



Document de position du SNDPI sur la cyber assurance

Rédigé pour le compte du SNDPI avec des suggestions de ses membres

par Gary Perkins/Colombie-Britannique

le 9 novembre 2017

INTRODUCTION

La cybersécurité est un enjeu de risque pour une entreprise. La cyber assurance est un service de gestion du risque offert aux entreprises et aux individus. Elle peut contribuer à réduire les coûts d'une cyber atteinte, à contourner les brèches lorsqu'elles surviennent ainsi qu'à accompagner l'organisation pour l'amélioration de sa cybersécurité.

POSITION

Le SNDPI considère que le marché des assurances contre la cybercriminalité est « immature et qu'il y a de la place pour amélioration¹ ». Les assureurs n'ont pas prévu tous les scénarios possibles qui peuvent survenir ainsi que les conditions pour lesquelles une compagnie d'assurance pourrait accepter ou rejeter une réclamation. Les organisations ont des résultats variables pour leurs réclamations en vertu de ces polices et de leurs primes. Celles qui se sont munies d'une cyber assurance à leurs débuts apprennent les limites des critères pour recevoir des indemnités. Prenons le cas de *Brick Warehouse v. Chubb Insurance*, où la Cour a jugé que bien que le courriel ait été utilisé pour faciliter le crime, ce dernier avait l'ingénierie sociale comme cause principale, qui, elle, n'était couverte pas par l'assurance contre la cybercriminalité².

Plusieurs assureurs utilisent des tactiques alarmistes pour faire leurs offres aux organisations. Ces stratégies sont utilisées en dépit du manque de données actuarielles pour fixer des primes basées sur « ce que les produits et les contrôles de sécurité ont comme efficacité² ». La cybersécurité est l'un des risques auxquels une organisation doit faire face. Les cyberrisques pour les gouvernements qui décident de s'autoassurer ne sont pas différents.

La principale raison pour une organisation de contracter une assurance contre la cybercriminalité est d'être indemnisée pour des pertes financières qui résulteraient d'une cyberattaque. Les pertes les plus importantes pour une organisation sont souvent liées à la propriété intellectuelle ou aux informations privées sur des artéfacts qui lui donnent un avantage sur ses concurrents. Les organisations du secteur privé devraient considérer les assurances contre la cybercriminalité tout comme celles contre le feu ou autre risque. L'achat de cette cyber assurance doit être vue comme un autre item sur la liste qu'elles peuvent pointer aux médias, vérificateur et conseil d'administration pour démontrer qu'elles se préparent à toute éventualité. Après tout, aucune organisation n'est entièrement protégée contre les impacts d'une cyberattaque qui peut coûter très cher.

Les gouvernements ne représentent pas les clients idéals pour la cyber assurance, puisqu'aucune indemnité ne saurait compenser pour une ombre à son image, une atteinte à sa réputation ou la perte de confiance de ses intervenants. Les dommages résultants de la perte de réputation sont difficiles à indemniser. Les assureurs



admettent qu'elle est difficile à mesurer et donc à assurer³. Sur la base de ces informations et sur le constat que l'industrie de la cyber assurance est encore immature, **les membres du SNDPI s'entendent pour dire que la cyber assurance n'est pas une valeur ajoutée nécessaire en ce moment pour les organisations du secteur public.**

Les cyberattaques peuvent avoir des impacts de grande portée et être parfois même de nature mondiale. Il demeure une inquiétude que les incidents cybernétiques d'envergure avec répercussions immédiates provoquent un nombre important de demandes d'indemnités par des organisations sur un court laps de temps. Ce déferlement de demandes pourrait causer des problèmes de solvabilité, de faillites et d'incapacité à verser les indemnités aux organisations. Avec une convergence croissante des environnements incorporel et physique, il reste à voir si la cyber assurance couvrira les dommages physiques causés par une cyberattaque. Cela deviendrait de plus en plus important en cas d'attaques qui cibleraient des infrastructures critiques.

Les entreprises et les assureurs doivent être sensibilisés aux regroupements des risques advenant une attaque unique qui provoquerait des pertes à de nombreuses firmes qui pourraient causer un risque de contrepartie pour l'assuré et un échec potentiel de l'assureur⁴.

Il est essentiel que les organisations fassent des recherches pour vérifier qu'une cyber assurance ou une police d'assurance adéquate existe pour elles. Une lecture des petits caractères peut permettre à une organisation de savoir à l'avance s'ils doivent travailler avec une firme en particulier qui agira à titre d'accompagnateur, de gestionnaire ou de négociateur en matière de cybersécurité. En cas de cyberviolation, une organisation peut constater après avoir fait une demande d'indemnités qu'un tiers parti est maintenant responsable d'intervenir après l'incident. Certaines clauses additionnelles d'une cyber assurance peuvent exiger une déclaration obligatoire aux forces de l'ordre, aux ministères fédéraux ou autres parties.

Après une demande d'indemnité acceptée en vertu d'une police d'assurance, une organisation peut constater qu'elle n'en sort pas indemne puisque le règlement ne couvre pas la perturbation importante des activités ou le vol de propriété intellectuelle duquel il est impossible de récupérer. La recherche et les coûts nécessaires pour reconstituer la propriété intellectuelle peuvent être si importants qu'ils peuvent provoquer la faillite de l'organisation. Les organisations qui se retrouvent dans cette situation peuvent conclure qu'il est préférable d'investir dans des mesures de contrôle nécessaires pour prévenir tout incident plutôt que de récupérer et de tenter de reconstituer la propriété intellectuelle, qui n'a pas de prix.

Peu importe qu'une organisation ait l'intention ou non de se procurer une cyber assurance, elle doit investir pour avoir un niveau de sécurité qui correspond à sa tolérance au risque. Autrement, elle risque de constater que la compagnie d'assurance ne couvre pas les frais dus aux cyber atteintes puisque l'organisation ne prend pas, dès le début, toutes les mesures nécessaires pour les prévenir. Si une organisation n'est pas prête à atteindre un niveau minimum de sécurité, alors les primes pour une cyber assurance n'en valent pas la peine. La cyber assurance ne remplace pas un bon programme de cybersécurité, mais les primes de cyber assurance peuvent valoir la peine pour couvrir la responsabilité civile.

Dans le secteur public, des atteintes à la protection des données incluent souvent les informations personnelles des citoyens. Ceux-ci méritent de pouvoir faire leurs transactions en ligne en sachant que les informations ainsi confiées aux gouvernements le sont en toute sécurité. Lorsqu'il y a une faille, les citoyens perdent confiance en leur gouvernement, ce qui nuit à son image de marque et à sa réputation. Une assurance implique un transfert de risque,



mais le risque de l'atteinte à la réputation ne peut, lui, être transféré. Ainsi, la cyber assurance offre des bénéfices limités aux organisations du secteur public et ne remplace pas un robuste programme de sécurité.

RÉFÉRENCES

- 1 : <https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu-cyber-insurance-cyber-risk-management-strategy-03032015.pdf>
- 2 : <http://www.insurancebusinessmag.com/ca/news/cyber/court-rules-social-engineering-attacks-not-covered-under-cyber-policy-83950.aspx>
- 3 : <https://www.ft.com/content/25bf97e8-3a27-11e7-821a-6027b8a20f23>
- 4 : https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf