LA CYBER-ASSURANCE : UN ALLIÉ DE TAILLE POUR LA CONTINUITÉ D'ACTIVITÉ DE L'ENTREPRISE

Alors que la fréquence et la gravité des cyber-attaques n'ont cessé d'augmenter au cours des deux dernières décennies, moins de 5% des entreprises françaises possédaient une cyber-assurance en 2015.
Les entreprises, de plus en plus exposées à ce risque avec une moyenne de 28 nouvelles vulnérabilités découvertes chaque jour, très largement médiatisées, semblent peu à peu prendre conscience du danger. Les dernières attaques d'envergure mondiale qui ont touché les grands groupes autant que les PME ne sont pas étrangères à cette évolution... tout comme l'arrivée du prochain RGPD...
Eléments de réponses avec le cabinet de courtage en assurances Gramaglia.

Guillaume de Drouas, Annabel Roubiscoul, Olivier Labedan, experts au sein du cabinet Gramaglia, dévoilent leur offre cyberassurance.

Cyber-assurance

Indéniable. Les dernières attaques cyber du premier semestre 2017 ont contribué à accroitre la sensibilisation des entreprises sur ce risque de grande envergure. Une réelle prise de conscience commence à s'opérer sur les besoins de se protéger à la fois en amont, grâce aux technologies sécuritaires, mais aussi en aval avec une assurance cyber-risques. Les différentes attaques ont en effet démontré *« le risque systémique des cyber menaces »* souligne Olivier Labedan, directeur Gramaglia Assurances. Dans un monde dématérialisé en pleine transformation numérique, nul n'est à l'abri face aux risques multiformes : grands groupes, PME, ETI ou TPE peuvent être touchés directement mais aussi par effet de ricochet.

DE L'IMPORTANCE DE LA GOUVERNANCE DES DONNÉES

Beaucoup d'entreprises collectent, traitent et manipulent des masses considérables de données. Mais la valeur qu'elles représentent n'est pas toujours bien évaluée. Cela s'effectue donc sans véritable cadre sécuritaire. Ce constat appelle une nouvelle prise de conscience de la part des entreprises, primordiale face aux risques évoqués mais aussi au regard de la mise en conformité exigée par le Règlement Général sur la Protection des Données (RGPD). *« Notre volonté est avant tout d'accompagner les entreprises dans cette prise de conscience de la valeur réelle de leur patrimoine immatériel, avec l'ensemble des opportunités que cela peut générer. Dès lors qu'elles ont intégré le fait que les données dont elles disposent constituent un de leurs principaux actifs, elles mesurent alors la nécessité de les protéger par une assurance spécifique. Elles adoptent ainsi une véritable politique de gouvernance des données et intègrent naturellement les différentes approches et étapes de sécurisation de leurs datas comme de leurs systèmes de traitement. »* précise Olivier Labedan.

UNE MISE EN CONFORMITÉ GLOBALE

Mais force est de constater qu'à quelques mois de l'entrée en vigueur du RGPD qui, rappelons-le, impose de nombreuses mesures, dont le renforcement des

process de cybersécurité et expose les entreprises à des sanctions exemplaires, la plupart d'entre elles n'évaluent pas pleinement les impacts de cette nouvelle règlementation et l'impérieuse nécessité de protéger les données inhérentes à leur activité. « *Il est impératif que les entreprises envisagent leur mise en conformité de manière globale, en intégrant à la fois les aspects organisationnel, juridique et technique. Les enjeux sont réels car, au-delà des pertes financières générées par une cyber-attaque, les entreprises pourront voir leur responsabilité engagée. En effet, responsable du traitement des données compromises, l'entreprise pourrait voir son existence remise en cause ! Pour relever ce défi, la démarche de mise en conformité doit s'intégrer dans une stratégie globale de développement.* » souligne Annabel Roubiscoul, en charge du développement assurances Cyber-risques et Fraude au sein du cabinet Gramaglia.

La cyber-assurance doit nécessairement devenir un enjeu abordé et traité par la direction générale de l'entreprise. Les dernières prévisions de McAfee annonçant que les cyberattaques pourraient coûter à l'économie mondiale entre 300 et 1.000 milliards par an, ajoutés aux 4% du CA correspondant aux sanctions prévues par le RGPD devraient sensibiliser les dirigeants et développer le marché de la cyber-assurance.

CARTOGRAPHIER LES RISQUES

Aujourd'hui, les risques sont extrêmement évolutifs mais la majorité des cyber-attaques sont introduites par des emails contaminés par des virus, des malwares, des spams, du phishing ou encore des ransomwares qui tendent à la destruction/paralysie des systèmes informatiques ou à la compromission des informations confidentielles voire stratégiques de l'entreprise. Il est évident que la centralisation des données favorisée par le Big Data et l'utilisation massive des solutions « Cloud » rendent de plus en plus complexe leur sécurisation. « *La fuite de données personnelles et sensibles constitue un risque majeur générant de lourds préjudices. C'est pourquoi, nous préconisons fortement de mettre en place une véritable cartographie des risques afin d'identifier les failles mais aussi d'analyser la teneur et la gravité des risques encourus pour définir les mesures correctives à mettre en œuvre.* » explique Guillaume de Drouas, responsable E-business chez Gramaglia Assurances et ancien DSI au centre nucléaire de Cadarache.

S'équiper de solutions de détection et de prévention des intrusions ou anomalies semblent évident pour absorber l'impact et conserver un système d'information opérationnel. Toutefois, quel que soit son niveau de sécurisation, toute « forteresse numérique » demeure vulnérable. Le risque zéro n'existe pas. « *C'est alors que le choix de s'équiper d'une assurance cyber-risques prend tout son sens.* » poursuit Guillaume de Drouas.

Un message visiblement partagé et entendu par près de 60 à 70 % des groupes du CAC 40 qui seraient, selon les dernières analyses publiées, assurés contre le risque cyber. En revanche, seuls 2 à 3 % des PME françaises le seraient, pour un volume de primes total d'environ 30 millions d'euros en 2016… « *Cela peut s'expliquer notamment par le fait que beaucoup d'entreprises pensent encore être couvertes par leurs contrats d'assurances habituels. Il s'agit le plus souvent d'une grave erreur car la grande majorité des contrats Responsabilité Civile Professionnelle ou Dommage intègre de nombreuses exclusions relatives aux cyber-risques (divulgation de données personnelles, de secrets professionnels, les dommages aux tiers engendrés par un virus, les dommages immatériels non consécutifs, etc.). Ces entreprises connaissent ainsi un réel déficit de garanties car aucun de leurs contrats d'assurance en cours ne permettra d'apporter des solutions concrètes face, notamment, à une intrusion de leur système, un ransomware ou un acte de malveillance informatique.* » précise Annabel Roubiscoul.

Face à la recrudescence des attaques, la prise de conscience de l'ampleur des dommages potentiels d'une cyberattaque booste la demande en assurance « cyber ». Ce marché représente entre 3 et 3,5 milliards de dollars dans le monde aujourd'hui. Selon les dernières estimations américaines, il pourrait peser 7,5 milliards de dollars à l'horizon 2020. Véritable opportunité de croissance pour les assureurs, la cyber assurance offre en contrepartie la garantie d'une continuité d'activité pour les entreprises victimes.

VERS UNE APPROCHE DE CYBER-RÉSILIENCE

Une couverture spécifique cyber-risques intègre trois volets indispensables et indissociables : Gestion de crise, Dommage et Responsabilité Civile. *« La constitution d'un tel contrat procède d'une véritable expertise préalable afin d'intégrer les attentes et besoins de chaque entreprise en fonction de son niveau de maturité face aux risques cyber, de la politique de ses directions générale ou financière ainsi que de la qualité de son système d'information. »* souligne Annabel Roubiscoul.

En cas de cyber-incident, les assurances cyber-risques permettent de bénéficier très rapidement de l'intervention des principaux acteurs et experts en la matière afin de déterminer l'origine de l'attaque et la maitriser, puis de définir les actions et les processus à activer rapidement dans le cadre du Plan de Continuité d'Activité, pour assurer la disponibilité des ressources informatiques et la continuité des activités critiques. *« La mise en place d'une telle gestion de crise avec l'appui de spécialistes informatique et juridique mais aussi de consultants permet à l'entreprise victime de bénéficier d'expertises et d'initiatives stratégiques déterminantes. Cela permet aussi la prise en charge, par l'assureur cyber-risques, des préjudices financiers qui se seraient avérés extrêmement lourds : frais d'expertise, restauration des données, pertes d'exploitation, frais d'enquête, atteinte à la réputation… »* précise l'équipe cyber assurance de Gramaglia.

Au-delà des impacts directs, le contrat spécifique couvre également les conséquences induites par les obligations du RGPD, *« comme les frais de notification, les frais d'enquête ou bien les sanctions administratives. »* La future obligation généralisée de notification en cas de compromission de données personnelles, redoutée par les entreprises, conduit déjà de nombreux cabinets d'avocats à se préparer à agir, aux côtés des victimes en responsabilité contre l'entreprise ou ses dirigeants. *« C'est pourquoi, il est indispensable d'être accompagné par de véritables experts afin de limiter ces dommages, d'assurer la protection de l'activité et de maintenir le développement post-cyber-rattaque. »* ajoute le cabinet.

L'entreprise entre alors dans une approche et une démarche de cyber-résilience incluant la conception et l'implémentation d'un Programme de Cyber-Résilience (PCR).

C'est au cœur de cette stratégie que la démarche assurantielle doit s'envisager, alliant politique d'équipements technologiques, sensibilisation et formation des salariés. Cette approche transversale implique donc tous les niveaux de l'entreprise.

Ainsi, au-delà de la simple couverture assurantielle, *« la problématique de cybersécurité de nos clients exige une approche et une réponse globale que nous apportons grâce à la qualité des partenariats que nous avons pu établir avec des spécialistes techniques et juridiques. Prestataires de confiance et de qualité, ils ajoutent une plus-value incontestable à un contrat d'assurance cyber-risques désormais indispensable. »* ajoute Annabel Roubiscoul.

Et Olivier Ladeban de conclure *« Nous nous félicitons de l'implication des organismes gouvernementaux ainsi que de l'ensemble des acteurs de la filière pour diffuser les bonnes pratiques et les actions de prévention à mettre en place au sein des entreprises. Le règlement européen, que nous attendions depuis 2016, va unifier et renforcer les moyens mis en place dans les entreprises pour lutter, ensemble, de manière efficace contre la prolifération des cyber-attaques. »*