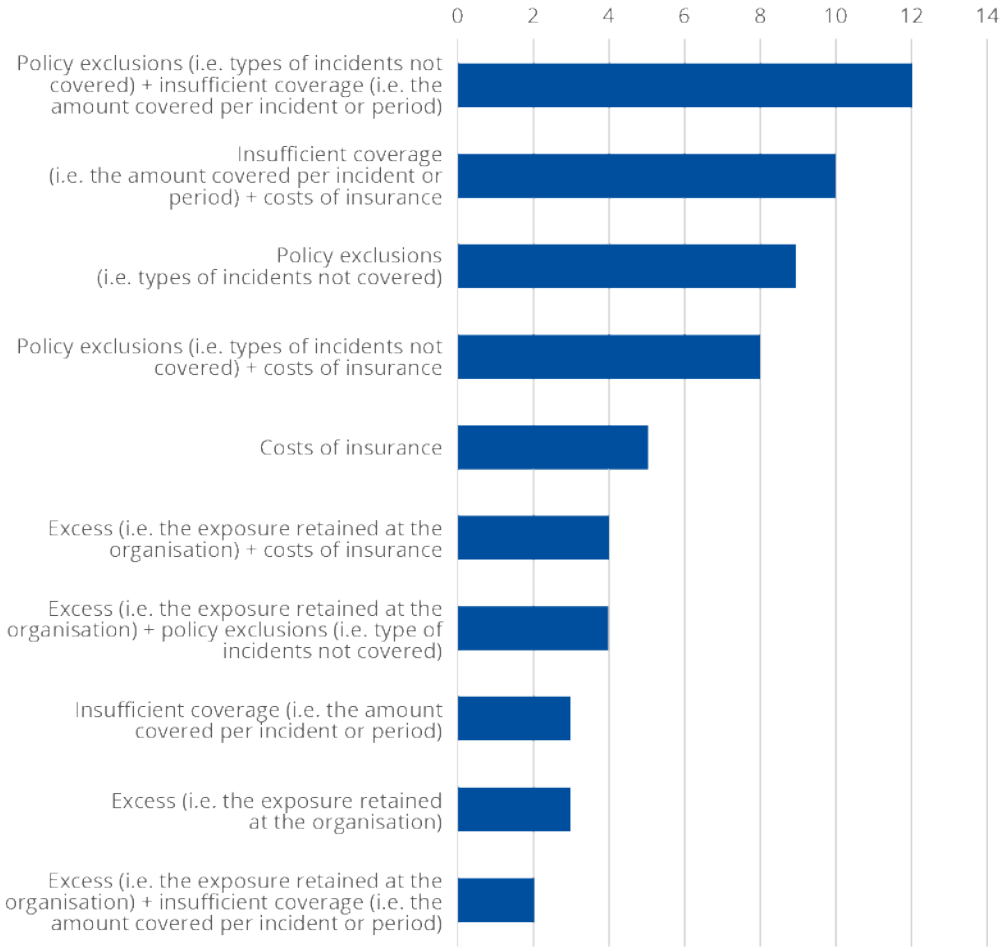


27. If your organisation does not have cyber insurance, what would you consider getting insurance coverage for?

Responses were varied and included: ransomware attacks, reputational damage, business interruption due to a cyberattack, data theft, restore basic services, legal coverage and incident response services, forensics support, etc.

28. What is the main reason for your organisation to purchase cyber insurance?

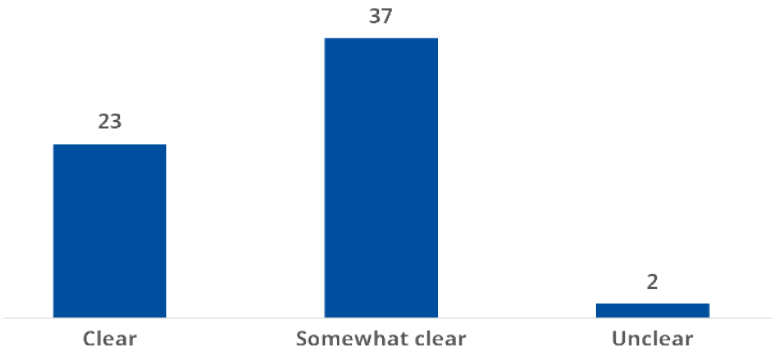
29. What do you see as a major challenge in your cyber insurance policy?



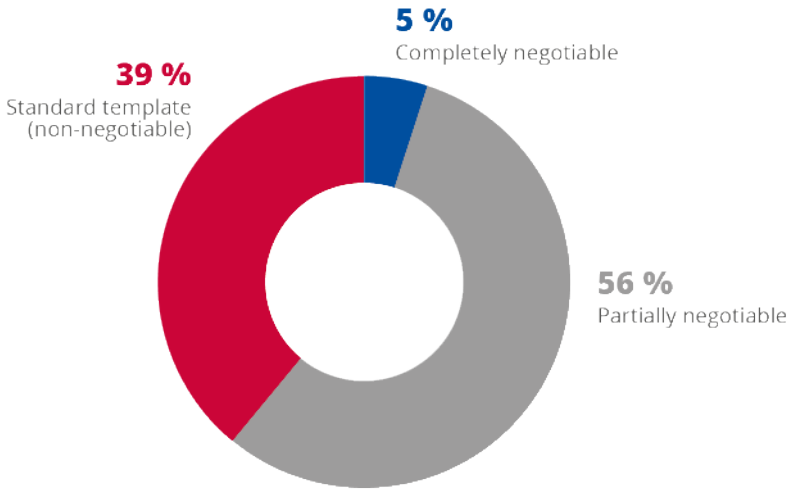
Section IV. Contractual phase

(Only presented if respondent has cyber insurance)

30. Are the contract and its annexes well written and easy to understand?



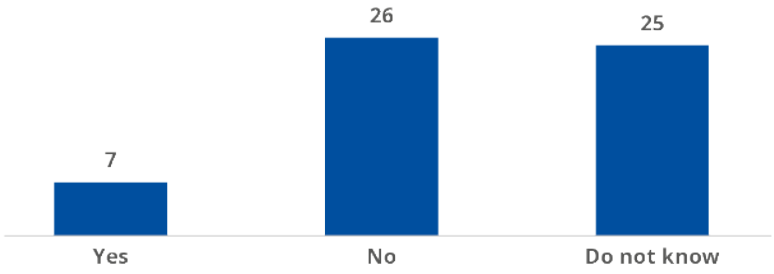
31. To what extent was the contract tailored to your organisation?



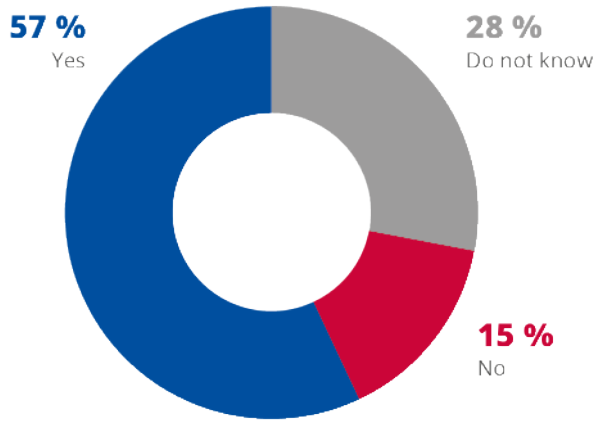
To what extent was the contract tailored to your organisation?	Total
Completely negotiable	3
Partially negotiable	34
Standard template (non-negotiable)	24
Grand total	61

32. Did the existence of certifications (e.g. ISO 27001) have an impact on the contractual agreement?

33. Did the assessment conducted by the insurer result in any exclusions or sub-limits?

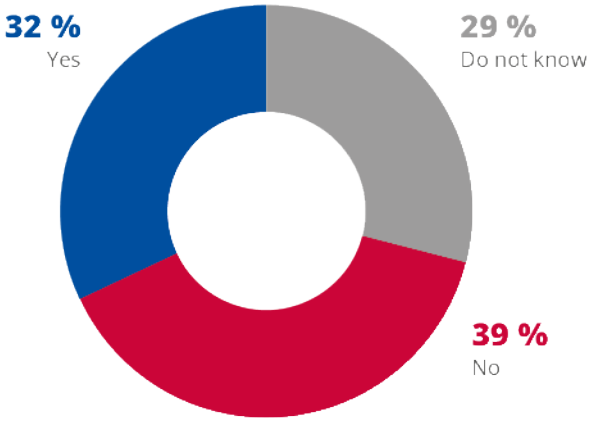


34. When purchasing cyber insurance were you clearly informed about any embedded exclusions and the limitations of the coverage, including for risks arising from a systemic event?



When purchasing cyber insurance were you clearly informed about any embedded exclusions and the limitations of the coverage, including for risks arising from a systemic event?	Total
Do not know	17
No	9
Yes	34
Grand total	60

35. When purchasing cyber insurance were you presented with a list of examples of events that are excluded from the coverage?

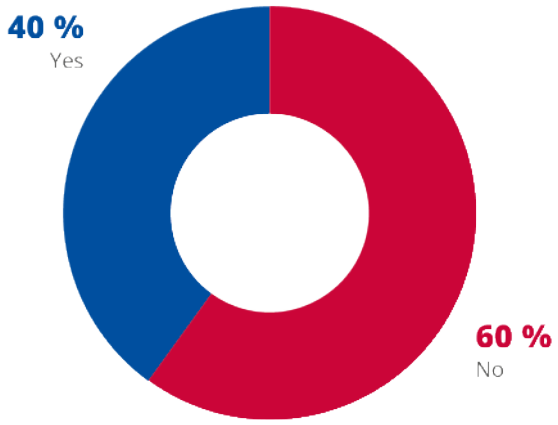


When purchasing cyber insurance were you presented with a list of examples of events that are excluded from the coverage?	Total
Do not know	17
No	23
Yes	19
Grand total	59

Section V. Coverage maintenance and support
(Question only presented if respondent has cyber insurance)

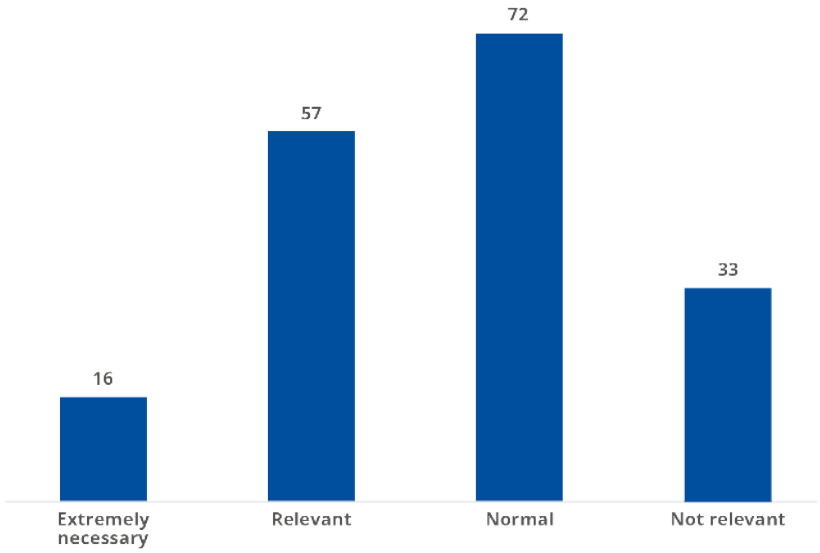
Pre-incident support

36. Did your insurance company provide support in prevention of cyber incidents?



Did your insurance company provide support in prevention of cyber incidents?	Total
No	36
Yes	24
Grand total	60

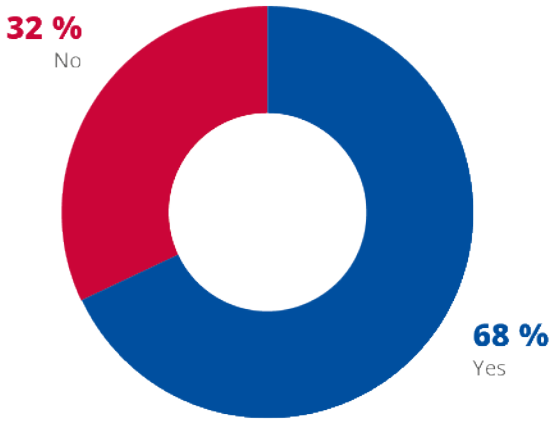
37. If you have yet not acquired cyber insurance, how relevant would this support be for you?



If you have not yet acquired cyber insurance, how relevant would this support be for you?	Total	Percentage
Extremely necessary	16	20
Relevant	57	32
Normal	72	40
Not relevant	33	18.5
Grand total	178	100

Post incident support

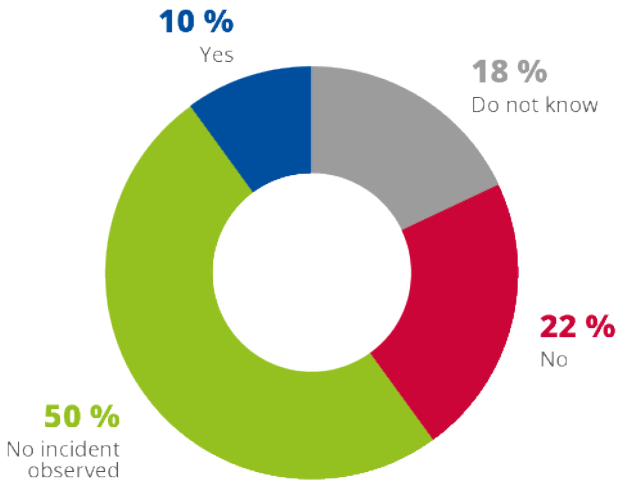
38. Does your cyber insurance company provide incident support?



Does your cyber insurance company provide incident support?	Total
No	19
Yes	40
Grand Total	59

Maintenance

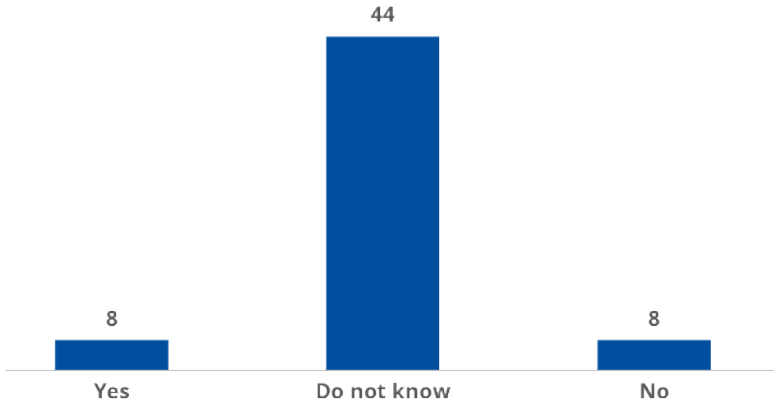
39. Has a cyber incident led to an increase of costs or denial of coverage?



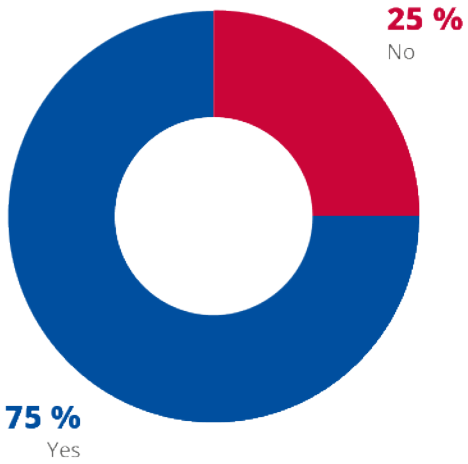
Has a cyber incident led to an increase of costs or denial of coverage?	Total
Do not know	11
No	13
No incident observed	30
Yes	6
Grand Total	60

Section VI. Claim procedure
(Question only presented if respondent has cyber insurance)

40. Has your organisation issued a claim with a cyber insurer?

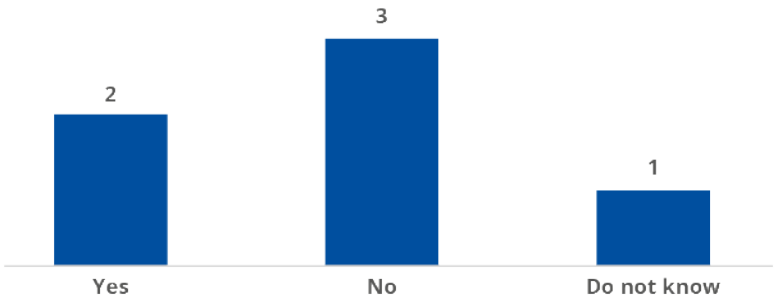


41. Was the claim approved?

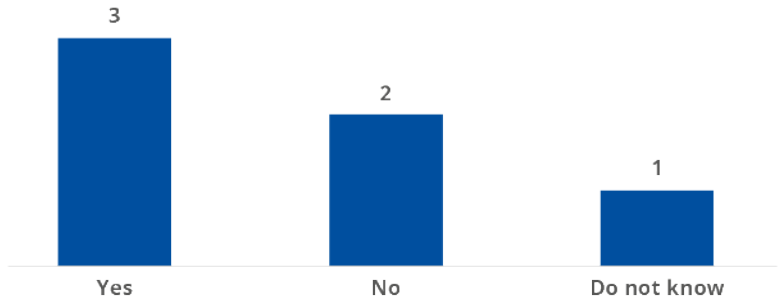


Was the claim approved?	Total
No	2
Yes	6
Grand Total	8

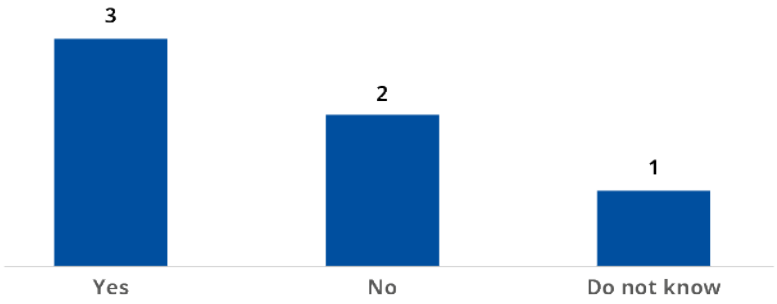
42. Was the reimbursement enough to cover the cost of the damage?



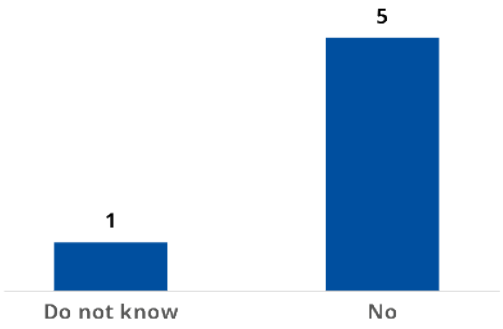
43. Was the claim processed in a timely manner according to the contract?



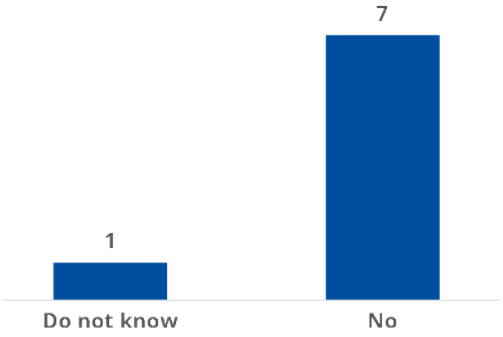
44. Was the methodology to calculate the amount of claim clear?



45. Was the claim followed by a legal dispute because of a disagreement with the insurer?



46. Have you issued a claim with your general insurer due to damages resulting from a cyber incident not covered by cyber standalone policies or policies with cyber add-ons?



47. Was your claim approved? (Following previous question)
No responses given.

Section VII. Respondent opinion

48. In your opinion what type of actions would lead to increased awareness of cyber insurance as a risk mitigation in OESs?
Top 10 responses

In your opinion what type of actions would lead to increased awareness of cyber-insurance as a risk mitigation in OESs?
Communication and dissemination
Communication and dissemination; better coverage
Better coverage
Communication and dissemination; peer-learning exercises; ad hoc collaborative networks
Research and scientific evidence; communication and dissemination
Communication and dissemination; public support; better coverage
Communication and dissemination; peer-learning exercises
Research and scientific evidence; communication and dissemination; peer-learning exercises
Communication and dissemination; peer-learning exercises; better coverage
Research and scientific evidence; peer-learning exercises; better coverages
Research and scientific evidence; communication and dissemination; better coverage
Grand total

49. In your opinion what type of actions would lead to increase purchase of cyber insurance in OESs?
Top 10 responses

In your opinion what type of actions would lead to increased purchase of cyber-insurance in OESs?	Total
Better coverage; fewer exclusions; clearer policy wording	34
Communication and dissemination	24
Communication and dissemination; better coverage; clearer policy wording	19
Better coverage; fewer exclusions	17
Communication and dissemination; better coverage; fewer exclusions	16
Better coverage	15
Communication and dissemination; better coverage	12
Better coverage; clearer policy wording	12
Communication and dissemination; clearer policy wording	12
Clearer policy wording	9
Grand total	170

50. In your opinion, what are the most relevant skills needed in your organisation at the time of acquiring an adequate cyber insurance coverage?
Top 10 responses

In your opinion, what are the most relevant skills needed in your organisation at the time of acquiring an adequate cyber-insurance coverage?	Total
Risk assessment; legislation; information management	40
Risk assessment	32
Risk assessment; functioning of the insurance market; legislation	25
Risk assessment; legislation	22
Risk assessment; information management	22
Risk assessment; functioning of the insurance market; information management	18
Risk assessment; data mining and analysis; information management	17
Risk assessment; functioning of the insurance market	12
Risk assessment; legislation; data mining and analysis	8
Information management	7
Grand total	203

TP-04-22-095-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 978-92-9204-586-9
doi: 10.2824/94949