L'AGEFI Quotidien
EDITION DE 7 H

PAYS :France
PAGE(S) :34;35
SURFACE :125 %
PERIODICITE :Quotidien

RUBRIQUE :Autre
DIFFUSION :(13000)
JOURNALISTE :Camille George

► 30 octobre 2023

L'assurance cyber, un petit marché à fort impact

Un socle minimum de bonnes pratiques reste nécessaire dans la gestion des risques numériques ©© AdobeStock

Les risques cyber représentent un segment réduit dans l'univers de l'assurance, mais sont particulièrement sensibles tant pour les assureurs et réassureurs que pour les entreprises exposées.

Au niveau mondial, l'assurance cyber cumule 13,5 milliards de dollars (12,7 milliards d'euros) de primes annuelles en 2022. En France, le secteur ne représente que 327 millions d'euros de primes annuelles sur la même période, soit moins de 1% de ce que représente l'assurance dommage (IARD) pour les assureurs français. Pour autant, il ne peut être négligé tant les conséquences économiques d'une cyberattaque peuvent être importantes.

En termes de souscriptions, le marché français est découpé en trois grandes familles : les grandes entreprises couvertes à 86%, les entreprises de taille intermédiaire (ETI) couvertes à un peu plus de 10% et les petites entreprises (TPE-PME) dont le taux de couverture ne dépasse pas 3% selon la dernière étude Lucy de l'Association pour le management des risques et de l'assurance des entreprises (Amrae). *«La maturité et la stabilité du marché passera donc par l'équipement du tissu PME et ETI puisque aujourd'hui le CAC 40 est équipé à 98% et le SBF 120 à près de 70%»* estime Lari Lehtonen, responsable de l'équipe cyberrisques chez Marsh France.

A lire aussi: Le programme de notre évènement du 9 novembre dédié aux assureurs

Après correction, les perspectives s'améliorent

«Après des cycles de renouvellement précédents qui s'étaient traduits par des corrections très importantes — fortes réductions des capacités, augmentation des points d'attachement et des franchises, accroissement significatif des tarifs – le marché de l'assurance cyber se détend», indique Florence Tondu-Mélique, directrice générale du cabinet de courtage et de conseil aux entreprises WTW en France.

«En 2020, 2021 et 2022, les primes ont bondi de 300%», confirme Lari Lehtonen. Des réactions dues aux difficultés de prévision du risque cyber, combinées à l'explosion de la sinistralité au-delà des volumes de primes collectées.

Mais à la suite des corrections opérées et à l'amélioration des résultats des assureurs sur cette ligne, l'appétit revient. Les assureurs historiques libèrent à nouveau leurs capacités, qui passent de 5 à 15 millions d'euros par risque après être redescendues à des seuils maximum de 5 millions ces dernières années. De plus, l'arrivée de nouveaux acteurs sur le marché français tels que Sampo, Arch ou encore Everest et ANV contribuent à augmenter le nombre de guichets disponibles.

Le retour à la performance des assureurs les amène à envisager de la croissance et un redéploiement de leurs capacités. Ce segment est à nouveau attractif et l'offre s'élargit, y compris pour les entreprises qui voudraient ouvrir une ligne cyber pour la première fois. *«La qualité des capacités s'améliore également*, constate Lari Lehtonen de Marsh. *On observe la réouverture de couverture sur les ransomwares, ce qui est une bonne nouvelle, car cela représente 80% des sinistres de cyberattaques.»* Au niveau des tarifs, Maud Vannier-Moreau, directrice générale associée du cabinet d'actuariat Galéa, s'attend à une stabilité des prix, voire une légère baisse de la prime pour les grands groupes.

L'ouverture aux PME

Sur le marché des PME, les acteurs historiques restent toutefois prudents. *«Ces risques évoluent très vite avec de potentiels effets systémiques particulièrement redoutés*

Tous droits de reproduction réservés

L'AGEFI Quotidien
EDITION DE 7 H

PAYS : France
PAGE(S) :34;35
SURFACE :125 %
PERIODICITE : Quotidien

RUBRIQUE : Autre
DIFFUSION :(13000)
JOURNALISTE : Camille George

► **30 octobre 2023**

des assureurs», souligne Maud Vannier-Moreau. Toutefois, l'apparition sur le marché français d'acteurs tels que Stoïk ou Dattak permet d'apporter des propositions destinées aux entreprises de petite et moyenne taille. Ces insurtechs, qui ne portent pas forcément le risque, mais le transfèrent auprès de tiers assureurs, ont le mérite d'améliorer la distribution d'assurance cyber et l'accès aux outils de prévention et de diagnostics au sein des PME et ETI.

Au-delà de l'apport de capacités nouvelles, ces acteurs offrent un accès à des processus de souscription simplifiés ainsi qu'à de la prévention industrialisée via l'accès à des services de types scan de vulnérabilité ou questionnaires d'audit. L'aspect prévention est donc ici combiné à l'aspect transfert de risque et assurance.

Pour Thibault Masson, directeur général délégué de l'insurtech Owen, c'est par la proposition de services simplifiés adossés à de l'assurance cyber que le taux de couverture des PME augmentera : *«Le marché manque de solutions d'entrée de gamme. Or, l'assurance cyber embarquée dans une offre de services, à travers les services de paiements par exemple, nous semble une piste intéressante.»*

L'écosystème en action

L'ensemble du secteur, les assureurs, les courtiers, mais aussi l'administration, ont un rôle très important d'accompagnement des PME dans la mise en place de bonnes pratiques.

La réflexion amorcée par Bercy autour de l'instauration d'un socle minimum de couverture obligatoire qui aurait le même type de fonctionnement que celui du régime des catastrophes naturelles (cat nat) fait partie des attentes du secteur. *«Cela pousserait mécaniquement la mutualisation avec pour effet de faire baisser la pression tarifaire»*, estime Maud Vannier-Moreau.

A lire aussi: La prise de conscience grandit face au fléau du cyber-risque

Pour Florence Tondu Mélique, un socle minimum de bonnes pratiques est nécessaire afin de renforcer les processus de gestion des risques numériques. *«Cela passe par des solutions de protection et d'identification de vulnérabilités en temps réel, mais aussi par la formation et la sensibilisation des collaborateurs et pourquoi pas des simulations d'attaques. Tout cela permettra aux entreprises de plus petite taille d'améliorer leur résilience face aux risques cyber et d'accéder à des couvertures en répondant aux attentes et prérequis des assureurs.»*

Camille George

Tous droits de reproduction réservés