VERSPIEREN
COURTIER EN ASSURANCES

# RISQUE CYBER

*Nos conseils pour protéger votre entreprise*

# RISQUE CYBER,
*une menace permanente*

Alors que 65% des entreprises ont constaté au moins une Cyber attaque et que plus de la moitié de ces attaques ont eu un impact sur leurs activités, et que l'attaque la plus répandue est l'attaque par rançongiciel, la menace cyber n'a jamais été aussi importante en France.

Le risque zéro n'existe pas et avec la mise en application du Règlement Général sur la Protection des Données (RGPD), il convient de prendre toutes les mesures possibles au niveau informatique, juridique, humain...

**ET VOUS, OÙ EN ÊTES-VOUS ?**

**1** Avez-vous un plan de continuité d'activité en cas de cyber-incident ?

**2** Comment compenserez-vous les pertes de revenus liées à une interruption de votre activité ?

**3** Savez-vous ce que vous devez faire en cas de violation de données ?

**4** Connaissez-vous le niveau de sécurité de vos prestataires de services informatiques ? (ex: hébergeur)

**5** Êtes-vous en conformité avec les standards et normes règlementaires ?

## LES 10 CONSEILS VERSPIEREN POUR OPTIMISER VOTRE DEFENSE CONTRE LES ATTAQUES CYBER

Mettez à jour régulièrement, les systèmes, les réseaux, les pare-feux, antivirus, et les applications y compris les sites web.

Mettez en place une politique de gestion des mots de passe pour vos collaborateurs, vos directions internes et pour vos clients.

Séparer les usages entre utilisateurs et administrateurs des réseaux.

Sécurisez l'accès à votre annuaire d'entreprise (Active Directory) en protégeant les mots de passe à l'aide de bastions d'administration et séparez les droits des administrateurs de domaines via le modèle de tiers (T0, T1, T2).

Intensifiez la surveillance des systèmes d'informations pour déterminer votre niveau de vulnérabilité.

Cloisonnez chacun de vos réseaux informatiques.

Limitez l'utilisation des clés USB.

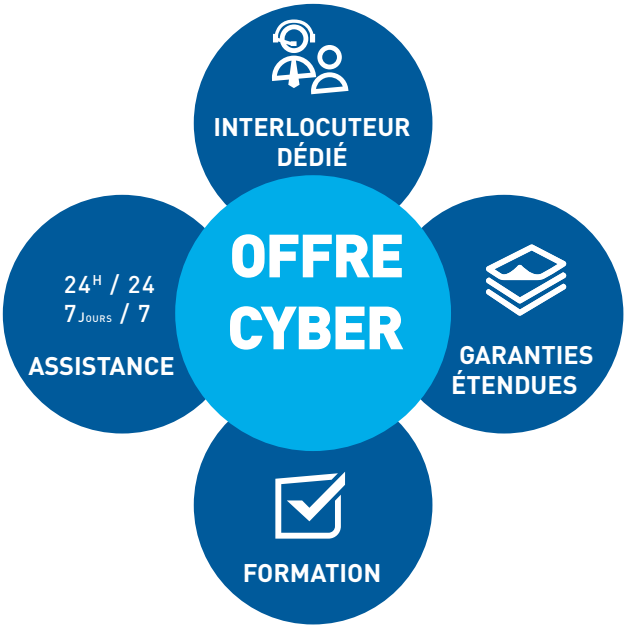
Contrôlez rigoureusement les accès externes aux systèmes d'information liés au nomadisme, au télétravail, etc. au moyen d'une solution d'authentification multifacteur (MFA).

Sensibilisez toujours plus les collaborateurs qui utilisent vos systèmes ainsi que les dirigeants de votre entreprise, en particulier au risque d'hameçonnage (phishing).

Transférez le risque résiduel à l'assurance « Cyber » : le risque Zéro n'existe pas et les conséquences financières d'une faille peuvent peser lourdement sur vos comptes.

# INTÉGREZ VERSPIEREN À VOTRE DÉMARCHE
*de gestion du risque cyber*

Depuis l'émergence du risque cyber et la recrudescence d'attaques de type ransomware, nous avons mis en place une vraie démarche d'accompagnement de nos clients pour les aider à mieux appréhender leurs risques, analyser et évaluer leur niveau d'exposition. En tant que courtier en assurances et expert du risque cyber, notre rôle est de vous aider à protéger votre entreprise et à prendre les bonnes décisions.




## NOTRE PROCESS

### 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 cyberattaque 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.
- Prise en charge des pénalités PCI-DSS en cas de violation de données cartes de crédit.

### 5. EXTENSION DE GARANTIE

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

**ETES-VOUS EN CONFORMITÉ AVEC LE RGPD ?**
Le RGPD ou Règlement Général sur la Protection des Données, instaure un cadre européen unique.

**QUEL EST L'OBJECTIF ?**
Encadrer et harmoniser la protection et l'usage des données à caractère personnel :
- gouvernance de la cyber sécurité / DPO (Data Protection Officer) ;
- formation et sensibilisation des usagers ;
- allocations de ressources spécifiques.

**QUI EST CONCERNÉ ?**
Toutes les entreprises traitant des données qui concernent les citoyens de l'Union Européenne.

**QUELLES SERONT LES SANCTIONS EN CAS DE NON-RESPECT DU RGPD ?**
Une amende pouvant aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires groupe.

**CONTACT**

Pour obtenir un conseil personnalisé,
contactez votre contact privilégié ou notre expert cyber :

**Edouard PRIN**
Expert en assurances de biens et responsabilités
eprin@verspieren.com
06 31 50 07 59

Verspieren, vocation client

verspieren.com

Verspieren - SA à conseil d'administration au capital de 1 000 000 € – 1, avenue François-Mitterrand – 59290 Wasquehal – Siren n° 321502049 – RCS Lille Métropole N° Orias : 07 001 542 – www.orias.fr –
Autorité de contrôle prudentiel et recours : 4 place de budapest CS 92459 75436 PARIS cedex 09 – Crédits photos : istock LS_DASC_CYBER_RISQUE_08/21