Assurance du risque Cyber : quel impact comptable ?

par Anne-Marie Jolys Bris

Temps de lecture estimé : 3 minutes

À la suite d'une concertation avec les acteurs concernés, la direction générale du Trésor a proposé en septembre 2022, dans un rapport dédié, un plan d'actions pour développer l'assurance du risque cyber. Dans un arrêté du 13 décembre 2022[1], le ministère de l'Économie, des Finances et de la Souveraineté Industrielle et Numérique a ajouté deux nouvelles catégories ministérielles portant sur les garanties du risque cyber. Cette modification, qui s'applique aux comptes afférents aux exercices ouverts à compter du 1er janvier 2023, poursuit un double objectif.

Favoriser une meilleure mesure du risque cyber

La création de deux catégories ministérielles dédiées au risque « cyber » :

- 32 – Dommages aux biens consécutifs aux atteintes aux systèmes d'information et de communication,
- 33 – Pertes pécuniaires consécutives aux atteintes aux systèmes d'information et de communication,

a notamment pour objectif d'améliorer l'évaluation des risques des assureurs et de permettre aux acteurs de mieux prendre en compte leur exposition au risque opérationnel cyber.
En effet, elles permettent de mieux isoler les garanties relatives au risque cyber, sans remettre en cause des principes généraux de comptabilisation des engagements d'assurance, tels que définis au règlement ANC n° 2015-11 relatif aux comptes annuels des entreprises d'assurance, notamment à travers les provisions techniques et les informations spécifiques figurant dans les notes annexes.

Évaluation des provisions techniques

Les organismes d'assurance doivent constituer et évaluer les provisions de telle sorte que celles-ci doivent être suffisantes pour le règlement intégral de leurs engagements vis-à-vis des assurés, des souscripteurs et bénéficiaires de contrats et des entreprises réassurées. **La difficulté réside dans leur estimation en l'absence de données historiques suffisantes**. Le rapport a donc préconisé de faciliter la transmission d'informations entre assureurs au sein d'une plateforme de partage de données sur les incidents cyber issue d'un partenariat public/privé, afin de disposer davantage de données sur ce risque.

Informations spécifiques dans les notes aux états financiers

Les entreprises d'assurance sont tenues de mentionner les modes et méthodes d'évaluation appliqués aux divers postes du bilan et du compte de résultat, ainsi que, comme indiqué à l'article 423-28 du règlement ANC précité, **la ventilation de l'ensemble des produits et charges des opérations techniques par catégorie, donc pour le risque cyber**. Il est à noter que le reporting au superviseur évoluera lui aussi, en particulier l'état FR 13 - le compte de résultat par catégorie.

Améliorer le partage de risque entre assurés, assureurs et réassureurs

La mise en place d'une provision dédiée apparait comme une solution pertinente pour permettre aux entreprises de mieux gérer leur risque cyber. C'est l'occasion de promouvoir des solutions innovantes, telles que l'assurance paramétrique qui permet le versement automatique d'une prestation établie en fonction de l'atteinte d'un indice défini et mesurable automatiquement ; le développement de solutions d'auto-assurance comme les captives de réassurance. Ces solutions pourraient contribuer à créer un marché de l'assurance du risque cyber.

Pour conclure

Il convient cependant de souligner qu'au-delà des aspects comptables, la croissance du risque cyber et son caractère systémique nourrissent les discussions avec l'ensemble des acteurs concernés : fédérations d'entreprises, assureurs, experts du monde académique et superviseurs, et d'autres actions concrètes permettront de développer un marché de solutions assurantielles, tout en renforçant la prévention du risque cyber.

[1] *Arrêté du 13 décembre 2022, modifiant l'article A. 344-2 du Code des assurances, JO du 20.*