Cyber assurance, prévention et gestion du risque pour assurer la pérennité de nos entreprises

MARIE SOYER,

Directrice Générale d'ALPTIS

ARNAUD GRESSEL,

Président de RESCO Courtage ET expert Cyber Assurances à l'IHEMI+ Master GGRC à la Sorbonne

Longtemps ignorés ou sous-représentés dans les baromètres et cartographies des risques, les risques cyber se sont manifestés avec virulence depuis 2017 lors de deux vagues d'attaques mondiales (Wannacry - mai 2017, NotPetya - juin 2017), sans laisser de répit depuis cette date aux entreprises et collectivités.

On a pu croire que le risque était à son apogée lors du passage au travail à distance nécessité par le confinement lié covid-19 en 2020. Or il n'en n'est rien, la menace n'a cessé de croître depuis. Celle-ci est devenu protéiforme, professionnelle quand elle n'est pas étatique, et dans tous les cas, systémique.

Désormais en tête des baromètres des risque des entreprises depuis 2020 (1), les risques cyber devraient se maintenir à ce niveau encore les 5 prochaines années (2) tel que le prévoit France Assureurs, devant les risques climatiques et les catastrophes naturelles.

Il est désormais convenu d'entendre « ce n'est pas SI mais QUAND cela vous arrivera … ».

Dans ces conditions, il est légitime de s'interroger sur la pérennité de l'assurance cyber (la question fait occasionnellement la une des médias) et sur l'intérêt d'y souscrire.

Voyons plutôt en quoi le recours à l'assurance va concourir à développer la résilience des entreprises et autres organisations, et pourquoi les autorités tentent de clarifier le marché de l'assurance cyber afin de favoriser son recours compte-tenu de son rôle clé dans la protection des entreprises

L'assurance cyber, condition nécessaire à la sécurité économique des PME et ETI

Si les entreprises font face à un risque croissant, les PME et les Entreprises de Taille Intermédiaires sont particulièrement exposées. Leur surface financière les rend attractives pour les attaquants et la plupart d'entre elles n'ont pas encore consenti aux investissements de protection jugés nécessaires par les assureurs. Ces deux facteurs les rendent difficilement assurables : seules 0,2% des PME sont assurées et 9% des ETI (3). Même si l'on peut estimer que ces chiffres ont quelques peu progressé en 2022, cela reste très insuffisant.

La méconnaissance de la plus-value de ces contrats d'assurance associée à une sous-estimation de la gravité du risque n'explique pas à elles seules cette sous-assurance. Ceci était vrai en partie jusqu'à la crise Covid.

Le marché a en effet connu un revirement

très fort depuis 2020, sous l'effet de la très forte dégradation de la sinistralité subie par les assureurs (4), et il s'est inversé : Avant 2020, il était encore « relativement » aisé de pouvoir souscrire des couvertures assurance, toute catégorie d'assurés confondue : TPE, PME, ETI et Grands Comptes. Ces derniers avaient d'ailleurs pour la plupart signé ces garanties, bénéficiant de cartographies des risques plus élaborés et de ressources financières supérieures. Les résultats de ces programmes étaient relativement rentables de l'aveu même des assureurs spécialisés. Ces derniers parvenaient à rendre leurs offres attractives avec des critères d'éligibilités accessibles, et des niveaux de primes et de garantie satisfaisants.

L'explosion des sinistres cyber, ransomware en tête, a eu des conséquences sur les conditions de souscription et de renouvellement dès 2021. Et les niveaux de primes, qui avaient même tendance à baisser jusqu'en 2019 du fait d'une relative concurrence, ont remonté brutalement, accompagnés par des limitations de montants garantis, une hausse des franchises, et désormais plus fréquemment, des sous-limitations pour certains risques (ransomware, carence du prestataire IT, risque systémique).

Aujourd'hui, malgré une meilleure sensibilisation au risque, les PME et les ETI rencontrent des difficultés pour s'assurer du fait des conditions de prix élevées et/ou d'accès à l'assurance (nouveaux critères d'éligibilité). L'assurance cyber peut être perçue comme dissuasive. Les grands-comptes recherchant même des solutions alternatives avec la création de captives telle que MIRIS (5).

Ce constat est jugé insatisfaisant par les pouvoirs publics qui veulent permettre à l'assurance de jouer un rôle essentiel dans la prévention du risque, dans l'aide à la gestion de crise et dans la protection des bilans des entreprises. Car, ne pas s'assurer sur le risque principal en pleine tempête, c'est faire peser un risque majeur sur les organisations, qu'elles soient privées ou publiques. Mais c'est également faire peser un risque sur toute la chaine de valeur clients / fournisseurs.

A titre d'exemples, voici quelques exemples de tarifs relevés sur la fin d'année 2022 (avec des disparités dans les niveaux de couvertures proposés – limitations, franchises – expliquant en partie les écarts)

PME (plasturgie) – CA 10 M€ - Plafond de garantie souhaité : 1 M€
- **Prime annuelle :** proposition variant de 2 à 5 K€

PME (édition de logiciels) – CA 30 M€ - Plafond de garantie souhaité : 2 M€
- **Prime annuelle :** proposition variant de 15 à 35 K€

Institution financière – CA 120 M€ - Plafond de garantie souhaité : 4 M€
- **Prime annuelle :** proposition variant de 80 à 150 K€

C'est pourquoi, sous l'impulsion de la Direction Générale du Trésor, la loi LOPMI a été débattue au parlement fin 2022 afin de permettre le recours à l'assurance, tout en le conditionnant à plusieurs mesures décisives dont l'obligation du dépôt de plainte sous 72 heures pour donner droit à toute indemnisation par l'assurance. Une autre décision majeure qui a fait, et fera encore débat : la licité du remboursement des rançons (à concevoir en ultime recours) par les assureurs, afin de débloquer un marché indispensable à la survie des entreprises.

D'autres mesures, moins spectaculaires mais non moins efficaces ont été reprise par la Direction Générale du Trésor : favoriser le partage des données et les synergies entre les acteurs publics et privés pour développer la connaissance de ces risques évolutifs, et accéder à une meilleure maîtrise du risque.

Une dynamique de promotion et d'organisation de la résilience s'est mise en marche. Il est désormais fréquent que les assureurs soient associés à des réunions de sensibilisation regroupant l'ANSSI, la gendarmerie, les acteurs de la cyber sécurité et des acteurs de l'assurance afin de porter à la connaissance des dirigeants le panel des moyens et ressources à mettre en œuvre.

Le risque cyber, un nouveau risque à maîtriser pour le secteur de l'assurance

Pour les assureurs, le risque cyber a ouvert un nouveau champ d'activité qu'il s'agit de maîtriser. Le principe de

(1) Baromètre des risques d'Allianz AGCS

(2) La cinquième édition de la cartographie des risques de France Assureurs

(3) Rapport AMRAE - Lucy 2022 (p 13)

(4) Rapport AMRAE - Lucy 2022 (p 19/20)

(5) https://www.argusdelassurance.com/assurance-dommages/risques-d-entreprise/cyber-miris-la-mutuelle-des-entreprises-obtient-son-agrement.209426

l'assurance est de déporter le risque de l'assuré vers l'assureur afin que l'assuré ne soit pas mis en danger par une situation critique à laquelle il ne saurait faire face. Pour accepter ce déport de risque et l'assumer de manière pérenne, l'assureur va travailler sur trois facteurs : l'analyse du risque, la prévention (pour éviter la survenance), la prise en charge financière et l'accompagnement à la gestion de crise (en cas de survenance).

L'analyse du risque

L'analyse de risque est réalisée par l'assureur avant l'entrée en garantie pour accepter ou refuser le risque et le tarifer. Cette étape est essentielle pour proposer aux entreprises assurées une pérennité du programme et une maîtrise des tarifs, garanties et conditions de souscription. Les effets de la sélection initiale sont renforcés par les questionnaires et / ou audits de renouvellement réalisés chaque année.

La prévention

La prévention vient compléter l'analyse du risque qui aura identifié les points de vigilance sur lesquels l'entreprise doit porter ses efforts de protection. A l'instar des assurances incendie obligeant le chef d'entreprise à installer sprinklers et extincteurs, l'assurance cyber requiert des mesures de protection qui s'ajustent dans le temps à l'évolution de ce risque. Au titre des précautions à prendre, la sauvegarde des données est systématiquement exigée afin de faciliter les actions de remédiation en cas de CryptoLocker, sans passer par le remboursement de rançon, ce que tout assureur cherche à éviter. Les contrôles d'accès au système d'information via MFA (authentification multi facteurs), la mise en œuvre de cloisonnement du SI (Tier Model) font partie des niveaux de sécurité à mettre en place. L'assureur partage avec l'entreprise assurée le besoin de limiter le risque au maximum.

La prise en charge financière et l'accompagnement en cas de crise

Toujours dans l'objectif de maîtriser le risque, la première action de l'assureur sera d'aider l'entreprise dans ses premiers pas dans la crise, car ils sont déterminants pour en limiter la portée. Cette prestation est assurée pour le compte des assureurs par des sociétés spécialisées, la plupart du temps sans limitation. Elle est particulièrement importante dans le contexte des PME et ETI qui n'ont généralement pas la capacité, en termes de ressources et de compétences nécessaires, de circonscrire la crise et éviter qu'elle ne s'étende. Ce n'est que dans un deuxième temps que les autres éléments de la garantie seront actionnés, selon le choix d'étendue des garanties opéré par l'entreprise : les garanties dommages : perte d'exploitation et frais supplémentaires d'exploitation (ex : mise en place d'une plate-forme tel pour informer les clients) ; les garanties en responsabilité civile (en cas de mise en cause de l'entreprise sur les conséquences d'une cyber attaque), le remboursement de la rançon (désormais encadrée par la loi LOPMI et à n'envisager qu'en dernier recours). La sélection initiale des risques et les démarches de prévention demandées par l'assureur limitent très fortement (et c'est le but) les situations ou le paiement de la rançon est nécessaire.

Les dispositifs d'assurance cyber contribuent à créer un écosystème de protection autour de nos entreprises. Ils représentent une force agissante pour compléter sur le terrain les actions de la gendarmerie, des acteurs de la cyber sécurité et bien sûr de l'ANSSI qui guident l'ensemble des travaux.

L'assurance cyber est en passe de devenir indispensable pour les 146 000 PME (7) et les 5400 ETI françaises (6) lorsqu'elles recherchent un financement auprès de banques ou de fonds d'investissement. Pour les mêmes raisons de garantie de continuité d'activité, elle devient rapidement une norme pour participer à des appels d'offres.

Les réseaux de distribution d'assurance, très agissants sur le terrain auprès des entreprises françaises (40 000 intermédiaires d'assurances) (8) doivent désormais évoluer et se former pour accompagner les entreprises dans la gestion de ce nouveau risque. ■

(6) https://www.economie.gouv.fr/files/2021-12/2022-0105-DP-strategie-nation-ETI.PDF)

(7) https://www.economie.gouv.fr/cedef/chiffres-cles-des-pme

(8) https://www.economie.gouv.fr/facileco/assurance-assureurs-mediation)