Commonality of risk assessment language in cyber insurance

Recommendations on Cyber Insurance

NOVEMBER 2017

www.enisa.europa.eu European Union Agency For Network and Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and EU citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For queries in relation to this paper, please use CyberInsurance@enisa.europa.eu
For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

For providing valuable information that helped shape the report (in alphabetical order):

Hans Allnut, Head of Cyber & Data Risk, DAC Beachcroft
Mark Bannon, Head of Cyber Liability, EMEA, Zurich
Mark Camillo, Head of Cyber, EMEA, AIG
Marie Louise Den Otter LLM, Sr. Underwriter Financial Lines at Allianz Global Corporate & Specialty, Allianz
Nils Hellberg, Head of Liability, Credit, Marine, Aviation, Accident and Legal Expenses Insurance, Assistance, Statistics, German Insurance Association
Xavier Marguinaud, Underwriting Manager - Cyber, Tokio Marine HCC
Jan Mori, Deputy Head of Professional Lines Europe , ArgoGlobal SE
Graeme Newman, Chief Innovation Officer, CFC
Joyce Peters, Product & Proposition Manager, MS Amlin
Scott Sayce, Global Head of Cyber - AXA Global P&C and Global Chief Underwriting Officer of Cyber - Axa Corporate Solutions
James Tuplin, Head of Cyber & TMT, International Financial Lines, XL Catlin
Erik van der Heijden, Senior Risk Engineer, If P&C Insurance
Christos Vidakis, Principal, Deloitte
David Warr, Underwriter – TMT & Cyber, QBE
Matthew Webb, Cyber Chief Underwriting Officer & Line Underwriter, Hiscox
Joppe Willeboordse, Senior Underwriter Casualty - Cyber at HDI Global SE, HDI
Erik Wolper, Underwriting Manager Financial Lines Benelux, XL Catlin

ISBN 978-92-9204-228-8, DOI 10.2824/691163

Table of Contents

Executive Summary

The cyber insurance market is growing rapidly and it is expected to further expand by the adoption of the GDPR and the NIS Directive which will incentivise organisations falling under their provisions to seek ways of residual risk transfer. As the EU cyber insurance market is still at its early development stages, with the exception of the more mature UK market, significant steps need to be taken towards its maturation if the EU economy is to reap the benefits of this emerging segment.

The industry perceives the lack of commonality in risk assessment language as both an indicator of market immaturity and as an obstacle to the market's growth. This is thought to be an inherent consequence of the changing nature and dynamics of cyber risk exposures. This lack of harmonisation, evident in various aspects of insurance – from coverage to underwriting questionnaires – reduces consumer trust and understanding of these products (especially for SMEs), creates difficulties for insurance carriers seeking to enter the market and limits the growth rate of cyber insurance adoption overall. The broad consensus in the industry is that steps towards harmonisation / standardisation will have significant benefits for all stakeholders involved and for the insurance market as a whole.

Moreover, the resulting increased adoption of cyber insurance would prepare the market to respond more effectively to large-scale incidents such as WannaCry and NotPetya and support the economic sustainability of organisations affected by similar major incidents.

However, while some initiatives have started to take form, the industry has yet to make significant steps towards harmonisation for a variety of reasons. **Competitive advantage**, **lack of incident and claims data**, **reluctance to share data**, **lack of generally accepted standards**, **insufficient in-house skills**, **lack of guidance**, **lack of legislation**, **market immaturity** and the **complexity of cyber insurance products and cyber risks overall**, all act as barriers towards language harmonisation. However, the industry stakeholders have enough incentives to achieve a higher level of language convergence as everyone stands to gain from it. The main drivers that are expected to act as catalysts behind the language harmonisation are:

- the adoption of **Regulations and Standards** that will provide the common framework on which to build harmonized terminology and offerings;
- the increasing **Availability of Data** which will allow better understanding and modelling of cyber risks;
- the **Evolution of the Demand Side** which will create the need for more standardised and easily comparable products;
- the overall **Market Maturation** which will naturally resolve a number of market frictions.

This report proposes two sets of recommendations, one towards the **industry** itself and one towards **policy makers** in order to support this evolution towards language harmonisation without stifling innovation. Specifically, the industry is encouraged to **standardise policy language and underwriting questionnaires**, **promote data sharing** between the stakeholders, **develop industry standards**, **build in-house expertise in cyber security**, contribute to the **collection of data on aggregated loss scenarios**, **build offerings around information security and privacy regulations**, adopt a **sectorial approach in harmonising language**, **address the needs of the SME market** and **improve overall data quality** by integrating various heterogeneous sources. EU and Member States Policy Makers are encouraged to **create minimum coverage requirements**, **leverage the upcoming mandatory incident reporting schemes** via the NIS Directive and the GDPR to produce meaningful data, **create a central EU repository** of incident data, **raise awareness** to increase demand and buyer maturity and **develop guidelines for cyber insurance**.

1. Introduction

1.1 Overview

Cyber insurance was created to address residual cyber risk. With the **General Data Protection Regulation** (**GDPR**)[1] being adopted in April of 2016, and the **Directive on Network and Information Security** (**NIS Directive**)[2] in July 2016 and coming into force in May 2018, the need for cyber insurance is anticipated to grow; a growth that can be embraced by enabling an informative product development and adoption.

To promote the adoption of cyber insurance, ENISA published a study in November of 2016[3] aiming to raise awareness for the most impactful market advances by identifying the most significant cyber insurance developments for the past four years, and to capture the good practices and challenges during the early stages of cyber insurance lifecycle. In this context, ENISA conducted a mapping of the common pieces of information that insurers use in order to carry out risk assessment before they issue a policy.

However, in spite of the significant overlap in topics examined as part of the insurance companies' risk assessment, the respective risk assessment language (i.e. the questions actually posed to prospective customers to assess their relevant risk status) is not yet harmonised across the industry for various reasons; a lack of harmonisation that also extends to coverage-related aspects. This fact is not in line with other facets of insurance (e.g. car insurance), thereby potentially reducing the appeal of cyber insurance products for customers and limiting the possibility of added-value offerings on top of more-or-less standardised products. The lack of a common risk assessment language may also affect the opportunities and prospect of insurance companies currently in the process of entering the market.

1.2 Scope and Objectives

While several risk assessment languages and frameworks exist, the industry has yet to take steps in the direction of harmonisation. This report aims at further investigating this issue by identifying the incentives and barriers for adopting a common framework and to propose recommendations towards the cyber insurance industry and EU policy makers to promote this harmonisation.

In terms of analysing the commonality of Risk Assessment Language, the focus of this report is on two specific use cases:

- Language used by insurance companies as part of their **information collecting process**, i.e. the questions asked to customers in order to feed a risk assessment process with information;
- Language used by insurance companies to define **insurance coverage**, i.e. what each coverage type addresses and/or includes.

While the focus of the study is in the EU cyber insurance market – and only the respective regulatory framework is considered - stakeholder engagement included industry representatives from non-EU countries as well, in order to benefit from the expertise of more mature markets.

[1] http://ec.europa.eu/justice/data-protection/reform/index_en.htm
[2] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
[3] https://www.enisa.europa.eu/news/enisa-news/cyber-insurance-a-look-at-recent-advances-good-practices-and-challenges-by-enisa

The scope of the analysis additionally included:

- Existing risk assessment language frameworks and how they compare to each other
- Current industry practices in terms of risk assessment language
- Evolution/trends of risk assessment language over the last years with a focus on points of convergence
- Documentation of the incentives for and barriers against adopting a harmonized framework in terms of risk assessment language from the insurance companies' perspective
- Any challenges deriving from the lack of a common framework from the consumer perspective

This report aims at providing a comprehensive analysis on the factors that influence the harmonization – or lack thereof – of risk assessment language in cyber insurance, its practical impact on the growth prospects of cyber insurance market and to understand the trends going forward. In order for the EU to benefit from this rapidly growing market segment, it is paramount to assist the cyber insurance market maturity and increase its adoption. Particularly at the stage where the evolution of the cyber threat landscape and the introduction of cyber security-related regulations is expected to increase the need of many organisations for cyber risk transfer.

Hence, a key objective of this report is to propose recommendations to European Commission policy makers and insurance companies, to promote the adoption of a common risk assessment language framework for cyber insurance.

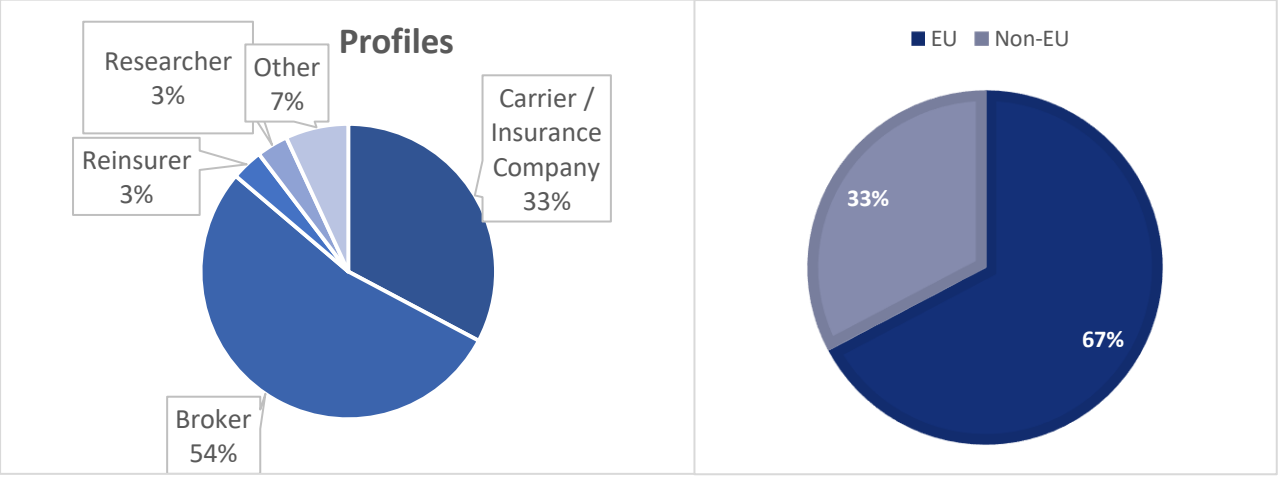
1.3 Methodology

This report was developed using information deriving from the following streams:

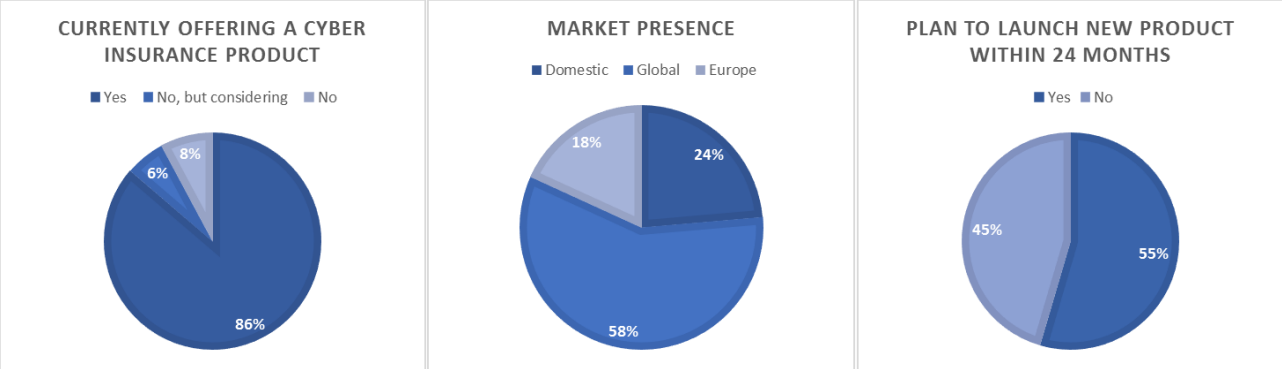
- Desk research;
- Commercial documents available at the time of writing; such as underwriting questionnaires and insurance policy documents;
- Direct industry stakeholder engagement via interviews and an online survey;

For the collection of the most pertinent feedback from industry stakeholders, both the interviews and the online survey were addressed to people within the cyber insurance industry who are either directly using or are developing a risk assessment language, such as **insurance companies/carriers**, **reinsurers** and **brokers**.

Most information was collected by a series of **19 in-depth, non-attributable structured interviews** with representatives of the aforementioned stakeholder groups. An **online survey** was also published, which resulted in the collection of feedback from an additional **39 respondents**. The information was gathered under condition of anonymization and non-individualised disclosure, which encouraged full and frank exchange of views and expert opinions. The key demographics of the entire panel are depicted in the following graphs:



With respect to those profiles directly involved in developing and/or selling cyber insurance products, such as carriers, brokers etc. the additional following panel demographics are also of relevance[4]:



Throughout the report, statistical analyses were conducted using the **ANOVA** methodology[5]. The one-way ANOVA is used to determine whether or not three or more independent (unrelated) groups of interest are statistically significantly different from each other. The one-way ANOVA was applied to various data groups analysed for this report (underwriting questionnaires, standards, policies etc.) to assess whether or not these groups were in fact correlated. The methodology is extensively used in scientific research, not excluding research on cyber security when a group comparison is made. A more comprehensive explanation including results is presented in more detail in Annex A: ANOVA Methodology and sample statistical analysis.

[4] **Note:** All panel members representing carriers / insurance companies stated that they actually plan to launch a new cyber insurance product over the next 24 months.

[5] Analysis of variance (ANOVA) is a collection of statistical models used to analyse the differences among group means and their associated procedures (such as "variation" among and between groups). In its simplest form, ANOVA provides a statistical test of whether or not the means of several groups are equal. ANOVAs are useful for comparing (testing) three or more means (groups or variables) for statistical significance.

1.4 Target Audience

The target audience of this study is primarily **cyber insurance industry stakeholders** that are using or developing risk assessment languages, such as **insurance carrier executives**, **underwriters**, **brokers**, **reinsurers** etc. The aim is to help them understand:

- The current status and evolving dynamics of the market in terms of harmonization of risk assessment languages;
- The convergence achieved so far and the main benefits of harmonization;
- Incentives towards and barriers against harmonization;
- The drivers of harmonization and ways of achieving it.

Moreover, this document is addressed to **policy makers** with the aim of helping them understand the cyber insurance market specificities, the benefits of the market maturing towards a harmonized risk assessment language approach and the ways the regulatory landscape can support this maturation process without hindering innovation in the domain.

This document may be of further interest to **researchers** active in the cyber insurance domain and to **carriers considering entering the market** with a new cyber insurance product.

1.5 Structure

The rest of this report is structured as follows:

- **Chapter 2** gives an overview of the cyber insurance market building blocks, including the underwriting methods and coverage types
- **Chapter 3** presents the main elements influencing the risk assessment language, i.e. standards, coverage types and underwriting questionnaires and analyses their harmonisation based on a sample of policies and questionnaires
- **Chapter 4** presents current industry practices in terms of coverage and underwriting methods based mainly on interview feedback and links them to language harmonisation
- **Chapter 5** provides an analysis of market dynamics towards market maturity and language harmonisation including incentive, barriers and key drivers
- **Chapter 6** provides two sets of recommendations, one towards the industry and one towards policy makers

2. Overview of the cyber insurance market

2.1 Cyber insurance and corporate risk management

Cyber risk is no longer considered an emerging risk. In fact, a recent Ponemon survey[6] ranked cyber risk as a Top-5 global risk[7], and at the same time, organizations have started considering the impact of cyber exposures on the financial statements. These may range from a successful cyber-attack highlighting the IT system or human weaknesses of an attacked company to completely shutting down company operations, stolen data sold on the dark web and major financial losses suffered by both the company and the company's customers.

Insurance is a means of loss protection and a form of risk management primarily used to hedge against the risk of a contingent and uncertain loss. Cyber insurance is an insurance product used to protect businesses (and individual users) from Internet-based risks, and more generally from risks relating to information technology infrastructure and activities. Risks of this nature are often excluded from traditional commercial general liability policies or are not specifically defined in traditional insurance products. Coverage provided by cyber insurance policies may include:

- **first-party coverage** against losses such as data destruction, extortion, theft, hacking, and denial of service attacks;
- liability coverage indemnifying companies for losses to others caused (**third-party coverage**), for example, by errors and omissions, failure to safeguard data, or defamation;
- **other benefits** including regular security-audit, post-incident public relations and investigative expenses, and criminal reward funds.

Corporate cyber security and privacy risk management becomes even more complicated due to a number of external factors that can be perceived as forms of market failures[8], including market failures related to infrastructure (e.g. networks) and asymmetric information[9] (e.g. identifying reliable market partners) or internal factors related to personal behaviour (e.g. privacy salience). Risk are mitigated more effectively where these underlying factors and risk drivers are well identified and managed.

2.2 Cyber threat landscape and its impact on cyber insurance

The transition of cyber threats to becoming key global risks is evident on a daily basis. The evolution of the cyber threat landscape is documented[10] and shows that high-impact cyber-attacks are becoming more and more prevalent in the daily news. On June 27, 2017, a widespread cyber-attack referred to by various names but most commonly including Petya or NotPetya[11], began impacting computer systems around the world. Similar and slightly preceding that, was the WannaCry[12] ransomware attack, where victims were

[6] http://www.aon.com/risk-services/thought-leadership/2017-global-cyber-risk-transfer-comparison-report.jsp?utm_source=StrozFriedberg&utm_medium=website&utm_campaign=ponemonglobalcyberrisk2017
[7] http://www.aon.com/risk-services/thought-leadership/2017-global-cyber-risk-transfer-comparison-report.jsp?utm_source=StrozFriedberg&utm_medium=website&utm_campaign=ponemonglobalcyberrisk2017
[8] https://www.cpb.nl/sites/default/files/publicaties/download/ad-kox-straathof-economic-aspects-internet-security.pdf
[9] https://www.scmagazineuk.com/industrys-cyber-security-market-failure-must-be-addressed/article/530970/
[10] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape
[11] https://www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware/
[12] https://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware

asked to pay a ransom of 300$ in bitcoin. According to new research from Lloyd's of London[13], released on June 28, 2017, organizations could face a much higher bill than they could expect or are prepared for, after falling victim of a cyber-attack like this – especially if aggregated losses influence reinsurance coverage and pricing. Inga Beale, CEO of Lloyd's, said[14]:

"*The reputational fallout from a cyber breach is what kills modern businesses. And in a world where the threat from cyber-crime is when, not if, the idea of simply hoping it won't happen to you, isn't tenable. To protect themselves businesses should spend time understanding what specific threats they may be exposed to and speak to experts who can help handle a breach, minimize reputational harm and arrange cyber insurance to ensure that the risks are adequately covered. By reacting swiftly to mitigate the impact of a cyber breach once it has occurred, companies will be able to minimize the immediate costs and their exposure to subsequent slow burn costs*."

The Lloyds of London report is apt, considering that some of the world's largest companies were hit by this latest attack, which significantly impacted availability.

The **Cyber Risk & Insurance Forum** (**CRIF**)[15] has analysed these and other cyber threats and impacts across multiple industries in a way similar to the method applied in this report. The CRIF matrix[16] lists several different (insurable) threats and impacts, and ranks these on their level of risk. A quick glance at the matrix illustrates that the **cyber risks associated with different industries differ quite a lot for both threats and impact**.

For some industries, certain cyber threats may form a high risk, while for other industries they do not. A Distributed Denial of Service (DDoS) attack, for example, is a high risk for Retailers and Financial Service Providers, while Non-Profits have a low risk of being attacked. The same can be said about the impact that cyber risks have. For instance, a Regulatory Investigation/Fine may have a high impact for the Professional and Financial service sector, while being a low risk for the Transport & Logistics sector.

These differences in threats and impacts indicate that it could be beneficial for both cyber insurance insurers and applicants to obtain **industry/sector-specific cyber coverage**. In fact, during the market consultation for this report it became clear that multiple insurers are working on **industry-specific wordings**. The matrix from CRIF indicates that this is not only to make the wording easier to understand for clients from a specific industry, but that some industries have different cyber threats and impact, as opposed to others. Specific industry coverages could be therefore beneficial for a more rapid uptake of cyber insurance.

However, these specific industry cyber coverages would still need to be harmonized to have a positive effect; without that being the case, it could lead to more confusion for buyers. The same can be said for the risk assessment, where it is likely to be beneficial to differentiate per industry for both buyer and supplier.

[13] https://www.lloyds.com/lloyds/about-us/what-do-we-insure/what-lloyds-insures/cyber/cyber-risk-insight/closing-the-gap
[14] https://www.lloyds.com/news-and-insight/press-centre/press-releases/2017/06/cyber-report-launch
[15] http://www.cyberriskinsuranceforum.com/
[16] http://www.cyberriskinsuranceforum.com/sites/default/files/pictures/CRIF%20EventImpact%20Chart_0.pdf

2.3 Underwriting methods

Underwriting is an important function performed each time an insurance application is made. Its purpose is to determine if an application represents acceptable risk to the insurer. If the underwriting information does not provide sufficient risk information, an insurer will generally decide to not issue a policy to an applicant. Underwriting is based on a variety of criteria established by each insurer, and regulated by state and federal law.

Some of the application factors that typically influence a cyber insurance offering are:

- **Combination with existing coverage:** Stand-alone vs combined coverage
- **Insurance policy design and implementation:** Open-broked[17] vs Pre-negotiated
- **Limits and sub-limits:** Primary layers vs Excess layers
- **Client relationship:** New Client applications vs Existing Clients
- **Coverage and services:** Role and type of loss adjuster panels
- **Placements and capacity:** Involvement of the reinsurance market

In practice, these underwriting methods are some of the primary points where risk assessment language is used; in this context, its use involves the drafting of specific questions to collect risk assessment information.

The most prevalent way in which a cyber-insurer collects information from potential customers is through a questionnaire. These questionnaires are furnished by the insurers or carriers to the applicant, and consist of a set of questions related to the use of information technology and information assets. These questions are used by the carrier to solicit a comprehensive understanding of the overall security profile of the applicant – or to get at least a reasonable approximation thereof. They are a critical mechanism used to assess a customer's cyber security posture, and thereby offer the opportunity to differentiate risks across applicants. For the purpose of this study ENISA has gathered and assessed **underwriting questionnaires from ten of the leading carriers**.

Each underwriting decision involves a balancing between the insurer's desire to earn the premium (or client retention, market share) with their ability to cover claims. This decision is supported by risk information, i.e. underwriting information. The type of risk assessment performed by carriers throughout the underwriting process comprises of one or more of the following types of information:

- underwriting questionnaire – both short form (max two pages) and long form (more than two pages)
- client meeting (i.e. underwriting meeting, mostly with risk engineers)
- desk research
- threat intelligence and/or open source intelligence (OSINT)
- risk audit or risk reports

The underwriting information ultimately shapes the final offer to the applicant (premium, conditions, exclusions etc.).

There is even underwriting risk, which generally refers to the risk of loss on underwriting. This may either arise from an inaccurate risk assessment or from factors wholly out of the underwriter's control. As a result, the policy may cost the insurer much more than it has earned in premiums.

[17] For reference purposes: https://www.lloyds.com/common/help/glossary?Letter=P

2.4 Cyber insurance coverage types

Information Technology (IT) infrastructure risks are typically excluded from traditional commercial general liability policies, or are not specifically defined in traditional insurance products. The respective risk transfer typically falls within the scope of cyber insurance coverage.

Desk research and stakeholder engagement conducted within the context of this study revealed that cyber insurance coverage types can generally be classified in one of the following 3 categories:

- **First party loss** coverage, i.e. coverage against direct losses incurred by the insured, mostly consist of business interruption and cost associated with mitigating a cybersecurity event
- **Third party loss** coverage, i.e. liability coverage indemnifying companies for losses to others
- **Other benefits**, i.e. related to assorted costs and services

This study has found that cyber insurance generally consists of the following coverage components for each of these categories, as depicted in Figure 1. Henceforth, this coverage type taxonomy is used for all analysis purposes in the document.

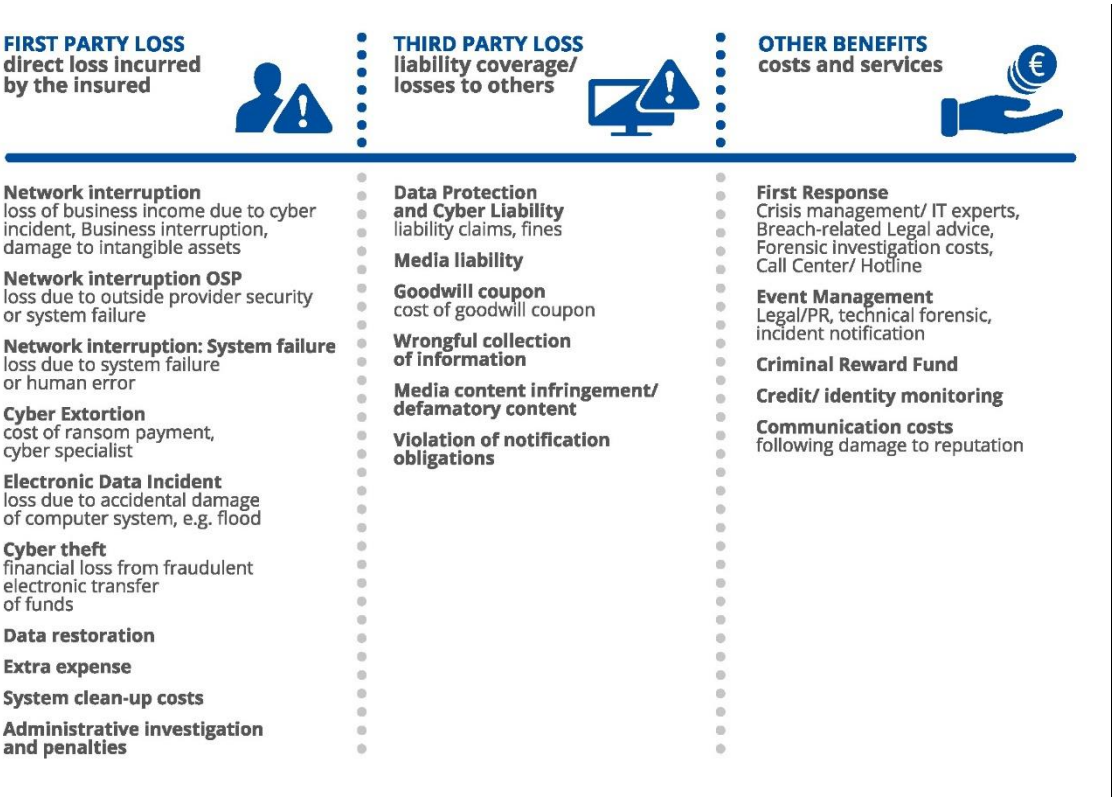


Figure 1: Proposed taxonomy of general cyber insurance coverage components

When it comes to language commonality with respect to cyber insurance coverage, harmonization refers to the extent that different carriers define the scope of the aforementioned coverage types in the same way. Insurance markets more mature than cyber have actually achieved this, making the different insurance products directly comparable and allowing innovation to focus on pricing models or on added value offerings on top of more-or-less standardized products. Moreover, the use of a consistent

terminology to define coverage types typically increases consumer trust in the insurance product[18], while the use of proprietary terms may lead to buyer misconceptions.

A 2015 study[19] revealed that misconceptions around cyber insurance are wide spread. Even today some organisations think cyber insurance has too many exclusions, or is too new, unproven or specialised, while there is also a perception that quotations require a lot of time. These perceptions are rarely challenged and organisations continue to rely on self-insurance. While IT systems focused cover has been available for more than 25 years, cyber cover is fairly new and developing. Getting an indication of price and exact coverage is relatively easy nowadays. Furthermore, many aspects that organisations do not expect to be covered (e.g. human error, third party incidents, system failures and notification costs to victims) are often included in cyber insurance policies, or can certainly be negotiated with insurers. With a tangible proposal that can be discussed at board level, organisations can make more deliberate and informed decisions about cyber insurance, rather than leaving it "out of sight, out of mind". This perception is depicted in Figure 2.

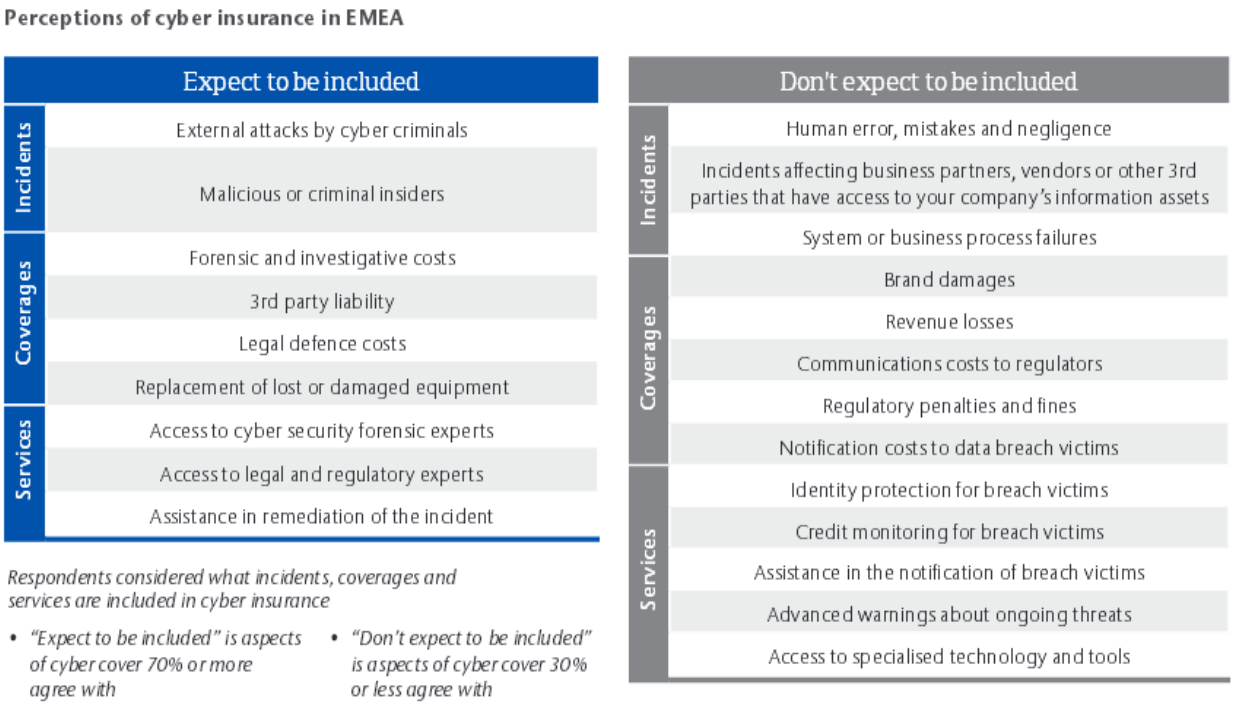


Figure 2: Perceptions of cyber insurance in Europe, Middle-East, and Africa[20]

[18] SANS Institute "Bridging the Insurance/InfoSec Gap: The SANS 2016 Cyber Insurance Survey" https://www.sans.org/reading-room/whitepapers/analyst/bridging-insurance-infosec-gap-2016-cyber-insurance-survey-37062

[19] 2015 EMEA Cyber Impact Report: The increasing cyber threat – what is the true cost to business? http://www.aon.com/sweden/attachments/Kunskapsledare/2015cyberimpactreport_ponemon.pdf

[20] http://www.aon.com/sweden/attachments/Kunskapsledare/2015cyberimpactreport_ponemon.pdf

2.5 Cyber insurance market growth and product standardisation

The EU market for cyber insurance is considered by many as still in its infancy. It currently comprises 50+ carriers offering cyber insurance. The market generates about $3bn-$4bn[21] in premiums annually, but Allianz, an insurance company, expects it to reach $20bn by 2025, making it one of the fastest growing segments of the industry[22]. As a reference: the US market has been writing the lion's share of all cyber insurance globally since the late 1990's. It currently has over 130 distinct insurance organizations writing cyber premiums for the year. The largest cyber insurance writers are AIG, XL Group Ltd, and Chubb Limited. These companies had a combined market share of approximately 40% at year-end 2016. The top 15 writers of cyber held approximately 83% of the market in 2016[23,24].

This study included the largest cyber insurance writers and others which resulted in a selection of **ten of the leading markets for Europe**. The markets used for this research consist of global insurers that offer many different insurance products and are primarily focused on insuring businesses (so excluding the consumer market). Moreover, 7 out of 10 of the markets used in this research are in the top 20 of largest global insurers[25].

When discussing product standardization in cyber insurance, a key aspect is whether certain coverage types are standard among cyber insurance products. The matrix below tabulates the type of coverage provided in standard standalone cyber insurance, as offered by the selected major insurance carriers. The types of coverage can be denoted as:

- **Covered**: The type of coverage is included in the standard cyber insurance the insurer offers. Insurance coverage refers to the amount of risk that is being transferred. It addresses both the risk type (content of the coverage) and the risk amount (limit of the coverage)
- **Endorsement**: A specific change to the coverage, that is added to the policy, describing exactly how the standard policy is modified.
- **Extension**: These types of coverage are optional and available to customers often at additional cost. While an endorsement is often a broader coverage, an extension is truly a new add-on which is not yet found in the coverage. Therefore, a type of coverage can be an endorsement for one insurer and an extension for another insurer. Such is the case for an Electronic Data Incident in Table 1.

Table 1: Type of coverage provided in standard standalone cyber insurance by a selection of EMEA carriers

COVERAGE TYPE	WHAT DOES IT COVER	1	2	3	4	5	6	7	8	9	10
First Response	Hotline, IT and Legal advisors	Covered	Covered	Covered	Covered	Covered	Covered	Covered	Covered	Covered	Covered
Event Management	Legal/PR, Technical forensics and notification	Covered	Covered	Covered	Covered	Covered	Covered	Covered	Covered	Covered	Covered

[21] These figures refer to standalone coverage and exclude cyber cover bundled in traditional policies ("silent wording")
[22] https://www.ft.com/content/25bf97e8-3a27-11e7-821a-6027b8a20f23
[23] https://www.reuters.com/article/fitch-us-cyber-insurance-industry-grows-idUSFit8PFGH3
[24] Financial Times: "*Cyber insurance market expected to grow after WannaCry attack*"
[25] http://www.relbanks.com/top-insurance-companies/market-cap

Data protection and cyber liability	Liability claims and fines	Covered	Covered	Covered	Covered	Covered	Covered	Covered	Covered	Covered	Covered
Network Interruption	Loss of income due to cyber incident (e.g. malware)	Covered	Covered	Covered	Covered	Covered	Covered	Covered	Covered	Covered	Covered
Network Interruption: OSP	Loss due to outside service provider security or system failure	Endorsement	Covered	Covered	Covered	Covered	Covered	Covered	Covered	Covered	Covered
Network Interruption: System failure	Loss due to system failure or human error	Endorsement	Endorsement	Covered	Endorsement	Extension	Covered	Extension	Extension	Covered	Covered
Cyber Extortion	Cost of ransom payment and cyber specialists	Covered	Endorsement	Covered	Covered	Covered	Covered	Covered	Covered	Covered	Covered
Electronic Data Incident	Loss due to accidental damage of computer system (e.g. flood)	Endorsement	Extension	Extension	Covered	Covered	Extension	Extension	Extension	Extension	Extension
Media Liability	Damages and defence cost of IP breach of electronic content	Extension	Covered	Covered	Covered	Covered	Covered	Extension	Covered	Covered	Covered
Cyber Theft	Financial loss from fraudulent electronic funds transfer	Extension	Extension	Extension	Extension	Extension	Covered	Extension	Covered	Extension	Extension
Goodwill coupon	Cost of goodwill coupon	Extension	Extension	Extension	Extension	Extension	Extension	Extension	Extension	Extension	Extension
Criminal Reward Fund	Cost of payment for information	Extension	Extension	Extension	Covered	Extension	Extension	Extension	Extension	Extension	Extension

It's worthwhile noting that different definitions are used for similar, or even identical, types of cyber exposures and coverage. For instance:

- A ***System Failure*** may typically leave systems idle and screens blank. There may be no property damage – after all, there is usually no material damage – but services are interrupted. This event is known as cyber business interruption, (contingent) business interruption, non-physical business interruption, network business interruption and even security failure business interruption or system failure business interruption.
- A ***Security Failure*** such as a data breach may also be referenced to as a privacy breach. Information assets are a much broader risk class than data privacy and the protection of personal identifiable information (PII).
- ***Product Liability*** risk may also be referred to as Internet-of-Things (IoT) risk. Applicants must be aware of the fact that cyber policies may contain exclusions for third-party claims, damages to tangible property, bodily injury, and product recalls. These sorts of liability exposures, however, may be precisely the types of losses caused by a cyber-attack made through the IoT[26].

[26] http://www.klgates.com/the-internet-of-things--is-your-cyber-insurance-protecting-you-11-30-2016/#_ftn8

2.6 Risk assessment language in the cyber insurance application process

Organizations can obtain cyber insurance in various ways by using an agent, a broker, using their own insurance captive, or engage with an insurance company directly. Regardless of the selected way, the application process generally includes the four distinct phases tabulated in Table 2.

Table 2: Application process phases

PHASE	DESCRIPTION
1. Risk identification and evaluation	• Table Program, loss analysis, benchmarking and analytics • Program design options • Market condition and insurer evaluation • Current risk assessment and future exposure review
2. Marketing of programme	• Data collection and submission preparation • Submissions to selected insurers, Underwriter meetings • Clarify data and obtain additional information • Receive preliminary quotes
3. Present options	• Evaluate and compare quotes and coverage terms • Negotiate collateral • Present marketing summary and proposal • Discuss alternatives • Final negotiations
4. Programme execution	• Bind selected programme • Invoicing and premium allocation processing • Obtain policies, review, and issue

Throughout this process, the impact of risk assessment language and terminology is evident, but it is more clear when it comes to feeding the insurer's risk assessment process, which affects phases 1 (Risk identification and evaluation) through 3 (Present options). The risk assessment will include various parameters, such as those tabulated in Table 3.

Table 3: Examples of risk assessment parameters

RISK ASSESSMENT PARAMETER	RELEVANT INFORMATION
Basic Exposures	Nature of the business, services performed and potential liabilities if such services are performed incorrectly, revenue, geography etc.
Contracts	Type of terms that the insured's contracts contain, limitation of liability provisions, type of representations and warranties which are contained within contracts, etc.
Litigation	Insured's claims experience (if claims suffered, what protections have been instituted to avoid repeats?), type of industry litigation, type of guidance on loss benchmarking, etc.
Privacy	Type of confidential or proprietary information, is the information maintained in-house or outsourced to third parties, type of certifications or assessments (PCI DSS, ISAE3402, ISO etc.)?

Risk Management	Type of risk management and quality controls in place. Fundamentally, does the insured care about risk management and evidence it through various means such as training and education, business continuity planning, and incident response?

A comprehensive overview of the underwriting factors will be provided and evaluated in Section 3.

Figure 3: Use of risk assessment language in the cyber insurance market submission process

3. Risk assessment language in cyber insurance

3.1 Overview

When it comes to insurance, risk assessment - also called underwriting - is the methodology used by insurers for evaluating and assessing the risks associated with an insurance policy. The same helps in calculation of the correct premium for an insured. While cyber exposures are developing and may not always be predefined, recognized, or well understood – so the risk assessment is developing.

In the context of cyber insurance, insurers traditionally perform a risk assessment of cyber exposure through an underwriting questionnaire (or other underwriting methods). Risk assessments often refer to industry standards for network security and data privacy. As such, the underwriting questionnaire is aimed at providing the insurer quantitative and qualitative information on the underwritten risk. Although insurers look for risk maturity indicators – the adoption of cybersecurity standards being an important one - they would typically not require adherence to that particular standard. Finally, insurance coverage defines the risk - and assorted parameters - against which insurance is taken.

Security standards, **cyber insurance coverage** and **underwriting information**, are the most common form of risk assessment that a (re)insurer uses before accepting the risk transfer, and are inherently linked to one another. Cybersecurity standards provide information and tools to mitigate a company's most crucial cybersecurity risks. Insurers want to provide coverage for the cybersecurity risks a company cannot – or will not - rule out. The underwriting information obtained through a questionnaire is used to assess those risks for insurers that interrelate with the coverage provided. This interconnectedness – and interdependency - is an ideal precondition given that the risk assessment (i.e. underwriting information) provides sufficient reliable information about the actual risk profile of the applicant.

Figure 4: Interdependencies between Security Standards, Underwriting Information and Insurance Coverage

Harmonization of the risk assessment language within the context of this report refers to:

- The **Underwriting Questionnaires**, i.e. what questions are asked of the insured to collect information about the risk assessment process.
- The **Cyber Insurance Coverage**, i.e. how are coverage components defined in insurance policies.

The lack of harmonization may severely affect or break the link between cybersecurity standards, cyber insurance and underwriting information; which affects the ability to determine loss correlation.

For example, an underwriting questionnaire may include a question about firewalls (e.g. *do you deploy web application firewalls that inspect all network traffic*?) because using firewalls is considered to be a critical security control. The answer to this question, a "yes" or a "no", does not provide the best possible underwriting information to determine the applicant's actual risk posture, since there are plenty of factors that determine the good utilisation of a security control (e.g. security updates, proper configuration management, etc.). An open question would thus be more appropriate, and better support the risk dialogue.

This could negatively impact the adoption rate of cyber insurance as the coverage is not linked to the most critical cyber threats and exposures, and leads to either large uninsured incidents or a high percentage of non-covered claims. The following section provides an analysis of several cybersecurity standards, underwriting information and cyber insurance coverage. The aim of this analysis is to see if – and to what extent – there is harmonization of risk assessment language frameworks in the EU cyber insurance market.

3.2 Existing risk assessment language frameworks

Before analysing underwriting questionnaires that insurers use as part of their risk assessment, it is necessary to examine available cyber risk assessments and initiatives for standardization. An interesting initiative in this respect is the Managing Cyber Accumulation Risk developed by the Cambridge Centre for Risk Studies in conjunction with, but not limited to, AIR and Lloyd's[27]. The report, which tries to capture cyber exposure in a standardized way, resulted in a schema, which, on its first version, identifies a total of 19 different loss coverages. The schema is made as simple as possible on purpose so as to limit the resources for insurers. For these 19 loss coverages a description is given as well as a distinction between 1st and 3rd party. The main motivation behind the framework is addressing the uncertainty of accumulation risk[28] of cyber incidents. Accumulation risk is more of an issue for insurers with cyber as opposed to other type of risks; for example, a fire cannot spread around the world in a single day, but a cyber incident could. This study also highlights the fact that accumulation risk makes insurers hesitant to offer cyber insurance.

The Cambridge report provides a framework for understanding and managing accumulation risk for cyber insurance through the identification and standardization of loss coverages. This specific approach provides a thorough enough basis to highlight what a harmonized framework might look like. In practice, many of the fields requested in the data schema can be considered impractical as companies would have difficulties in gathering correct and complete input. For example, an insurer would evaluate the cost of business interruption – knowing an organization's hourly loss – but the reality is, even if insurers had a system for tracking this, very few businesses would be able to provide this information.

A key industry-led initiative towards standardisation is Lloyd's Cyber Core Data Requirements[29], which seeks to establish a common core schema for cyber exposure data and common core features for input data used in cyber risk tools in the market, both in relation to key attributes that should be considered when evaluating cyber risk and in relation to the way in which this information should be collected in line with the existing industry-standard codes. Experts say the effort will encourage development of common

[27] Cambridge Centre for Risk Studies and Risk Management Solutions, Inc.; 2016; Cyber Insurance Exposure Data Schema v1.0; Cyber Accumulation Risk Management working paper.
[28] ENISA "Cyber Insurance: Recent Advances, Good Practices and Challenges" https://www.enisa.europa.eu/publications/cyber-insurance-recent-advances-good-practices-and-challenges
[29] https://www.lloyds.com/news-and-insight/risk-insight/emerging-risks-team/cyber-core-data-requirements

insurance policy language, which will enable insurers and reinsurers to more accurately measure risk aggregation[30].

3.3 Security standards and cyber insurance

Security standards play a significant role in the context of cyber insurance in two ways:

- They are used as an **indicator of the insured party's cybersecurity maturity and awareness** – questions regarding compliance with such standards are often part of the underwriting process;
- They are used as **reference points by insurance carriers to support their risk assessment process** and identify suitable security controls – questions regarding these controls will typically be part of the underwriting questionnaire.

In both cases, security standards influence the resulting language/terminology used in cyber insurance, so it is reasonable to examine how this impact is materialized, and how any commonalities and discrepancies among the most prevalent security standards affect the resulting risk assessment language.

Some of the most frequently used standards in the cyber insurance industry are **ISO 27001/2**[31], **NIST**[32], **COBIT 5**[33] and **NCSC**[34]. In addition, sector specific security standards, such as the **Payment Card Industry Data Security Standard** (**PCI DSS**) are often used to assess the insured party's security posture. Clearly, these standards are not directly comparable insomuch as they have different scope, target industry sector and conceptual level, but assessing their use in the risk assessment process provides indications regarding the existence, or lack thereof, of a market consensus.

This study confirms earlier findings[35] that all leading insurers see the use of cybersecurity standards as an indicator of risk awareness and maturity. Through enhanced and tailored cyber insurance questionnaires, both the applicant and the insurer will obtain better underwriting information. To further drive awareness and risk maturity an insurer may allocate a percentage of the premium for risk mitigation initiatives[36]. The use of standards to benchmark/assess the insured party's security maturity is exemplified by the inclusion of specific questions in the underwriting questionnaire; the questionnaire may ask a question about specific compliance to one or more of these standards or the partial application of any of these standards in certain domains, such as Business Continuity Planning, Network Security etc.

As there are no consensus security standards adopted across the cyber insurance industry, a buyer may face different questions regarding the compliance to or application of security standards from different carriers.

---

[30] http://www.businessinsurance.com/article/20160131/NEWS06/301319989/Lloyds-of-Londons-core-data-requirements-help-with-development-of-cyber-insura

[31] International Organization for Standardization. (2015). IT Security techniques (ISO/IEC Standard No. 27001). Retrieved from https://www.iso.org/standard/69378.html.

[32] https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[33] ISACA. (2016). A Business Framework for the Governance and Management of Enterprise IT. Retrieved from https://www.isaca.org/cobit/pages/cobit-5-framework-product-page.aspx

[34] National cyber security center. NCSC 10 steps (2016). Retrieved from https://www.ncsc.gov.uk/guidance/10-steps-executive-summary

[35] ENISA "Cyber Insurance: Recent Advances, Good Practices and Challenges"

[36] In the insurance industry this would be referred to as a bursary. A bursary can be explained as a discount on the premium with the contingency that the discounted amount is spend on certain risk mitigations. A cyber insurance example might be a discount on the premium that is spend on training employees in data security.

The second major use of security standards in cyber insurance directly influences the risk assessment process conducted by carriers. In practice, carriers will examine a security standard to understand best practices and security controls that reduce cyber risk; in turn, these practices/controls will be converted to questions in the underwriting questionnaire (e.g. *Do you have a formal patch management process?*).

Comparing the most prevalent security standards to one another gives an indication as to their own convergence in terms of good practices, which in turn is expected to influence the harmonization of underwriting questionnaires. In order to do the comparison, a selection of some of the most commonly used cybersecurity standards are compared on the basis of a set of twenty critical security controls. The results are tabulated in Table 4 and demonstrate that almost all of the twenty critical security controls are mentioned throughout all security standards – thus implying market consensus on what defines good cybersecurity practices. Important cybersecurity best practices like *Data recovery capabilities and Malware defences* are advised by all security standards.

Table 4: Percentage of security standards addressing each critical security control

SECURITY STANDARDS	SECURITY CONTROL	%
SANS - CSC Security Standards Council - PCI-DSS NIST - Cybersecurity Framework ISO 27001 ISO 27002 ISACA - COBIT 5 NCSC - 10 steps to cybersecurity NERC - CIP 5 ISA/IEC 62443	Inventory of Authorized and Unauthorized Devices	100%
	Inventory of Authorized and Unauthorized Software	100%
	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	100%
	Continuous Vulnerability Assessment and Remediation	100%
	Controlled Use of Administrative Privileges	100%
	Maintenance, Monitoring, and Analysis of Audit Logs	100%
	Email and Web Browser Protections	89%
	Malware Defences	100%
	Limitation and Control of Network Ports, Protocols, and Services	100%
	Data Recovery Capability	100%
	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	100%
	Boundary Defence	89%
	Data Protection	100%
	Controlled Access Based on the Need to Know	100%
	Wireless Access Control	78%
	Account Monitoring and Control	100%
	Security Skills Assessment and Appropriate Training to Fill Gaps	100%
	Application Software Security	100%
	Incident Response and Management	100%
	Penetration Tests and Red Team Exercises	89%

This convergence among the standards is certain to have some impact on the risk assessment language harmonization, as insurers will have similar points of reference to assess the risk profiles of applicants.

Even so, it is not straightforward that two insurers will ask the same question to assess the existence and pertinence of the same security control, despite using the same standard to conduct risk assessment.

To complete the assessment of commonality, the cyber coverage needs to be compared with the security standards. This is done by listing which security standard(s) give guidelines which could either prevent one of the twelve most common coverage types the insurers offer or provide an effective guideline. Table 5 gives an overview of this assessment. One can see that there appears to be some correlation between the coverage types and security standards, which is also confirmed by applying the ANOVA methodology on the sample. Although the comparison between coverage types and security standards gives a positive correlation, a caveat can be made. This is due to the fact that the security standards are broad and can therefore often be linked to a certain coverage type. Hence several security standards can be often linked to certain types of coverages.

Table 5: Security standards and cyber insurance coverage

TYPE OF COVERAGE	WHAT DOES IT COVER	% OF INSURERS THAT PROVIDE COVERAGE	% OF SECURITY STANDARDS THAT PROVIDE GUIDELINES FOR THIS COVERAGE	WHICH CRITICAL SECURITY STANDARD
First Response	Hotline, IT and Legal advisers	100%	100%	Incident Response and Management
Event Management	Legal/PR, Technical forensics and notification	100%	100%	Incident Response and Management
Data protection and cyber liability	Liability claims and fines	100%	100%	Several Security Standards
Network Interruption	Loss of income due to cyber incident (e.g. malware)	100%	100%	Several Security Standards
Network Interruption: OSP	Loss due to outside service provider security or system failure	90%	100%	Several Security Standards
Network Interruption: system failure	Loss due to system failure or human error	40%	100%	Security Skills Assessment and Appropriate training to fill gaps
Cyber Extortion	Cost of ransom payment and cyber specialists	90%	100%	Several Security Standards
Electronic Data Incident	Loss due to accidental damage of computer system (e.g. flood)	20%	100%	Several Security Standards
Media Liability	Damages and defence cost of intellectual property breach of electronic content	80%	100%	Several Security Standards
Cyber Theft	Financial loss from fraudulent electronic funds transfer	20%	100%	Controlled use of Administrative Privileges & Controlled Access based on the Need to Know
Goodwill coupon	Cost of goodwill coupon	0%	0%	None
Criminal Reward Fund	Cost of payment for information that leads to arrest and conviction	10%	0%	None

3.4 Underwriting information language

Underwriting questionnaires are used by insurers as a risk assessment tool. The information collected via underwriting questionnaires is used to conduct a risk assessment based on which an insurer decides whether to take on the risk and, if so, under what conditions. Underwriting questionnaire language refers to what sort of questions are asked of cyber insurance applicants to collect cyber risk information and how these questions are phrased. Typically, in more mature or better defined insurance markets, such as car insurance, insurers will ask the same questions as the type of information required to assess a buyer's risk is very standardized (e.g. *What model* or *how old is your car?*).

To assess commonality of risk assessment language frameworks in cyber insurance this study compared the prevailing risk assessment methodology of the insurance market: the underwriting questionnaire. Specifically, the findings below are based on a thorough analysis of the underwriting questionnaires used by 10 leading insurers, namely:

- AIG (Cyber Edge)
- Beazley (Information Security & Privacy Insurance)
- EmerginRisk (Lloyd's)
- Hiscox (Cyber and Data)
- Allianz (Cyber Protect Premium)
- Aon (Cyber, Cyber Enterprise Solution)
- XL Catlin (Cyber and Technology)
- QBE (Cyber)
- Tokio Marine HCC (Cyber Security)
- Chubb (Cyber ERM)

For each of these questions it is noted how many insurers ask this question in their cyber insurance questionnaire. Insurers tend to use long and short questionnaires based on the size and type of the company. This research only includes **long form questionnaires** as these ask more cyber related questions. The short forms tend to focus more on financial information of the company complemented with some general cyber related questions.

The analysis of the questionnaires sample is done by noting all the unique questions asked by each insurer. A question qualifies as **unique if it is posed by at least one insurer and not by another insurer**. By applying this method, **129 unique questions** were found. Moreover, while each insurer categorizes the questions differently – as there are no relevant requirements, the analysis identified **8 major categories** under which the 129 questions fall, specifically:

CATEGORY	DESCRIPTION
General information	General company information. Includes questions on number of employees and turnover in particular areas.
Data exposure	Questions on what type of data the applicant stores and shares with third parties.
Network interruption	Information on the impact of a network interruption as well as questions on what the applicant does to mitigate this impact.
Outsourcing exposure	Questions on access of outsourcing service partners.

CATEGORY	DESCRIPTION
Data security	Questions on how the applicant handles its data security. Backups, privacy policy and encryption questions among others.
Network security	Questions on how the applicant handles its network security. Firewalls, patch management and network access.
Security policies	Information on the security policies of the applicant.
Claim history	Questions on previous losses and incidents. Aim to get a better idea of the cyber insurance history of the applicant.

The largest category is Data security with 24 unique questions and Security policies the smallest with 7 questions. All the insurers ask at least one question in each category which hints at some level of generally accepted use of risk assessment language frameworks, but does not constitute harmonization on its own. However, assessing harmonization requires a deeper dive into the questionnaires; therefore, the analysis is done on the question level which means that for each individual question it is noted which insurer asks about that particular question. An insurer can either:

- Ask a question;
- Not ask a question;
- Partially ask a certain question.

Note: *Including a question in a questionnaire implies that the insurer will be able to use and assess the answer provided. The analysis does not rule out the possibility that some questions on a questionnaire will just serve the purpose of underwriting and not necessarily feed into a risk assessment*

The partially asked question is added due to the fact that insurers have different ways of asking about a certain topic. A question is noted partially asked when e.g. the insurer does inquire generally about a certain topic but does not ask the applicant specifically. An example of this could be that most insurers ask the question "*Do you store health related data?*" while another insurer uses an open text box with the question "*What type of data do you store?*". In this case, the latter insurer would be noted as partially asking the question. The logic behind this is that while open text boxes can capture a lot of information it can also miss a lot of information. Applicants filling in these questionnaires are not experienced cybersecurity experts and could therefore easily forget to fill in information that is not explicitly requested.

Questions like "*Do you have a business continuity plan?*" are asked by 82% of insurers. However other questions are only asked by a single insurer, such as "*Does your business rely on Big data / real time calculations?*". The ANOVA test and the correlations confirm that the questionnaires differ quite a lot. Correlations between the different questionnaires are not higher than 0.5 showing relatively weak signs of positive correlation. A potential reason that the questionnaires show no sign of harmonization could be claim history. Some insurers might adapt their questionnaires due to information they received from successful claims. An insurer might have had multiple claims from companies that work with Big Data. Hence, they explicitly ask potential customers if this type of risk is present.

Overall, the analysis shows:

- Different questions per carrier

- Different definitions for similar risk areas
- Overlapping questions for key risk areas
- Consistent reference to cybersecurity principles

These findings also reveal that the underlying security standards used by carriers to conduct risk assessment cover very similar topics and include similar practices and security controls – a convergence that is not evident in the underwriting questionnaires themselves.

Table 6 compares the analysis of the security standards with that of the questionnaires. More specifically for each of the twenty critical security controls, the percentage of security standards that incorporates this control is compared to the percentage of questionnaires asking one or multiple questions reflecting this particular control. Furthermore, the question(s) that align with the particular security control is noted. It is evident that the security standards and questionnaires differ and no relationship between the two is apparent.

Table 6: Security standards and cyber insurance questionnaires

SECURITY CONTROL	% OF SECURITY STANDARDS	% OF INSURERS THAT ASK QUESTION	QUESTION FROM QUESTIONNAIRE
Inventory of Authorized and Unauthorized Devices	100%	0%	None
Inventory of Authorized and Unauthorized Software	100%	63%	Are you using any unsupported operating system or software
Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	100%	63%	Do you carry out server and application security configuration handling
Continuous Vulnerability Assessment and Remediation	100%	73%	Utilization of proactive vulnerability scanning
Controlled Use of Administrative Privileges	100%	100%	Do you have a group-wide privacy policy
Maintenance, Monitoring, and Analysis of Audit Logs	100%	54%	Do you keep an incidents log of all system security breaches and network failures
Email and Web Browser Protections	89%	100%	Several questions
Malware Defences	100%	45%	Describe how you monitor and actively block advances malware
Limitation and Control of Network Ports, Protocols, and Services	100%	100%	Several questions
Data Recovery Capability	100%	100%	Is all critical data backed-up at least weekly
Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	100%	82%	Is your network configured to limit access to sensitive data
Boundary Defence	89%	73%	Do you have a data classification policy with adequate levels of security for sensitive data
Data Protection	100%	91%	Is all stored sensitive data encrypted

Controlled Access Based on the Need to Know	100%	82%	Is your network configured to limit access to sensitive data
Wireless Access Control	78%	100%	Are employees allowed to work on own devices (laptop etc.)? Are they allowed to use company hardware
Account Monitoring and Control	100%	36%	Do you have a lifecycle management process for assessing and replacing system and network equipment
Security Skills Assessment and Appropriate Training to Fill Gaps	100%	73%	Continuous awareness training for employees
Application Software Security	100%	64%	Do you carry out server and application security configuration handling
Incident Response and Management	100%	82%	Do you have an incident response plan which includes a team with specific roles and responsibilities
Penetration Tests and Red Team Exercises	89%	82%	Is regular penetration testing carried out by a 3rd party

While all security standards advise to have "Malware defences" only 45% of the questionnaires specifically ask if applicants do this. The security control of "Maintenance, Monitoring, and Analysis of Audit Logs" is also asked only by half of the insurers. This security control which entails keeping logs of events so future cyber incidents can be better understood is only asked in 54% of the questionnaires. The correlations reflect the differences between the critical security controls and the questionnaires. The correlation of -0.31 is slightly negative which means that the higher the percentage of security standards that advise a certain cybersecurity control the lower the percentage of questionnaires that ask for that same control. This shows that harmonization is not present between security standards and questionnaires.

3.5 Insurance coverage language

Commonality of language in terms of insurance coverage – in the context of the present study – refers to how insurers define the different coverage types they offer and to what extent the definitions are homogeneous. Generally speaking, insurance coverage language needs to strike a balance between the conflicting goals of buyers who want the broadest coverage at minimum cost and insurers who aim for the opposite. Moreover, a critical factor to consider is the fact that insurers compete on both price and the coverage they offer.

In this context, while harmonization appears counterintuitive as it may be perceived as limiting an insurer's ability to compete, competition on coverage in most type of insurances is actually in the details not so much on what type of risks to cover. Business interruption from a data breach is a good example as almost all cyber insurers offer coverage for this. However, some apply a longer waiting period[37] than others. In addition, large multinational companies can get bespoke solutions from insurers, which are confidential

[37] A waiting period is a period of time that consists of the difference between the start of the business interruption and the moment from which the insurer will cover the cost of the business interruption. While competing on this so called waiting period the insurers are harmonized on the type of risks they cover and what this coverage means in terms of providing compensation for business interruption due to a data breach.

and therefore hard to compare. For these reasons, the cyber insurance coverage of several insurers has been compared on the type of coverage they offer.

Figure 5 examines the harmonization between the insurance coverage provided by different insurers. It becomes clear that some harmonization among insurers is present, e.g. **network interruption** and **data protection and cyber liability** are covered by all insurers in the sample. The insurers also seem to agree on **which types of coverage are not included by default**. **Goodwill coupons**[38] and **Cyber Theft** are mostly seen as optional extensions for which companies need to pay a higher premium. The coverage types that insurers have not yet reached harmonization on is **Network Interruption due to system failure**, **Electronic Data Incidents** and **Cyber Theft**.

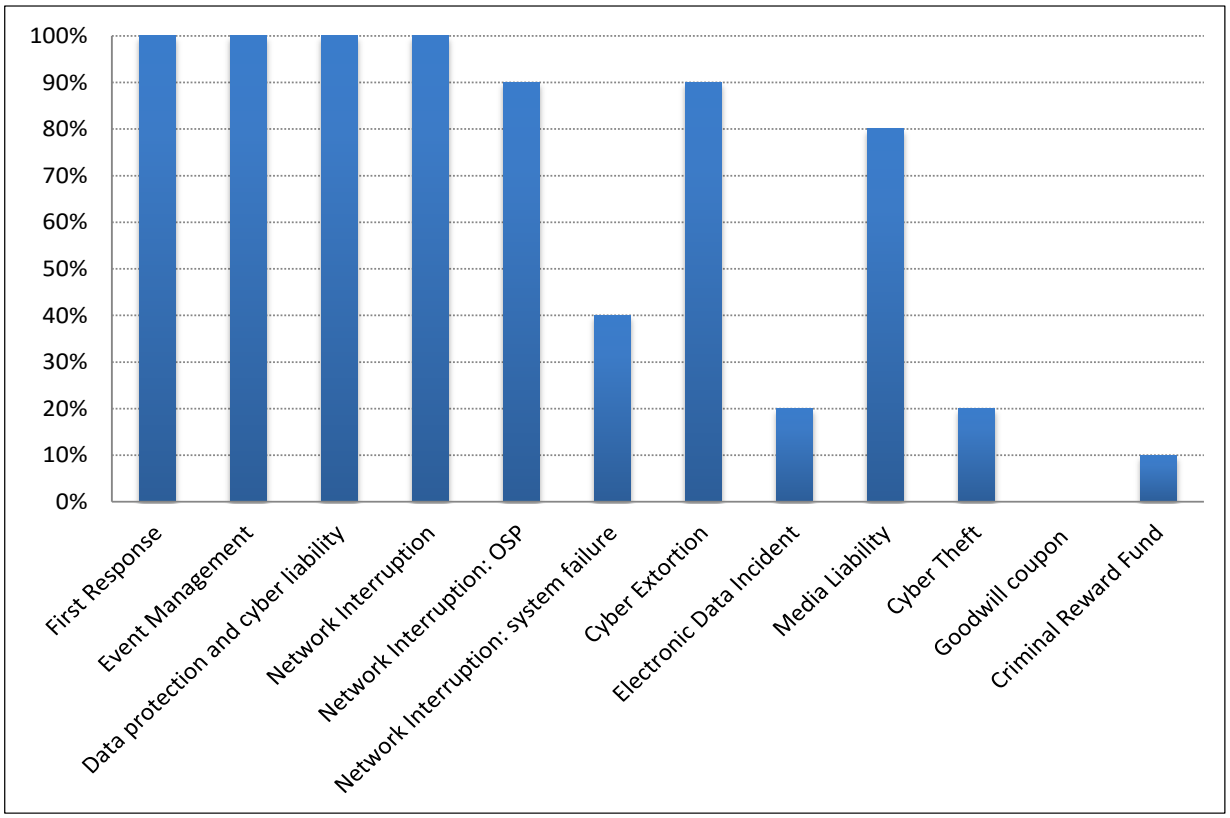


Figure 5: Percentage of insurers providing coverage per loss scenario

Despite some differences (in coverage, wording, premium etc.) the ANOVA test states that the different insurers do not provide statistically different coverage. In other words, regardless of differences in both traditional insurance policies and standalone cyber policies, it is legitimate to refer to 'a cyber insurance policy'. This is also reflected in the fact that correlations between different insurers are mostly higher than 0.6, meaning that there is a positive relationship between the coverage the different insurers offer. This is in line with expectations and hints at harmonization between insurers on the type of coverage they provide.

In Table 7 each of the twelve coverage categories are denoted once again. In the third column it is noted what percentage of insurers provides this type of coverage. The fourth column shows the percentage of

[38] Goodwill coupon refers to coverage for the cost of rebates and discounts which are offered to customers which are negatively impacted by a cyber-incident of the insured

insurers that asks any type of relevant question for this particular category. Furthermore, the questions that align with the particular coverage category are noted. It appears that harmonization between the cyber insurance questionnaires and coverage is present. The cybersecurity risks that all insurers provide coverage for are also the risks the insurer assesses through the underwriting questionnaire. A clear example is **Cyber Extortion**; this risk is covered by 90% of the insurers and is asked in all the questionnaires. On the other hand, **Criminal Reward Fund** is part of the standard coverage for only 10% of the insurers, and is not asked in any of the questionnaires. This pattern is also reflected in the correlation of 0.66. This positive correlation indicates some harmonization between cyber insurance coverage and the underwriting information questionnaires. This comes as no surprise knowing the questionnaires are used by the insurers to assess the risks they provide coverage for.

Table 7: Cyber insurance coverage and risk assessment questions

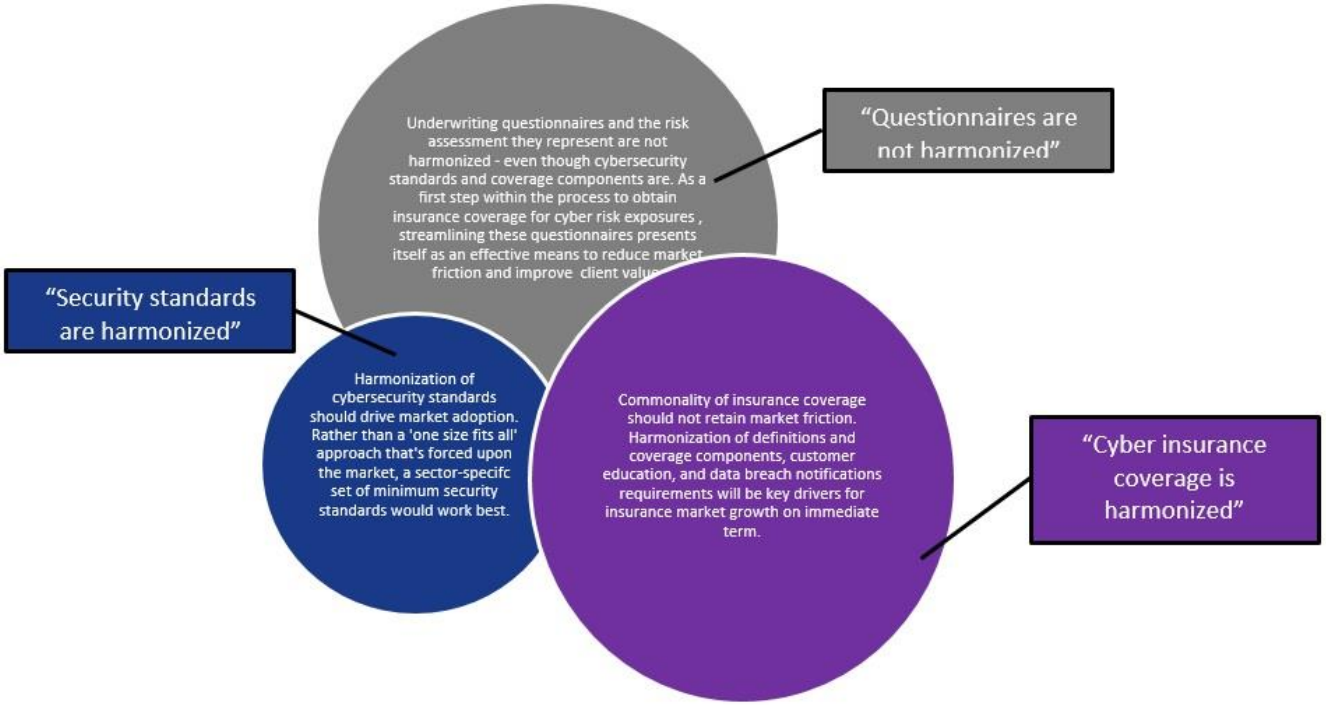
TYPE OF COVERAGE	WHAT DOES IT COVER	% OF INSURERS THAT PROVIDE COVERAGE	% OF INSURERS THAT ASK QUESTION	QUESTION FROM QUESTIONNAIRE
First Response	Hotline, IT and Legal advisers	100%	82%	Do you have an incidents response plan which includes a team with specified roles and responsibilities?
Event Management	Legal/PR, Technical forensics and notification	100%	82%	Do you have an incidents response plan which includes a team with specified roles and responsibilities?
Data protection and cyber liability	Liability claims and fines	100%	73%	Do you have a data classification policy with adequate levels of security for sensitive data?
Network Interruption	Loss of income due to cyber incident (e.g. malware)	100%	100%	Several questions
Network Interruption: OSP	Loss due to outside service provider security or system failure	90%	100%	Several questions
Network Interruption: system failure	Loss due to system failure or human error	40%	100%	Several questions
Cyber Extortion	Cost of ransom payment and cyber specialists	90%	100%	Several questions
Electronic Data Incident	Loss due to accidental damage of computer system (e.g. flood)	20%	100%	Several questions
Media Liability	Damages and defence cost of intellectual property breach of electronic content	80%	55%	Screening of website content / social media presence?

Cyber Theft	Financial loss from fraudulent electronic funds transfer	20%	27%	Do you have an identity theft program
Goodwill coupon	Cost of goodwill coupon	0%	0%	None
Criminal Reward Fund	Cost of payment for information that leads to arrest and conviction	10%	0%	None

3.6 Risk assessment language across Security Standards, Underwriting and Insurance Coverage

The analysis revealed several ways in which the risk assessment language used in cyber insurance is influenced and is evolving. Some key findings are summarized below:

- More regulated or 'risk mature' industries focus more on certain standards;
- The types of coverage insurers are offering is generally harmonized but the policy wording itself is different across the board;
- Cybersecurity standards and insurance coverage are complimentary; not supplementary;
- Cyber insurance underwriting is not uniform;
- Little harmonization is found between the questionnaires (underwriting information) and the cyber security standards;
- Differences have been found in application processes and forms, risk assessment methodologies and risk acceptance criteria;
- Insurers who have rich information from claims history adapt their questionnaire to allow them to focus on mitigating those risk where they historically have had most claims;
- Analysing loss scenarios and claim statistics did not reveal significant correlation with underwriting questionnaires and other type of risk assessments so far;
- The availability of many cyber security standards might lead insurers to take a reluctant approach as long as there is no specific standard adopted across the board;
- Insurance coverage typically is not conditional to compliance with a certain security standard;
- Much of the risk assessment - and the best practices that it promotes - is reflected in the coverage components that cyber insurance provides;
- Overall, security standards and coverage components are harmonized, and underwriting questionnaires are not.


Underwriting questionnaires and the risk assessment they represent are not harmonized - even though cybersecurity standards and coverage components are. As a first step within the process to obtain insurance coverage for cyber risk exposures , streamlining these questionnaires presents itself as an effective means to reduce market friction and improve client valu
"Questionnaires are not harmonized"
"Security standards are harmonized"
Harmonization of cybersecurity standards should drive market adoption. Rather than a 'one size fits all' approach that's forced upon the market, a sector-specifc set of minimum security standards would work best.
Commonality of insurance coverage should not retain market friction. Harmonization of definitions and coverage components, customer education, and data breach notifications requirements will be key drivers for insurance market growth on immediate term.
"Cyber insurance coverage is harmonized"

4. Current cyber insurance industry practices

The following chapter focuses on an analysis of typical current practices within the cyber insurance industry, mainly based on data collected through the industry consultation (interviews and survey). The focus of the analysis is placed on commercial practices related to coverage offerings and risk assessment / underwriting practices and how these influence the commonality, or lack thereof, of risk assessment language in the market.

4.1 Cyber insurance coverage offerings

Industry representatives were consulted in order to collect information about cyber insurance coverage offerings and understand the different factors that may affect their development, including the wording and policy triggers. These offerings were examined across the following main dimensions:

- Types of coverage
- Geographic areas were the offerings are available
- Business sectors covered
- Types of customers

In terms of types of **coverage offered**, 100% of responses confirmed that they offer coverage for all three coverage categories defined in section 2.4, that is **First party loss**, **Third party loss** and **Other benefits.** Most insurers offer standard coverage but there is often a differentiation based on the insurer's size and/or customer's size. Specifically, larger insurers can offer more customised solutions, while smaller ones tend to offer more standardized products.

This aspect is often related to the characteristics and size of the customer as well. Typically, larger corporate organisations tend to favour bespoke solutions specifically tailored to their needs and can support this via internal Risk Management teams that can conduct thorough cyber risk assessments. On the other hand, SMEs do not have the same internal capacity for risk assessment or even incident response, which makes them more suitable for standardized offerings but also ideal candidates for **added value services**, such as Incident Response, Cyber Espionage, IT Forensics, Emergency Costs, Regulatory Proceedings and Data Restoration. This differentiation on the basis of customer size has been cited as highly common and clearly has a direct impact on the harmonization of cyber insurance language due to customized wordings. An interesting point raised was that while the areas of cover are all broadly the same, carriers may just call it differently (privacy risk vs data risk, business interruption vs network interruption etc.). Hence, it often falls to underwriters and brokers to explain the details of the policy to the customer.

Another critical factor that determined the coverage wording is the **geographical areas** (markets) that each insurer might target. Most providers in fact provide global coverage, though certain regions - particularly North America - were found to be covered generally independently, a fact attributed to the increased market maturity in the USA and Canada and the applicable legislative environment. Providing coverage to multiple countries increases the need for "product localization" which implicitly denotes potential divergence in terms of wording. One interviewee cited the need for "*10 – 15 different sets of insurance wording*" to cope with the smaller or larger discrepancies in their domestic and international market(s). Some of the more mature carriers opt for a modular approach to coverage types offered, which allows for a more streamlined customization to specific market needs.

In terms of **business sectors covered**, most cover holders address all sectors. However, a few exclusions would be around Finance (e.g. banking, hedge funds), Healthcare, CII (e.g. Transport, Energy, Power) and Data Aggregators, depending on the insurance carrier's risk appetite. Among the sectors identified as high risk, Financial Institutions stand out as a particularly risky domain in terms of volatility and severity; in many cases, while carriers may offer cyber risk coverage to FI's the required underwriting information would need to be much more comprehensive. Interviewees cited an increasing interest from clients that process personal data, such as retail Companies, which is driven by the GDPR. Moreover, there is a foreseeable need to develop the sectors of IoT and ICS/SCADA. With respect to the IoT, while the respective risk does not necessarily need a different type of insurance compared to traditional IT, it does require particular attention due to its quick-to-market nature.

A cyber insurance offering is influenced by multiple application factors. These factors include the current relationship (clients vs prospects) and insurance programme (standalone vs combined), the level of standardization of the underwriting process (open-broked vs pre-negotiated[39]), the structure of the offering itself (primary layers vs excess layers[40]), and the role and type of loss adjusters and the reinsurance market. The industry consultation found that each offer is influenced by four to five additional application factors on average and the percentage of respondents identifying each application factor as influencing their offering is depicted in Figure 6.

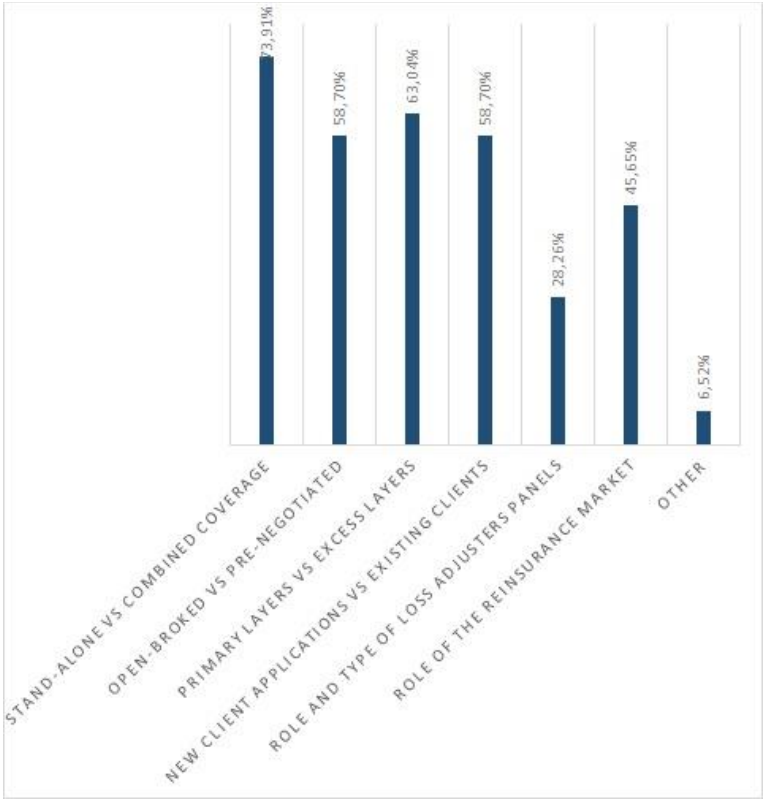


Figure 6: Application factors influencing insurance offerings

[39] Pre-negotiated refers to a higher level of standardisation of the underwriting process than in the case of open-broked. See also: https://www.lloyds.com/common/help/glossary?Letter=P

[40] Layered programs involve a series of insurers writing coverage, each one in excess of lower limits written by other insurers

The vast majority of cyber insurers plan to launch a new and/or updated cyber insurance coverage product within the next two years. The most notable reasons for doing so are listed below:

- Make wording more clear (i.e. harmonize terms and definitions)
- Improve offerings
- Localization
- Keep pace with market / develop offerings
- Broaden cover
- Dynamic and fluid cyber exposures and solutions / ever-changing cyber landscape
- Develop products to provide primary cyber coverage to customers
- Update market standards
- Revising questions
- Update coverage

A key factor to consider when discussing the need for harmonization in cyber insurance language is the industry's own perception about whether or not harmonization of risk assessment language is either already in place or is needed to reduce market frictions. Figure 7 depicts the respondents' replies to this question.

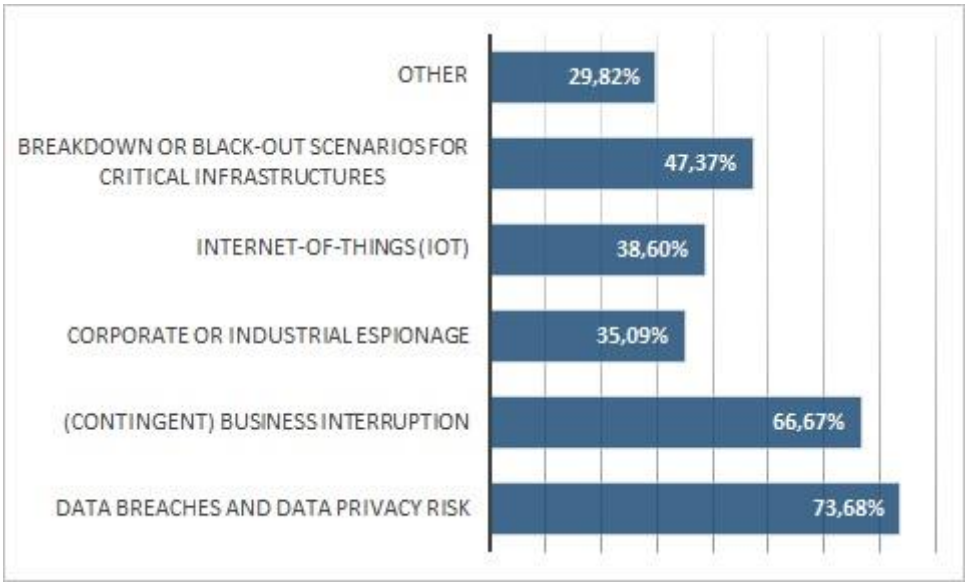


Figure 7: For what type of (cyber) coverage do you expect harmonization of risk assessment language to be in place (as-is) and/or needed to reduce cyber insurance market frictions (to-be)?

Interestingly enough, while the key questions are found to already have made a step towards harmonization - specifically in the area of compliance and governance due to market experience in this area that has driven a marker convergence to an extent - harmonization of risk assessment language is not considered to be in place by the individual respondents for any type of cyber insurance coverage. A main reason cited for this is the **lack of common framework for minimum requirements**[41] – similar to those existing for property or car insurance. Without a commonly adopted and proven set of mitigating measures to be included in the risk assessment it is difficult to move from a "value judgement" model to more mature models. Moreover, for cyber exposures, aggregation or correlation scenarios are just very

[41] Initiatives like Cyber Essentials were cited as good examples

difficult to model, a fact complemented by the complexity of embedded vs standalone (reinsurance treaties are covering cyber exposures silently). Going forward, the role of reinsurance could be important in that regard.

Overall, the coverage for Data Breaches and Data Privacy Risk is considered to qualify for harmonization of risk assessment language by most respondents. A main driver for this is the adoption of the GDPR, while many respondents believe that the NIS Directive will have a similar impact on other types of coverage. Still, most respondents believe that the market is nowhere close to achieving harmonization for cyber perils like IoT or Espionage, though frequent risks are identified as more likely candidates for harmonization.

4.2 Cyber insurance risk assessment practices

All insurers (100% of participants identified as insurance companies / carriers) require some form of risk assessment while offering cyber insurance coverage. Most insurers that offer advanced, mature cyber products and services use "natural moments" like policy renewals or reported claims as a means to interact with their clients and drive risk aware behaviour. Risk assessment is globally recognised as key to consistent information, while pre-policy risk assessment in particular is found to lower the risk and may return a better premium or coverage.

Not performing a risk assessment after a policy renewal is considered a high risk as it can lead to outdated information, a risk that has been cited in previous ENISA reports as well[42][43]. Even so, most carriers consider that a deep pre-policy risk assessment is usually enough for large organizations. One factor to be considered here is that recurring risk assessments are justified only if the premium is high enough, since they incur a cost for the insurance company conducting them.

In certain cases, risk assessment may not be conducted or may be based on a sub-set of the full-blown risk assessment process (e.g. relying on far fewer questions to the customer). Such cases almost always involve SME customers and the underwriting factors may include:

- Underwriting meeting
- Small questionnaire that covers the basics
- Turnover/industry
- News research (score-driven)
- Basic information on claims and security
- Desk research

In terms of the underwriting methods used, all insurers use an underwriting questionnaire (or application form) when offering cyber insurance coverage. Typically, and depending on the case, the questionnaire is complemented by an underwriting meeting. Moreover, the majority of insurers conduct desk research and use threat intelligence and/or open source intelligence during data collection for establishing a risk maturity score.

The most common types of risk assessment include long form and/or short form underwriting questionnaires, client meetings and desk research, while threat intelligence and/or open source intelligence, risk audits and third-party assurance (TPA) reports are less common.

The underwriting methods used are often dependent on factors such as the customer size/type, the industry, the cyber risks involved etc. and take into consideration also the trade-off between the

[42] https://www.enisa.europa.eu/publications/incentives-and-barriers-of-the-cyber-insurance-market-in-europe
[43] https://www.enisa.europa.eu/publications/cyber-insurance-recent-advances-good-practices-and-challenges

respective complexity and resulting underwriting information. For instance, for the middle and SME markets a short form would be typically used as additional questions may be considered a nuisance from a customer perspective or in terms of time needed. Another example is that long-form questionnaires may typically require multiple people to fill out so they are complemented by cyber underwriting meetings for better coordination of the parties involved.

A summary of the most prevalent underwriting methods used in the industry is depicted in Figure 8.

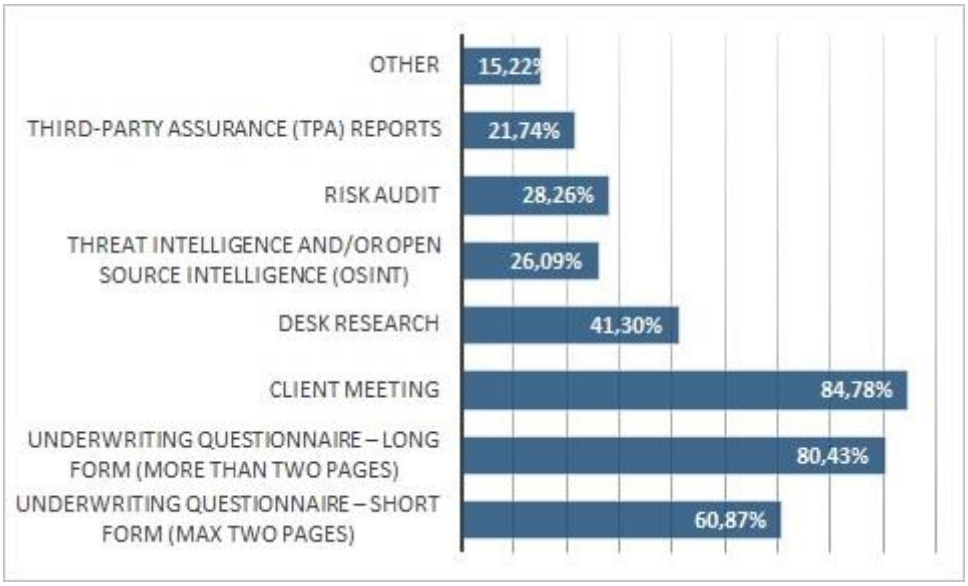


Figure 8: Frequency of use for most common underwriting methods

The insurers' perception seems to be very divided on whether or not current underwriting methods provide sufficient underwriting information, as evident in Figure 9.

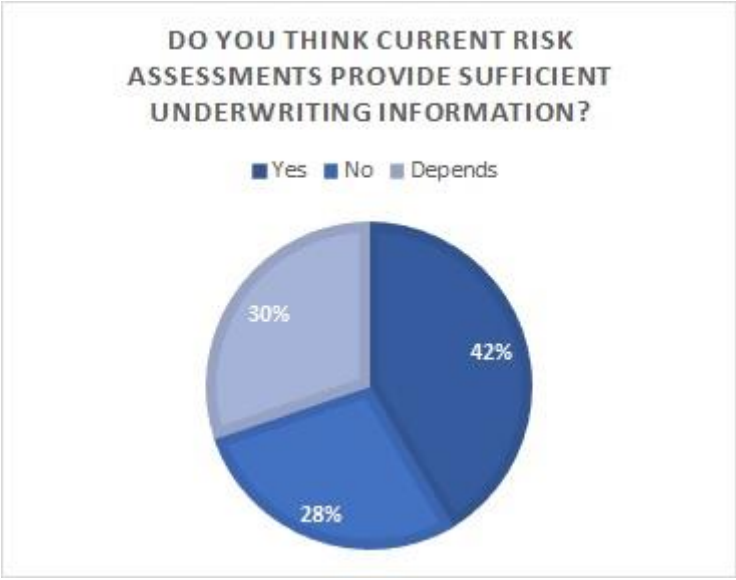


Figure 9: Perception on adequacy of current underwriting methods

It should be noted that the percentages depicted in Figure 9 are impacted by the very high number of brokers who believe the current methods to be sufficient. When examining only the insurers sample in the panel, there seems to be a lot more doubt as to the adequacy of these methods.

A lot of the lack of trust in current underwriting methods has to do with the availability and pertinence of relevant data. Questionnaires generally provide a reasonable overview of threats and mitigating measures, and there are indeed some basic elements, but these differ from one industry to another. Moreover, what information is relevant today may quickly be rendered irrelevant due to the rapidly evolving cyber landscape. The current underwriting methods are generally perceived to be more adequate for smaller customers but are considered insufficient to capture all necessary information for larger organisations. Moreover, existing questionnaires receive binary answers (i.e. yes or no) and thus may not provide accurate risk information. Open and more comprehensive questions may, in some cases, be better suited to evaluate vulnerabilities.

In practice, the market is lacking realistic information on risk quality and, often, the in-house skills to process this information and translate IT concepts to the existing underwriting methods. The latter results in many carriers outsourcing this part of the process to more specialised companies, but this may create a logical barrier between the cyber risk analysis and the enterprise risk analysis. In terms of the quality of information, there is often a gap between the information provided before a policy and the claims information, on top of the fact that the number of variables and parameters to query is anyway very high. The latter implies a need for insurers to start using different sources of information to better understand the IT security posture of their clients.

Figure 10 depicts the percentage of respondents using common security standards in their risk assessment process.

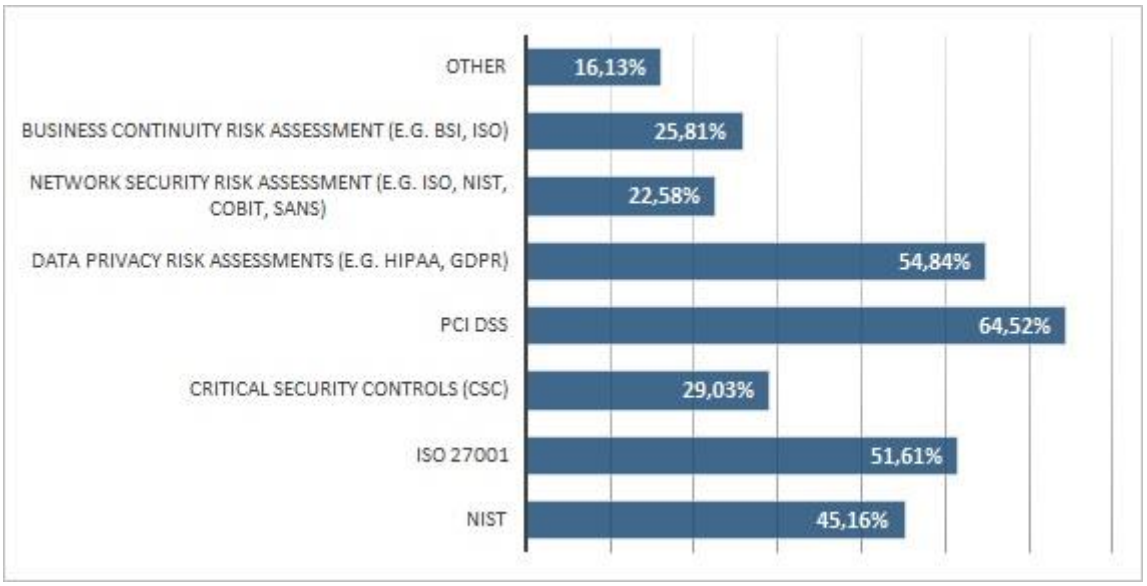


Figure 10: Use of standards in cyber insurance risk assessment

The application of cybersecurity standards for cyber insurance appears to be fragmented. The most prevalent standards used by the industry include NIST and the ISO series (e.g. 27001) though not one particular standard appears to be applied by a majority of the market.

PCI DSS (Payment Card Industry Data Security Standard) seems to be an exemption to the rule as almost three out of four insurers explicitly takes this standard into consideration. This is directly linked to the fact that this standard is mandated by the card brands and administered by a security standards council. Aside from the payment card industry, other industries generally (are mandated to) use sector-specific standards (e.g. HIPAA for Healthcare), while other factors may also mandate the compliance with specific standards, including company size (listed companies versus SME), and region (e.g. NEN for The Netherlands and BSI for the UK). This fact implies that **language harmonization may occur on a per-sector/industry basis as opposed to horizontally**.

One of the key factors influencing the development of the risk assessment language and all assorted cyber wording are **noticed and paid claims/incidents**. While traditionally viewed as drivers for insurance wording development, their importance is highlighted in the rapidly evolving cyber landscape. While most of the insurers interviewed reported having received no claims yet or having received very uncorrelated claims, they all acknowledged their potential impact on cyber wording; for instance, the publicity of recent ransomware attacks, such as WannaCry, would cause an insurer to proactively include security patching in their risk assessment if this topic is not already addressed. In fact, this questionnaire update in response to a rising risk as opposed to a claim is both faster and more efficient, while it allows revisiting risk assessments by asking follow-up questions to customers and re-evaluating the risk.

In order to prepare and update the underwriting forms, the vast majority of insurers have underwriters preparing the risk assessment forms, with only a few having a specialised cyber team of underwriters addressing these. In some cases, input from cyber risk and security engineers is integrated or external experts to provide industry-specific feedback. The frequency of updating cyber insurance wording does not appear to be standard across the industry but rather aligned to the insurers' continuous development of new products, to internally defined periods (e.g. annually) or triggered by specific events such as claims or incidents.

5. Cyber insurance market dynamics

The following chapter focuses on the dynamics of the cyber insurance market with respect to the harmonization of risk assessment language across the industry.

5.1 Assessing the impact of harmonization

It is important to assess what the potential impact of the cyber insurance market moving towards increased harmonization of risk assessment language would be. To that end, the respondents were asked to give their views by assigning a score on a scale of 1 to 5 (1 - Very negatively, 2 - Generally negatively, 3 - No significant impact, 4 - Generally positively, 5 - Very positively) on the respective impact of this harmonization for:

- The cyber insurance market in general
- Large Customers (Multinationals/Large Corporate etc.)
- SME (micro, small and medium-sized enterprises) customers
- Carriers offering cyber insurance products
- Insurance companies considering to enter or currently entering the market

The respective results are depicted in Figure 11.

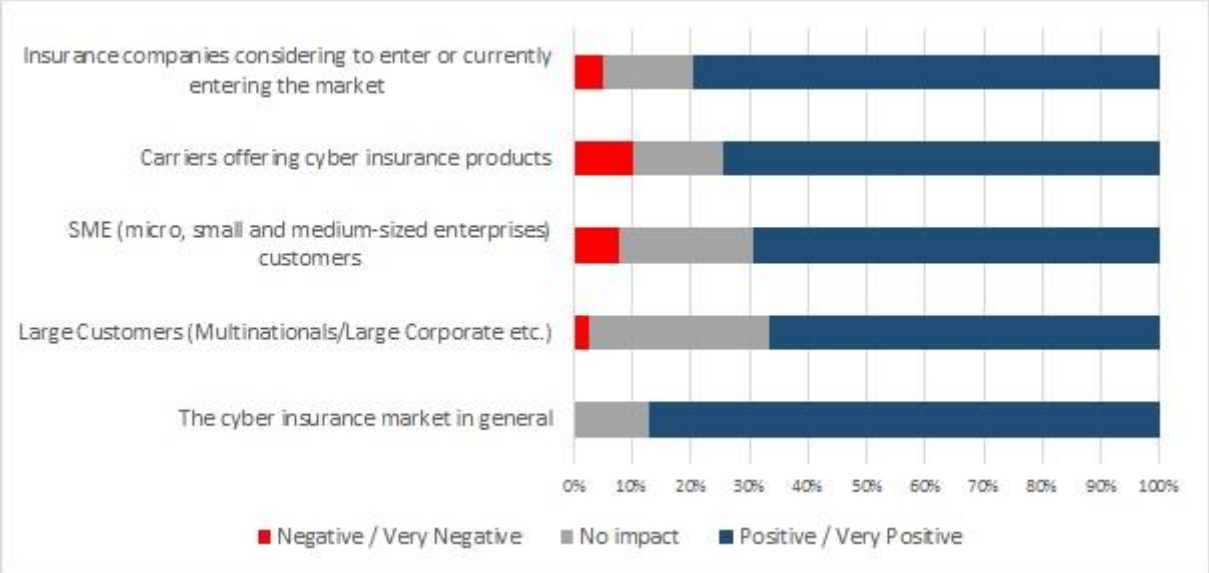


Figure 11: Assessment of the impact of risk assessment language harmonization

It should be noted that even though a lot of concerns were raised particularly with respect to the impact of harmonization to the competitive advantage of insurance carriers, the overall opinion appears to be overwhelmingly in favour of at least some degree of harmonization in the market. A summary of the expected impact for each of the main stakeholders is given below (in parenthesis is the average score for the impact to each stakeholder, where the higher the value the more positive the impact).

Carriers offering cyber insurance products (3,85)

- Competition between carriers will heavily shift to pricing and added value offerings

- Harmonization is expected as a natural result of the market maturation as most policies are already similar at a high-level
- Harmonization and standardization will help address the "education problem" wherein insurers have currently difficulty defining risks/incidents (e.g. is social engineering fraud or not?)
- It may make it easier to provide quotes to customers
- It will require more work to maintain due to the dynamics of the cyber landscape
- Competitive advantage of carriers with existing methodologies, wordings and IP will diminish
- Harmonization may make price (insurance premium) the dominant factor; this price competition may have the opposite result as whenever a cyber insurance portfolio of a certain carrier would become loss making (premium too low, losses too high) the premiums would eventually rise.
- Coverage is difficult to harmonize; while market would benefit from top-line harmonization, it is impossible to harmonize the risk assessment if the coverage itself is not harmonized
- For the insurer, harmonization will result in more clarity
- Improved communication with buyers who now think cyber insurance is not valuable, is too expensive, is not tailored to their needs, or is offering too little capacity with too much exclusions.

Insurance companies considering to enter or currently entering the market (4,00)

- Coverage is difficult to harmonize; while market would benefit from top-line harmonization, it is impossible to harmonize the risk assessment if the coverage itself is not harmonized
- Some degree of harmonization will be good, because there is a difference on understanding terminologies for example
- Clearer framework for developing cyber insurance products

SME customers (3,84)

- Since SME is an underdeveloped market, a harmonized questionnaire and wording can help develop it and establish a common understanding
- Less aware customers will better understand the options available to them
- Standardized products will be more attractive to SMEs and accompanied by simpler underwriting methods

Large Customers (3,77)

- Most products are bespoke and will remain so but the modularity that comes with harmonization will be beneficial
- Harmonization will allow clients to better understand the premium calculation
- Comparing products is difficult without a common point of reference

The cyber insurance market in general (4,02)

- Harmonization of policy triggers and wording definitions will be globally beneficial
- Industry will become less complex, more reliable, and gain credibility in the eyes of the customer
- Harmonisation will ease the work of brokers, since they would have less deltas to compare.

- While it would be easier for insurers and clients, markets have different philosophies and strategies, which might be a challenge to tackle with
- Easier adoption would drive growth
- Brokers will assess the correct insurer more easily and provide the right coverage for a particular client
- Increased rate of adoption as customers better understand the products

5.2 Barriers against harmonization

In spite of the near consensus on the benefits of risk assessment language harmonization, the market dynamics towards achieving it are halted by certain barriers. The main barriers against harmonization are depicted in Figure 12 and the key ones are briefly presented below.

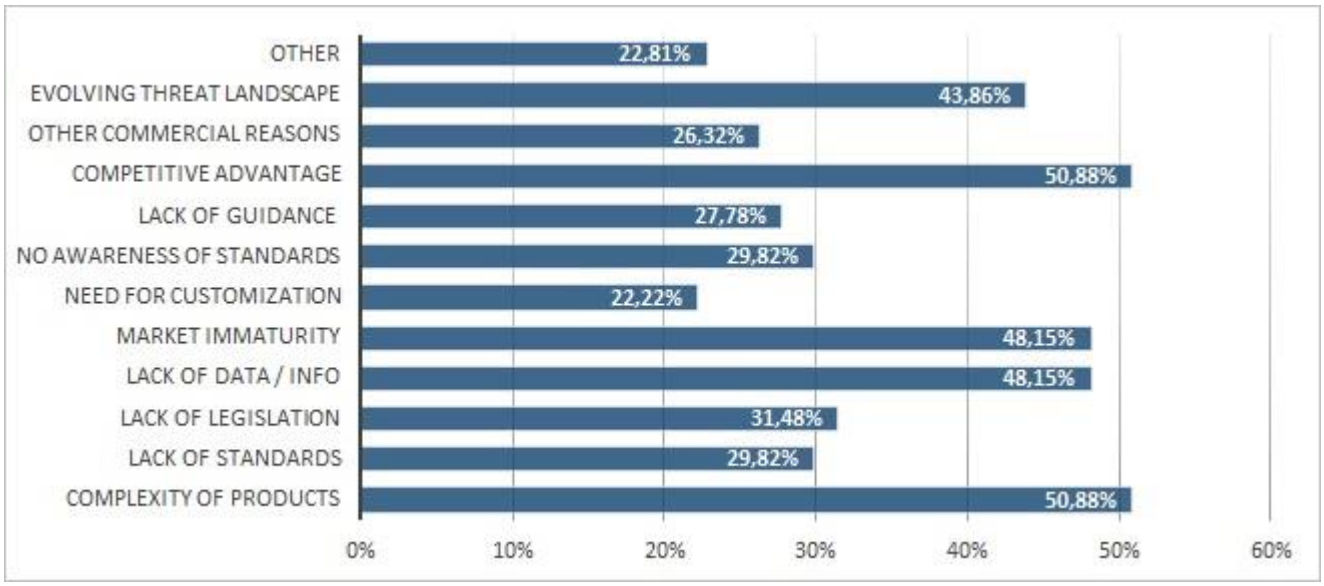


Figure 12: Barriers against harmonization of the risk assessment language in cyber insurance

- **Competitive advantage** was cited as one of the key barriers against harmonization. Insurers may often be reluctant to harmonize as they might perceive this as a loss of their unique selling points and depreciation of their intellectual property in terms of their existing risk assessment approaches. Currently the supply side is greater than the demand side which makes insurers prone to maintaining any competitive advantage as opposed to competing on price (currently a carrier may even accept a customer with poor or little underwriting information). A key reason cited against harmonization in this context is the limitations it may pose to the insurers' ability to innovate.
- **Lack of data / information** is another key factor against harmonization. Lack of data makes it very difficult for insurers to properly understand which industries are facing which threats, what is the motivation behind them, what is the loss frequency or severity, what is the loss correlation between industries, countries etc. On top of that, cyber insurance carriers are very reluctant to share their existing information amongst them. The resulting unavailability of incident data makes it very hard to produce consistent and converging risk assessment models.
- **Complexity of cyber insurance products and risk assessment** is a factor that increases the difficulty of risk assessment model convergence. The cyber risk assessment process requires the analysis and processing of multiple parameters and variables making it difficult for the market to naturally come up

with converging approaches. The dynamic cyber environment makes this even harder as it triggers frequent wording changes. Overall, compared to other insurance products, cyber is clearly much more complex and less uniform making product standardization difficult.

- **Market immaturity** provides a natural explanation regarding the lack of harmonization. As the market, especially in the EU, is considered to be at its early development stages, it is normal for carriers to compete by trying to develop the best possible product with little experience, a course that logically leads to "innovation by trial". This is additionally exemplified by the lack/shortage of cyber insurance specialists who would normally create enough knowledge and market osmosis to naturally lead to harmonization. IT Security firms have long been the dominant players and their view is one of a control environment with binary measures (focus is on vulnerabilities) whereas the insurers' focus is on exposures and want to understand insured losses.
- **Evolving threat landscape** is a key differentiator of cyber compared to other domains and acts as a barrier against harmonization. As carriers adapt their wordings and risk assessment to a risk environment that is highly dynamic, harmonization and language convergence is slower to catch-up. Even more so, maintaining a level of harmonization in a constantly varying environment is a difficult and resource-consuming task for carriers.
- **Lack of legislation** is a barrier that is expected to be shortly lifted in the EU with the adoption and enforcement of the GDPR and the NIS Directive. After data breach notification requirements became mandatory, the cyber insurance industry saw a definite uptake in the US cyber market, whereas the overall maturity was previously low. Security legislation tends to facilitate a more honest dialogue around cyber exposures which creates more of a partnership, where insurers want to 'incentivize' their clients as their security posture matures.
- **Lack of standards** and **No awareness of standards or frameworks** result in insurers adopting a fragmented approach and not converging on specific points of reference for conducting risk assessments. In practice, while security standards do exist the industry has yet to reach a consensus on which ones may be globally applicable – the latter is also related to the existence of industry-specific standards which often necessitate a sectorial approach to risk assessment.
- **Lack of guidance and alignment by European insurance market authorities** is another factor that leads to fragmented approaches in risk assessment. The absence of minimum coverage requirements removes a potential common point of reference that would support language convergence.
- **Need for customization and bespoke solutions** is particularly relevant for large corporate customers who have specific requirements and in-house Risk Management departments. Such customers are usually the key accounts for insurers and tend to favour highly customised solutions thus pushing the supply side in this direction.
- **Other commercial reasons** include customer budget constraints, the need to engage multiple stakeholders, customer privacy issues, changing market dynamics that naturally compete with harmonization (which benefits from a stable or less volatile environment), insurers' desire to satisfy individual and different customer needs and fear that the cyber insurance market will become commoditised

5.3 Incentives for harmonization

The incentives towards harmonization are very much aligned to the perceived benefits of this market evolution for the different stakeholders involved, as presented in section 5.1. Industry stakeholders engaged for this study were asked to select which quotes of a given set best describe the market incentives towards harmonization; the results are tabulated in Table 8.

Table 8: Key incentives for harmonization of risk assessment language frameworks

INCENTIVES FOR HARMONIZATION	%
"insurers that (wish to) enter the market will likely adopt proven risk assessment language and methodologies to satisfy client demand"	42,11%
"insurers that are already in the market will choose cyber insurance risk assessments as a business driver or competitive advantage"	50,88%
"the insurance market as a whole is being confronted with a complex and dynamic risk to underwrite – resulting in a standardization or harmonization of risk assessment frameworks"	43,86%
"risk assessment framework and risk prevention will be(come) tied to cyber insurance coverage leading to better risk pricing and/or loss reduction"	57,89%
"Awareness among customers is now increasing (GDPR as being key driver) and so is demand. Cyber insurance market growth may thereby harmonize risk assessment language frameworks (for data privacy risk) but not necessarily so in general"	56,14%
Other	26,32%

Insurance carriers were generally found to have the following key incentives to pursue harmonization of risk assessment language:

- **The risk assessment itself is in need of a form of harmonization**. There are reports of premiums with significant differences. In a recent example, it was found that the quoted premiums would differ as much as EUR 100K vs EUR 300K with no explanation as to how these differences came to be - clients do not understand either.
- Insurers understand the overall benefit of moving towards some level of harmonization and its potential impact on **the growth of the cyber insurance market**. Respondents also believe that this will create a virtuous cycle as the market growth will in turn lead to further harmonization of language frameworks.
- **Broker wording** may also be a very interesting topic for future development of harmonizing risk assessment language. More decision power to local branch offices as a result of increasing maturity of the market.
- **Addressing the needs of un-tapped market segments, particularly SMEs** that can better understand more standardized products or at least comparable offerings. Small buyers often "have a hard time quantifying" their risk exposures, which creates uncertainty about coverage needs and the cost/benefit generated from risk transfer.
- **Development of better products** as more data becomes available and cyber risks are better understood and quantified.
- **Legislation regarding information security and data protection** creates both increased demand and uniform requirements. Carriers have the incentive to converge to risk assessment language harmonization to address this growing market.
- Address a customer base that is maturing in terms of understanding cyber risk and has **growing expectations from risk transfer options**. Buyers with increased awareness expect to be able to compare products by price and value.

- **Industry-specific regulatory compliance** regarding IT security is a clear incentive for carriers to adopt a harmonized approach in order to provide offerings tailored to and understood by specific industries.
- Carriers seeking to enter the cyber market will likely **adopt good practices of other carriers**, while competition in general will lead to good practices gradually being adopted by the majority of the market.
- The type of insurance, and specifically insurance pooling should promote collaboration amongst the panel of insurers with an impact on harmonization as well.

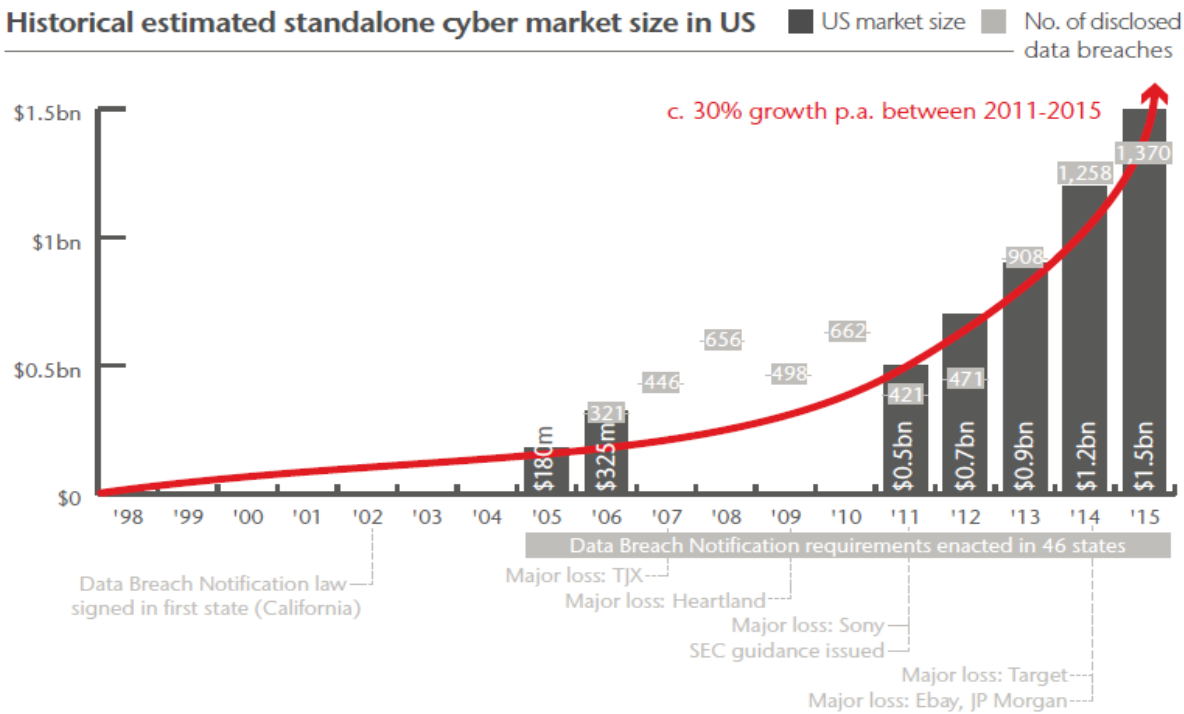
5.4 Main drivers of market dynamics

The following paragraphs examine in more detail the main drivers that are expected to steer the evolution of the cyber insurance market towards increased risk assessment language harmonization.

5.4.1 Regulations and Standards

One of the key developments in the EU that is expected to have a significant impact on the cyber insurance market is the adoption of legislation specifically addressing information security, namely the NIS Directive and the GDPR.

Both the NIS Directive and the GDPR mandate organisations subject to their provisions to have certain security controls in place and also to notify security incidents (in the case of GDPR, data breaches). The former creates common requirements for all affected organisations and, thus, a convergence in terms of security practices and residual risks, which in turn creates a natural common ground for insurance carriers to develop harmonized products. The latter not only creates similar requirements but has historically been one of the biggest drivers for market adoption of cyber insurance in the United States.



Sources: Betterley Report, Advisen, PropertyCasualty360, Business Insider, Marsh, Aon, datalossdb.org, Identity Theft Resource Center, NCSL, Ponemon Institiute, Aon Global Risk Survey, Aon Inpoint analysis

Within the context of this report, the questionnaires that were examined as part of the analysis presented in chapters 2 and 3 were found to reflect most of the major requirements of the GDPR such as Data Breach Notification, Accountability and Privacy by Design. This is a direct example of how well-defined regulatory requirements naturally drive cyber insurance products to language convergence.

A similar result is expected to come from the increased adoption of specific security standards both from the demand side, i.e. industries seeking to obtain cyber insurance products, but also from the supply side. While the market is currently fragmented in that regard, the adoption of specific standards as points of reference will result in consistent definitions and taxonomies, as well as a set of generally accepted principles on critical security controls and a standardized set of terms and conditions for cyber insurance.

5.4.2 Data Availability

One of the key problems the cyber insurance industry is currently facing is the lack of adequate data to support modelling and risk assessment in a sufficient manner. This is especially evident in cases involving 3rd party data and risk aggregation data. Combined with the lack of cybersecurity skills – as often cited – in the cyber insurance market, this results in carriers frequently having limited understanding of the risks. This issue also manifests itself in other ways, one being the fact that there is asymmetry of information between markets; currently there are 5 to 6 dominant market and about 60 to 80 markets with little data.

As more data on cyber incidents, financial impact, and claims become available, the cyber insurance industry will be in a position to develop improved risk assessment models driven by more client-specific data. As the data sources expand to include other feeds, such as threat intelligence, and with the development of the cybersecurity skillset within the industry, the underwriting process will become more efficient, more automated and more in-depth via improved information gathering and benchmarking.

5.4.3 Demand Side Evolution

The demand side for cyber insurance offerings in the EU is expected to grow significantly within the next few years and its evolution may be a key driver for carriers to adopt a more harmonized approach in their offerings.

A key factor in this demand side evolution will be SMEs; contrary to large organisations with internal Risk Management resources and complex environments, SMEs will likely pose different requirements, opting for standardized, understandable, easily comparable and transferable cyber insurance products. In order for carriers to tap this market segment, they will need to better communicate their offerings and to exhibit consistency in terminology, coverage types, policy triggers and pricing among others in order to build the buyers' trust.

Additional aspects of the demand side evolution that will push the suppliers towards harmonization include compliance with emerging regulations, education and awareness when it comes to cyber risks and increased investment in cybersecurity in general. As the complexity of many cyber insurance wordings currently creates uncertainty, the carriers are expected to start providing more guidance and harmonized, simplified wordings to end customers, while also partnering up with them to better understand the actual needs.

5.4.4 Market Maturity

Industry stakeholders expect harmonization of risk assessment language to be the natural result of market maturation. While opinions are divided as to the extent of harmonization in terms of coverage, questionnaires, terminology, policy triggers etc. the general consensus is that the current language fragmentation, albeit including elements of IP, proprietary approaches and competitive advantages, is largely the characteristic of a market still in its early maturation stages.

A number of factors are expected to play a role in the market maturation, aside from those mentioned earlier in relation to increased availability of data and market evolution to adapt to the regulatory framework.

Harmonization will come naturally as the market evolves, converges and shares information about loss scenarios, risk assessments, policy wording and claims. Interaction will drive harmonization as the market matures, as will data sharing via industry initiatives like ISACs.

Moreover, reaching a consensus on a minimum of standards will naturally enhance the ability of the insurance industry to improve the information gathering and benchmarking, and thereby the final results delivered to the buyers' market as a whole. This can take the form of defining loss scenarios and assorted costs, underlying factors and prevention controls.

Another driver of harmonization found in more mature markets is, surprisingly, the direct result of the mechanics of competition. As certain practices - or in the case of cyber insurance terminologies - are found to be useful and identified as industry best practices, market players tend to adopt them in order to improve their offerings. For instance, a carrier currently developing a cyber insurance product will take a page off an established player's playbook or a carrier already selling such products will seek to improve its practices by copying what seems to be working best. This best practice "osmosis" is further supported by the domain experts moving from one carrier to another and bringing with them acquired expertise.

6. Recommendations

Analysis of the study's findings together with the invaluable feedback provided by the interviewees resulted in the following set of recommendations. These recommendations are split in two groups based on the target audience and aim to support the growth of the cyber insurance market within the EU, with emphasis on how risk assessment language harmonisation can support this growth without limiting the carriers' ability to innovate.

Figure 13: Recommendations and their mapping to key market dynamics drivers

6.1 Recommendations towards the cyber insurance industry

The following recommendations are made to the cyber insurance industry and especially stakeholders involved in the development and use of risk assessment language.

- **Standardise policy language and underwriting questionnaires** to help insurers and customers mutually understand what they are selling and buying while avoiding the potential for coverage disputes and costly litigation
  - Standardise policy language and coverage to provide clarity and simplified wordings
  - Claims triggers should be part of language harmonisation / standardisation
  - Engage the demand side to focus standardisation efforts on customer needs
  - Standardise underwriting methods addressing the same risk / develop common questions to assess cyber risks based on industry best practices

  - Develop specific use cases and examples of claims triggers for different types of coverage and make them publicly available to potential buyers or include them as annex to contracts
  - Use high risk use cases such as IoT to develop common policy wordings and underwriting language; an industry-wide approach in these cases could support better risk assessment and a harmonised view of the potential aggregated risk
- **Promote data sharing between the industry stakeholders** via dedicated platforms or Information Sharing and Analysis Centres (ISACs)
  - Define data sharing formats that respect customer confidentiality (e.g. via anonymization) but provide enough data to support accurate risk assessment
  - Develop an industry template for sharing data to produce useful information (e.g. types of incidents, parameters/thresholds, cause, impact etc.)
  - Agree on means for industry to voluntarily share relevant information/data
  - Use information sharing platforms as means to define language commonalities
- **Develop industry standards** to define terminology, use cases, coverage, incident types, policy trigger parameters etc. The standards need not cover the full scope of cyber insurance products but can serve as a point of reference for suppliers and buyers of cyber insurance alike.
  - Standardisation efforts should be industry-driven and could build on existing efforts, such as those related to aggregated loss modelling
  - Standardisation efforts should prioritise incident taxonomies, coverage types, terminology and policy triggers parameters
  - Standards relating to the minimum amount of information collected during the application process could ensure that this race-to-the-bottom does not lead to irresponsible underwriting
  - More research on usage of open source intelligence to build customer risk profiles
- **Develop in-house expertise in cyber security** to support all aspects of the risk assessment process and provide the link between IT risks and business risks.
  - Develop underwriting methods for cyber with Information Security experts
  - Build in-house teams of cyber insurance experts or build networks of expertise
  - Develop knowledge bridge programs both for insurance experts and for Information Security experts
  - Investigate the possibility for insurance industry certification of cyber underwriters / risk engineers
- **Contribute in the collection of data** on aggregated loss or correlation scenarios
  - Support existing/emerging industry initiatives aiming to model aggregated risk
  - Such modelling requires common terminology/taxonomy and can be used as basis for language harmonisation
- Use **information security and data privacy regulations** (e.g. GDPR, NIS Directive) as the basis on which to develop common product frameworks.
  - Harmonise underwriting and coverage terminology based on regulations for offerings addressing risks regarding compliance
  - Define coverage modules based on the respective regulatory requirements for baseline security measures and incident reporting
  - Produce regulation-specific underwriting questionnaires
- **Focus language harmonization efforts on an industrial/sectorial basis** to benefit from the commonalities of the specific customer bases (e.g. threat landscape, vulnerabilities, compliance requirements).
  - Work together with customers to understand the specific sectorial needs

  - Understand and document the cyber risk landscape on a sectorial basis
  - Build common terminology based on sectorial compliance requirements and/or standards
- **Address the needs of the SME market** for more flexible and lightweight underwriting procedures and standardized/comparable offerings.
  - Simplify policy coverage wordings for SMEs
  - Define a lightweight underwriting process for customers with limited internal risk management capabilities
  - Underwriting for SMEs can be more automated and efficient, e.g. via a score-card approach.
- Support the cyber incident data collection process with various heterogeneous sources and **improve overall data quality**.
  - Augment the risk assessment process with additional sources such as threat analyses, open source intelligence etc.
  - Increase available data granularity
  - Improve incident data collection to include cause as much as possible in addition to the incident impact
  - The risk models commercial vendor risk assessment providers are offering to build a vendor risk posture profile might also be of value
- **Improve communication and information sharing** on affirmative or silent coverage for cyber exposures whenever policy language and conditions change.

6.2 Recommendations towards Policy makers

The following recommendations are addressed to EU and Member State Policy Makers.

- Create **minimum coverage requirements per type of coverage** on top of which insurers can build extra coverage.
  - These requirements should define what should **at least** be included for each type of coverage to provide a common, comparable point of reference. For instance, providing a minimum definition of what should be covered under a data breach cover policy would increase consumer trust in products offering this coverage via clarity and transparency and it will not be limiting to carriers developing offerings on top of that.
  - Regulatory authorities could define these minimum coverage requirements as common definitions organically emerge from the insurance industry.
  - Minimum coverage requirements should be aimed at providing modules/building blocks and not at imposing insurance obligations to buyers.
- **Leverage the upcoming mandatory incident reporting schemes** via the NIS Directive and the GDPR to produce meaningful data that could be used, among others, by the cyber insurance industry to expand its evidence base. Specific actions may include:
  - Consulting the Cyber Insurance industry stakeholders to map specific industry requirements as to useful information
  - Defining anonymization criteria that could make the data appropriate for sharing with the industry
  - Incident reporting will lead to a static snapshot at the time the notification takes place so data needs to be updated over time and versioning control should be used
- **Create a central EU wide repository** of incidents to provide aggregate data from multiple sources. Identify ways for sectorial ISACs to contribute to the data collection and to determine cross-sectorial impact of incidents.

- **Raise awareness** about cyber security and cyber risk management in organisations to build up demand and buyer maturity and to increase the cybersecurity posture of organisations seeking to transfer risk. Governments and policymakers should drive initiatives that raise awareness about cyber risks and the fact that cyber insurance can be part of the solution. This should reflect the fact that cyber insurance itself is not only a risk transfer mechanism, but also a means of risk prevention and risk mitigation and has therefore a positive effect in making businesses more cyber-secure.
- Encourage the active participation of the European Commission and ENISA in **developing guidelines for cyber insurance**. Specific actions may include:
    - Specific unbinding policy wording models and underwriting questionnaires
    - Good practices as to which questions, terms or concepts might be used by insurers to improve their questionnaires going forward
    - Recommendations about the type of underwriting information required for a thorough risk assessment
    - Pointing to key measures across existing security standards and through the use of terminology from bodies such as ISO
    - EU R&D funds towards activities that relate to threat modelling, aggregated risk analyses and definitions of common taxonomies specifically for Enterprise Risk Governance and Cyber Insurance

Annex A: ANOVA Methodology and sample statistical analysis

The one-way ANOVA compares the means between the groups of interest and determines whether any of those means are statistically significantly different from each other. This statistical difference is resembled in the **P-value**. When the P-value is below 0,05 the groups are said to be statistically different. It is important to note that the one-way ANOVA test statistic cannot specify which groups were statistically significantly different from each other, only that at least two groups were. More elaborate information on one-way ANOVA tests can be found in: "*Permutation Tests for Stochastic Ordering and ANOVA: Theory and Applications*" by Dario Basso, Fortunato Pesarin,Luigi.

Some samples of the statistical analysis conducted in the context of this study to examine the statistical differences among Security Standards, insurance coverage and underwriting questionnaires is given in the following:

ANOVA Security Standards						
Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	0,211111	8	0,026389	0,97043	**0,46084**	1,9929
Within Groups	4,65	171	0,027193			
Total	4,861111	179				

Security Standards. As the P-value is not below 0,05 the different security standards are not significantly different from one another. This also highlighted by the fact that F is smaller than F crit, which shows that the security standards are harmonized.

ANOVA Insurance Coverage						
Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	3,366667	9	0,374074	0,412168	**0,926298**	1,966054
Within Groups	99,83333	110	0,907576			
Total	103,2	119				

Insurance coverage. As the P-value is not below 0,05 there is no significant difference within the group. This also highlighted by the fact that F is smaller than F crit.

ANOVA Underwriting questionnaires						
Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	96,63284	10	9,663284	13,03112	**0,0001**	1,837413
Within Groups	1044,109	1408	0,741554			
Total	1140,741	1418				

Underwriting questionnaires. As the P-value is smaller than 0,05 the conclusion is that underwriting questionnaires are significantly different from one another. This also highlighted by the fact that F is larger than F crit. This shows that the cyber underwriting questionnaires are statistically different from one another.

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

TP-04-17-907-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-228-8
DOI: 10.2824/691163