Episode 7 | Les tendances du marché Cyber, par Anne-Yvonne Autia, Directrice du département Cyber, Marsh France

Sandra Magny

Bonjour à tous, j'ai le plaisir aujourd'hui de vous recevoir pour le dernier épisode de notre série de Poscasts 2024 « A l'écoute du marché de l'Assurance ». Je suis Sandra Magny, Directrice des Marchés pour Marsh en France et je reçois aujourd'hui Anne-Yvonne Autia, notre Directrice Cyber. Bonjour Anne-Yvonne.

Anne-Yvonne Autia : Bonjour Sandra.

Sandra Magny

Peux-tu nous dire quelle est la tendance générale du marché du Cyber pour cette fin d'année ?

Anne-Yvonne Autia

On peut dire aujourd'hui, sans trop se tromper, qu'on est dans un marché Cyber qui s'est beaucoup assoupli ces derniers mois, depuis à peu près 18 / 24 mois.

Cela fait suite, inversement, à une période de *hard market*, grosso modo entre 2020 et 2022, qui avait été assez brutale. Je pense que les assurés ne sont pas prêts de l'oublier et nos équipes non plus d'ailleurs.

Alors on s'attendait à ce que les choses se stabilisent. On voyait bien qu'il y avait un petit essoufflement et qu'on était arrivé à des niveaux de franchises et de primes qui avaient atteint un certain seuil. On ne s'attendait pas en revanche à ce que le retournement se fasse de manière aussi importante. Alors, qu'est-ce qui explique ce changement ?

Plusieurs raisons. La première et comme je le disais, les primes, les franchises avaient atteint des niveaux relativement importants. Donc c'est un marché, et des conditions, qui étaient devenus très attractifs pour attirer de nouveaux assureurs, donc de nouveaux acteurs capables d'apporter des capacités sur le marché. Donc ça, c'est une des premières raisons.

Les acteurs historiques, entre guillemets, qui étaient déjà présents et qui avaient assaini leur portefeuille, retrouvaient également de la marge de manœuvre pour apporter plus de flexibilité et également eux-mêmes augmenter les capacités individuelles qu'ils pouvaient proposer à nos assurés.

Donc l'ensemble de ces éléments ont fait que, on s'est retrouvé dans un marché finalement qui est devenu très concurrentiel, avec beaucoup d'assureurs, plus de capacités et par conséquent beaucoup d'appétit de la part des assureurs pour répondre à une demande qui elle, certes, est en augmentation, mais peut-être pas au même rythme.

Sandra Magny

Très bien. Donc gros retournement de marché et malgré tout surprenant car on n'anticipait pas cela aussi vite que cela est arrivé. Est-ce que tu peux nous dire si les événements de type Jeux Olympiques ou même la panne mondiale que nous avons tous vécue en juillet dernier, ont-ils ou vont-il affecter ces perspectives positives que tu nous évoques ?

Anne-Yvonne Autia

Alors peut-être même avant de reparler de ces événements-là, je voudrais quand même rappeler un point, c'est que certes, le marché s'assouplit, mais la menace, elle, elle est toujours là.

Si je prends l'exemple des *ransomware*, qui sont à l'origine du *hard market* qu'on a reçu au départ puisqu'il y a eu une énorme vague de *ransomware* en 2019-2020 et c'est ça qui a déclenché le *hard market* à l'époque. Ces *ransomware* sont toujours présents, sont toujours importants et continuent d'augmenter. On avait eu un petit recul en 2022 mais c'est reparti à la hausse et en plus on est sur des modalités d'attaque aussi qui deviennent de plus en plus sophistiquées. On a l'intelligence artificielle qui est également utilisée par les hackers pour justement rendre leurs attaques encore plus performantes, même si l'intelligence artificielle est également utilisée côté entreprises pour mieux organiser leur défense. Mais voilà, juste pour rappeler quand même ce contexte général de menaces qui continue d'augmenter.

Donc effectivement, on va dire que l'année 2024, c'était un peu entre guillemets, l'année, enfin c'était, je parle au passé, mais ce n'est pas terminé, l'année de tous les dangers. Il y a le contexte géopolitique que l'on connaît, il y a effectivement sur le territoire français le fait que se déroulaient les Jeux Olympiques et Paralympiques, et je reparlerai effectivement de cet incident et de la panne de fin juillet.

Si je reparle des Jeux Olympiques, grand ouf de soulagement. Tout s'est bien passé, de tout point de vue. Il est intéressant de noter quand même que l'ANSSI (l'Agence nationale de la sécurité des systèmes d'information) a publié un rapport* là tout récemment justement, un genre de feedback sur ce qui s'est passé pendant les Jeux Olympiques. Ce que j'ai trouvé amusant, entre guillemets, de noter, c'est qu'ils disent dans le rapport, « il y a eu un nombre limité d'incidents », ce qu'ils appellent un nombre limité d'incidents, c'est quand même 548 événements de cybersécurité qui ont affecté des entités en lien avec les J.O. et cela entre le 8 mai et le 8 septembre. Voilà, je suis très précise. Il n'y a pas eu d'impact sur le déroulement des Jeux, donc ça montre que la résilience est là, la prévention est là, et que tout le monde était bien préparé et adapté. Donc au moins un point qui s'est bien passé.

Ensuite, et c'est là où effectivement ça a été la grosse surprise, il y a eu cet événement fin juillet, vendredi noir entre guillemets, qui a quand même cloué au sol des milliers d'avions, perturbé de nombreuses entreprises dans des secteurs très différents, la santé, etc. Alors première chose quand même, première précision importante, il ne s'agissait pas d'une attaque cyber, donc il ne s'agit absolument pas d'un événement de nature malveillante. C'est vraiment, entre guillemets, un événement purement accidentel, une mise à jour qui s'est mal passée et qui est venue perturber plus de 8 millions d'ordinateurs qui tournaient sous Windows. Ça me donne l'occasion de rappeler deux choses.

La première, c'est que nos garanties Cyber couvrent certes les attaques malveillantes et c'est généralement à cela qu'on pense quand on pense assurance cyber, mais couvre aussi, en tout cas quand c'est souscrit, ce n'est pas systématiquement souscrit et parfois les assureurs ne veulent pas l'accorder, mais couvrent également ce type d'événements accidentels. Donc voilà, c'est intéressant de l'avoir en tête.

Le deuxième point intéressant, c'est que cet événement-là, on a vu qu'il a eu donc des répercussions dans le monde entier. Et quelque part, il illustre très bien ce qui fait extrêmement peur aujourd'hui aux assureurs dans le monde du cyber, c'est ce qu'on appelle le risque systémique, c'est-à-dire le fait qu'un même événement puisse avoir des répercussions dans le monde entier, avec du coup des impacts financiers énormes.

Comment tout ça va impacter le marché et comment ça va se traduire ?

Honnêtement, c'est encore un petit peu tôt pour le dire. On a eu la chance que cet événement-là, en tout cas, ait été quand même assez circonscrit dans le temps. Assez rapidement, il y a un correctif qui a été déployé, etc. Il y a quand même eu pas mal de déclarations de sinistres qui ont été faites, notamment aux Etats-Unis. On ne pense pas que ça va ébranler, en tout cas, pour le moment, on n'a pas de signe de la part de nos partenaires assureurs de durcissement, de retournement. On les sent quand même, ayant toujours pas mal d'appétit pour accompagner nos clients. Donc pour le moment je dirais tout semble continuer dans la lignée de ce qu'on a connu jusqu'à présent.

Sandra Magny

Si je résume : des risques sous-jacents qui sont toujours là, des attaques qui se multiplient, néanmoins, on comprend que la tendance reste très positive, nos clients étant mieux armés.

Est-ce que tu aurais, dans ce contexte-là, des préconisations à fournir à nos clients qui t'écoutent ?

Anne-Yvonne Autia

Le risque cyber est un risque très technique. Mon premier conseil, c'est évidemment de poursuivre une politique active d'investissement pour améliorer la prévention. Ça reste évidemment très important du point de vue des assureurs et d'ailleurs, c'est une bonne chose à mon avis, les assureurs continuent, malgré l'assouplissement du marché, continuent, à être vigilants sur la qualité du risque qu'ils souscrivent. Donc ça, je ne peux que recommander d'œuvrer en ce sens. Et je m'adresse peut-être plus d'ailleurs aux petites et moyennes entreprises, puisque les grosses sont très souvent déjà des *Best-in-Class* dans le domaine. Simplement, il faut quand même continuer parce-que le risque évolue, donc il faut s'adapter en permanence. Je crois que je n'apprends rien à personne en donnant ce conseil.

Le deuxième, c'est que l'actualité réglementaire, quelque part, favorise aussi cette évolution puisqu'elle contraint les entreprises à investir et à se mettre en conformité désormais avec des exigences, des niveaux de sécurité un peu harmonisés, etc. Il y a notamment la directive « Venise 2 » qui va rentrer en vigueur en octobre 2024, donc c'est vraiment très bientôt, avec une application progressive dans le temps ou la directive DORA qui est plus spécifiques aux entreprises du secteur financier.

Et il y a quand même un dernier point en termes de réglementation sur lequel je voudrais attirer l'attention de nos clients. En tout cas, faire un rappel à nos clients, parce qu'on en a beaucoup parlé, c'est la loi LOPMI qui est en vigueur depuis avril 2023 et qui a ceci de particulier qu'elle impose à une entreprise qui serait victime d'une attaque informatique et qui est couverte en assurance Cyber de déposer plainte pour pouvoir être indemnisée. Ce dépôt de plainte doit être réalisé dans un délai de 72 h à partir du moment où l'entreprise a pris connaissance qu'elle est victime d'un acte de malveillance. Donc ça c'est quand même une contrainte qu'il est important d'avoir en tête, parce-qu'encore une fois, ce délai de 72 h est assez court et c'est une condition sine qua non pour faire fonctionner la garantie.

Et dernier conseil, peut être que je peux donner à nos clients et aux futurs assurés qui nous écoutent, c'est de profiter au maximum de l'assouplissement du marché que l'on connaît aujourd'hui pour améliorer les garanties, acheter plus de capacité à être mieux protégé. Par exemple, il y a plein de marchés vraiment plus souples, donc qui offrent pas mal de nouvelles extensions de garanties, si je

n'en retiens qu'une, c'est la possibilité désormais qui est vraiment toute naissante, de mettre en place ce que l'on appelle des LTA (*Long term agreement*), donc de renouveler son contrat d'assurance sur deux ans et non pas uniquement un an, ce qui offre l'avantage de stabiliser les conditions sur les deux prochaines années et donc de donner un peu de visibilité.

C'est vrai que l'on reproche beaucoup à ce marché de l'assurance cyber d'être très volatile et on l'a vu au début de ce podcast, cela peut être quelque chose d'intéressant à approfondir.

Sandra Magny

Très bien, merci beaucoup Anne-Yvonne. C'était très clair et passionnant.

Ainsi s'achève cette première saison de nos podcasts « A l'écoute du marché de l'Assurance ». L'ensemble de nos experts reste bien entendu à votre disposition pour poursuivre les discussions.

Quant à moi, je vous remercie de nous avoir été aussi fidèles et à très bientôt.

À propos de Marsh

Marsh, une entreprise de Marsh McLennan (NYSE : MMC), est leader mondial du courtage d'assurance et du conseil en risques. Marsh McLennan est un leader mondial de services professionnels en risques, en stratégie et en ressources humaines, conseillant des clients implantés dans 130 pays, au travers de quatre entreprises : Marsh, Guy Carpenter, Mercer et Oliver Wyman. Avec un chiffre d'affaires annuel de 23 milliards de dollars et plus de 85 000 collaborateurs, Marsh McLennan aide ses clients à bâtir la confiance pour réussir grâce à la puissance de la perspective.
Pour plus d'informations, visitez notre site marsh.com ou suivez-nous sur LinkedIn et X.

* Rapport ANSSI : https://cyber.gouv.fr/actualites/bilan-cyber-des-jeux-olympiques-et-paralympiques-de-paris-2024