ASSURER LE RISQUE CYBER : QUELS ENJEUX ?

La question pour une entreprise n'est plus aujourd'hui de savoir si elle va être ou non confrontée au cyber risque. Elle l'est d'ores et déjà. Et les conséquences de ce risque ont pris une telle ampleur que sa gestion n'est plus un sujet technique relevant des seules directions informatiques. Il est devenu un enjeu de gouvernance.

De multiples exemples récents illustrent la généralisation de la menace et la nécessité pour tous les secteurs économiques d'une mobilisation. 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.

Le législateur s'est emparé du sujet. Ainsi, la loi informatique et liberté de 1978 et celle de programmation militaire pour la période 2014-2019 avaient déjà introduit des obligations, tant en matière de sécurité que de protection des données personnelles.

L'entrée en vigueur, en mai 2018, du régime de responsabilité issu du règlement européen sur la protection des données personnelles (RGDP) et de la directive sur la sécurité des réseaux et des systèmes d'information (NIS - Network and Information Security) viendront compléter et renforcer cet arsenal juridique.

Les fortes sanctions que pourront désormais 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. Elles vont vraisemblablement aussi accélérer le transfert du risque à l'assurance. La « non action » devient désormais une faute de gestion pouvant entraîner la responsabilité d'un dirigeant en cas d'incident cyber impactant significativement les résultats de son entreprise.

Les entreprises françaises sont encore aujourd'hui insuffisamment couvertes contre le risque cyber. Une telle assurance a pourtant une double vertu.

D'une part, elle impose à l'entreprise une cartographie de ses risques, une analyse de ses vulnérabilités et une évaluation des enjeux. Ce travail contribue à la prise de conscience de l'exposition au risque cyber et permet d'arbitrer rationnellement entre les dépenses de prévention et protection et celles du transfert du risque à l'assurance.

D'autre part, seule l'assurance pourra protéger l'entreprise contre les pertes qu'une attaque cyber ou qu'une erreur non intentionnelle de manipulation peuvent générer. Ces pertes peuvent être conséquentes et mettre en cause la survie de l'entreprise. L'assurance est là pour couvrir l'aléa que la prévention n'a pas suffi à éviter.

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. Le développement de ce marché ne dépendra pas uniquement d'une demande accrue mais aussi d'une amélioration de l'offre.

Les défis que doivent relever les assureurs face à ce nouveau risque sont nombreux.

Il y a d'abord celui d'évaluer le niveau de vulnérabilité d'une entreprise. Cette vulnérabilité ne dépend pas seulement de son action propre, mais aussi de son environnement (sous-traitants, chaînes d'approvisionnements, clients, etc…) qui peut être source d'infection.

S'ajoute à cette difficulté, la réticence de beaucoup d'entreprises à partager avec leur assureur l'ensemble des informations stratégiques et confidentielles ou relatives au niveau de résilience de leur système d'information. Or celles-ci sont indispensables pour apprécier le risque à la souscription, mais également pour indemniser au mieux après un sinistre.

Par ailleurs, le risque cyber est en continuelle mutation. Il évolue au rythme des technologies des systèmes informatiques et électroniques, mais aussi des capacités techniques des individus et des organisations dédiées à la cyber-malveillance. Autant de facteurs qui limitent la valeur prédictive des incidents passés et imposent de bâtir des scenarios prospectifs et disruptifs.

Dans ce contexte de risques et de contraintes réglementaires, les assureurs sont amenés à assumer un rôle élargi d'accompagnement des entreprises.

Pour un transfert rationnel et éclairé du risque cyber vers l'assurance, la commission cyber risque du Club des Juristes a rédigé dix préconisations pour mieux assurer le risque cyber :

- A l'attention des assureurs et des gestionnaires de risques, pour 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, afin de développer un cadre homogène de sécurité numérique, de mutualiser la connaissance des incidents cyber, de mieux appréhender les expositions aux risques et leurs cumuls ;

- A l'attention des instances européennes, pour définir un ensemble de normes techniques facilitant l'évaluation du niveau de sécurité cyber des entreprises et pour établir les conditions d'une concurrence équitable entre les assureurs cyber ;

- A l'attention des pouvoirs publics et des investisseurs, pour orienter l'investissement public et privé vers l'émergence d'une filière d'excellence en cyber technologie.