

# Cyber insurance

Stay covered in the face of ever-increasing cybersecurity risks!



Companies are increasingly reliant on technology to achieve their business objectives, while cyber risks have increased exponentially in recent years.

In this environment, cyber insurance is more important than ever, and our partner's insurance solution helps you stay one step ahead by helping you manage your risks.

Cyber attacks are the most volatile risks facing businesses today. Ransomware, for example, can lead to the unavailability of customer IT or business systems, and can have a considerable impact on operations.

At the same time, regulations are intensifying, resulting in stricter requirements for notification of data subjects and/or the relevant administrative authorities in the event of a breach of customer or employee personal data.

## Cyber insurance offers a complete

### response to the main cyber risks:

- ◆ Data protection: covering the consequences of breaches of the pillars of data confidentiality, integrity and availability
- ◆ Handling incidents related to hacking, ransomware, phishing attempts and other fraudulent attacks
- ◆ Image protection: a guarantee against the consequences of damage to your company's reputation
- ◆ Business continuity: compensation following interruption of your activities

## Emergency actions

The first 72 hours are crucial when it comes to responding to a cyber incident, and insurers' Emergency Actions service provides first-rate legal and IT expertise within an hour of calling the helpdesk. This service can be used whenever customers have, or even suspect, a cyber incident, with no deductible, regardless of policy coverage.

## MAIN GUARANTEES COVERED BY CYBER INSURANCE



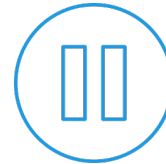
Crisis Management



Administrative inquiry



Third-party liability



Business interruptions



Image damage



Cyber-extortion



Cyber theft



Phone-hacking

- ◆ **Crisis Management** : Coverage of event management costs: analysis, response, communication, data restoration, etc.
- ◆ **Administrative inquiry** : Payment of defense costs and financial penalties imposed by an administrative authority (within legal limits).
- ◆ **Third-party liability** : Compensation and legal defense in the event of a third-party claim related to a security breach or violation of personal or confidential data.
- ◆ **Business interruptions** : Compensation for loss of net profit, additional costs related to the temporary shutdown of the IT system.
- ◆ **Image damage** : Coverage of claims relating to defamation, unintentional infringement of copyright or trademark.
- ◆ **Cyber-extortion** : Assistance in the event of a threat or ransom demand by cybercriminals.
- ◆ **Cyber theft** : Reimbursement of theft due to fraudulent access to the system (theft of money or material goods).
- ◆ **Phone hacking** : Settlement of costs incurred through fraudulent use of the company's telephone system.

### A healthy infrastructure to minimize risks !

The purchase of cyber insurance must be accompanied by a proactive cybersecurity strategy, including the implementation of preventive measures needed to reduce vulnerabilities and strengthen resilience in the face of digital threats.