MINISTÈRE
DE L'ÉCONOMIE,
DES FINANCES
ET DE LA SOUVERAINETÉ
INDUSTRIELLE ET NUMÉRIQUE

Liberté
Égalité
Fraternité

COMMUNIQUÉ DE PRESSE

Assurance du risque cyber : publication du rapport de la direction générale du Trésor

Paris, le 07/09/2022
N°103

À la suite d'une concertation avec les acteurs concernés, la direction générale du Trésor propose, dans un rapport dédié, un plan d'actions pour développer l'assurance du risque cyber.

La numérisation de l'économie engendre de nouvelles vulnérabilités pour les entreprises, et contribue, en particulier, à l'émergence d'un risque nouveau : le risque cyber. La dépendance du tissu économique au numérique a facilité la multiplication de risques ayant une origine cyber, en particulier les cyberattaques. La crise sanitaire a encore accéléré cette tendance, notamment à travers l'adoption de nouveaux modes de travail. Alors qu'elles s'accroissent en volume, fréquence et complexité, les cyberattaques sont aujourd'hui susceptibles de menacer la survie d'une entreprise. **La résilience face au risque cyber constitue donc un enjeu majeur de souveraineté.**

Malgré cette situation, le risque cyber est encore relativement peu assuré, et ne représente que près de 3 % des cotisations en assurance dommage des professionnels. Ce constat est le fruit de deux facteurs : une sous-estimation, ou en tout cas une difficulté à appréhender le risque cyber pour les entreprises (en particulier les plus petites), et des difficultés à estimer ses impacts pour les acteurs de l'assurance, en particulier lors d'incidents de grande ampleur. **L'assurance du risque cyber constitue pourtant un levier essentiel du renforcement de la résilience de notre tissu productif.**

Pour répondre à ces défis, à la demande de Bruno Le Maire, ministre de l'Economie, des Finances et de la Souveraineté industrielle et numérique, la direction générale du Trésor a mis en place, en juin 2021, un groupe de travail portant sur le développement d'une offre assurantielle de couverture des risques cyber, associant, outre les services de l'État, des

représentants des entreprises, des organismes d'assurance et de réassurance et des experts du monde académique.

À l'issue des travaux, la direction générale du Trésor publie un rapport sur le développement de l'assurance du risque cyber qui propose un plan d'actions décliné en quatre axes :

(i) **Clarifier le cadre juridique de l'assurance du risque cyber.** La poursuite des efforts de clarification des clauses des contrats traditionnels constitue une priorité pour mettre fin aux incertitudes qui peuvent entourer la couverture éventuelle de dommages consécutifs à la réalisation d'un risque cyber. Il est ainsi recommandé de diffuser des bonnes pratiques de rédaction pour améliorer la prise en compte de ce risque. À moyen terme, il est proposé de renforcer l'information des assurés sur l'étendue de leurs garanties. Enfin, l'obligation d'un dépôt de plainte de la victime pour permettre l'assurabilité d'une cyber-rançon, ainsi qu'un principe général d'inassurabilité des sanctions administratives sont également proposés pour lever des ambiguïtés dommageables aux assurés comme aux assureurs.

(ii) **Favoriser une meilleure mesure du risque cyber.** Le rapport recommande d'améliorer l'évaluation des risques des assureurs afin de permettre aux acteurs de mieux prendre en compte leur exposition au risque opérationnel cyber. La création d'une catégorie de *reporting* au superviseur dédiée au risque « cyber » puis, à moyen terme, d'une branche cyber dédiée est également recommandée. Il est, par ailleurs, 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 de davantage de données sur ce risque.

(iii) **Améliorer le partage de risque entre assurés, assureurs et réassureurs.** Outre la promotion de solutions innovantes, comme l'assurance paramétrique qui permet le versement automatique d'une prestation établie en fonction d'un indice mesurable automatiquement, le développement de solutions d'auto-assurance telles que les captives de réassurance pourrait permettre de créer un marché de l'assurance du risque cyber. La mise en place d'une provision dédiée apparait, à cet égard, être une solution pertinente pour permettre aux entreprises de mieux gérer leur risque cyber.

(iv) **Accroître les efforts de sensibilisation des entreprises au risque cyber.** Il est préconisé de développer les coopérations entre acteurs publics et privés sur les territoires pour sensibiliser le tissu économique local, ainsi que d'accroître les efforts de formation des professionnels de l'assurance. La définition de référentiels de sécurité partagés et un travail sur l'harmonisation des questionnaires de sécurité utilisés par les assureurs constituent également un levier pour renforcer la résilience des entreprises.

Afin de mettre en œuvre ces orientations, une *task force* dédiée à l'assurance du risque cyber, associant les acteurs concernés, sera mise en place d'ici la fin du mois de septembre. La mesure dédiée aux cyber-rançons (obligation de dépôt de plainte pour être indemnisé) sera partie

intégrante du projet de loi d'orientation et de programmation du ministère de l'Intérieur (LOPMI) présenté ce mercredi 7 septembre en Conseil des Ministres.

Bruno Le Maire, ministre de l'Economie, des Finances et de la Souveraineté industrielle et numérique, a déclaré : « *Ce rapport propose des actions concrètes et crédibles pour développer un marché de solutions assurantielles, tout en renforçant la prévention du risque cyber. Il est issu d'une large concertation avec l'ensemble des acteurs concernés : fédérations d'entreprises, assureurs, experts du monde académique et superviseurs. Je souhaite que ces orientations soient mises en œuvre le plus rapidement possible. L'enjeu est crucial : il s'agit d'affirmer la souveraineté numérique de notre économie face à un accroissement des menaces cyber, pour renforcer la résilience de nos entreprises.* »

Pour consulter le rapport : https://bit.ly/Rapport-assurance-cyber

Annexes

Membres du comité de pilotage

- l'Agence nationale de la sécurité des systèmes d'information
- l'Autorité de contrôle prudentiel et de résolution
- la Direction générale du Trésor
- l'Association pour le management des risques (AMRAE)
- France Assureurs

Repères chiffrés

- **54 %** : c'est la part des entreprises françaises qui auraient fait l'objet d'une cyberattaque en 2021 (source baromètre de la cybersécurité en entreprise CESIN 2022) ;
- **219 M€** : c'est le chiffre d'affaires du marché français de l'assurance cyber en 2021, soit 0,35% du chiffre d'affaires des assurances de biens et responsabilité (source : France Assureurs) ;
- **52 %** : c'est la croissance des cotisations en 2021 de l'assurance du risque cyber, ce qui en fait le segment le plus dynamique du marché des assurances de biens et responsabilité (source : France Assureurs) ;
- **97 %** : la part des sinistres cyber couverts par une assurance cyber en France qui ont donné lieu à une indemnisation inférieure à 3 M€ en 2021, ce qui souligne que le risque cyber reste pour l'essentiel maîtrisable (source : AMRAE) ;
- **84% et moins de 0,3%** : il s'agit des taux de couverture respectifs par un contrat d'assurance cyber des grandes entreprises et des PME en France en 2021. Ce chiffre témoigne d'une prise de conscience très hétérogène face au risque cyber (source : AMRAE).

Cabinet de Bruno Le Maire
01 53 18 41 13
presse.mineco@cabinets.finances.gouv.fr

139, rue de Bercy
75012 Paris