

- Frais de **notification** aux clients affectés et aux régulateurs
Les dernières évolutions réglementaires européennes vont avoir pour conséquence l'élargissement en France à tous les acteurs de l'obligation de notification en cas de violation de données personnelles.
- Frais d'**expertise IT** des systèmes endommagés
- Frais de **réparation** et de **restauration** des données
- Honoraires d'**avocats** (frais de défense)
- Frais de relations publiques pour **communication de crise**
- Frais de veille et **credit monitoring** des données affectées



- **Domages & intérêts** versés aux tiers
- Pénalités et sanctions infligés par les **régulateurs**
Notre politique est de les assurer chaque fois qu'elles sont jugées assurables.
- Domages à la **réputation de l'entreprise / perte de confiance**
- Perte d'éléments de **propriété intellectuelle**
- **Pertes financières** en cas d'interruption d'activité
- Rançon en cas d'**extorsion** pour éviter la **divulgaration de données**

1

Assistance

- **Frais d'expertise** sécurité informatique (identification et correction de la faille)
- **Frais d'avocat** (constitution d'un dossier de recours, gestion des recours de tiers, identification des obligations de notification)
- **Frais de communication** et de gestion de crise (auprès du public, des clients, des actionnaires, etc.)
- **Frais de récupération** des données perdues, volées ou endommagées
- ...

2

Dommages subis par l'entreprise

- **Perte de revenus** consécutive à une cyber-attaque et coût des mesures correctives mises en place
- **Frais de notification** de la violation de données aux régulateurs (CNIL) et aux personnes physiques

3

Dommages causés à des tiers

- **Violation de données personnelles** : si réclamation, indemnisation des individus concernés
- **Dommages & intérêts** en cas de **compromission de données confidentielles** de tiers ou de transmission de virus
- **Prise en charge** des réclamations de tiers consécutives à la **diffusion de contenu** sur les sites internet et les comptes de réseaux sociaux de l'entreprise (diffamation, atteinte à la vie privée, etc.)

4

Enquêtes et sanctions

- **Accompagnement** en cas d'**enquête administrative** (type CNIL), et prise en charge des **sanctions** prononcées quand elles sont assurables (dans la limite de 500k€, seule sous-limite par défaut de la police)
- **Prise en charge** des **pénalités PCI-DSS** en cas de violation de données cartes de crédit

5

Garanties optionnelles

- **Cyber-extorsion** : rançon / négociation – *inclus en standard*
- **Cyber-fraude** : fraude commise via une intrusion dans le système d'information
- **Piratage de lignes téléphoniques** générant une surfacturation par l'opérateur télécom