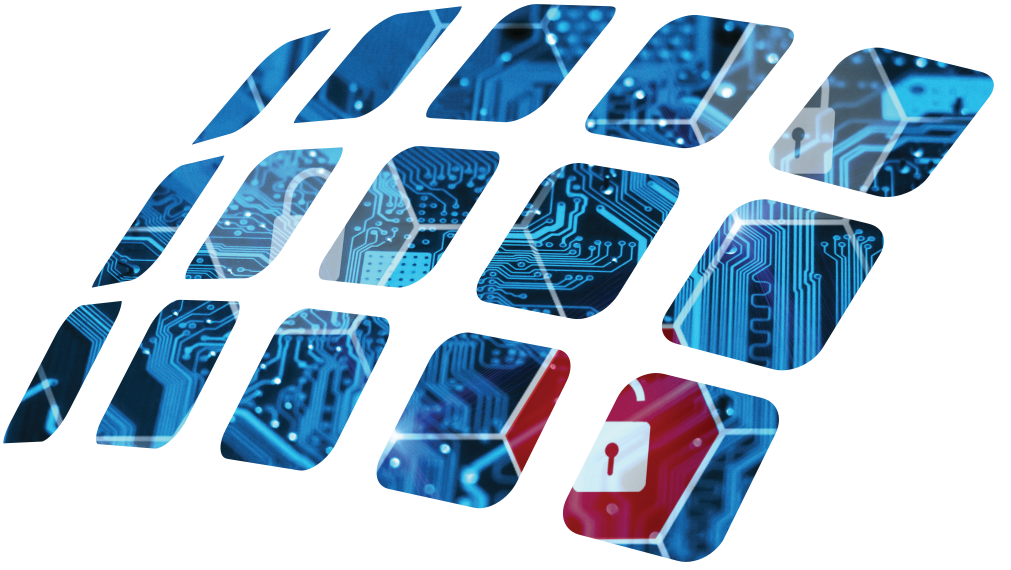
insurance europe



Insurers' role in EU cyber resilience

Introduction

Reliance on digital technologies is growing — opening the door to innovation, efficiency and convenience for citizens and companies. Yet those benefits come at a cost; they increase vulnerability to cyber attacks and exposure to privacy risks.

According to the World Economic Forum's 2019 "Global Risks Report", respondents ranked cyber risks highly among the issues that concern them most. Specifically, around two-thirds of respondents expected the risks associated with fake news and identity theft to increase in both likelihood and impact in 2019, while three-fifths said the same about loss of privacy.

While the EU has recently made huge advances in terms of bolstering Europe's cyber resilience (see box on p4), there is still a long way to go. Companies and citizens are increasingly aware of the risks to which they are exposed, but struggle to translate this awareness into concrete measures to protect themselves. This is where insurance can help.

The role of insurance

The insurance industry has key roles to play in assisting the EU in its efforts to increase cyber resilience and competitiveness.

- Insurers can ensure business continuity by helping companies swiftly recover from cyber attacks.
- Insurers can increase citizens' and companies' awareness of the cyber risks to which they are exposed and offer effective protection against them.
- Insurers can advise European and national policymakers on cyber risks and how they can be better managed and mitigated.

Insurance has always played an important role in companies' risk management. It acts as a mechanism to transfer risk and provides companies with compensation for losses that cannot be fully prevented.

In the case of cyber risks, insurers also assist policyholders in dealing with some of the non-pecuniary aspects of an attack by helping to prevent cyber attacks and mitigating the effects of successful attacks.

What does insurance cover?

Cyber insurance can cover a variety of the consequences of cyber risks, such as the phishing, data breaches or malware that can affect companies. It can provide first-party cover, such as for damage to digital assets, business interruption and incident response costs, as well as third-party cover, such as for privacy and confidentiality-related liabilities.

In addition to this, some cyber insurance policies provide policyholders with a service element that helps them assess their potential exposure and also provides technical, legal and public relations assistance in the event of an incident. The overall offering helps to improve the cyber resilience of policyholders and assists with mitigating action should an incident occur.

Cover varies greatly depending on the needs of the buyers, the type of cyber risks to which they are exposed and/or their level of digitalisation, as well as their size and the kind of services they provide.

Cover can be sold as a stand-alone cyber insurance product or as part of an insurance product in a traditional business line. For example, certain types of cyber losses can be covered by property, directors and officers, fidelity or civil liability policies. Under traditional products, cover can be offered either explicitly or not.

This varied landscape is one reason why good communication between insurer and insured is so important[1].

1 See "Preparing for cyber insurance", Insurance Europe, BIPAR and FERMA, October 2018

The EU regulatory landscape

Under President Juncker's European Commission, cybersecurity became an EU priority for the first time, leading to important advances:

NIS Directive

The Network and Information Security (NIS) Directive, adopted in 2016, is the first piece of EU-wide legislation on cybersecurity, providing the legal measures that boost overall levels of cybersecurity.

The NIS Directive also obliges companies under its scope — notably operators of essential services and digital service providers — to notify the relevant authority of serious cyber incidents. More importantly, these companies have to implement adequate cybersecurity measures.

GDPR

The General Data Protection Regulation (GDPR) came into full effect in May 2018 and is the core of Europe's digital privacy legislation.

The GDPR obliges companies to comply with strict rules relating to the private data they handle. It also requires companies to notify their national data protection authority of (personal) data breaches. Non-compliance with the GDPR can result in fines of €20m or 4% of annual turnover, whichever is higher.

Cybersecurity Act

The Cybersecurity Act, adopted in December 2018, gave the European Union Agency for Cybersecurity (ENISA) a permanent mandate and strengthened its role. The Act also establishes an EU framework for cybersecurity certification.

The development of an EU cyber insurance market

By most estimates, Europe accounts for less than 10% of the global market for cyber insurance. However, it is difficult to be precise, as most data refers only to stand-alone cyber insurance products or focuses exclusively on larger companies, where insurance penetration tends to be higher. Indeed, the cyber insurance market in the EU currently depends mostly on demand from large companies and, to a lesser degree, SMEs. Although the market for cyber insurance in personal lines is growing, it is currently very limited in most EU member states.

What is clear, though, is that there are still several hurdles that need to be overcome before cyber insurance becomes a mainstream product. One of those is the fact that cyber risks are difficult to quantify and assess.

Particularly challenging is estimating the possible losses stemming from cyber incidents, which can be very complicated. This is due to a number of factors, including:

- **Uncertainty of potential future losses**
  With cyber attacks increasing in frequency and severity and the legal landscape evolving to respond to new threats, forecasting future losses is difficult for insurers.
- **Highly correlated risks due to widespread use of certain operating systems**
  As certain operating systems increasingly dominate, a cyber incident with one of them can have far-reaching effects.
- **Little available data on cyber incidents and losses**
  Insurers traditionally model losses using actuarial and historical data. However, for cyber risks, historical data is scant and actuarial data is practically non-existent.
- **Increasingly intangible losses**
  For example, a company that has been attacked and suffered a breach of personal data can face reputational damage that is very hard to quantify.

Insurers that have decided not to offer cover for cyber risks are nevertheless reviewing their existing portfolios and business lines for "silent", or unintended, exposures. Those that do decide to cover cyber risks, meanwhile, are gathering the underwriting expertise and data needed to price risks more accurately, as well as ensuring that their portfolios take account of these new risks.

Policy recommendations: Dos and Don'ts

Despite the challenges, cyber insurance has a huge potential to help Europe increase its cyber resilience. EU policymakers are in a position to support the role insurance can play in a variety of ways:

DO

- Promote awareness-raising, which is key to increasing cyber resilience
- Support public-private cooperation on catastrophic risks
- Urge member states to act to increase cybersecurity
- Support efforts to make cyber-incident data available

DON'T

- Introduce premature standardisation, which can harm both customers and insurers
- Introduce mandatory insurance for cyber risks, which would be counterproductive

Policy recommendations: Do

Promote awareness-raising, which is key to increasing cyber resilience

Companies of all sizes are at risk of cyber attacks and many are either not yet aware of or are still grappling with how to mitigate their risk exposure. Businesses also need to understand that cybersecurity matters are not just the domain of the IT experts in a company. Rather, cybersecurity should be discussed at board level to ensure that all parts of a company are aware of the measures that need to be implemented.

More needs to be done at European and national level to help businesses and individuals understand and handle cyber risks. This step is key before companies decide whether to integrate insurance into their overall risk management strategy.

Raising awareness about the role of insurance in dealing with cyber risks is also vital in decreasing gaps in protection. This has been the case for other risks such as natural catastrophes, where insurance has become increasingly crucial in the protection of citizens and companies against increases in weather-related events.

Insurers and policymakers should work together to accelerate the development of a cyber-risk culture among citizens, businesses and public authorities and the creation of a digital security framework for micro-businesses and SMEs. Insurance associations are already taking steps at national level to raise awareness. Examples of their actions can be found at the back of this booklet and on the Insurance Europe website[2].

Support public-private cooperation on catastrophic risks

In order to tackle cyber risks adequately and increase cyber resilience, public authorities and the private sector need to work together to develop solutions for large and complex risks. Open dialogue is needed to assess how the industry can help authorities achieve greater cybersecurity across all sectors and how public authorities and insurers can cooperate in the event of catastrophic losses.

Forms of cooperation could include:

- Simulating cyber attacks and implementing lessons learned.
- Starting a discussion on large-scale, state-on-state or terrorism-driven cyber scenarios and the limits to insurability.
- Managing large or accumulated risk exposures. Certain risks may be too large for the insurance industry to cover and may require solutions involving the state, such as state risk pools.

Insurance Europe and its members are ready to engage with policymakers on all these issues and to provide their unique expertise where needed.

2 www.insuranceeurope.eu/cyber-insurance

Urge member states to act to increase cybersecurity

Member states have a crucial role to play in increasing Europe's cybersecurity. Cyber risks do not respect borders, so member states should:

- Coordinate their intelligence-sharing and efforts to raise preparedness with other states.
- Cooperate on identifying the sources of cyber attacks, as this will enhance preparedness and prevention.
- Look to revise legal frameworks to ensure that cyber crimes can be prosecuted and that punishments act as a deterrent.
- Direct public and private investment to the development of European excellence in cyber technology.
- Develop certifications and labels to attest to the cybersecurity of products and services. Cybersecurity of products is a key prerequisite for preventing cyber attack-related losses.

Support efforts to make cyber-incident data available

Lack of available data on cyber risks is one of the primary barriers to the development of the cyber insurance market. Due to the rapid pace at which technology and its associated risks develops, there is very little historical and actuarial data. This makes it difficult for insurers to understand and price cyber risks, as the European Insurance and Occupational Pensions Authority (EIOPA) has acknowledged[3].

National and EU-wide data is currently being gathered as a result of the requirements in several pieces of legislation that oblige companies to report cyber incidents. These include the EU's General Data Protection Regulation (GDPR) and the Network Information Security (NIS) Directive (see p2).

These data collection exercises could be leveraged to help the insurance industry increase its knowledge of cyber risks. Insurance Europe would like to discuss with policymakers ways in which the insurance sector could access, on an anonymised basis, the data relevant for underwriting purposes. It believes that the European Union Agency for Cybersecurity (ENISA) would be the right EU platform to initiate these discussions.

3 https://eiopa.europa.eu/Publications/Reports/EIOPA%20Understanding%20cyber%20insurance.pdf

Policy recommendations: Don't

⊗ Introduce premature standardisation, which can harm both customers and insurers

It is sometimes argued that standardising insurance policies will stimulate the supply of and demand for insurance. However, this would currently not work. The cyber insurance market is continually evolving to meet the changing landscape of risks and consumer demands. Standardisation would inevitably become quickly outdated and would not provide adequate guidance for businesses. As with prematurely making insurance mandatory (see section below), standardisation at this stage would negatively impact policyholders and insurers:

- Policyholders forced to buy standardised products are more likely to purchase cover that is not tailored to their needs and/or to buy either more or less coverage than they actually need.
- Insurers need the flexibility to tailor the policies to their clients' risks, and policy language is still evolving to reflect changing threats.

Insurance Europe opposes imposing premature standardisation in cyber insurance. Standardisation will occur organically as the market develops.

⊗ Introduce mandatory insurance for cyber risks, which would be counterproductive

It is often thought that compulsory insurance schemes are the best way to ensure the availability or take-up of insurance, particularly for new risks such as cyber. However, compulsory insurance is, generally speaking, not appropriate for new risks.

In general, choosing whether to purchase insurance should be a decision for individuals to take based on their risk appetite. Exceptional circumstances nevertheless exist in which insurance is legally mandated so that third parties always have access to compensation. Motor insurance is one example. Such compulsory insurance schemes only work if specific conditions are met. If they are not, inappropriate provisions can do more harm than good.

In the case of cyber risks, where the insurance market is still at a very early stage, these conditions are not yet met:

- Penetration rates for cyber insurance in Europe are currently very low. Increasing them to 100% would require an expansion in (re)insurer capacity that would not be possible, even if the obligation were implemented over a number of years. This is particularly the case in some member states in which the number of insurers offering cyber protection is currently very low.
- There would need to be enough reinsurance capacity to allow risks to be sufficiently spread, particularly large and long-term ones. Although reinsurance capacity is growing in line with the primary insurance market, it is subject to the same barriers and is therefore still developing.
- Unlike in other areas in which insurance is mandatory, eg for motor risks, the risks covered in cyber are very diverse. A mandatory insurance scheme would not be able to capture all

the different risks stemming from the use of millions of digital devices across the world. In addition, there could be large coverage gaps in certain sectors in which insurers have insufficient expertise and thus little appetite to provide cover.

- There is currently insufficient data for insurers to assess the expected frequency and level of claims for a wide pool of risks. Data is crucial for insurers to be able to price policies.

Compulsory schemes would actually be counterproductive for both buyers and insurers:

- There would be a strong risk of less loss prevention and of increased moral hazard because policyholders who have been forced to purchase insurance tend to not implement adequate protection measures or to behave in a riskier manner, as they feel the burden is on the insurer.
- Building cyber resilience is a task for the whole of society and cannot be replaced by the use of mandatory insurance.
- Premiums would be higher due to:
    - the uncertainty created by the lack of data on which to base underwriting judgements;
    - the lack of a competitive market in several EU member states; and,
    - the additional administrative costs associated with compulsory schemes.
- It would be costly to quickly attract vast amounts of capital to address the new demand for coverage.
- Businesses could be required to purchase more cover than they need, while others could be underinsured due to a lack of flexibility in distinguishing between risk levels.
- Insurers could be more unwilling to offer cover under the restrictions imposed by a compulsory scheme. This would mean individuals would be unprotected or businesses would be unable to operate or grow because they could not obtain the cover required by law.

Insurance Europe is the European insurance and reinsurance federation. Through its 37 member bodies — the national insurance associations — it represents insurance and reinsurance undertakings that account for around 95% of total European premium income.

E-mail: info@insuranceeurope.eu
Twitter: @InsuranceEurope

www.insuranceeurope.eu