BAC
Bureau d'assurance
du Canada

**PAR COURRIEL**

Montréal, le 30 mars 2023

Me Philippe Lebel
Secrétaire et directeur général des affaires juridiques
Autorité des marchés financiers
Place de la Cité, tour Cominar
2640, boulevard Laurier, 3e étage
Québec (Québec) G1V 5C1
consultation-en-cours@lautorite.qc.ca

**Objet : Consultation réglementaire concernant l'assurance de responsabilité professionnelle et les activités externes**
**Volet : Cyberrisques en assurance de responsabilité professionnelle**

Maître Lebel,

Le BAC salue l'initiative de l'Autorité des marchés financiers (l'Autorité) d'entamer une réflexion sur l'exposition des représentants aux cyberrisques dans le cadre de leurs activités professionnelles.

L'augmentation du télétravail et l'essor des activités commerciales en ligne confrontent plus que jamais les organisations au risque de cyberattaques. La gestion et la mitigation des risques opérationnels font partie intégrante de la saine gestion des entreprises et il est judicieux de travailler à l'amélioration continue des meilleures pratiques en la matière. Aussi, nous partageons les préoccupations de l'Autorité visant à anticiper et mieux comprendre les répercussions de l'évolution des technologies sur la protection des consommateurs.

**Couverture obligatoire contre les cyberrisques**

D'abord, le BAC est d'avis que la détention d'une telle couverture devrait faire partie des meilleures pratiques pour la protection des consommateurs. Le cyberrisque prend de l'ampleur et leurs renseignements personnels doivent être protégés.

Le BAC souhaite cependant souligner les enjeux que représente l'obligation réglementaire de souscrire une couverture d'assurance contre les cyberrisques. Il s'agit d'une assurance très spécialisée comportant des couvertures qui varient en fonction des besoins de chaque entreprise et de leur maturité en ce qui concerne la sécurité informatique. Selon la protection qui sera exigée par la règlementation, une mise à niveau pourrait être requise par l'assureur et nécessiter des investissements financiers importants pour le cabinet, surtout sur les cabinets de petites tailles disposant de revenus plus limités.

De plus, il s'agit d'une ligne d'affaires relativement nouvelle pour laquelle les indemnités ont dépassé les primes demandées au cours des dernières années. Une telle situation se traduit généralement par un ajustement des normes de souscription (acceptation ou refus, exigences pour assurer, etc) et une hausse corrélative des primes exigibles, notamment lorsque le représentant ou le cabinet n'est pas en mesure de rencontrer les exigences de l'assureur.

Cela étant dit, au stade prospectif de la réflexion, nous ne disposons pas de données suffisantes pour effectuer une analyse coût-bénéfice d'une telle mesure. Nous vous soumettons par ailleurs que l'Autorité devra, dans l'élaboration de ses critères, prendre en considération le large spectre des activités des représentants, la taille des cabinets, la nature et la portée des produits de cyberrisques actuellement offerts. Il faudra identifier et circonscrire avec prudence la couverture d'assurance exigée afin d'éviter des coûts prohibitifs, qui auraient pour effet de mettre en péril la poursuite des activités de certains cabinets. La conciliation entre la protection du public et la pérennité des affaires devra être considérée.

**Étendue de la couverture et des risques**

L'assurance contre le cyberrisque est relativement nouvelle et en constante évolution. On retrouve principalement deux types de protection :

A- Protection en responsabilité civile visant les atteintes à la confidentialité des données :

- Perte et/ou accès non autorisé à des informations confidentielles ou personnelles ou leur divulgation occasionnant des dommages aux tiers, des frais juridiques (poursuites, actions collectives, etc.) et le paiement d'amendes, de sanctions et de pénalités administratives ou réglementaires. ;

B- Protection en dommages directs pour couvrir les coûts résultant de ces événements, comme :

- Les frais de notification et d'élimination des failles de sécurité : informer les parties concernées et atténuer les dommages potentiels d'une violation de la vie privée, par exemple en fournissant une surveillance gratuite du crédit ;
- Les frais d'enquêtes spécialisées: embauche d'une entreprise pour enquêter sur la porte d'entrée et la portée de la violation des données ;
- Les frais de restauration des programmes informatiques et des données électroniques : restauration ou récupération de données endommagées ou corrompues par une violation, une attaque par déni de service ou un rançongiciel.;
- Frais de gestion de l'incident ou de gestion de crise
- Pertes d'exploitation
- Cyberextorsion : paiement de rançon sous la menace de causer des dommages aux données de l'entreprise comme la mise hors service des opérations ou la compromission de données confidentielles.

Les protections qui précèdent peuvent être souscrites séparément et soumises à des primes et des franchises très variables. Ces dernières seront généralement beaucoup plus élevées pour les risques retrouvés dans la section B (dommages directs). Au surplus, la souscription de ces protections doit faire l'objet d'une vérification exhaustive de la sécurité interne en place chez le représentant ou le cabinet, laquelle ne sera pas toujours possible, ou suffisamment concluante pour que l'assureur accepte d'offrir la couverture ou de proposer une prime raisonnable eu égard à la capacité de payer du demandeur. La question du montant de la franchise applicable demeure également un élément à considérer dans l'établissement de la prime.

Considérant les particularités de l'assurance cyberrisques, il ne serait probablement pas approprié de l'intégrer à la police d'assurance responsabilité professionnelle des représentants (*E&O*). Plusieurs polices

BAC
Bureau d'assurance du Canada

*E&O* offertes aux représentants en assurance incluent actuellement une exclusion visant les cyberrisques et/ou les atteintes à la vie privée. Le BAC est d'avis qu'il serait probablement préférable que cette couverture soit plutôt souscrite à même la police d'assurance responsabilité civile commerciale (*CGL*) des cabinets d'assurance, les représentants autonomes ou les sociétés autonomes, sous forme d'un avenant ou dans une police séparée.

A ce stade-ci du processus, le BAC recommande à l'Autorité de considérer une obligation de couverture minimum commune à tous les cabinets ou représentant, selon leurs statut (ex : représentant automne) , dans le but premier de protéger les consommateurs. Il s'agirait de souscrire la protection visée à la section A qui précède soit une protection en responsabilité civile pour protéger les cabinets contre la perte et/ou l'accès non autorisé à des informations confidentielles ou des renseignements personnels des consommateurs ainsi que leur divulgation.

Il est important de rappeler que l'assurance cyberrisques à elle seule n'est pas suffisante pour protéger les inscrits et les consommateurs des cyberattaques, puisqu'elle n'intervient qu'après la survenance d'un sinistre. La meilleure protection contre les cyberattaques demeure la mise en place proactive par les inscrits de mesures de prévention et de protection de leurs systèmes informatiques. Encourager les inscrits à détecter de façon proactive leurs failles leur permettra d'améliorer leur assurabilité auprès de potentiels assureurs cyberrisques et facilitera leurs accès aux produits disponibles.

L'encadrement règlementaire des inscrits devrait donc refléter cette obligation d'avoir des processus robustes de protection des données en place, au-delà de l'obligation de souscrire une assurance cyberrisques.

**Suite des travaux de l'Autorité**

En conclusion, le BAC réitère qu'il est favorable à une éventuelle obligation pour le cabinet, le représentant autonome et la société autonome de souscrire une couverture d'assurance contre les cyberrisques, sous réserve des commentaires et suggestions susmentionnés.

Le BAC poursuit depuis plusieurs années déjà des activités visant à sensibiliser les entreprises aux cyberrisques et, à ce titre, a réalisé des sondages, créé un site web sur le sujet (https://cybersavvycanada.ca/ ) et mis en place différentes campagnes de sensibilisation.

C'est donc naturellement que nous vous offrons notre pleine et entière collaboration et souhaitons prendre part activement à la poursuite de vos travaux sur cet enjeu d'importance pour l'industrie de l'assurance de dommages.

Nous vous prions d'agréer, Maître Lebel, l'expression de notre considération distinguée.

[redacted]

Johanne Lamanque
Vice-présidente, Québec
Bureau d'assurance du Canada

[redacted]

JL/jl