Ania

Associazione Nazionale
fra le Imprese Assicuratrici

Cyber risk insurance in Italy

Insights from a survey across Italian insurers

Carlo Savino

Senior Economist - ANIA

11 October 2018

Introduction

In recent years, cyber risk has gained increasing attention. It has climbed to the top of the agenda of Institutions, public opinion, private sector and the insurance sector

As a consequence, there has been a strong rise in the interest towards instruments capable of preventing, mitigating and transferring this class of risks

Amongst these, a primary role can, and should, be played by cyber insurance coverages

However, in the present, most of the premiums in the global Cyber insurance market cover risks in the United States, leaving to the rest of the world less than 10% of the business

The state of the Italian Cyber insurance market

Italian Cyber insurance market makes no exception appearing at best to be still at an embryonic stage of development

According to an interview-based study on 5 Italian insurance groups carried out by IVASS, the Italian Supervisory and Regulatory Authority, outstanding Cyber insurance products are approximately:

- 2,000 in the retail (personal insurance) market insuring an average capital of €300
- 5,000 in the small business enterprise market, with an average insured capital of €30,000
- Less than 50, largely bespoke, contracts in the large corporation market insuring capital in the tens of millions

ANIA's Survey on Italian Cyber insurance

For all of these reasons, ANIA conducted a voluntary based survey across its Associates to increase knowledge on the some of the main characteristics of Italian cyber insurance market

- from the supply side (nature of risks, product specifications, pricing)
- from the demand side (customer base, drivers of its evolution, influence of the regulatory environment)

A few months later, EIOPA independently ran a surprisingly similar survey across 13 European (re)insurance groups on the same subject

This allowed us to get some additional interesting insight from the comparison between the Italian Cyber insurance landscape and the European one

The questionnaire

The questionnaire is divided into four sections

A. Perception and characteristics of cyber risk

This section assesses the level of the insurers perception of the impact of cyber risk on the overall economy, in terms of size and complexity, both in the present and in the medium-term, also taking into account recent regulatory changes (GDPR, NIS)

B. Features of cyber coverages

The objective is to gather information on the characteristics of cyber coverages currently available on the market, in terms of: types of coverages, the nature of the events covered, as well as some critical issues such as non affirmative cyber risk (silent risks)

C. Customer base/industrial sectors

This section focuses on the main characteristics of the demand for cyber coverages and the market to which they are addressed

D. Risk classification and underwriting practices

In addition to investigating the risk classification criteria and the practices adopted in the underwriting phase, this section asks participants for information on the main drivers of the present and future demand

The sample

20 (re)insurance companies participated in the survey. Direct companies added up to 34% of total direct non-life premiums collected in 2017 Amongst these:

- 4 companies with a premium volume of over € 1 billion
- 4 companies with premiums between € 300 millions and € 1 billion
- 10 companies with premiums up to € 300 millions

Representing around 10% of non-life premiums, 6 companies answered questions included in all four sections of the questionnaire and therefore could be identified as companies that include cyber policies/coverages in their products on offer

The remaining 12 insurers plus 2 reinsurers essentially replied to the questions in the general section (section A) and therefore it was not possible to obtain information about their cyber products

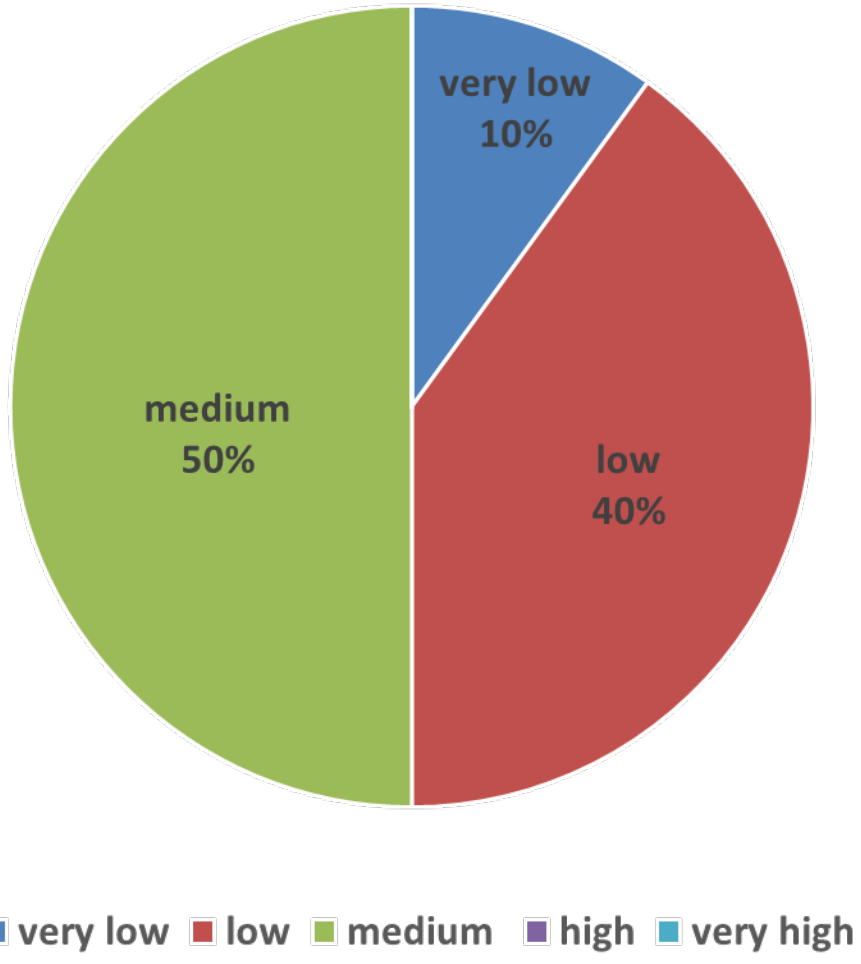
Cyber risk perception in the overall economy

Insurers do not (yet) perceive the **current** level of cyber risk in the economy as a particularly serious threat

On a scale of 1 (very low) to 5 (very high), half of the companies judge the severity of the threat to be very low or low, while the other half judge it to be at a medium level

Companies that provided information on their cyber offer give a more pessimistic opinion about the threat

On the other hand, insurers coincide that cyber risk awareness of the public is generally poor

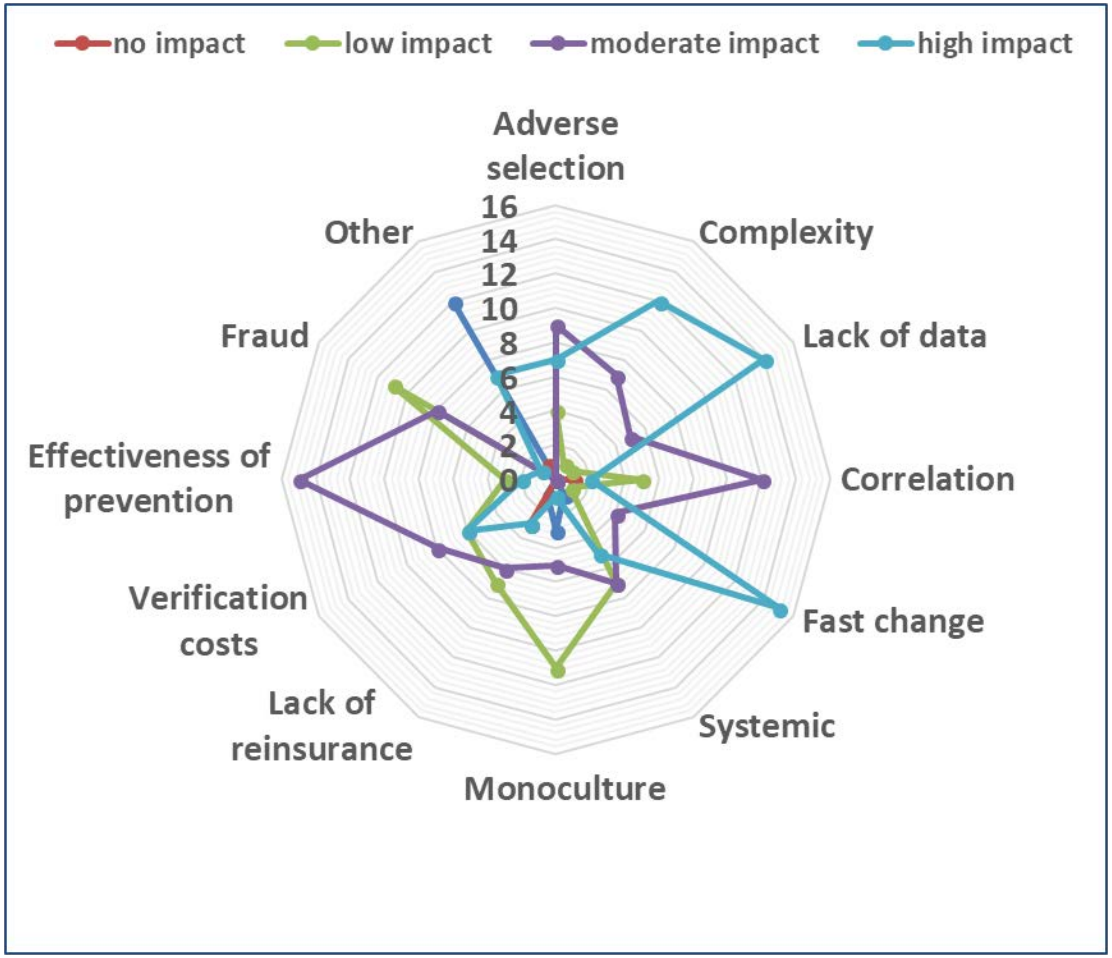


Barriers to Cyber risks insurability

Analysts generally agree that some features peculiar to cyber risk make its insurability more complex

This emerged clearly from the survey. When asked about the factors that could hinder underwriting, most insurers highlighted complexity, speed of change and lack of reliable databases

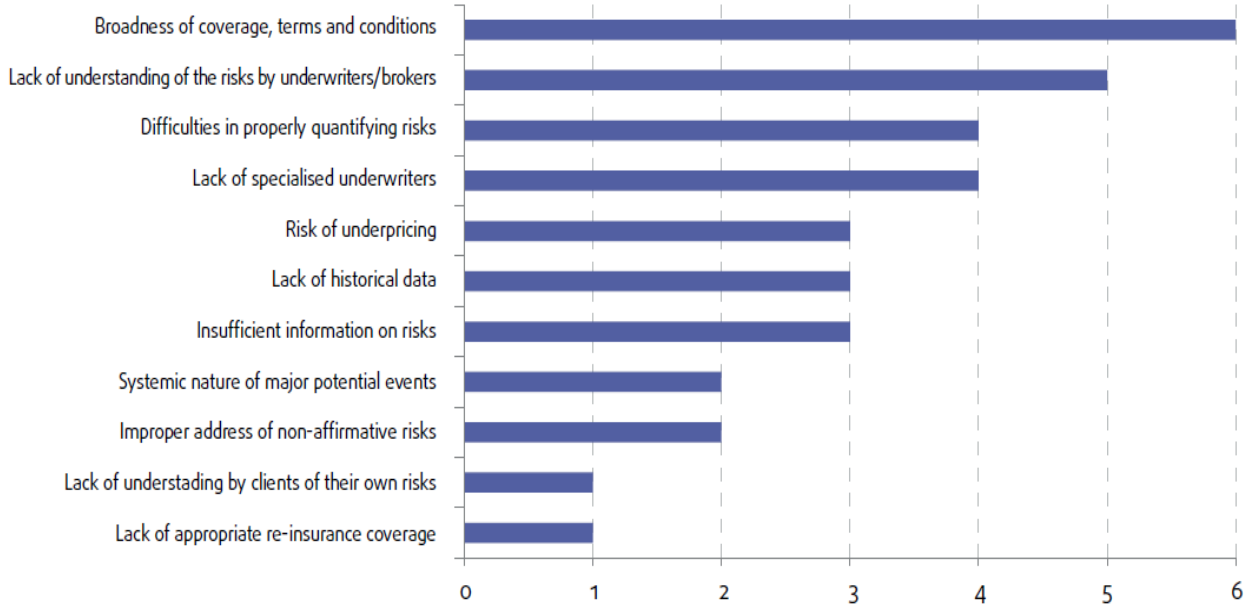
However, factors such as vulnerability to fraud and monocultures, such as the limited variety of operating systems adopted, are not considered that important



EIOPA: European insurers concerns

According to EIOPA's survey European insurers' first preoccupation comes from currently commercialised products that feature excessive broadness in terms of coverage, terms and conditions

Apart from this, European insurers share with Italian players a remarkably high number of critical concerns: Lack of understanding (due to complexity) and scant historical data appear as major critical issues

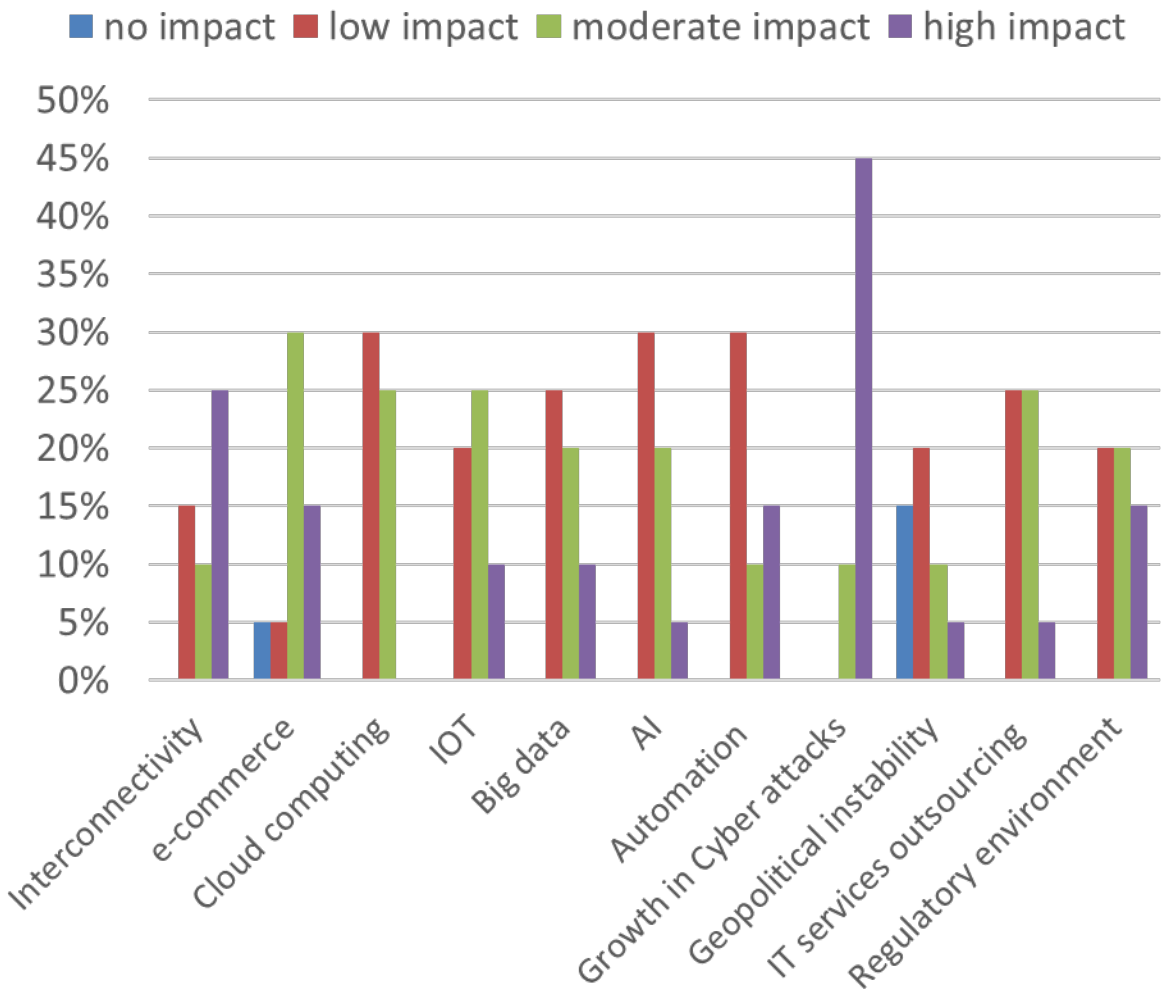


Drivers of cyber insurance demand

According to the survey demand is driven mainly by the increased importance of the threat of cyber attacks

9 out of 10 respondents to this question reported that most cyber incidents come from deliberate attacks

This is pretty much in line with the view of insurers interviewed by EIOPA, who indicated the recent global cyber attacks (WannaCry and NotPetya) as key factors behind the recent growth in demand



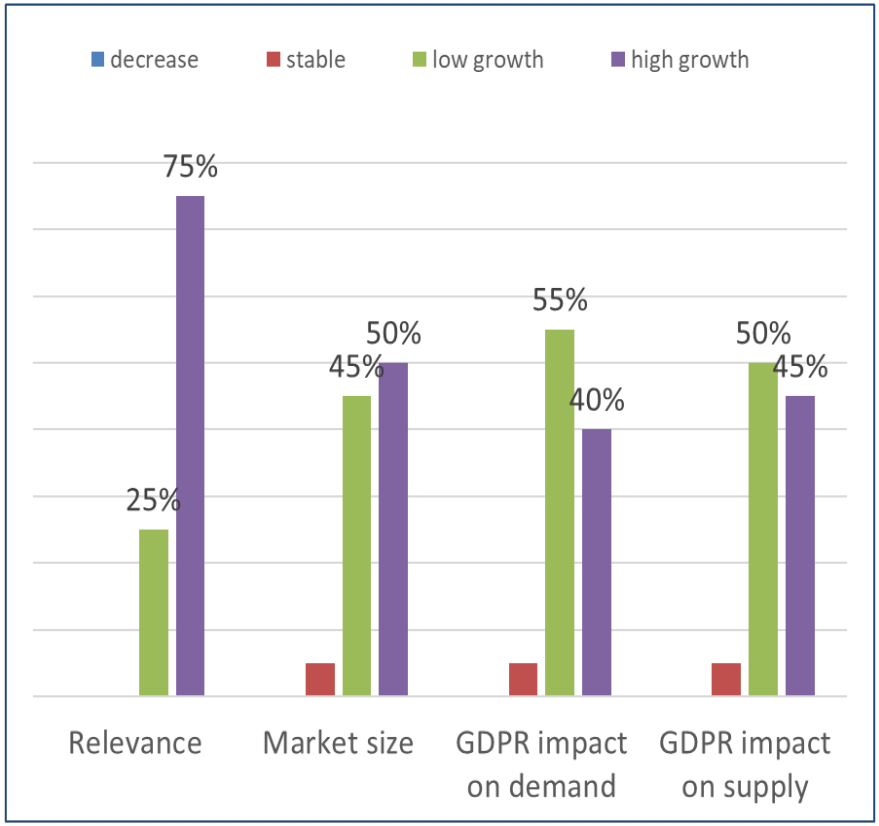
Cyber insurance market prospects

The survey shows that most insurers agree that increasing digitalisation and interconnectivity will be accompanied by an increase in the importance of cyber risks

There is less agreement on the market opportunities that this growth will offer

Almost all respondents expect the GDPR implementation to push further demand and supply of Cyber insurance coverages

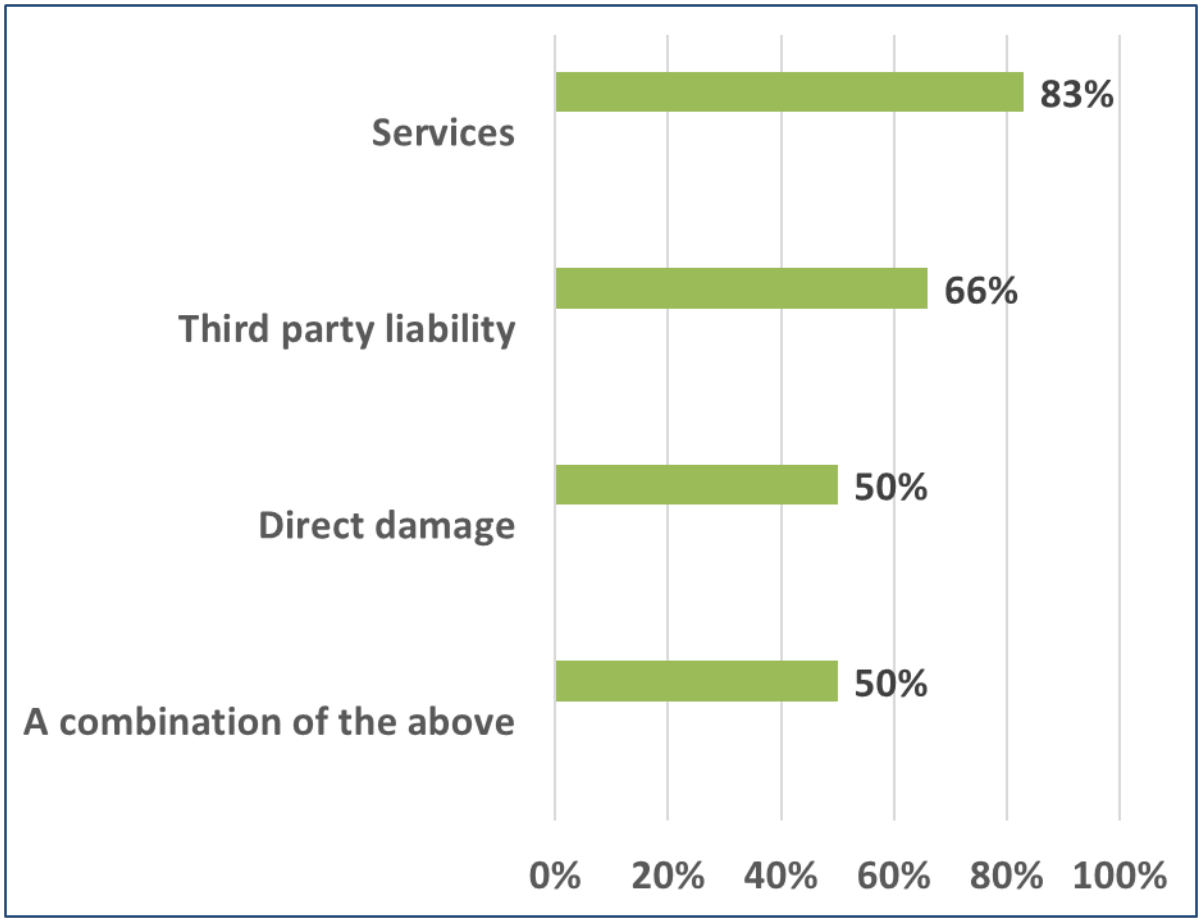
EIOPA's study highlights similar views on the impact of GDPR, with participants predicting a slow but steady increase in Cyber insurance demand along with increased awareness of the risk



Characteristics of Cyber insurance products marketed in Italy

Insurers operating in the Cyber insurance market offer: pre and post-event solutions, coverage of damages suffered by third parties and direct damages

Half of the companies offer bundled products

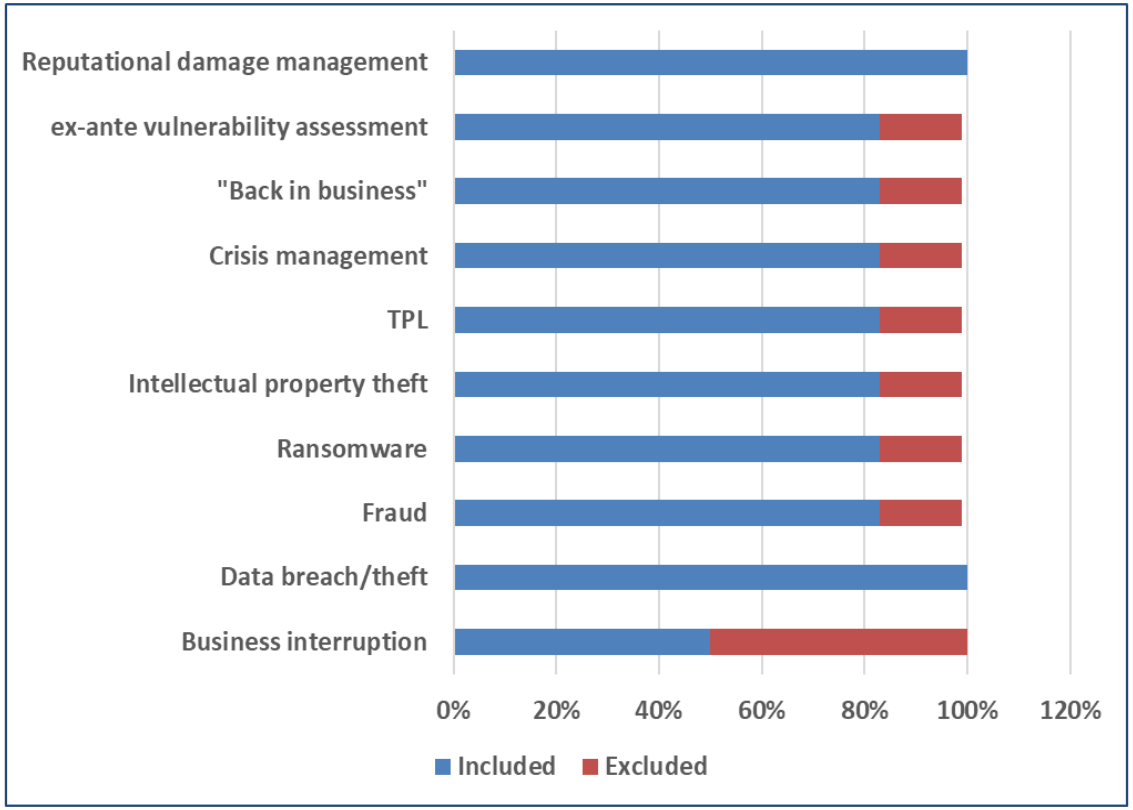


Guarantees included in Cyber policies marketed in Italy

As regards of type of coverage/service, there is a certain homogeneity in the product offer: all insurers offer reputational damage management and almost all cover typical coverages/services.

The most critical coverage, business interruption, is not offered by half the sample (not surprisingly)

The picture emerging from EIOPA's study show few or no similarities. There doesn't appear to be a clear pattern with all insurers offering different combinations of guarantees/services



Non-affirmative cyber insurance (silent risks)

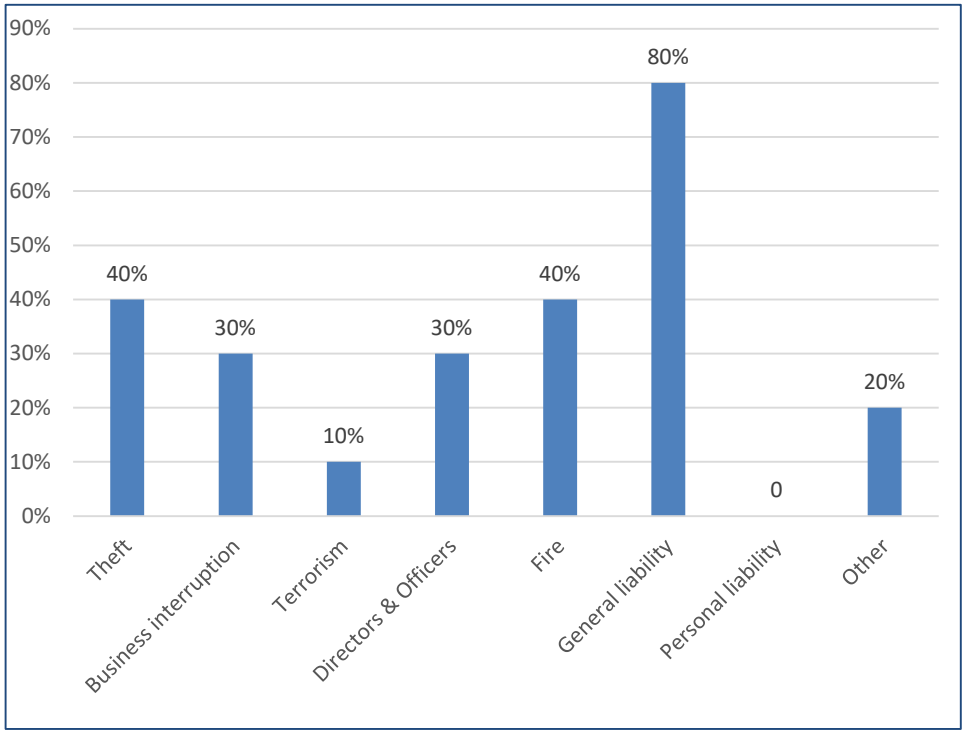
Overall, insurers believe that their general liability products implicitly covers risk. A smaller, though not negligible, number believe that the cyber risk is implicitly covered by theft, fire, business interruption and directors & officers coverages

Nevertheless, on the whole the companies that have answered this question judge their exposure to the overall medium-low risk

All insurers selling multi-risk policies report that Cyber risk is explicitly excluded

European insurers have similar views on this subject although they specify that impact of NARs is difficult to assess

They however differ on the level of concern of NARs they perceive, considering their impact potentially substantial

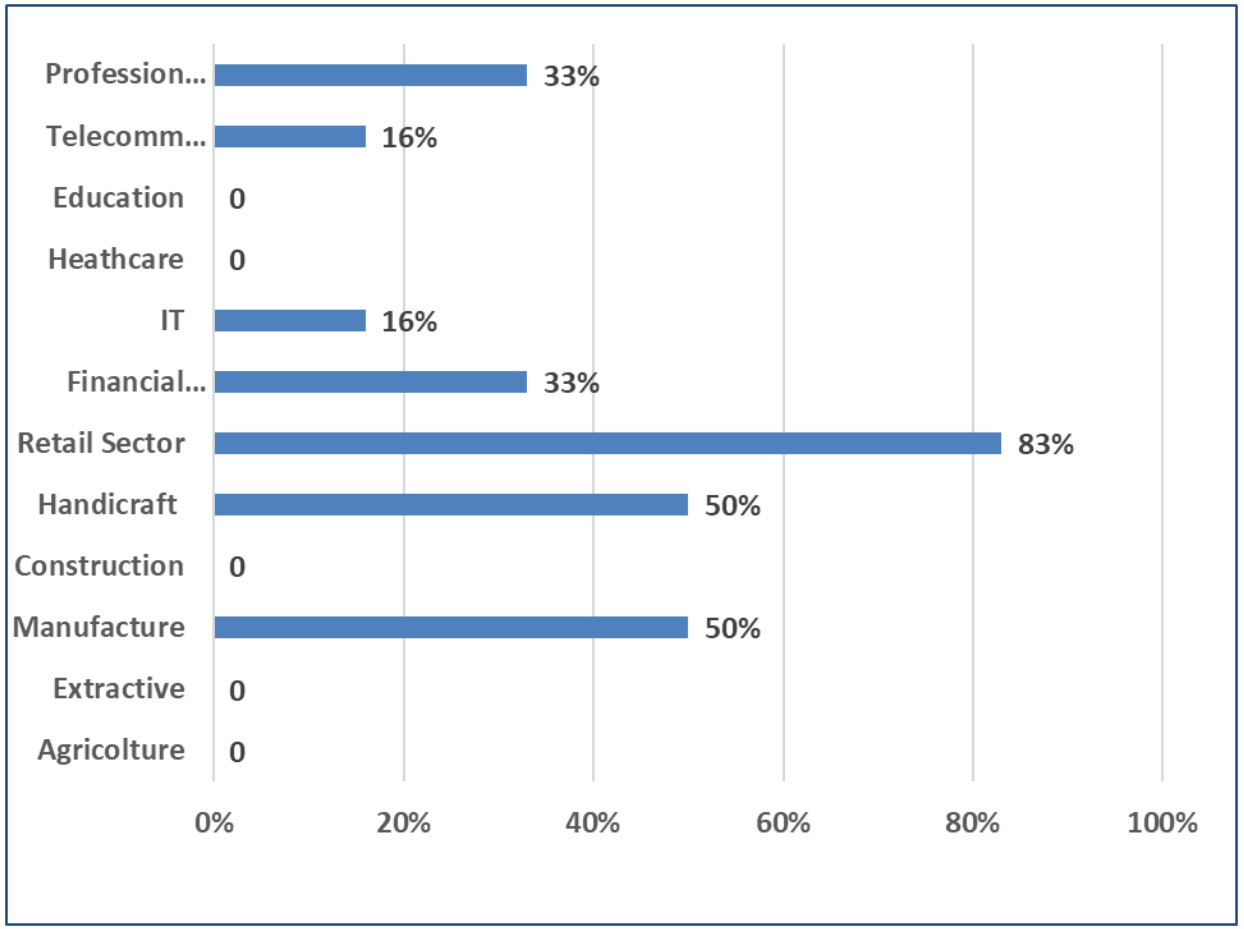


Corporate clients by industrial sector

Cyber insurance products are predominantly directed to corporate clients, but offer of solutions for the retail market is growing

Most corporate clients are from sectors with a predominance of small and micro-sized enterprises: retail sector, handicraft and manufacture

Surprisingly financial services, healthcare and IT services (generally considered most exposed to cyber risk) resulted to be only marginal in this market

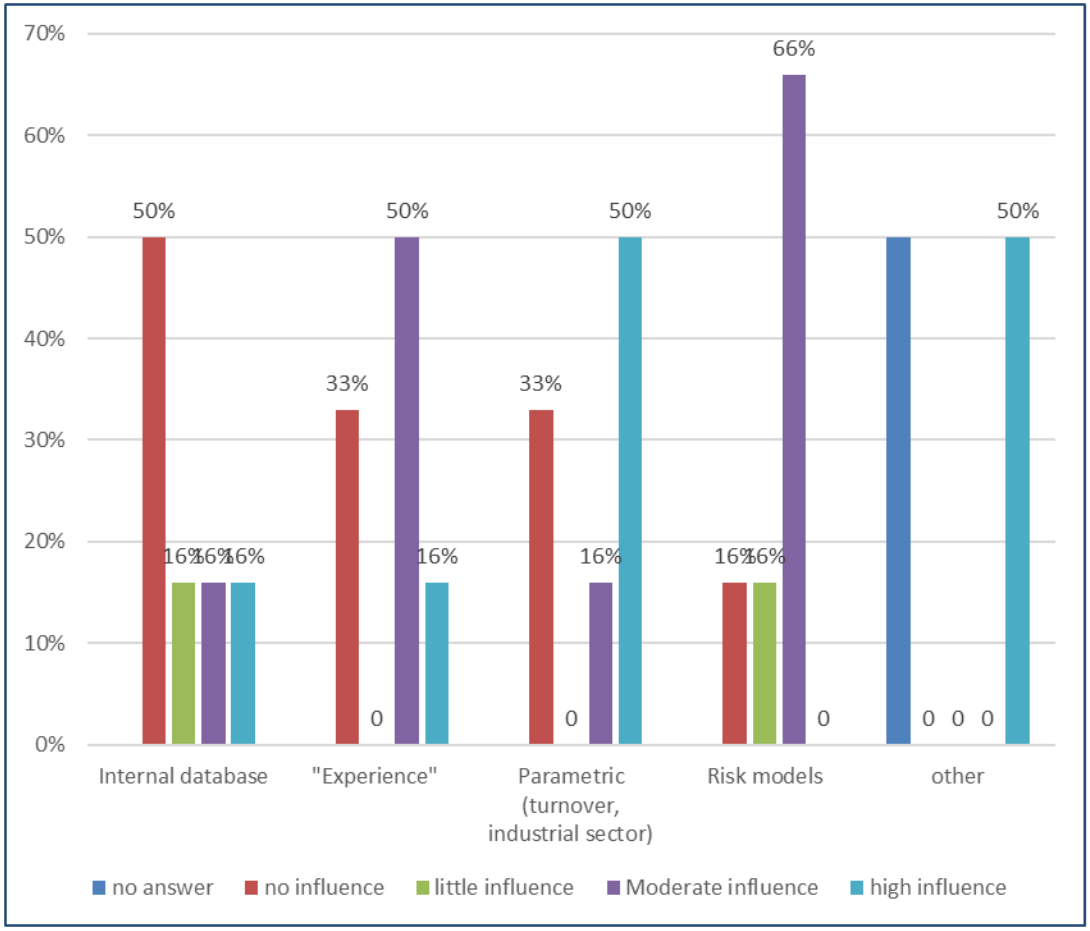


Pricing criteria

No clear picture about which criteria are more frequently adopted to classify and price cyber risk

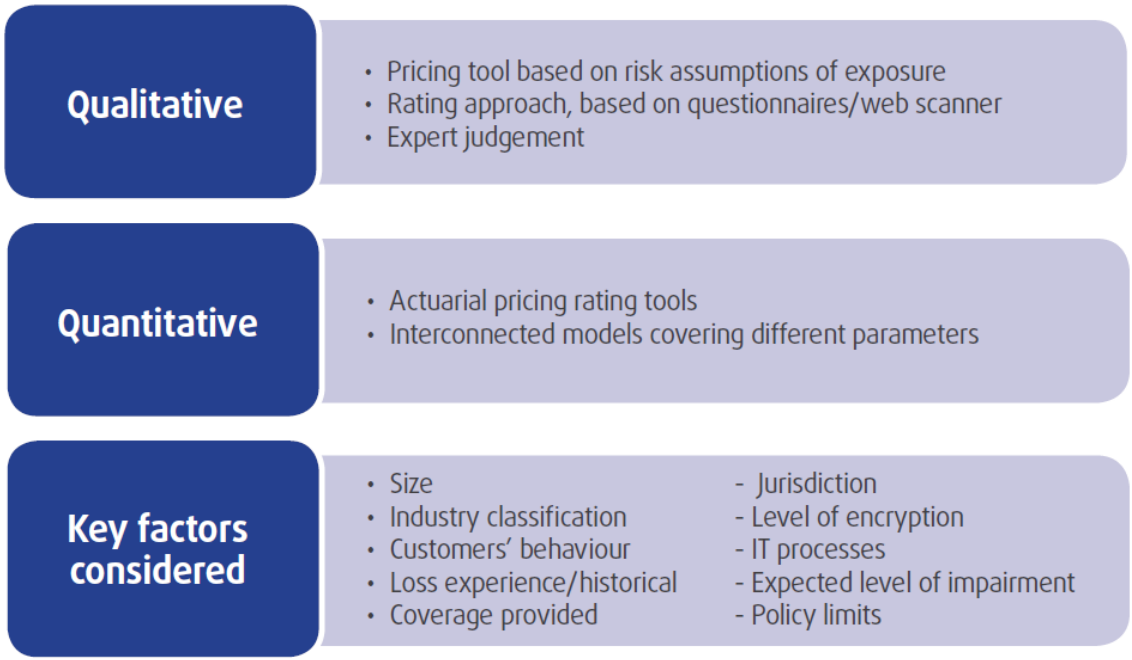
A minority of companies rely on internal databases, probably because they are not yet sufficiently rich, resorting in most cases to assessments based on risk models, international experiences, generic parameters (turnover, business sector) and the cost of reinsurance

All companies reported the employment of pre-underwriting risk assessment



European insurers pricing criteria

European companies responded to a similar (however more articulated question) pretty much in the same way



Summing up

- Diffusion of cyber insurance policies in Italy is at a very initial stage
  - Weak demand due to low awareness in the general public coupled with…
  - …limited offer of insurance solutions owing to:
    - Lack of reliable historical data on claims/incidents
    - Growing complexity and fast change
    - Accumulation/Aggregation
    - …
- Incidents are expected to be on rise in the next future
  - Increasing digitalisation of the economy
  - Changes in the regulatory environment

- We have to be prepared!

Future challenges: three pillars

- **Awareness**
  - At present, the cyber threat is highly overlooked by many stakeholders involved
  - Cyber threat is by its own nature elusive: most people don't even realise they've been attacked
  - Ingnorance is NOT bliss: the less acquainted is someone with their vulnerabilities, the most vulnerable they end up being
- **Knowledge**
  - Being wary on one's cyber vulnerability isn't enough to avoid incidents
  - Inherent complexity and fast dynamics of the cyber environment calls for significant investments – especially in human capital
  - For insurers this would result in a better understanding of risk and costs profiles, impact of accumulation/aggregation, role of human factor. This will eventually lead to efficient underwriting and more accurate pricing
- **Cooperation**
  - Insurance coverage capacity can be improved, but not without limits
  - Cyber risks needs a multidisciplinary approach, in which insurance operates along with reinsurers, risk-managers, IT security experts, Academia, trade associations, regulators, governments

Ania

Associazione Nazionale
fra le Imprese Assicuratrici

Thank you

Cyber risk insurance in Italy

Findings from a survey across Italian insurers

Carlo Savino – Senior Economist

11 October 2018