



Dans un monde dominé par les informations et leur dématérialisation, les cyber-risques sont une réalité incontournable.

Les professionnels exploitent des données électroniques à caractère confidentiel ou personnel et utilisent des réseaux et supports informatiques pour échanger et conserver ces données.

Le caractère sensible de ces informations oblige ces professionnels à veiller à leur protection et leur conservation dans le respect strict de la réglementation. Ils sont tout particulièrement exposés aux cyber-risques : perte d'informations confidentielles, piratage informatique, vol de matériels informatiques et dangers spécifiques liés au cloud computing...

Pour permettre une meilleure maîtrise de ces nouveaux risques, le PACK Cyber constitue une solution d'assurance qui vous offre des garanties adaptées.



Points Forts

Offre des garanties cyber adaptées aux PME - PMI

Couvre une grande diversité de risques qui ne sont pas pris en charge par les produits classiques (RC, dommage, ...)

Permet d'assurer la continuité de l'activité en atténuant l'effet domino d'un incident cyber

Offre les services de spécialistes des cyber-incidents et l'assistance de cabinets d'avocats pour accompagner les victimes de cyber-attaques

Intègre l'expertise d'AIG en matière de prévention et d'assurance des risques et de gestion de crise

Que couvre le PACK Cyber PME - PMI ?

La responsabilité liée aux données

Les conséquences financières suite à la perte ou au détournement de données confidentielles ou personnelles d'un client.

La restauration des données électroniques

Les coûts de récupération et de reconstitution des données après une fuite ou une atteinte à la sécurité des données.

Les enquêtes administratives

Les frais liés à une enquête administrative (notamment de la CNIL) ainsi que les sanctions pécuniaires prononcées suite à une violation de la réglementation relative à la protection des données personnelles.

La gestion de crise

Les frais d'expert informatique pour sécuriser le réseau du professionnel, les coûts de notification et de surveillance associés à une atteinte à la protection des données et les frais de consultant en relations publiques suite à une atteinte à la réputation du professionnel.

L'interruption du réseau

La perte de résultat net consécutive à une interruption matérielle du réseau du professionnel après une attaque par déni de service ou une atteinte à la sécurité de ce réseau.

La cyber-extorsion

Le remboursement de la rançon versée à des tiers qui menacent de divulguer des informations confidentielles piratées via le réseau utilisé par le professionnel.