La cyber-assurance
EN 10 RECOMMANDATIONS

Toutes les entreprises sont, désormais, confrontées au cyber-risque. Alors, comment gérer et optimiser au mieux la gestion de ce risque qui est devenu bien plus qu'un enjeu de gouvernance.

Assurer le Cyber Risk

La commission Cyber Risk du Club des juristes vient de présenter son rapport « Assurer le Cyber Risk ». Face à la généralisation de la menace, réaction et mobilisation sont les maîtres mots des entreprises, « les assureurs et les réassureurs participent à la construction d'une filière française et européenne de la cyber-protection tout en travaillant à la création d'offres d'assurance cyber dans un environnement en perpétuelle évolution ».

Des obligations de protection des données personnelles ont déjà été posées avec la loi informatique et liberté de 1978 et celle de programmation militaire pour la période 2014-2019.

Le 25 mai 2018, la règlementation européenne (RGPD ou GDPR), appuyée par la directive sur la sécurité des réseaux et des systèmes d'information (NIS) va entrer en vigueur, l'heure est aux responsabilités !

Non-action = faute de gestion

Les sanctions guettent les organisations qui sont poussées à agir, « les sanctions que pourront infliger les autorités régulatrices (jusqu'à 20M € ou 4% du chiffre d'affaires mondial) en cas de non-notification par les responsables de traitement des violations de données personnelles, vont inciter les entreprises à investir dans la prévention et la protection de leurs systèmes d'information ».

Se couvrir contre les cyber-risques devient une priorité et l'heure est la prise de conscience. Dans cette vision, l'assurance impose une prévention avec :

- La cartographie des risques
- L'analyse des vulnérabilités
- L'évaluation des enjeux
- La prise de conscience de l'exposition
- Une prise de décisions éclairée

Les défis des assureurs

« En France, et plus généralement en Europe, le marché de l'assurance cyber progresse mais demeure embryonnaire : l'Europe représente moins de 10% du marché mondial de l'assurance cyber »

Les défis se multiplient et consistent à

- **Évaluer le niveau de vulnérabilité d'une entreprise**

  Cette vulnérabilité dépend de l'action de l'entreprise et de son environnement (sous-traitants, chaînes d'approvisionnements, clients...)

- **Mettre en confiance les entreprises réticentes**

  Les entreprises doivent partager avec leur assureur les informations stratégiques et confidentielles ou relatives au niveau de résilience de leur SI, pour apprécier le risque à la souscription et indemniser après un sinistre

- **Mesurer la mutation continuelle du risque cyber**

  Le risque évolue au rythme des technologies des SI et électroniques, des capacités techniques des individus et des organisations dédiées à la cyber-malveillance

- **Assumer un rôle élargi d'accompagnement des entreprises**

Les 10 recommandations clés

Pour finir, voici les 10 préconisations de la commission cyber risque du Club des Juristes :

A l'attention des assureurs et des gestionnaires de risques

- accélérer le développement d'une culture du risque cyber
- expliquer le contenu des couvertures
- renforcer le dialogue et la confiance avec les assurés

A l'attention des assureurs, réassureurs, de l'ANSSI et de la CNIL

- développer un cadre homogène de sécurité numérique,
- mutualiser la connaissance des cyber incidents
- mieux appréhender les expositions aux risques et leurs cumuls

A l'attention des instances européennes

- définir un ensemble de normes techniques facilitant l'évaluation du niveau de sécurité cyber des entreprises
- établir les conditions d'une concurrence équitable entre les assureurs cyber
- mettre en place au niveau européen et international une veille réglementaire et un suivi de l'évolution des marchés

A l'attention des pouvoirs publics et des investisseurs

- orienter l'investissement public et privé vers l'émergence d'une filière d'excellence en cyber technologie

> Par Sabine Terrey