par Isabelle Pottier

Cyber-risques : l'assurance peut intervenir quand la sécurité n'a pas suffit…

Nicolas Hélénon, Directeur Associé, NeoTech Assurances du groupe LSN Assurances (*)

Pouvez-vous nous dire en quoi consiste votre activité au sein du Groupe LSN ?

NeoTech Assurances est l'entité au sein de LSN Assurances (groupe Diot LSN, 5ème groupe de courtage français) dédiée aux risques du numérique.

Notre activité consiste à accompagner nos clients dans la prévention et dans la gestion de leurs risques et de négocier et de concevoir des contrats d'assurance en adéquation avec leurs risques.

Nous sommes le courtier conseil de Syntec Numérique et nous gérons le programme d'assurance « Syntec Numérique Assurances ».

Quels sont les cyber-risques assurables ? piratage informatique, virus, perte de données, etc. ?

Actuellement, il y a plusieurs offres d'assurance sur le marché provenant essentiellement de compagnies anglo-saxonnes comme Beazley. Il s'agit de couvrir les conséquences (préjudice des tiers, les frais de restauration des données, les pertes financières de l'assuré, les frais de défense, les frais de représentation, les frais de communication et de notification) des atteintes (divulgation, intégrité, disparition) aux données des systèmes d'informations mais aussi à la réputation d'une société.

Avec le futur règlement européen, la notification deviendra une obligation pour toute entreprise, de prévenir ses clients en cas d'atteinte à ses données informatiques. Les contrats du marché couvrent les frais de notification (Data Risks Protection). L'estimation de ce que vaut réellement une donnée n'est pas facile car le contexte local, en particulier la législation a un impact important.

Le coût d'une donnée est estimée à la somme de frais engagés en moyenne pour remédier à un « data breach » (consultants, avocats, agences de communication, etc.). A titre d'exemple en 2011, le coût moyen d'une donnée personnelle pour une entreprise française se situait entre 100 € et 150 €.

Parmi les autres faits dommageables qui seront évoqués lors du petit-déjeuner du 19 juin 2013, on peut citer :

- Perte, vol, divulgation non autorisée, altération, destruction de données
- Défaillance du système informatique entrainant une atteinte aux données
- Transmission d'un programme malveillant
- Attaque par déni de service
- Retard ou défaut de révélation des incidents ci-dessus
- Non-respect de la charte de protection des données/loi sur la protection des données, etc.

L'externalisation en mode cloud computing change-t-elle l'analyse du risque ?

Oui, en fonction de la qualité de l'hébergeur. Les activités très porteuses du « cloud computing » exposent les utilisateurs à de nouveaux risques opérationnels tels que la carence de fournisseur, la non disponibilités de données suite à des problèmes réseaux. Donc l'analyse du risque sera impactée par la qualité de l'hébergeur.

Il faut également noter que si l'hébergeur subit un data breach (violation de données), le contrat d'assurance de la société cliente interviendrait en premier lieu et exercera son recours à l'encontre de l'hébergeur et l'assureur Responsabilité Civile Professionnelle de l'hébergeur.

Il peut arriver que la société cliente de l'hébergeur soient assurée additionnel sur la police RC Cyber du prestataire pour permettre à celle-ci d'intervenir en premier lieu et éviter tout recours entre client et prestataire dans les cas où le prestataire serait à l'origine du data breach.

(*) http://neotech-assurances.fr/

© ALAIN BENSOUSSAN – 2013