beazley

Article

Risque systémique en cyber

Luc Vignancour • octobre 15, 2023

Afin d'approfondir le sujet du risque systémique dans le domaine cyber, il est utile de le définir.

Le risque systémique est un évènement provoquant des répercussions mondiales sans qu'aucun cantonnement des impacts ni limitation géographique ne soient possibles. L'une des particularités du risque cyber est que, parmi les risques assurables, c'est le seul qui présente une telle exposition systémique. Les autres secteurs d'assurance étant limités à une population, une zone géographique, ou bien un secteur d'activité etc.

Un bon exemple de ce risque systémique en cyber est une attaque informatique qui exploiterait une vulnérabilité présente dans l'ensemble des entreprises du monde. L'attaque NotPetya en 2017 en est le parfait exemple. Cette attaque cyber apparue en Ukraine a touché des entreprises de tous les secteurs d'activité (logistique, industrie pharmaceutique, secteur maritime, construction) et dans le monde entier. NotPetya, dont les conséquences financières ont dépassé le milliard de Dollars a démontré l'impact sans précédent du risque systémique cyber.

Ce sujet est extrêmement préoccupant et les régulateurs internationaux s'en sont emparés pour éviter que le marché de l'assurance se trouve dans une situation d'insolvabilité. Le cas échéant, les acteurs de l'assurance ne seraient plus à même de remplir leur obligation d'indemniser les sinistres. Pour faire face à un tel scénario, il a été demandé à l'ensemble des assureurs de démontrer qu'ils étaient en mesure d'identifier et de gérer le risque systémique au sein de leur portefeuille.

Le Lloyds a été l'un des premiers à modifier les textes de garantie afin que les assureurs ne s'exposent pas au risque systémique. Beazley déploie ces modifications depuis avril 2023.

Le risque systémique cyber regroupe 3 grandes catégories :

1. La guerre et cyber guerre

2. Les infrastructures extérieures, c’est à dire les dépendances externes des entreprises aux réseaux télécom, internet, énergies….
3. Les dépendances aux grands opérateurs cloud et les vulnérabilités dans les systèmes d’exploitation

En ce qui concerne la cyber guerre, le législateur français n’a pas défini cette notion, il appartient donc à chaque assureur de la définir et d’expliquer sa démarche.

Selon Beazley, la définition d’une cyber guerre est : une atteinte sponsorisée par un Etat impactant les infrastructures critiques d’un pays. Il faut donc combiner deux éléments pour que l’exclusion puisse s’appliquer, et se limiter, géographiquement aux impacts financiers du pays concerné.

S’agissant de la deuxième catégorie (dépendance aux infrastructures extérieures), il s’agit surtout d’une clarification dans la mesure où les exclusions de la dépendance aux infrastructures sont déjà présentes dans les polices cyber

S’agissant de la troisième catégorie (vulnérabilités des systèmes d’exploitation et dépendance aux grands opérateurs cloud), une analyse du portefeuille a été nécessaire pour évaluer l’impact d’un tel scénario. Suite à cela, Beazley a fait le choix de sous limiter le risque uniquement aux entreprises dont le chiffre d’affaire est inférieur à 100M€ plutôt que de l’exclure sur l’intégralité de son portefeuille.

Au sein de Beazley, ces dispositifs nous permettent d’être sereins quant à la pérennité de notre organisation. Ils ne remettent pas en cause les services que nous offrons à nos assurés dont nous restons bien entendu à l’écoute. L’équipe cyber est à votre disposition pour discuter ou partager des informations supplémentaires à ce sujet ou bien tout simplement pour répondre à vos questions.

Luc Vignancour

Head of Europe, Large Accounts & Private Equity, Cyber Risks

beazley