



Chronique No 5 : Les Cyberrisques et l'assurance : pleins feux sur les pertes d'exploitation et la fraude d'ingénierie sociale

L'équipe de responsabilité professionnelle | 15 janvier 2020

Lors de notre dernière chronique, nous avons souligné deux garanties que l'on retrouve maintenant dans la plupart des polices d'assurance contre les cyberrisques, mais qui traditionnellement faisaient l'objet de polices d'assurance « biens » et « vols et détournements » : les pertes d'exploitation et la fraude d'ingénierie sociale.

Pertes d'exploitation

Cette garantie vise à compenser la perte de revenu qu'un assuré pourrait subir en raison de l'interruption de ses affaires causée par un sinistre couvert. Alors que sur une police d'assurance « Biens », la garantie serait

déclenchée par la réalisation d'un sinistre comme un incendie ou un dégât d'eau, il en va autrement dans le cadre d'une police d'assurance contre les cyberrisques. Bien que l'intention de la garantie soit similaire, elle sera plutôt déclenchée par la survenance d'une atteinte à la sécurité du réseau ayant comme conséquence de paralyser les activités de l'assuré.

Certaines polices prévoient une période d'indemnisation s'étalant jusqu'à la date de reprise des activités, sous réserve d'un nombre maximal de jours (généralement entre 30 et 180), alors que d'autres étendent la période d'indemnisation jusqu'au moment où l'assuré retrouve le niveau d'activité qu'il aurait eu n'eût été l'atteinte, sous réserve, toujours, d'un délai maximal. Au lieu d'une franchise en dollars, une franchise en nombre de jours s'applique, par conséquent, la période d'indemnisation commence après cette période d'attente, qui est généralement de 8 à 24 heures.

On retrouve également sur certaines polices une garantie pour les « frais supplémentaires » qui vise à couvrir les frais engagés par l'assuré afin d'accélérer la reprise des activités et donc de réduire la perte de revenu. Il peut s'agir de dépenses en heures supplémentaires des employés ou de frais de livraison rapide, par exemple.

Vous croyez qu'il s'agit là d'un ajout un peu superflu à une police d'assurance contre les cyberrisques? Cet exemple de réclamation pourrait vous convaincre de son importance :

Une entreprise de vente au détail de vêtements, ABC inc., a été victime d'un pirate informatique qui, en introduisant un code malveillant dans son système d'exploitation, a complètement paralysé son réseau informatique. ABC inc. réalise 60% de ses ventes en ligne. Comble de malheur, l'atteinte à la sécurité du réseau s'est produite juste avant la période des Fêtes, une période évidemment très achalandée. Heureusement, ABC inc. souscrivait une police d'assurance contre les cyberrisques comprenant la garantie Pertes d'exploitation. En agissant rapidement, l'équipe d'intervention de l'assureur a permis à ABC de reprendre ses activités 2 jours plus tard et l'a indemnisé pour la perte de revenus qui s'est chiffrée à près de 40 000 \$.

Fraude d'ingénierie sociale

Les fraudes de type « ingénierie sociale », aussi appelées « fraudes du président », sont devenues un véritable fléau au cours des dernières années, et elles ne touchent pas seulement les grandes organisations connues du public. De plus en plus de petites et moyennes entreprises sont visées par des fraudeurs dont les méthodes se raffinent sans cesse.

La garantie Fraude d'ingénierie sociale protège un assuré contre la perte financière résultant d'un transfert de fonds effectué de bonne foi, mais sur la base d'instructions frauduleuses communiquées par un imposteur. Généralement, les fraudeurs visent un employé de l'organisation ciblée disposant de l'autorité de transférer des fonds. Ils communiquent avec cet employé, par téléphone ou par courriel, en se faisant passer pour le directeur financier, par exemple. Ils vont souvent invoquer une situation imprévue exigeant un transfert de fonds urgent ou encore, un changement de compte bancaire d'un fournisseur. L'employé pensant exécuter les directives de son patron participe ainsi, bien malgré lui, à un détournement de fonds vers le compte bancaire d'une organisation fraudeuse.

Bien que l'intention cette garantie greffée à une police d'assurance contre les cyberrisques soit similaire à celle que l'on retrouve sur une police « vols et détournements », elle n'est pas déclenchée de la même façon. Alors qu'avec la police « vols et détournements » cette garantie interviendrait dès lors que l'assuré peut démontrer qu'il a subi une perte du fait de la fraude, avec la police « cyberrisques » la fraude doit être la conséquence d'une atteinte à la sécurité (généralement, un accès non autorisé au système d'exploitation).

La meilleure façon de se prémunir contre ce type de fraude réside dans l'adoption de procédures et contrôles adéquats tant en matière de pratiques comptables, qu'en matière de sécurité informatique, par exemple : confirmer les directives de paiement au moyen d'un canal de communication distinct de celui par lequel les directives sont parvenues.

Dans notre prochaine chronique, nous aborderons quelques éléments susceptibles de faire la différence lorsqu'il s'agit de déterminer l'étendue de la couverture offerte par une police d'assurance contre les cyberrisques.