Les cyberrisques dans le secteur des assurances

Rapport de consultation téléphonique A2ii – AICA

SEP

2019

Les Consultations téléphoniques sont organisées dans le cadre du partenariat entre l'Initiative Accès à l'assurance (A2ii) et l'Association internationale des contrôleurs d'assurance (AICA). Ces consultations constituent une plateforme d'échanges utile pour que les contrôleurs puissent partager leurs expériences et les enseignements relatifs au développement de l'accès à l'assurance.

Introduction

La cybercriminalité gagne du terrain partout sur la planète et les répercussions de ce type d'incident sur le secteur financier dans son ensemble, mais en particulier sur le secteur des assurances, suscite de plus en plus d'inquiétudes. Le document de réflexion[1] de l'AICA sur les cyberrisques dans le secteur des assurances stipule que les risques en matière de sécurité informatique sont une menace grandissante pour le secteur des assurances, et que, en vertu des principes de base d'assurance (PBA), les autorités de contrôle n'ont pas d'autre choix que de contre-attaquer. En effet, les assureurs recueillent, stockent et traitent des volumes importants de données personnelles et commerciales confidentielles et donc hautement sensibles. Parce qu'ils disposent de ces imposantes banques de données, les assureurs deviennent des cibles privilégiées au regard des cybercriminels qui, motivés par l'appât du gain, recherchent des informations qu'ils peuvent ensuite utiliser pour extorquer des fonds, usurper des identités et poursuivre diverses activités illégales. Parce que les assureurs contribuent grandement au secteur financier mondial, toute interruption des systèmes d'assurance causée par des incidents en matière de cybersécurité a des répercussions considérables.

La contribution des experts réunis à l'occasion de cette consultation téléphonique a été préparée et présentée par Marcelo Ramella (directeur adjoint du département de la stabilité financière de l'Autorité monétaire des Bermudes [BMA]) lors de l'appel en espagnol et du deuxième appel en anglais. Andrea Camargo, (Directrice d'*Inspowering* et Experte technique auprès de l'A2ii) a présenté les contributions des expert.e.s dans le cadre des appels en anglais et en français. Glory Kasasi (contrôleur principal, TIC-Service de supervision des pensions et des assurances, *Reserve Bank of Malawi* [RBM]), Jennifer McAdam (conseillère juridique principale, *National Association of Insurance Commissioners* [NAIC], États-Unis) et Marcelo Adrián Borre (Coordinateur de l'*Evaluación Normativa, Superintendencia de Seguros de la Nación* [SSN], Argentine) se sont joints à eux pour partager leurs expériences dans leurs pays.

1 Consultable à l'adresse suivante : https://www.iaisweb.org/page/supervisory-material/issues-papers/file/61857issues-paper-on-cyber-risk-to-the-insurance-sector

Définitions

Les cyberattaques sont des tentatives, abouties ou non, visant à obtenir un accès non autorisé à des informations ou à des systèmes d'information, afin de voler ou de modifier des informations ou de bloquer des systèmes informatiques. **Le cyber-risque** est la combinaison de la probabilité qu'une cyber-attaque se produise, susceptible d'engendrer des dommages causés par ce type de cyber-attaque.[2] **La cybersécurité**, en revanche, désigne « les stratégies, les politiques et les normes englobant toute la gamme des activités d'atténuation de la menace, de réduction de la vulnérabilité, de dissuasion, d'implication à l'échelon international, d'intervention en cas d'incident, de résistance et de rétablissement des systèmes, ainsi que les politiques concernant la sécurité des opérations d'un assureur[3] ».

Les cyberattaques peuvent causer un grand nombre de dommages, allant de l'interruption de services et d'entreprises jusqu'à la destruction de données et de biens, ainsi que le vol de données, etc. pour donner lieu potentiellement à une instabilité financière. Les cyberattaques peuvent générer des dommages économiques considérables (à ce titre, le coût mondial des cyberattaques en 2018 a été estimé à 800 milliards de dollars)[4]. Le secteur financier a subi proportionnellement plus de cyberattaques que tous les autres secteurs économiques.

Les cyberattaques et le secteur financier

Le secteur financier est particulièrement vulnérable aux cyberattaques notamment parce que les entreprises disposent de données personnelles de grande valeur sur les consommateurs et les actifs financiers de ces derniers. Un rapport portant sur le coût de la cyberactivité malveillante sur l'économie américaine[5] met en évidence les cyber-événements et leur répartition dans les différents secteurs d'activité américains. Par rapport à d'autres secteurs tels que la santé et l'éducation, c'est le secteur financier qui a connu, en 2016, le plus grand nombre d'infractions signalées par rapport à sa contribution au produit intérieur brut (PIB) (voir pages 19 – 20, *Council of Economic Advisers* 2018).

Le document de réflexion de l'AICA sur le risque cybernétique pour le secteur des assurances (2016)[6] stipule que « le secteur des assurances est confronté à un risque cybernétique provenant de sources internes et externes, y compris par l'intermédiaire de tiers. Les sociétés d'as-

2 Cyber Lexique FSB (2018). Consultable à l'adresse suivante : https://www.fsb.org/wp-content/uploads/P121118-1.pdf

3 AICA (2018) Application Paper on Supervision of Insurer Cybersecurity. Consultable à l'adresse suivante : https://www.iaisweb.org/page/supervisory-material/application-papers/file/77763/application-paper-on-supervision-of-insurer-cybersecurity

4 McAfee (2018) Impact économique de la cybercriminalité. Consultable à l'adresse suivante : https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html

5 Consultable à l'adresse suivante : https://info.publicintelligence.net/US-MaliciousCyberActivityCost.pdf

6 Consultable à l'adresse suivante : https://www.iaisweb.org/page/supervisory-material/issues-papers/file/61857/issues-paper-on-cyber-risk-to-the-insurance-sector

surance Les institutions financières doivent définir les rôles et les responsabilités du personnel nécessaire à la mise en œuvre, à la gestion et à la supervision de l'application des stratégies en matière de cybersécurité. En outre, les assureurs doivent fournir les ressources nécessaires pour mettre en œuvre la stratégie et le cadre de cybersécurité. Ce principe est conforme au PBA 7, appelant les contrôleurs à exiger des assureurs qu'ils établissent et mettent en œuvre des cadres de gouvernance d'entreprise qui sous-tendent une administration et un contrôle stable et raisonnable des activités des assureurs, et qui reconnaissent et protègent adéquatement les intérêts des assurés. Voici quelques exemples de considérations :

- Perte de données confidentielles : Les assureurs sont une cible de choix pour les criminels en raison des renseignements personnels qu'ils recueillent.
- Interruption des activités : Les cyberattaques sont susceptibles de perturber les activités commerciales courantes et entraîner des coûts de rétablissement importants.
- Atteinte à la réputation : La confiance des assurés risque d'être ébranlée en cas de cyberattaque menant à la divulgation d'informations confidentielles sur les assurés. Les cyberattaques constituent un risque de réputation susceptible d'affecter le secteur de l'assurance dans son ensemble.

Plusieurs exemples tirés du rapport « Le coût de la cybercriminalité »[7] ont été soulevés sur la manière dont les types et les coûts des cyberattaques peuvent se manifester dans le domaine des assurances :

- L'analyse menée dans 11 pays a permis de démontrer que les secteurs des assurances et le secteur bancaire continuent de subir le coût annuel moyen associé à la gestion de la cybercriminalité le plus élevé par rapport aux autres secteurs d'activité.[8] Le coût annuel moyen des cyberattaques dans le secteur de l'assurance était de 12,93 millions USD en 2017 et de 15,76 millions USD en 2018 (p. 12, Accenture 2019).
- En ce qui concerne le type d'attaques auquel le secteur financier dans son ensemble est confronté, les logiciels malveillants, les attaques en ligne et celles perpétrées par déni de service sont les principaux incidents qui contribuent à la perte de revenus (p. 17, Accenture 2019).

7 Consultable à l'adresse : https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

8 Par rapport aux assurances, les 5 secteurs qui continuent d'avoir le coût le plus élevé attribuable à la cybercriminalité sur les 16 secteurs comparés dans le rapport sont la banque, les services publics, les logiciels, l'automobile et les industries de haute technologie (voir p.12, Accenture, 2019)

Réglementation et supervision du cyber-risque

La présente section s'inspire de l'état des lieux demandé par l'AICA sur la cybersécurité dans le domaine de l'assurance (2018).[9] Un certain nombre d'organisations internationales, nationales et sectorielles des secteurs public et privé ont élaboré des cadres et des orientations en matière de cybersécurité qui se révèlent utiles pour le secteur des assurances. Les éléments fondamentaux de la cybersécurité pour le secteur financier du G7 (G7FE) constituent une source d'orientation essentielle à laquelle les autorités de surveillance des assurances peuvent se référer.[10] Le G7FE est un ensemble concis de principes de cybersécurité non contraignants pour les entités publiques et privées du secteur financier. Il se destine aussi bien aux entreprises qu'aux autorités de surveillance. Les huit éléments fondamentaux identifiés par le G7 sont les suivants :

1. Stratégie et cadre de cybersécurité
2. Gouvernance
3. Évaluation des risques et des contrôles
4. Surveillance
5. Réponse
6. Récupération
7. Partage des informations
8. Apprentissage continu

Conformément à cette politique d'application, les huit éléments sont examinés dans le contexte des assurances et mis en correspondance avec les PBA (Principes de base d'assurance ou *Insurance Core Principles*) pertinents.[11] Voici un résumé de chaque élément, des PBA auxquels ils relèvent et des exemples apportés lors de la consultation téléphonique :

G7FE 1 – Stratégie et cadre de la cybersécurité

Les assureurs doivent pouvoir identifier, gérer et réduire leurs cyber-risques de manière intégrée et exhaustive. Ce point du G7FE est à mettre en relation avec le PBA 8.1, demandant aux contrôleurs d'exiger des assureurs qu'ils mettent en place un système efficace de gestion des risques et des systèmes de contrôle interne fonctionnant dans ce cadre. Voici quelques exemples de considérations :

1. Existe-t-il une stratégie et un cadre précis en matière de cybersécurité ?
2. La stratégie et le cadre de cybersécurité déterminent-ils les objectifs de l'assureur en matière de cybersécurité et sa tolérance au risque, ainsi que la façon dont il peut atténuer et gérer ses cyber-risques ?

9 Consultable à l'adresse suivante : https://www.iaisweb.org/page/supervisory-material/application-papers/file/77763/application-paper-on-supervision-of-insurer-cybersecurity

10 Consultable à l'adresse suivante : https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf

11 Toutes les références dans cette section à des PBA spécifiques sont basées sur la version de novembre 2018, consultable à l'adresse suivante : https://www.iaisweb.org/page/supervisory-material/insurance-core-principles-and-comframe/file/87203/all-icps-adopted-in-november-2018

3. Les cyber-risques sont-ils soumis à une analyse en vertu du cadre de cybersécurité de l'assureur ? À quand remonte la dernière analyse ?

G7FE 2 – Gouvernance

Les institutions financières doivent définir les rôles et les responsabilités du personnel nécessaire à la mise en œuvre, à la gestion et à la supervision de l'application des stratégies en matière de cybersécurité. En outre, les assureurs doivent fournir les ressources nécessaires pour mettre en œuvre la stratégie et le cadre de cybersécurité. Ce principe est conforme au PBA 7, appelant les contrôleurs à exiger des assureurs qu'ils établissent et mettent en œuvre des cadres de gouvernance d'entreprise qui sous-tendent une administration et un contrôle stable et raisonnable des activités des assureurs, et qui reconnaissent et protègent adéquatement les intérêts des assurés. Voici quelques exemples de considérations :

1. Le conseil d'administration et la direction supérieure de l'assureur prennent-ils part aux questions de cybersécurité de l'assureur ? Participent-ils par exemple, à la définition d'une stratégie pour l'assureur, et surveillent-ils sa tolérance au cyber-risque ?
2. Y a-t-il des politiques et des procédures claires en vigueur ? Sont-elles efficacement mises en œuvre ?
3. Les ressources sont-elles suffisantes pour mettre en œuvre les politiques ?
4. Quel est le budget consacré à la cybersécurité ?

G7FE 3 – Évaluation des risques et contrôle

Les assureurs doivent pouvoir identifier les fonctions, les activités et les services (y compris les services sous-traités) potentiellement vulnérables quant aux cyber-risques. Les assureurs doivent être en mesure de comprendre et d'évaluer les risques et de mettre en place les contrôles appropriés. Cet élément est conforme au PBA 8, qui demande aux contrôleurs d'exiger des assureurs qu'ils « disposent, dans le cadre de leur gouvernance d'entreprise globale, de systèmes efficaces de gestion des risques et de contrôles internes ». Le PBA 19.12 demande que les contrôleurs exigent des assureurs et des intermédiaires la mise en place de politiques et de procédures pour la protection et l'utilisation des informations des consommateurs. Voici quelques exemples de considérations :

1. Quel est le niveau de connaissance de l'assureur sur ses cyber-risques ? Existe-t-il un registre des cyber-risques ? Est-il utilisé et mis à jour ?
2. Le cyber-risque fait-il partie du profil de risque général de l'assureur ?
3. Quel est le niveau de protection des informations des consommateurs ?

G7FE 4 – Surveillance

Les assureurs doivent disposer de systèmes de surveillance leur permettant de détecter rapidement les cyberattaques et qu'ils évaluent constamment l'efficacité des contrôles mis en place pour les cyber-risques, notamment par des simulations de cyberattaques. Ce point est conforme avec le PBA 8.1 appelant les contrôleurs à exiger des assureurs qu'ils mettent en place des systèmes efficaces de gestion des risques, y compris des systèmes d'alerte avancée et de réponse aux risques. Ceci est également conforme au PBA 8.2, appelant les contrôleurs à exiger des assureurs qu'ils disposent de systèmes de contrôle pour effectuer régulièrement des tests d'efficacité.

Voici quelques exemples à considérer :

1. Existe-t-il des systèmes permanents de surveillance des activités à haut risque (l'accès à des informations confidentielles) ? La surveillance est-elle effectuée en temps réel ?
2. Qu'est-ce qui est surveillé (par exemple, le matériel et les logiciels à risque) ?
3. Existe-t-il des traces de ces simulations effectuées par l'assureur ?
4. Quelle utilisation est faite des résultats de ces simulations ?

G7FE 5 and 6 – Intervention et rétablissement

Il faut donc que les assureurs puissent réagir rapidement aux cyberattaques, en tenant compte de la gravité de l'attaque, en limitant ses répercussions, en émettant des notifications adaptées à l'intention des personnes concernées et en coordonnant et en mettant en œuvre des réponses qui leur permettent de reprendre leurs activités courantes. Le PBA 8.1.2 établit les éléments nécessaires que les assureurs doivent prendre en considération afin de répondre efficacement à la matérialisation des risques, et proportionnellement au risque matérialisé. Voici quelques exemples de considérations :

1. Quelles sont les politiques et procédures en place chez l'assureur pour améliorer la sensibilisation aux cyber-risques (par exemple, programmes de renforcement des capacités du personnel axés sur les cyber-risques) ?
2. Existe-t-il des plans précis avec des descriptions détaillées sur la manière de faire face aux attaques ?
3. Existe-t-il des plans précis expliquant en détail le retour à des opérations normales ?
4. Existe-t-il des politiques et des procédures de notification des cyberattaques ?
5. Quelles sont les enquêtes mises en place par l'assureur après une cyberattaque ?

G7FE 7 – Partage des données

Les assureurs doivent donc fournir des informations sur les menaces, les faiblesses, les attaques et les réponses aux attaques afin d'améliorer les réponses aux attaques, de limiter les dommages, d'accroître la sensibilisation et de promouvoir l'apprentissage au sein de l'entreprise. Les assureurs doivent fournir ces renseignements aussi bien en interne qu'en externe, et également notifier les autorités gouvernementales. Le PBA 8.1.2 et plus particulièrement les exigences en matière de planification d'urgence s'appliquent sur ce point. En ce qui concerne le partage de renseignements techniques, le PBA 16 (Gestion des risques d'entreprise aux fins de la solvabilité) prévoit l'établissement de normes en matière de gestion des risques d'entreprise aux fins de la solvabilité, obligeant les assureurs à faire face à tous les risques pertinents et importants. Les PBA 3, 25 et 26 traitent de la question de l'échange d'informations entre contrôleurs, ainsi que de la coopération entre contrôleurs, y compris la coopération dans le cadre de la gestion des crises internationales. Voici quelques exemples de considérations :

1. L'assureur appartient-il à des groupes spécialisés échangeant des informations sur les cyber-risques ?
2. L'assureur échange-t-il des informations avec ses fournisseurs de services tiers concernant le cadre de cybersécurité afin de promouvoir une compréhension mutuelle de l'approche de chacune des parties en matière de sécurisation des systèmes reliés ou interfacés ?

G7FE 8 – Formation continue

Les assureurs doivent régulièrement revoir leurs systèmes de gestion des cyber-risques, afin de s'assurer qu'ils soient au fait des nouveaux cyber-risques et qu'ils soient dotés de ressources adéquates. Le PBA 16.10 appelle les contrôleurs à exiger que le système de gestion des risques des assureurs intègre une boucle de rétroaction fondée sur des informations pertinentes, des processus de gestion ainsi qu'une évaluation objective, leur permettant de prendre les mesures nécessaires en temps opportun, en réponse aux changements du profil de risque de l'assureur. Voici quelques exemples de contrôles :

1. Existe-t-il des indications de l'existence de boucles de rétroaction dans les systèmes de gestion des cyber-risques des assureurs ? Dans l'affirmative, existe-t-il des preuves que ces boucles fonctionnent efficacement (sont-elles utilisées) ?
2. Quelle est la fréquence d'analyse ou de mise à jour des systèmes de gestion des risques ? Quel est le degré d'exhaustivité de ces analyses ?

ÉTUDE DE CAS : LE MALAWI

L'étude de cas du Malawi a été présentée par Glory Kasasi de la *Reserve Bank of Malawi* (RBM)

La *RBM* est l'unique autorité de réglementation du secteur financier au Malawi, y compris dans le secteur de l'assurance. La RBM applique pleinement une approche de supervision fondée sur les risques. Une enquête sur le paysage informatique a été menée auprès des assureurs il y a 5 ans. Celle-ci a mis en avant une utilisation importante des technologies informatiques parmi les assureurs, en particulier l'utilisation de systèmes d'information de gestion, de services mobiles et de portails clients en ligne. À l'échelon national, la réglementation de la cybernétique comprend une loi sur la cybersécurité de 2016 et une stratégie nationale de cybersécurité datant de 2018. La reconnaissance de la cybersécurité au niveau national a renforcé de manière positive les efforts de la RBM dans le domaine de la cybersécurité.

En 2011, la RBM a publié une directive de gestion des risques à l'intention des assureurs. Cette directive demande aux assureurs de mettre en place des mesures, des stratégies, des cadres, des politiques et des procédures de gouvernance efficaces pour la gestion des risques. De plus, la RBM observe des lignes directrices plus contraignantes en matière de gestion des risques, qui fournissent des directives précises aux institutions financières (banques et administrateurs de régimes de retraite). Ces directives ont pour but de renforcer leur gouvernance informatique, d'établir une gestion saine et solide des risques technologiques et de renforcer la sécurité, la fiabilité, la résistance et la capacité de récupération des systèmes.

En ce qui concerne les outils de supervision des TIC, la RBM a recours à des demandes d'analyses préventives, des formulaires contenant des questions sur les contrôles attendus utilisés pour la supervision sur site ainsi qu'un questionnaire à l'intention des responsables informatiques et les gestionnaires des risques, actuellement en phase pilote. Les faiblesses et les défis que la RBM a pu constater sur son secteur comprennent :

- Un manque de compréhension du cyber-risque par certains assureurs
- Qu'il n'y a actuellement pas de vue d'ensemble du paysage de la cyber-menace pour le secteur des assurances
- Une absence de structure de cyber-réponse au sein de la RBM
- Une absence de directives officielles sur la manière dont les incidents dans les institutions réglementées doivent être communiqués aux autres divisions potentiellement touchées au sein de la RBM ou dans les autres autorités compétentes du Malawi

En ce qui concerne les développements actuels et futurs, la mission d'assistance technique (AT) bilatérale du Fonds monétaire international (FMI) sur la surveillance des risques liés à l'information et à la cybersécurité visant à élaborer un cadre de surveillance du risque cybernétique est en cours. La RBM actualise également ses directives de gestion des risques informatiques pour les banques afin d'y intégrer les questions

de cyber-risque. En 2020, des lignes directrices sur la gestion des risques liés à la cybersécurité seront publiées à l'intention des banques et, par la suite, adaptées pour être applicables à l'ensemble des établissements financiers supervisés concernés. La RBM prévoit également de formaliser un plan de gestion des cyber-crises, d'organiser des exercices de crise et de mettre en place un mécanisme de notification des incidents cybernétiques pour les institutions supervisées.

Pour toute question ou information complémentaire sur les activités pertinentes de la RBM, veuillez contacter gkasasi@rbm.mw

ÉTUDE DE CAS : LES ÉTATS-UNIS

L'étude de cas des États-Unis a été présentée par Jennifer McAdam de la *National Association of Insurance Commissioners* (NAIC)

La NAIC a commencé à rédiger la Loi type sur la sécurité des données en 2016, avant d'être adoptée par les membres de la NAIC en octobre 2017. La Loi type de la NAIC sur la sécurité des données d'assurance (no. 668) a été élaborée en réponse à des atteintes majeures à la protection des données impliquant de grands assureurs. Une violation massive des données de l'un des plus grands assureurs santé, *Anthem*, a été découverte en 2015, et a fait l'objet d'études dans plusieurs États avant l'adoption de la Loi type sur la sécurité des données d'assurance. Pour remédier à la violation des données d'*Anthem*, les commissaires aux assurances de tous les États-Unis ont collaboré entre eux, ainsi qu'avec les autorités chargées de l'application de la loi afin de mener des études dans plusieurs États dans le but d'évaluer cette cyberattaque et de sécuriser les données de ses assurés. Les examens ont permis de superviser les mesures de correction visant à réparer les systèmes d'Anthem et à éviter de nouvelles cyberattaques. Les examens menés en collaboration entre plusieurs États ont constitué un point de départ pour les discussions sur le type de législation standard qui peut être utilisé par les régulateurs pour faire face à une situation similaire à l'avenir.

La Loi type de la NAIC est conforme à la réglementation de la NYDFS *(New York Department of Financial Services)* sur la cybersécurité pour les entreprises de services financiers. La Loi type de la NAIC sur la sécurité des données s'applique aux assureurs, aux agents et aux entités titulaires d'un permis ou tenus de l'être par le ministère américain des assurances. Il s'agit notamment d'établir des normes pour : la sécurité des données, l'enquête sur tout « événement relevant de la cybersécurité » ; et la notification au commissaire aux assurances de l'État de tout « événement relevant de la cybersécurité ». La loi de la NYDFS est davantage fondée sur des règles que la loi modèle de la NAIC sur la sécurité des données, laquelle est davantage fondée sur des principes. En outre, la Loi type de la NAIC sur la sécurité des données prévoit d'autres exigences en matière

de sécurité des données et octroie plus de pouvoir aux organismes de réglementation pour faire appliquer les recommandations faites aux assureurs, y compris les avis au commissaire en cas de cyber-événement ou de violation de données.

L'Article 4, l'élément le plus important de la loi type, énonce les exigences du programme de sécurité de l'information du titulaire de licence :

- Le titulaire de licence doit désigner une personne responsable du programme de sécurité des informations.
- Les titulaires de permis sont tenus d'effectuer une évaluation des risques afin de déterminer les menaces potentielles à la sécurité de leurs données et à la sécurité des systèmes stockant ces données.
- Les titulaires de permis sont tenus d'évaluer ces menaces potentielles de façon continue et d'évaluer ce programme annuellement.Les titulaires de permis sont

tenus d'atténuer les risques identifiés en fonction de leur taille et de leur complexité, entre autres facteurs de risque en vertu de la disposition sur la gestion des risques.

La Loi type de la NAIC est modulable en fonction de la taille, de la complexité et de la portée des activités du titulaire de permis. Les titulaires de permis peuvent donc déterminer les mesures de sécurité à prendre en fonction de leur évaluation des risques. La Loi type, toutefois, prévoit certaines exigences auxquelles le titulaire de la licence doit satisfaire :

- **Surveillance du conseil :** la direction générale doit informer le conseil d'administration chaque année, par écrit, de l'état général et du respect de la présente Loi.
- **Prestataires de services tiers :** le titulaire de licence est également tenu de faire preuve de diligence et effectuer les vérifications nécessaires lors du choix de prestataires de services tiers, en s'assurant que ces derniers mettent également en œuvre les mesures administratives, techniques et physiques nécessaires pour protéger et sécuriser les systèmes d'information.
- Les autres obligations comprennent les mesures suivantes :
  - Le titulaire de licence doit surveiller, évaluer et ajuster son programme de sécurité de l'information afin que celui-ci demeure conforme aux changements technologiques et à l'évolution de ses propres procédures commerciales.
  - Le titulaire de permis est tenu d'établir par écrit un plan d'intervention en cas d'incident de cybersécurité, lequel doit être évalué et révisé si un événement se produit.
  - Les assureurs doivent présenter annuellement une déclaration écrite attestant qu'ils se conforment aux exigences énoncées dans l'Article 4 de la Loi type.

En outre, les organismes de réglementation effectuent des études sur site afin d'évaluer la situation financière globale des assureurs, ce qui comprend une évaluation de leurs cadres de TI et de cybersécurité. Le « manuel des inspecteurs de la situation financière » de la NAIC fournit ainsi des directives que les autorités de réglementation des différents États utilisent dans le cadre du processus d'examen financier, et comprend un examen de la façon dont l'assureur gère son risque cybernétique. Le « manuel des inspecteurs » a été récemment mis à jour afin d'y intégrer le cadre de cybersécurité du *National Institute of Standards and Technology* (NIST) et ses cinq axes : « Identifier, Protéger, Détecter, Répondre et Rétablir ».

La Loi type sur la sécurité des données de la NAIC a été adoptée en août 2019 ; elle est, à ce jour, adoptée dans huit États. Bien que la Loi n'ait pas été adoptée dans tous les États du pays, les commissaires aux assurances disposent néanmoins du pouvoir de contrôler les entreprises et de faire des recommandations afin d'actualiser leurs pratiques en matière de cybersécurité.

Pour des questions ou de plus amples renseignements sur les activités de la NAIC, veuillez contacter avec JMcAdam@naic.org

ÉTUDE DE CAS : L'ARGENTINE

L'étude de cas de l'Argentine a été présentée par Marcelo Borré de la *Superintendencia de Seguros de la Nación* (SSN), Argentine

Le SSN a récemment mis en place un Conseil d'innovation de l'assurance et de l'InsurTech (ou pôle d'innovation). Le pôle réunit différents acteurs du secteur technologique et du secteur des assurances dans le but d'instaurer un dialogue, afin de promouvoir l'innovation dans le secteur des assurances. Le pôle d'innovation est un espace de collaboration public-privé visant à créer un contexte de dialogue concernant l'utilisation de la technologie dans le domaine de l'assurance. Le pôle a pour but :

- d'établir un canal de communication pour faire connaître les nouveaux modèles de gestion et les nouvelles technologies dans le domaine des assurances,
- d'identifier les défis réglementaires liés aux risques et aux opportunités d'InsurTech,
- de contribuer à la compétitivité du secteur de l'assurance, et
- de promouvoir l'efficacité et la concurrence dans le secteur de l'assurance.

La SSN prépare des directives internes concernant le fonctionnement de ce pôle d'innovation, lesquelles pourront être modifiées en fonction des changements qui se produiront dans l'espace InsurTech. À cet égard, la SSN établira les mesures nécessaires pour protéger les intérêts des assurés, avec l'adoption de nouvelles technologies et la garantie du bon fonctionnement du secteur de l'assurance.

La SSN reconnaît que la mise en œuvre du pôle d'innovation est d'une importance capitale, car elle stimulera le développement de solutions et de technologies innovantes au profit du secteur des assurances et des assurés. De même, le pôle d'innovation contribuera à la conformité avec les PBA, en analysant les nouveaux comportements du marché résultant de l'adoption de la Résolution SSN N° 219/2018, autorisant l'émission d'assurance sous forme numérique.

Le pôle d'innovation possède également une composante liée au risque cybernétique, composée de membres des compagnies d'assurance, des fournisseurs de services (par exemple, les « BigTechs », sociétés de logiciels), de personnel de la SSN, du *Ministerio de Modernización*, et enfin d'experts et de consultants en matière de risque cybernétique. Leur objectif consiste à élaborer de bonnes pratiques de gestion des risques et des mesures de prévention de la cybercriminalité.

Pour poser vos questions ou pour en savoir plus sur les activités concernées de la SSN, veuillez contacter mborre@ssn.gob.ar ou mesadeinnovacion@ssn.gob.ar pour plus d'informations sur le pôle innovation d'InsurTech

Questions et discussion

Comment maintenir l'équilibre entre la gestion du cyber-risque et l'innovation financière ? Les cyber-risques et les risques liés à l'innovation doivent être considérés comme distincts autant que liés les uns aux autres. Les assureurs doivent évaluer et déterminer leur tolérance au risque de cyber-menaces et leur propension au risque pour l'innovation, et indiquer clairement dans leurs déclarations de risque le niveau de risque qu'ils sont prêts à assumer et la façon dont ils entendent gérer ces risques. Les autorités de surveillance s'intéressent généralement à la justesse de l'évaluation et de la gestion des risques par les assureurs, à la transparence et à la gouvernance du processus de décision sur le niveau de risque qu'un assureur peut prendre et sur la manière de le gérer. En dernier ressort, les contrôleurs doivent s'assurer de vérifier dans quelle mesure tous ces engagements sont concrètement tenus.

Comment les inspections/inspecteurs des TIC sont-ils structurés au sein des autorités ? Existe-t-il différents spécialistes en fonction des différents domaines des TIC ? Il existe au sein de la RBM trois services distincts responsables de différents domaines de supervision. Chaque service dispose d'experts en TIC qui sont chargés de mener des inspections des TIC dans leur domaine respectif. À la Commission des services financiers de Gibraltar (GFSC), le Directeur général des questions informatiques (CIO) a instauré la supervision des contrôles des TIC, incluant la cyber-sécurité, la sécurité des données, les contrôles et la gouvernance des systèmes, la continuité des activités et la reprise après sinistre dans tous les secteurs. Cela fait plus de quatre ans que le GFSC a mis en œuvre ces procédures. Ce modèle a fonctionné pour l'autorité et a fait partie de leurs processus sur site et de supervision. Il fait également partie intégrante de leur processus d'autorisation.

Existe-t-il des exemples antérieurs de cyber-attaques dans le domaine des assurances et comment les structures en place ont-elles contribué à les résoudre ? Au Malawi, la RBM n'a pas été informée de cyberattaques spécifiques, que ce soit dans le secteur des assurances ou dans le secteur bancaire. Il est toutefois essentiel de disposer d'un mécanisme de réponse afin de faire face efficacement à de telles attaques. Aux États-Unis, avant l'adoption de la Loi type sur la sécurité des données d'assurance, la violation des données d'Anthem, en 2015 a été gérée en effectuant des inspections à travers plusieurs États et de manière concertée. Les organismes de réglementation des États ont collaboré avec Anthem, le FBI américain ainsi que les entreprises de cybersécurité pour étudier les attaques et prendre des mesures de correction.

En ce qui concerne les cyber-menaces interconnectées ou transfrontalières, comment les contrôleurs peuvent-ils fixer des exigences de sécurité pour la supervision du cloud[12] afin de traiter simultanément des données provenant de secteurs et de territoires différents ? Les services de technologie numérique, comme la technologie de dématérialisation des données informatique « dans le nuage », sont souvent externalisés. Comme la plupart de ces

12 Pour en savoir plus sur le *cloud computing*, voir le document du *Financial Stability Institute* (FSI) intitulé « *Regulating and supervising the clouds : emerging prudential approaches for insurance companies* » (Réglementation et supervision des serveurs dématérialisés : approches prudentielles émergentes pour les compagnies d'assurance) consultable à l'adresse suivante : https://www.bis.org/fsi/publ/insights13.pdf. Le document a été présenté dans le cadre de la consultation téléphonique A2ii-AICA du 28 novembre 2019. Le rapport de la conférence est en cours de rédaction.

avancées numériques ne sont pas encore réglementées dans de nombreux pays, les autorités de surveillance ne peuvent pas encore s'appuyer sur des mécanismes transfrontaliers. Toutefois, il est important que les assureurs soient conscients des risques existants et qu'ils disposent de cadres d'intervention appropriés en matière de gestion des risques.

Combien de notifications ont été faites à la NAIC concernant les cyberattaques et quels sont les principaux problèmes qui retardent l'adoption de la Loi type dans les autres États ? Les assureurs ne sont pas tenus de faire des notifications à la NAIC, mais plutôt d'en informer directement les commissaires. À l'heure actuelle, on ne dispose pas de données sur le nombre de notifications d'attaques cybernétiques. Le principal défi dans l'adoption uniforme de la Loi type sur la sécurité des données dans tous les États américains a été l'opposition des acteurs du secteur des assurances. La loi est toutefois progressivement adoptée dans tous les États.

Comment les autorités de surveillance peuvent-elles assurer une surveillance efficace du risque cybernétique en l'absence d'experts en TIC au sein de l'autorité de surveillance ? Il existe à cet égard plusieurs possibilités que les contrôleurs peuvent adopter. Le contrôleur peut faire appel à des experts externes en cas de besoin, y compris s'il ne dispose pas d'experts internes et/ou s'il n'a pas la masse critique ni le budget pour obtenir des compétences internes. Il est essentiel que le contrôleur puisse évaluer la qualité de la gestion du cyber-risque par l'entreprise elle-même, indépendamment des « connaissances techniques » en matière de cyber-risque. On peut faire la comparaison avec la supervision des modèles actuariels internes utilisés par les assureurs, que les contrôleurs peuvent ne pas être en mesure de techniquement comprendre. Au Canada, par exemple, le Bureau du surintendant des institutions financières (BSIF) planche sur une note d'orientation pour la supervision des modèles internes utilisés pour déterminer les exigences de capital réglementaire (voir le lien http://www.osfi-bsif.gc.ca/Eng/Docs/e25-dft.pdf). La logique sous-jacente s'applique également au cyber-risque.

L'Initiative est un partenariat entre :

IAIS 25 YEARS
INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS

Soutenu par :

coopération allemande
DEUTSCHE ZUSAMMENARBEIT

Ministry of Foreign Affairs of the Netherlands

Hébergée par :

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Initiative Accès à l'assurance
Hébergée par le Projet Financial Systems Approaches to Insurance de la GIZ
Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH
Dag-Hammarskjöld-Weg 1-5
65760 Eschborn, Germany

Téléphone : +49 61 96 79-1362
Fax : +49 61 96 79-80 1362
E-mail : secretariat@a2ii.org
Site web : www.a2ii.org

a2ii_org

Promouvoir l'accès pour tous à une assurance responsable et inclusive.