BAC
Bureau d'assurance du Canada

Mémoire

Projet de Règlement sur la gestion et le signalement des incidents de sécurité de l'information de certaines institutions financières et des agents d'évaluation du crédit

Présenté à

M^e^ Philippe Lebel, secrétaire et directeur général des affaires juridiques
Autorité des marchés financiers

Bureau d'assurance du Canada – Québec
Février 2024

Table des matières

Le Bureau d'assurance du Canada (BAC) est l'association nationale qui représente 90 % des sociétés privées d'assurance habitation, automobile et entreprise au Canada. L'industrie de l'assurance de dommages joue un rôle de premier plan dans l'économie québécoise en permettant à la population de se prémunir contre des sinistres pouvant avoir un impact important sur sa sécurité financière en protégeant son patrimoine.

Le BAC au Québec œuvre auprès des consommateurs, des entreprises, des médias, des groupes d'intérêt et des gouvernements dans le but de les informer et de les sensibiliser sur divers sujets et enjeux qui les touchent de près.

Introduction

Le Bureau d'assurance du Canada (BAC) expose ci-après les commentaires de ses membres à l'occasion de la consultation de l'Autorité des marchés financiers (l'Autorité) sur le Règlement sur la gestion et le signalement des incidents de sécurité de l'information de certaines institutions financières et des agents d'évaluation du crédit (Règlement). Le BAC remercie l'Autorité de l'attention qu'elle accordera à ses commentaires.

Les assureurs de dommages reconnaissent la nécessité d'encadrer efficacement la gestion et le signalement des incidents de sécurité de l'information. D'ailleurs, le BAC soutient l'industrie de l'assurance de dommages dans sa volonté d'optimiser et de simplifier le signalement des incidents de sécurité de l'information.

C'est guidé par ces principes d'innovation et de leadership que le BAC insiste, dans ce mémoire, sur les préoccupations des assureurs de dommages et propose des solutions précises, efficaces et réalistes.

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

Sommaire des recommandations

En réponse à la présente consultation sur le Règlement, le BAC fait les 16 recommandations suivantes :

1. Privilégier l'adoption d'une structure organisationnelle de gestion du risque liée aux incidents de sécurité de l'information plutôt que d'une politique.
2. Préciser dans quelles circonstances le signalement aux dirigeants et gestionnaires de l'institution financière doit être fait lorsque l'incident survient au sein d'un tiers.
3. Limiter l'obligation de signalement des incidents à l'Autorité et aux « *personnes concernées par un incident qui présente un risque qu'un préjudice sérieux leur soit causé* ».
4. Préciser l'étendue du rôle du responsable de surveiller la gestion et le signalement des incidents de sécurité de l'information.
5. Préciser le seuil de déclenchement d'un signalement à l'Autorité, en fonction de la matérialité de l'incident de sécurité qui doit présenter un « *risque de préjudice sérieux* ». Ainsi, le premier alinéa se lirait comme suit :

    i. *« Une institution financière ou un agent d'évaluation du crédit doit signaler à l'Autorité tout incident de sécurité de l'information qui engendre ou est susceptible d'engendrer une perturbation, un ralentissement ou une interruption des activités critiques de l'institution et qui pourrait occasionner des pertes financières ou une atteinte à sa réputation et duquel les hauts dirigeants sont informés immédiatement au plus tard 24 heures suivant cet incident. »*

6. Préciser l'étendue de l'obligation de signalement dans le cas où un incident impliquerait un assureur, mais se déroulerait exclusivement hors Québec et n'occasionnerait pas de préjudice au Québec.

    Contextualiser et préciser l'étendue des personnes et organismes concernés par le signalement à « *une personne ou un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois* ».
7. Retirer l'article 6 puisque les signalements à la Commission d'accès à l'information (CAI) sont déjà visés par l'article 5.
8. Adopter la recommandation du BAC national quant à la simplification du signalement des incidents, en simplifiant et harmonisant la procédure, notamment par l'usage, le cas échéant, d'un formulaire unique.
9. Adapter le contenu exigé pour les avis subséquents, en précisant qu'ils doivent énoncer les nouveaux renseignements sur l'incident au fur et à mesure que ceux-ci deviennent disponibles.

    Éviter de fixer un échéancier ferme pour les avis subséquents, en précisant que ceux-ci doivent être transmis à l'Autorité sur une base périodique, au fur et à mesure que des nouveaux renseignements deviennent disponibles, et ce, jusqu'à ce que tous les renseignements importants au sujet de l'incident aient été fournis.
10. Définir la notion de « *clôture de l'incident* ».

11. Supprimer le paragraphe 2 et reformuler le paragraphe 3 pour qu'il se lise ainsi :

    i. *«[…] les leçons apprises à la suite de la survenance des incidents de sécurité de l'information et les moyens pris, au moment de rédiger le rapport, pour réduire la probabilité que de nouveaux incidents de même nature ne se reproduisent ».*

12. Reformuler le paragraphe 4 de l'article 11 pour qu'il se lise ainsi :

    i. *« […] une description détaillée de celui-ci, incluant les renseignements contenus au paragraphe 3 de l'alinéa 1 de l'article 10 ».*

13. Retirer le paragraphe 8 de l'article 11 concernant « *l'acceptation ou non du risque résiduel et les justificatifs afférents* ».

14. Retirer les paragraphes 4 et 5 de l'article 13 qui concernent les sanctions applicables pour les contraventions en matière de suivi.

15. Procéder à des vérifications et prendre des mesures afin d'éviter tout risque de double sanction pour une même infraction.

16. Ajouter une disposition transitoire octroyant aux assujettis un délai d'un an afin d'assurer la mise en conformité.

Commentaires généraux

I. Optimisation de la charge de conformité

Considérant que l'optimisation de la charge de conformité est une orientation stratégique de l'Autorité et une préoccupation de premier ordre pour les assureurs de dommages, le BAC souhaite attirer l'attention de celle-ci sur la possibilité de bonifier plusieurs des dispositions du Règlement. Cet exercice de clarification vise à mitiger les risques de contradiction et à faciliter la mise en conformité des institutions financières. À cet égard, il est primordial que les incidents à signaler soient clairement identifiés dans le Règlement.

Également, le BAC tient à souligner qu'à l'heure actuelle, au Québec, les incidents de sécurité de l'information sont encadrés notamment par la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*[1], la *Loi sur la protection des renseignements personnels dans le secteur privé*[2], le *Règlement sur les incidents de confidentialité*[3], la *Ligne directrice sur la gestion des risques liés aux technologies de l'information et des communications*[4], la *Ligne directrice sur la gestion du risque opérationnel*[5] et la *Ligne directrice sur la gestion de la continuité des activités*[6]. Il est important de considérer que la multiplication des encadrements engendre des risques de dédoublement et complexifie la gestion des incidents pour les assujettis.

Puisque l'encadrement actuel couvre déjà l'ensemble des règles à suivre en cas d'incidents de sécurité pouvant avoir un impact sur les opérations des assureurs, il y a lieu d'être prudent en ce qui concerne l'élaboration des dispositions du présent Règlement. En effet, le risque de confusion est grand puisque les institutions financières devront continuer à appliquer les lignes directrices et lois susmentionnées tout en respectant le Règlement alors que celles-ci encadrent les mêmes événements et ciblent les mêmes obligations.

Nous comprenons qu'un règlement n'a pas le même impact qu'une ligne directrice, mais soulignons que dans le reste du pays, les autorités réglementaires ont opté pour un encadrement prudentiel plutôt que réglementaire.

[1] RLRQ c A-2.1
[2] RLRQ P-39.1
[3] RLRQ c A-2.1, r. 3.1
[4] Ligne directrice sur la gestion des risques liés aux technologies de l'information et des communications | AMF (lautorite.qc.ca)
[5] Ligne directrice sur la gestion du risque opérationnel | AMF (lautorite.qc.ca)
[6] Ligne directrice sur la gestion de la continuité des activités | AMF (lautorite.qc.ca)

II. Harmonisation et allègement des pratiques

Le BAC et ses membres sont d'avis que la recherche d'une plus grande harmonisation avec le Bureau du surintendant des institutions financières (BSIF) et les autres provinces canadiennes est primordiale afin de faciliter l'application des dispositions concernant la gestion et le signalement des incidents de sécurité de l'information. Tant les assureurs que les consommateurs en bénéficieraient. Pour que le signalement et la gestion des incidents de sécurité de l'information fonctionnent, il faut que les assureurs puissent agir rapidement et efficacement, gouvernés par un encadrement clair. Si le processus de signalement est trop complexe et le nombre d'organismes à qui les signaler est trop grand, les assureurs ont moins de temps pour gérer l'incident et minimiser les dommages pour l'organisation et les consommateurs.

Le siège social du BAC (BAC national) a d'ailleurs élaboré un cadre pour une norme unique de signalement des cyberincidents et il effectue des représentations auprès des autorités réglementaires provinciales (dont le BC Financial Services Authority (BCFSA) et l'Autorité ontarienne de réglementation des services financiers (ARSF)) en faveur de l'introduction de cette norme dans l'ensemble du pays. Le but premier d'une telle initiative est d'harmoniser et de simplifier le processus de signalement des incidents au BSIF et aux organismes de réglementation provinciaux.

L'idée développée par l'industrie de permettre la transmission du formulaire de signalement du BSIF aux autorités réglementaires des autres provinces est un exemple patent d'une mesure d'harmonisation et d'allègement simple à mettre en œuvre. L'alignement des seuils de déclenchement et des échéanciers à travers tout le pays représente une mesure tout aussi prometteuse.

Commentaires et recommandations du BAC

I. Politique de gestion des incidents et responsable (art. 3 et 4)

Le BAC est d'avis qu'il serait plus approprié de favoriser l'adoption et la mise en œuvre d'une « Structure organisationnelle de gestion du risque lié aux incidents de sécurité de l'information », plutôt que d'une « Politique de gestion des incidents de sécurité de l'information », devant être approuvées par le conseil d'administration de chaque institution financière. Il s'agirait alors d'un alignement sur les exigences de la Ligne directrice B-13 du BSIF *Gestion du risque lié aux technologies et du cyberrisque* à son paragraphe A.3 et d'un mode de gouvernance mieux adapté à la réalité et aux pratiques des assureurs.

Recommandation n° 1

Privilégier l'adoption d'une structure organisationnelle de gestion du risque liée aux incidents de sécurité de l'information plutôt que d'une politique.

Signalement aux dirigeants

Le BAC est également préoccupé par la référence aux « tiers à qui cette institution, cette caisse ou cet agent a confié l'exercice de toute partie d'une activité », une disposition qui, telle que rédigée à l'alinéa 2 de l'article 3, ne semble pas appropriée. Le BAC est d'avis qu'il y aurait lieu d'apporter des clarifications quant aux intentions de l'Autorité à cet égard.

En effet, on semble dire que le signalement aux dirigeants doit être fait pour tout incident de sécurité de l'information survenu au sein d'un tiers visé par le premier alinéa. Or, ce signalement à l'institution financière ne devrait être requis que lorsque l'incident a un impact sur la disponibilité, l'intégrité ou la confidentialité des systèmes d'information ou des informations de l'institution financière. Si l'institution financière n'est pas affectée, la notification à ses dirigeants ne devrait pas être requise. Le BAC recommande d'apporter une précision en ce sens.

Recommandation n° 2

Préciser dans quelles circonstances le signalement aux dirigeants et gestionnaires de l'institution financière doit être fait lorsque l'incident survient au sein d'un tiers.

Signalement aux « parties prenantes »

Aussi, au deuxième alinéa de l'article 3, on mentionne que le signalement doit être fait aux autres parties prenantes, notamment aux clients, aux tiers visés à l'alinéa 1 et aux consommateurs. Or, l'Autorité ne précise pas si ces personnes doivent risquer d'encourir un préjudice sérieux pour que le signalement leur soit obligatoirement fait.

Dans le *Règlement sur les incidents de confidentialité*, l'avis à la Commission d'accès à l'information (CAI) porte sur un incident de confidentialité présentant un risque qu'un préjudice sérieux soit causé aux personnes concernées.

Le BAC recommande d'adopter une approche similaire de façon à limiter le nombre de

signalements inutiles.

Recommandation n° 3

Limiter l'obligation de signalement des incidents à l'Autorité et aux « *personnes concernées par un incident qui présente un risque qu'un préjudice sérieux leur soit causé* ».

« Responsable »

L'article 4 oblige les institutions financières à désigner, par écrit, un de ses dirigeants « responsable de surveiller la gestion et le signalement des incidents de sécurité de l'information ». Ce rôle hybride de surveillance et de signalement est une nouveauté.

Les assureurs se questionnent sur le positionnement de cette fonction dans une stratégie globale de gestion de l'information et de protection des renseignements personnels, comportant déjà des politiques internes. Dans ce cadre, il est utile de rappeler que les organisations ont déjà un *Responsable de la protection des renseignements personnels* ainsi qu'un *Responsable de la sécurité des systèmes d'information* (CISO) et d'autres personnes responsables de la surveillance et de la gestion des risques.

Il serait donc utile pour nos membres que l'Autorité précise l'étendue de ce rôle et s'il est de son intention de permettre la délégation de certaines tâches.

Recommandation n° 4

Préciser l'étendue du rôle du responsable de surveiller la gestion et le signalement des incidents de sécurité de l'information.

II. Incidents de sécurité à signaler – critère de matérialité (art. 2, 5 et 6)

L'article 2 du règlement propose comme définition du terme « incident de sécurité » une « atteinte à la disponibilité, à l'intégrité ou à la confidentialité des systèmes d'information ou aux informations qu'ils contiennent ». Quant aux critères permettant de déterminer qu'il s'agit d'un incident à signaler en vertu du règlement, ils se retrouvent à l'article 5. Le BAC souligne que les assureurs devraient aisément être en mesure de définir et de caractériser le seuil au-delà duquel un incident de sécurité de l'information doit être rapporté. Or, l'expression « un risque d'occasionner des répercussions négatives » vise un nombre d'incidents beaucoup trop élevé. La charge administrative et la charge de conformité seraient alors démesurées par rapport au résultat recherché par l'Autorité.

En effet, les responsables de la sécurité informatique des institutions financières peuvent détecter des centaines de tentatives d'attaques quotidiennement et ce, malgré l'implantation de systèmes de protection extrêmement performants. Évidemment, toutes ces tentatives ne se matérialisent pas en attaques susceptibles d'occasionner des répercussions importantes, mais, de façon générale, on peut affirmer qu'il s'agit de « répercussions négatives ».

Les incidents sont déjà documentés par les assureurs et, dans certains cas, des plans d'urgence sont enclenchés, dont par exemple l'interruption des systèmes informatiques afin d'effectuer des vérifications et d'apporter des correctifs. Des mesures préventives sont aussi mises en

œuvre afin de réduire le plus possible la survenance d'incidents. Ces pratiques sont habituelles et permettent de maintenir de hauts standards de sécurité.

Ces incidents sont rapportés aux dirigeants de différents niveaux hiérarchiques à différentes périodicités, en fonction de leur matérialité. Les incidents qui entraînent des répercussions négatives mineures pourraient être rapportés aux dirigeants trimestriellement dans un rapport comportant des données consolidées alors que les incidents non critiques, mais plus importants pourraient être rapportés à un dirigeant intermédiaire au moment où l'événement survient afin que ce dernier décide des actions à prendre dans l'immédiat. Lorsqu'un incident engendre ou est susceptible d'engendrer une perturbation, un ralentissement ou une interruption des activités critiques de l'institution et pourrait occasionner des pertes financières ou une atteinte à sa réputation, les hauts dirigeants en sont informés sans délai.

Le BAC est d'avis que la formulation actuelle du premier alinéa de l'article 5 ne permet pas de faire la distinction entre les incidents en fonction de leur niveau critique, car tous les incidents ayant des répercussions négatives signalées à un dirigeant doivent être rapportés à l'Autorité. Il recommande donc de préciser la matérialité des incidents qui doivent être signalés et le niveau hiérarchique du dirigeant à qui cet incident est rapporté dans le cadre normal des activités.

La matérialisation d'un « risque de préjudice sérieux » retenu par la CAI dans le *Règlement sur les incidents de confidentialité* ou encore le critère retenu par l'Autorité dans sa lettre du 20 décembre 2019 aux premiers dirigeants permettrait de clarifier le critère de déclenchement du signalement.

Évidemment, toutes les incertitudes afférentes à l'alinéa 2 pourraient être atténuées par les précisions qui, nous l'espérons, seront apportées quant à la matérialité de l'incident de sécurité.

Recommandation n° 5

Préciser le seuil de déclenchement d'un signalement à l'Autorité, en fonction de la matérialité de l'incident de sécurité qui doit présenter un « *risque de préjudice sérieux* ». Ainsi, le premier alinéa se lirait comme suit :

« Une institution financière ou un agent d'évaluation du crédit doit signaler à l'Autorité tout incident de sécurité de l'information qui engendre ou est susceptible d'engendrer une perturbation, un ralentissement ou une interruption des activités critiques de l'institution et qui pourrait occasionner des pertes financières ou une atteinte à sa réputation et duquel les hauts dirigeants sont informés immédiatement, au plus tard 24 heures suivant cet incident. »

Nos soulignés

Délai de 24h

En ce qui a trait à l'exigence de divulgation au plus tard 24 heures suivant l'incident, il est difficile pour les assureurs de dommages de prendre position présentement, dans la mesure où l'on considère que la matérialité du critère ou de la situation entraînant le déclenchement de la procédure de signalement doit d'abord être précisée. Le BAC est d'avis que plus le critère revêtira un caractère « sérieux », plus il sera réalisable de divulguer l'incident dans un

délai de 24 heures. Si l'Autorité décidait de maintenir le critère de « répercussions négatives », le délai proposé serait nettement insuffisant.

Une autre variable à considérer en ce qui concerne le délai de 24 heures est le niveau de détails attendu au stade du signalement. Le BAC a pris connaissance des informations à consigner dans le registre des incidents, à l'article 11 du Règlement. Sur la base de cette nomenclature, il est nécessaire de spécifier lesquelles de ces informations devront être communiquées au stade du signalement initial à l'Autorité. Aussi, il sera primordial d'accorder aux assureurs une certaine tolérance quant à la divulgation, car les incidents ont un caractère évolutif et qu'il n'est pas toujours évident d'en brosser un portrait clair et exhaustif à tout moment.

Signalement à d'autres organismes

Le deuxième alinéa de l'article 5 énonce l'exigence de signaler à l'Autorité tout incident de sécurité de l'information qui a été signalé à un organisme de réglementation. L'Autorité omet de mentionner, dans son projet de Règlement, l'étendue de cette obligation. Il serait utile de préciser à quels organismes de réglementation il est fait référence. Par exemple, qu'adviendrait-il dans le cas où un incident impliquerait un assureur, mais se déroulerait exclusivement hors Québec et n'occasionnerait pas de préjudice au Québec? L'Autorité devrait-elle tout de même en être notifiée?

Relativement au signalement à « une personne ou un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois », le BAC est d'avis qu'il serait utile de contextualiser cette obligation et d'avoir davantage de précisions sur l'étendue des personnes et organismes concernés.

Recommandation n° 6

- **Préciser l'étendue de l'obligation de signalement dans le cas où un incident impliquerait un assureur, mais se déroulerait exclusivement hors Québec et n'occasionnerait pas de préjudice au Québec.**
- **Contextualiser et préciser l'étendue des personnes et organismes concernés par le signalement à « *une personne ou un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois* ».**

Incidents rapportés à la CAI

Finalement, nous ne comprenons pas la nécessité de réitérer à l'article 6 que les incidents rapportés à la CAI doivent être rapportés à l'Autorité puisque cette obligation se retrouve à l'alinéa 2 de l'article 5 : « qui a été signalé à un organisme de réglementation ». Le BAC recommande donc de retirer l'article 6 afin de regrouper dans un même article les obligations de signalement dites « secondaires ». La rédaction du Règlement en serait allégée et gagnerait en cohérence.

Recommandation n° 7

Retirer l'article 6 puisque les signalements à la CAI sont déjà visés par l'article 5.

III. Avis initial et suivi (Articles 7, 8 et 9)

En ce qui concerne le formulaire que l'Autorité compte utiliser pour le signalement des incidents via le portail Web, il est impossible pour les assureurs de dommages d'en commenter la forme ou le fond dans la mesure où il n'a pas encore été publié. Les membres du BAC apprécieraient avoir l'occasion de le commenter et recommandent qu'il soit rendu public le plus rapidement possible.

Comme mentionné en introduction, le BAC national a élaboré un cadre pour une norme unique de signalement des cyberincidents et effectue des représentations auprès des autorités réglementaires provinciales (dont le BCFSA et l'ARSF) en faveur de l'introduction de cette norme dans l'ensemble du pays. Le but premier d'une telle initiative est d'harmoniser et de simplifier le processus de signalement des incidents au BSIF et aux organismes de réglementation provinciaux.

Nos membres sont d'avis qu'une initiative de la sorte est plus que nécessaire, car elle permettra d'uniformiser les exigences concernant les informations devant figurer dans les rapports, les seuils de déclenchement et les échéanciers à travers le pays.

Ainsi, pour les assureurs assujettis à la surveillance du BSIF, la proposition du BAC prend en compte l'exigence de fournir un rapport détaillé et contemporain au BSIF. Au lieu d'exiger des assureurs qu'ils produisent un rapport supplémentaire pour chaque province, les organismes de réglementation provinciaux devraient accepter et considérer les rapports d'incidents du BSIF comme étant conformes aux exigences provinciales en matière de déclaration d'incidents. Si une telle proposition était retenue, les assureurs seraient disposés à inclure une ventilation provinciale (propre à la province en question) dans leur rapport.

Pour les assureurs assujettis aux organismes de réglementation provinciaux, il est légitime que chaque province développe son propre cadre de gestion et de signalement des incidents de sécurité. Cela dit, il serait tout autant opportun que les assureurs ne soient pas soumis à des exigences provinciales en matière de déclaration qui excéderaient les critères déjà en vigueur dans la province.

Le BAC rappelle aussi l'importance pour les organismes de réglementation de veiller à ce que les exigences provinciales en matière de déclaration des incidents respectent les privilèges de communication, notamment en protégeant les rapports d'incidents contre les demandes d'accès à l'information et contre la divulgation dans le cadre d'un litige avec une tierce partie.

Recommandation n° 8

Adopter la recommandation du BAC national quant à la simplification du signalement des incidents, en simplifiant et en harmonisant la procédure, notamment par l'usage, le cas échéant, d'un formulaire unique incluant une ventilation provinciale.

Avis subséquents

En ce qui concerne les avis subséquents prévus à l'article 8, le BAC s'interroge sur le délai de trois (3) jours établis par l'Autorité pour l'aviser de l'évolution de la situation et les avis subséquents tous les trois jours jusqu'à la clôture de l'incident. Un délai strict comme celui-ci permet-il réellement de s'adapter à la réalité propre à la gestion d'un incident de sécurité de l'information?

En effet, l'Autorité doit prendre en compte la période durant laquelle les équipes de sécurité informatique effectuent des recherches afin de circonscrire l'incident, d'en évaluer la gravité et de prendre les mesures de mitigation et de correction requises. Ainsi, le BAC recommande à l'Autorité de privilégier une certaine souplesse dans la nomenclature des informations à soumettre et d'être flexible en ce qui concerne les délais de divulgation. À cet égard, le BAC invite l'Autorité à s'inspirer de la procédure mise en place par le BSIF qui exige dans son *Préavis sur le signalement des incidents liés à la technologie et à la cybersécurité*, que les signalements subséquents se fassent « périodiquement à mesure que de nouveaux renseignements deviennent disponibles, et ce, jusqu'à ce que tous les renseignements importants au sujet de l'incident aient été fournis ».

Recommandation n° 9

- **Adapter le contenu exigé pour les avis subséquents, en précisant qu'ils doivent énoncer les nouveaux renseignements sur l'incident au fur et à mesure que ceux-ci deviennent disponibles.**
- **Éviter de fixer un échéancier ferme pour les avis subséquents, en précisant que ceux-ci doivent être transmis à l'Autorité sur une base périodique, au fur et à mesure que des nouveaux renseignements deviennent disponibles et ce, jusqu'à ce que tous les renseignements importants au sujet de l'incident aient été fournis.**

Clôture de l'incident

Enfin, le BAC soumet que l'interprétation de l'article 9 serait facilitée par l'inclusion d'une définition de ce que l'Autorité entend par « clôture de l'incident ». S'agit-il du moment où l'incident est maîtrisé ou du moment où il est entièrement résolu ?

Recommandation n° 10

Définir la notion de « *clôture de l'incident* ».

IV. Rapport (article 10)

Le BAC est préoccupé par le paragraphe 2 de l'article 10 qui prévoit l'obligation de rapporter « l'appréciation de l'institution financière ou de l'agent d'évaluation du crédit quant à la récurrence potentielle de l'incident ». Le BAC s'interroge quant au niveau de détails attendu. En effet, il est épineux pour les assureurs de se commettre sur la récurrence potentielle d'un incident de sécurité, dans la mesure où les développements technologiques et les techniques imaginés par les pirates informatiques ou « hackers » sont impossibles à prévoir.

Conséquemment, le BAC recommande le retrait du paragraphe 2, car il est inapplicable. Le BSIF, dans son Préavis sur le signalement des incidents liés à la technologie et à la cybersécurité, insiste plutôt sur la démonstration par les institutions financières des « leçons apprises ». Cette exigence est à notre avis mieux adaptée à la réalité de la gestion des incidents de sécurité et pourrait se retrouver au paragraphe 3.

Le paragraphe 3 concerne « les moyens pris pour réduire la probabilité que de nouveaux incidents de même nature ne se reproduisent pas ». Il est entendu qu'à la suite d'un incident de sécurité de l'information, des actions immédiates seront prises pour éviter qu'il ne se reproduise. D'autres actions seront prises subséquemment sur un long continuum. Ainsi, il peut être difficile pour un assureur de rendre compte, dans les 30 jours suivant la clôture d'un incident, de tous les moyens pris. Certaines mesures, comme le changement de fournisseur de services informatiques, peuvent prendre plus de temps et tout de même s'avérer extrêmement efficaces pour prévenir la survenance de futurs incidents. Il y aurait donc lieu de préciser qu'on vise les moyens pris au moment de rédiger le rapport.

Recommandation n° 11

Supprimer le paragraphe 2 et reformuler le paragraphe 3 pour qu'il se lise ainsi :

« … les leçons apprises à la suite de la survenance des incidents de sécurité de l'information et les moyens pris, au moment de rédiger le rapport, pour réduire la probabilité que de nouveaux incidents de même nature ne se reproduisent. »

V. Registre des incidents (Art. 11-12)

Il y a ici apparence de double emploi, car le registre des incidents de sécurité de l'information renfermerait très fréquemment les mêmes informations que le registre des incidents de confidentialité de la CAI, dans la mesure où les incidents de confidentialité peuvent également constituer des incidents de sécurité de l'information au sens du présent Règlement.

En ce qui concerne le paragraphe 4 de l'article 11, le BAC suggère de le reformuler, afin qu'il reflète la suggestion de supprimer le paragraphe 2 de l'article 10 et les modifications proposées au paragraphe 3 de l'article 10.

Recommandation n° 12

Reformuler le paragraphe 4 de l'article 11 pour qu'il se lise ainsi :

« … une description détaillée de celui-ci, incluant les renseignements contenus au paragraphe 3 de l'alinéa 1 de l'article 10 ».

Évaluation des incidents de même nature

Quant au paragraphe 8 de l'article 11 sur « l'acceptation ou non du risque résiduel et les justificatifs afférents », il s'agit d'information stratégique et la divulgation requise à cet égard est préoccupante surtout dans le cadre d'une reddition de compte au cas par cas. Les évaluations de risques ne sont pas réalisées systématiquement pour chaque incident de sécurité de l'information et leur réalisation sera fonction du degré de matérialité.

Aussi, pour l'obtention de résultats probants, il peut être plus efficace de procéder à une analyse globale des incidents de même nature que de faire cette analyse pour un incident en

particulier. Conséquemment, le BAC est d'avis que cette mesure alourdit indûment la gestion des incidents et n'est pas utile à la surveillance de l'Autorité. Le BAC recommande donc le retrait du paragraphe 8.

Recommandation n° 13

Retirer le paragraphe 8 de l'article 11 concernant « *l'acceptation ou non du risque résiduel et les justificatifs afférents* ».

VI. Sanctions administratives pécuniaires (art. 13-14)

Les assureurs estiment qu'une tolérance devrait être observée en ce qui a trait aux délais de transmission des avis prévus aux articles 8 et 9 du présent Règlement. Comme mentionné précédemment, le délai de trois (3) jours peut être inapproprié dans certaines circonstances et une plus grande latitude permettrait d'harmoniser la remise des rapports aux différents organismes exigeant des suivis à la suite d'un incident. Si les assureurs disposent du temps nécessaire pour fournir l'information, l'Autorité obtiendra des données pertinentes et de qualité et le fardeau réglementaire sera diminué.

Les assureurs de dommages ont su démontrer au fil du temps leur diligence et leur sérieux dans la gestion des incidents de sécurité de l'information. L'Autorité peut compter sur leur pleine et entière collaboration. Le BAC recommande donc le retrait des paragraphes 4 et 5 l'article 13.

Recommandation n° 14

Retirer les paragraphes 4 et 5 de l'article 13 qui concernent les sanctions applicables pour les contraventions en matière de suivi.

Double sanction

Plus généralement, le BAC recommande qu'une vérification soit effectuée et que des mesures soient prises afin d'éviter tout risque de double sanction pour une même infraction déjà prévue dans une loi ou un règlement en vigueur.

Recommandation n° 15

Procéder à des vérifications et prendre des mesures afin d'éviter tout risque de double sanction pour une même infraction.

VII. Disposition finale (art. 15)

Le BAC et ses membres sont d'avis qu'une disposition transitoire devrait être prévue au Règlement et qu'elle devrait accorder un délai raisonnable afin de permettre aux assureurs de dommages de procéder à la mise en conformité de leur organisation respective.

Les changements apportés par ce nouveau Règlement auront de nombreux impacts, qu'il s'agisse de l'élaboration de politiques et de registres, de l'adaptation des systèmes informatiques, de la centralisation des registres, de la modification des contrats ou de la formation des équipes à l'interne. Un délai minimum d'un an permettrait aux institutions financières de franchir toutes les étapes susmentionnées et d'être fins prêtes au moment où le Règlement entrera en vigueur.

Recommandation n° 16

Ajouter une disposition transitoire octroyant aux assujettis un délai d'un an afin d'assurer la mise en conformité.

Conclusion

Les recommandations formulées par le BAC visent à bonifier le Règlement dans une optique d'optimisation de la conformité et de recherche d'une plus grande harmonisation et d'allègements, au bénéfice des assureurs et des consommateurs.

La gestion et le signalement des incidents de sécurité de l'information doivent pouvoir être effectués dans un encadrement clair et fluide, car les assureurs doivent agir efficacement. L'identification de la nature des incidents et des personnes et organismes concernés doit se faire rapidement et les actions pour mitiger les préjudices et corriger la situation doivent être prises sans délai. Il s'agit d'une course contre la montre et tout obstacle ou incertitude risque de compromettre les intérêts des institutions financières, de leurs clients et des tiers.

Le BAC et ses membres assureurs de dommages souhaitent remercier l'Autorité de l'opportunité qui leur est donnée de commenter ce projet de Règlement. La gestion et le signalement des incidents de sécurité de l'information sont des enjeux prioritaires pour les assureurs et nous sommes pleinement engagés à participer à l'effort requis pour simplifier et harmoniser l'encadrement qui sera en vigueur au Québec.

Nous demeurons disponibles pour en discuter plus amplement.

Fin du mémoire