Risques cyber : des pistes pour la protection des entreprises

A+ A-

07/09/2022

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 et répondre aux défis croissants qui peuvent menacer la santé économique des entreprises.

©Viacheslav Iakobchuk stock.adobe.com

54 % : c'est la part des entreprises françaises qui auraient fait l'objet d'une cyberattaque en 2021, en constante augmentation ces dernières années.

La numérisation de l'économie engendre de nouveaux risques pour les entreprises, et tout particulièrement le risque cyber.

Consulter le rapport de la direction générale du Trésor : **le développement de l'assurance du risque cyber < https://www.tresor.economie.gouv.fr/Articles/00367730-14c0-4303-95af-eeb6442fb19b/files/8a344142-fcd5-4d21-a3d7-abb0a404087f>**

Des risques cyber en augmentation et des entreprises peu assurées face à cette menace

La dépendance du tissu économique au numérique a facilité la multiplication de nouveaux risques ayant une origine cyber, en particulier les cyberattaques. La crise sanitaire a encore accéléré cette tendance, à travers l'adoption de nouveaux modes de travail et de consommation.

On constate aujourd'hui un accroissement des cyberattaques que ce soit en volume, en fréquence ou en 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.

Qu'est-ce que le risque cyber ?

Le risque cyber peut revêtir des formes diverses pour les entreprises. Il s'agit de l'ensemble des risques liés à l'usage des technologies numériques et peut être défini comme un risque opérationnel portant sur la confidentialité, l'intégrité ou la disponibilité des données et systèmes d'informations.Il peut s'agir d'une erreur humaine et non intentionnelle (téléchargement involontaire d'un logiciel malveillant par exemple) ou d'un accident.Il peut s'agir également d'une malveillance informatique volontaire telle que l'attaque d'un hacker via un logiciel installant un virus informatique (*malware*), une tentative de récupération d'informations confidentielles en se faisant passer pour une entité connue (*phishing*), l'interception de communications sur des réseaux wifi public, l'exploitation de failles dans des logiciels sans oublier les rançongiciels. Aujourd'hui, la grande majorité des sinistres cyber est liée à une cyberattaque, en forte hausse depuis 2019.

Malgré cette situation, ce risque est encore relativement peu assuré. Il ne représente en effet que près de 3 % des cotisations en assurance dommage des professionnels.

Ce constat est le fruit de deux facteurs : une difficulté à appréhender le risque cyber pour les entreprises (en particulier les plus petites) d'une part, et d'autre part des difficultés à estimer ses impacts pour les acteurs de l'assurance, en particulier lors d'incidents de grande ampleur.

Des actions concrètes proposées pour développer les solutions assurantielles et renforcer la prévention du risque cyber

Le rapport propose des actions concrètes et crédibles autour de quatre axes :

Clarifier le cadre juridique de l'assurance du risque cyber

Autour de cet axe plusieurs aspects sont concernés : la clarification des clauses de contrats traditionnels, la diffusion de bonnes pratiques pour la rédaction des contrats, l'amélioration de l'information des assurés sur l'étendue de leurs garanties ou encore l'obligation d'un dépôt de plainte de la victime pour permettre l'assurabilité d'une cyber-rançon.

Favoriser une meilleure mesure du risque cyber

L'objectif est d'avoir le plus de données sur ce risque afin de permettre aux acteurs de mieux prévoir et prendre en compte leur exposition. Pour ce faire, la création d'un observatoire de la menace cyber, ou encore la transmission d'informations entre assureurs au sein d'une plateforme de partage de données dédiées, sont encouragées.

Améliorer le partage de risque entre assurés, assureurs et réassureurs

Ici, plusieurs pistes sont abordées comme la promotion de solutions innovantes dans l'assurance ou le développement de solutions d'auto-assurance.

Accroître les efforts de sensibilisation des entreprises au risque cyber

Dans les préconisations, le rapport propose de développer les coopérations entre acteurs publics et privés sur les territoires pour sensibiliser le tissu économique local, la formation des professionnels de l'assurance, sans oublier la définition de référentiels de sécurité partagés.

> Consulter le rapport de la direction générale du Trésor : **le développement de l'assurance du risque cyber < https://www.tresor.economie.gouv.fr/Articles/00367730-14c0-4303-95af-eeb6442fb19b/files/8a344142-fcd5-4d21-a3d7-abb0a404087f>**

Afin de mettre en œuvre rapidement 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.

Presse

Communiqué : **Assurance du risque cyber : publication du rapport de la direction générale du Trésor < https://presse.economie.gouv.fr/07-09-2022-assurance-du-risque-cyber-publication-du-rapport-de-la-direction-generale-du-tresor/>** – 07/09/2022

Aller plus loin

Cybersécurité des entreprises : un nouveau dispositif d'alerte en cas d'incident cyber majeur

---

Partager la page