

# Cyber operational resilience and cyber insurance

## What is cyber risk and cyber insurance?

Cyber risks are “the combination of the probability of cyber incidents occurring and their impact”, according to the Cyber Lexicon of the Financial Stability Board (FSB).

According to IAIS, the definition of cyber risks is “Any risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks. It also encompasses physical damage that can be caused by cybersecurity incidents, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity, and confidentiality of electronic information – be it related to individuals, groups, or governments.”

## What risks and opportunities for the markets?

Cyber risks are considered as a top global risk for the financial sector and the economy as a whole. The type of Information and Communication Technology

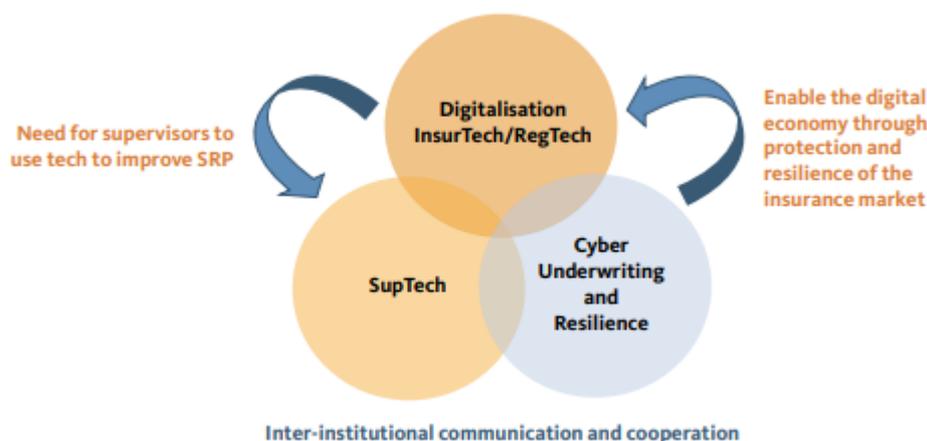
(ICT) risks to which the undertakings are exposed have not changed in the past years, however the frequency of incidents and the magnitude of their impact on financial entities has increased.

The increasing frequency and sophistication of cyber-attacks and the continued digital transformation also make insurers increasingly susceptible to cyber threats, as more and more insurance undertakings are embracing new technologies and making use of big data.

These risks affect the insurance sector on two levels:

- The security of the insurance business itself, and
- Covering and managing cyber risk

In the context of cyber risk, many different areas are correlated and interdependent. Digitalisation in Insurance (InsurTech), SupTech and Cyber Underwriting and Resilience are all closely inter-related.



EIOPA's report on cyber risks for insurers provides information about cyber risk for the European insurance sector, both from an operational risk management perspective and an underwriting perspective.

EIOPA is also monitoring cyber risks for insurance in its regular publication of the Financial Stability Report and Risk Dashboard.

## How is EIOPA addressing cyber operational resilience and cyber underwriting?

In order to enhance the cyber security and resilience of insurance undertakings,

EIOPA has, together with other ESAs, published a [Joint Advice on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector and the 'Joint Advice on the costs and benefits of a coherent cyber resilience testing framework for significant market participants and infrastructures within the whole EU financial sector'](#).

EIOPA issued Guidelines addressed to the supervisory authorities to provide guidance on how insurance and reinsurance undertakings should apply the governance requirements in the context of information and communication technology security and governance. The objective of these Guidelines is to:

- provide clarification and transparency to market participants on the minimum expected information and cyber security capabilities, i.e. security baseline;
- avoid potential regulatory arbitrage;
- foster supervisory convergence regarding the expectations and processes applicable in relation to ICT security and governance as a key to proper ICT and security risk management

The European Commission published a proposal for new regulation regarding digital operational resilience (DORA). EIOPA is supporting the Commission together with the other ESAs for the implementation (ITS and RTS drafting).

The European Systemic Risk Board has published a [Recommendation](#) for the establishment of a pan-European systemic cyber incident coordination framework (EU-SCICF). It would aim to strengthen coordination among authorities (financial and non-financial) in the European Union and key actors at international level. This work is strongly linked with the work on DORA by the ESAs and would complement the existing EU cyber incident response frameworks.

The last piece of the puzzle for EIOPA's digital and cyber strategy is cyber underwriting, i.e. the acceptance of cyber risks by insurance undertakings from its policyholders.

[LEARN MORE ON THE CYBER UNDERWRITING STRATEGY](#)

[READ MORE ABOUT THIS TOPIC](#)

LAST UPDATED ON:  
18 Mar 2022