Face au risque cyber, donnons-nous les moyens de protéger les Français

FRANCK LE VALLOIS,

Directeur Général
de France Assureurs

« Avec la guerre en Ukraine, les cyberattaques ont bondi l'an dernier de 140 % en Europe » a indiqué mercredi 5 avril 2023 dans le journal Les Echos Thierry Breton, commissaire européen au marché intérieur. Ce chiffre illustre bien l'enjeu que représente le risque cyber pour notre société, d'autant plus perceptible depuis le début du conflit russo-ukrainien. Les assureurs ont depuis plusieurs années identifié les cyberattaques comme une des principales menaces pour la société[1]. Un débat s'est d'ailleurs instauré sur l'assurabilité des cyberattaques. Et ce pour plusieurs raisons.

D'abord, pour une raison technique. Les cyberattaques peuvent-être assurables ?

Le risque cyber se caractérise par une sinistralité de fréquence mais également d'intensité. De plus, ces attaques sont susceptibles d'entraîner un sinistre majeur tels que certains acteurs ont pu en connaître par le passé (Saint Gobain, Altran…). Toutes les strates de la société peuvent être touchées : les grandes entreprises, les TPE et PME, les particuliers ou encore les établissements publics comme les hôpitaux.

Le phénomène est mondial. Par exemple, aux Etats-Unis, la *National Association of Insurance Commissioners* (NAIC), l'association des superviseurs américains, indique que les violations de données en 2021 sont supérieures de 68 % par rapport à 2020[2], tout particulièrement dans le domaine de la santé. Selon le rapport de l'ANSSI[3] « Panorama de la cybermenace en 2022 », la menace se maintient à un niveau élevé en 2022 en France. L'ampleur de ces cyberattaques et leur caractère potentiellement systémique questionnent la capacité des assureurs à pouvoir les couvrir. Or, le marché de l'assurance cyber est encore un marché naissant. En 2022, le marché français du risque cyber représente 327M € de cotisations soit seulement 0,5 % du chiffre d'affaires des assurances de dommages et responsabilité. C'est encore trop peu pour en faire un marché mature. A titre de comparaison, le marché de la cyber assurance aux États-Unis représente environ 6,5 milliards de dollars en primes directes souscrites, selon la NAIC, en augmentation de 61 % par rapport à l'année précédente. Par ailleurs, ce marché est très disparate : le taux de couverture des grandes entreprises en 2021 était de 84 % quand il est de 0,2 % pour les TPE, PME et micro-entreprises[4]. C'est le jour et la nuit.

Ensuite, pour une raison juridique. Les cyberattaques doivent-elles être assurables ?

Le phénomène rançongiciel a représenté près de 80 % des cyberattaques en 2020, selon le Sophos 2022 Threat Report. Le débat portant sur la légalité de la couverture assurantielle des remboursements des demandes de rançons a été vif en 2022. Il était donc urgent d'avoir une position claire. C'est, en substance, ce que pointaient différents

1/ Cartographie prospective des risques, France Assureurs, 2023

2/ *Report on the Cyber Insurance Market*, NAIC, 2022

3/ Agence nationale de la sécurité des systèmes d'information

4/ Enquête Lucy, Lumière sur la cyberassurance, édition 2022, AMRAE,

rapports sur le développement de l'assurance du risque cyber notamment celui du Haut Comité Juridique de la Place Financière de Paris (HCJP) ou encore de la Direction générale du Trésor. Ces rapports ont éclairé les débats sur l'indemnisation par l'assurance du remboursement des rançons payées par l'assuré en évoquant la possibilité de couvrir ce risque sous certaines conditions.
Ce fut utile.

La loi du 24 janvier 2023 d'orientation et de programmation du ministère de l'Intérieur a permis cette clarification très attendue par la profession. Elle a reconnu la licéité de l'assurance du remboursement des pertes liées à une cyberattaque en la conditionnant à une obligation de dépôt de plainte dans un délai de 72 heures.
Ce fut bienvenu.

Les cyberattaques peuvent donc être assurables. Nous pouvons nous en satisfaire. Pourquoi ? Prévoir une interdiction purement nationale de ce type de garantie aurait eu peu d'effet puisque aucun autre État membre de l'Union européenne n'a formellement interdit l'assurabilité du remboursement des rançons en cas de cyberattaque. Cela aurait donc nui au développement de l'assurance et aux mesures de prévention que mettent en place les assureurs, en laissant les cibles privilégiées de ce type d'attaques sans protection.

Car c'est bien là **l'objectif principal que nous devons collectivement atteindre : protéger.** Protéger les entreprises, notamment les TPE, PME et ETI qui sont la cible de 40 % des rançongiciels[5] et qui disposent de moyens largement inférieurs aux grands groupes. Protéger les particuliers, qui peuvent parfois estimer la menace plus lointaine ou incertaine. Enfin, protéger les établissements publics, à commencer par les hôpitaux : 10 % des cyberattaques frappent des établissements publics de santé selon le rapport de l'ANSSI en 2022.

Pour protéger, il faut sensibiliser. La sensibilisation doit être une priorité nationale pour favoriser la prise de conscience des Français. Un chiffre l'illustre : en 2022, 45 % des entreprises ont subi au moins une cyberattaque selon *OpinionWay*[6]. Or, cette étude révèle que le non-respect des fondamentaux dans les pratiques informatiques et les vulnérabilités résiduelles permanentes sont les principales causes des cyberattaques (38 % et 37 %

5/ Panorama de la cybermenace 2022, ANSSI, 2022

6/ Baromètre de la cybersécurité des entreprises, OpinionWay pour Cesin, janvier 2023

respectivement). Plus de la moitié des patrons de PME n'ont pas de référent sécurité informatique. Tout est dit.

Les assureurs participent activement à cette prise de conscience. C'est en effet par l'assurance que se développent les mesures de prévention car elles sont intégrées aux contrats. L'assurance protège à la fois par la garantie du contrat et par la prévention. Les assureurs ont ainsi développé des mesures d'accompagnement spécifiques au risque cyber afin de prévenir une attaque et d'en réduire les conséquences dommageables.

Et cela commence à porter ses fruits. L'assurance cyber est le segment qui enregistre la plus forte croissance du marché des assurances de biens et responsabilité avec +53 % de progression des cotisations en 2022[7]. France Assureurs accompagne la profession à renforcer cette prise de conscience au niveau de la société française. Ainsi, la Fédération des assureurs a par exemple signé en 2021 un partenariat avec la gendarmerie nationale et agéa, le syndicat des agents d'assurance, afin de sensibiliser les entreprises au risque cyber sur tout le territoire. France Assureurs est également membre fondateur de cybermalveillance.gouv.fr qui a pour missions d'assister les victimes de cybermalveillance, d'informer sur la menace et les moyens de s'en protéger.

Il faut néanmoins aller plus loin. **Il faut une prise de conscience généralisée, incluant toutes les parties prenantes : les citoyens, les entreprises, les assureurs et bien sûr l'Etat.** Il faut développer et diffuser une véritable culture du risque cyber. Les assureurs, dont le métier est de gérer les risques, disposent d'un savoir-faire certain en la matière. C'est la raison pour laquelle France Assureurs propose d'inclure une sensibilisation cyber dans le parcours des jeunes élèves dans les écoles, sur le modèle de ce qui peut se faire en matière de prévention routière. Il faut également amplifier l'effort auprès des entreprises et des collectivités territoriales. En ce sens, la mise en place du Campus Cyber doit être saluée.

Les assureurs sont une partie de la solution. L'Etat, les citoyens et les entreprises ont également dans leurs mains les outils pour mieux se protéger. Travaillons ensemble à mieux protéger les Français. ■

7/ France Assureurs