ACPM | ACARR
The Association of Canadian Pension Management
L'Association canadienne des administrateurs de régimes de retraite

[VERSION FRANÇAISE NON OFFICIELLE]

Le 1er novembre 2023

Bureau du surintendant des institutions financières
255, rue Albert, 12e étage

Ottawa (Ontario) K1A 0H2

Lettre envoyée à pensions@osfi-bsif.gc.ca

À qui de droit :

Objet : Préavis du BSIF – Signalement des incidents liés à la technologie et à la cybersécurité pour les régimes de retraite

L'ACARR est le principal organisme de défense d'un système de revenu de retraite équilibré, efficace et durable au Canada. Les promoteurs et les administrateurs des régimes de retraite des secteurs privé et public gèrent les régimes de retraite de millions de participants, tant actifs que retraités.

Le 30 juin 2023, le BSIF a publié une version à l'étude d'un préavis intitulé *Signalement des incidents liés à la technologie et à la cybersécurité* (le « Préavis sur les régimes de retraite »), ainsi que le formulaire qui l'accompagne (le « Rapport d'incident »). Nous convenons que les cyberrisques constituent un enjeu important pour les organisations en général, y compris les régimes de retraite, et que le BSIF devrait être au fait des incidents majeurs. Nous craignons toutefois que, dans le cas des régimes de retraite sous réglementation fédérale (RRF), le processus de divulgations s'avère trop large, qu'il mènerait au signalement inapproprié d'incidents ou à des dédoublements, ou encore qu'il limiterait les ressources à un moment charnière.

Principes

Le Préavis sur les régimes de retraite semble s'inspirer du *Signalement des incidents liés à la technologie et à la cybersécurité* pour les institutions financières fédérales (IFF), publié en août 2021 (le « Préavis sur les IFF »). Bien que le contenu ait été quelque peu révisé, nous sommes d'avis que d'autres changements sont nécessaires pour reconnaitre les différences entre les risques technologiques et les cyberrisques auxquels font face les IFF et les RRF. Les IFF constituent un rouage essentiel au bon fonctionnement de l'économie canadienne en étant, entre autres, responsables de l'infrastructure des marchés et des liquidités partout au pays. Dans le cas des RRF, cependant, la plupart des risques technologiques et des cyberrisques sont beaucoup plus restreints, axés sur les bénéficiaires du régime et les caisses de retraite elles-mêmes, et les effets de cascade de ces risques sont plus limités.

1255, rue Bay, bureau 304, Toronto (Ontario) M5R 2A9
Téléphone : 416-964-1260 Télécopieur : 416-964-0567 www.acpm-acarr.com

- Bénéficiaires du régime : Dans la plupart des RRF, l'administrateur du régime est aussi l'employeur. Pour les RRF, les risques technologiques et les cyberrisques sont donc semblables à ceux que les employeurs courent lorsqu'ils stockent ou transmettent des données sur les membres du personnel. Comme ces employeurs sont des organisations sous réglementation fédérale assujetties à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), une structure est déjà en place pour signaler ce type d'incident.
- Caisses de retraite : Comme l'indique le Préavis sur les régimes de retraite, certains risques concernent les placements et les activités des caisses de retraite et pourraient ne pas être assujettis à la LPRPDE. Toutefois, comme les régimes de retraite font généralement affaire avec les IFF, la majorité de ces activités (p. ex., le versement de rentes par le régime de retraite, les règlements sur les marchés financiers ou les services de garde de biens) sont déjà assujetties aux exigences du BSIF en matière de signalement pour les IFF.

Pour assurer l'efficacité des exigences du BSIF en matière de signalement, le Préavis sur les régimes de retraite devrait viser à répondre à trois objectifs :

1. **Réduire au minimum les dédoublements** – Dans la mesure du possible, les structures existantes devraient être exploitées. Par exemple, le BSIF pourrait recevoir une notification en cas de violation s'inscrivant dans les critères de la LPRPDE et affectant les régimes de retraite. Par ailleurs, l'ensemble des organisations doivent mettre en place des protocoles de cybersécurité. Comme les secteurs sous réglementation fédérale regroupent les services bancaires, le transport et les sociétés d'État, bon nombre de ces protocoles sont particulièrement rigoureux. Même si les risques technologiques et les cyberrisques sont importants pour les régimes de retraite, ceux-ci n'ont rien de particulier en comparaison avec ceux qui affectent les employeurs qui financent les RRF. Plutôt que d'imposer un ensemble de critères indépendants, le BSIF devrait encourager les employeurs à étendre aux RRF leurs stratégies en matière de cyberrisques, y compris la documentation appropriée sur le cadre de gouvernance de ces dernières.
2. **Demeurer à l'intérieur de la juridiction du BSIF** – Alors que les IFF sont assujetties à la réglementation du BSIF, les employeurs qui administrent les RRF, eux, ne sont sous la juridiction du BSIF que lorsqu'ils exercent leurs responsabilités d'administration des régimes de retraite (leurs activités en tant qu'employeur ne relèvent pas du BSIF).
3. **Être significatif** – Les dispositions de la LPRPDE en matière de préavis s'appliquent si une violation crée un risque réel de préjudice important. Les facteurs pertinents comprennent la sensibilité des données concernées et le risque qu'elles soient utilisées à mauvais escient. Nous recommandons d'appliquer des critères semblables à tout signalement au BSIF.

Critères pour le signalement

Outre la définition d'un seuil, nous formulons les commentaires suivants sur les critères énoncés :

- Contrairement aux IFF, qui sont souvent interreliées et soumises à des risques de contagion, les risques technologiques et les cyberrisques qui ont une incidence sur les RRF auront rarement des conséquences sur d'autres RRF ou sur le système financier canadien dans son ensemble. Tout effet de contagion se produirait vraisemblablement à l'échelle d'une IFF ou d'une autre partie

fournissant un service à un RRF (p. ex., traitement des rentes ou règlements sur les marchés financiers).

- Les répercussions sur les opérations, l'infrastructure, les données ou les systèmes de l'employeur ne relèvent pas de la compétence du BSIF. Il ne faut déclarer ces incidents que s'ils ont une incidence sur les activités des RRF.
- Bien qu'il soit avisé de mettre en place un plan de résilience pour les RRF, il faut savoir que ces plans sont généralement intégrés dans le plan de résilience de l'organisation. À titre d'exemple, la pandémie de COVID-19 a mené au déclenchement du plan de résilience de l'ensemble des organisations, et les activités des caisses de retraite se sont poursuivies sans encombre.
- Le critère indiquant qu'« une atteinte à la réputation de l'administrateur du régime, de l'employeur ou des employeurs participants et des fournisseurs de services se profile » est beaucoup trop vague et peut dans certains cas contrevenir à la législation en matière de valeurs mobilières, sans divulgation publique.
- La référence à un incident « signalé au conseil d'administration, à la haute direction ou au conseil des fiduciaires » pourrait décourager les signalements internes prudents.
- L'inclusion d'incidents signalés au Commissariat à la protection de la vie privée, à un autre ministère fédéral et à d'autres organisations ou agences de surveillance ou de réglementation soulève la question du dédoublement des signalements, comme nous l'avons indiqué plus haut.
- La référence à « un avocat interne ou externe » comme critère de signalement n'est pas appropriée. Il faut plutôt encourager les RRF à faire appel aux conseils d'un avocat en cas de besoin, et ce, sans hésitation.
- Lorsque les participants et les bénéficiaires sont informés d'un incident encore non résolu, nous convenons qu'il serait prudent d'en informer le BSIF. Toutefois, il ne nous semble pas nécessaire de signaler les infractions concernant des personnes ou de petits groupes qui ont été résolues dans le cadre de la LPRPDE.

Exigences en matière de déclaration

Le Préavis sur les régimes de retraite exige l'envoi d'un rapport d'incident au BSIF, à une boîte de courriel générique, dans un délai de 24 heures. Il faut faire régulièrement le point sur la situation et procéder à un examen après l'incident faisant notamment état des leçons tirées.

Nous craignons que le cadre proposé pour les signalements en temps réel ne détourne les ressources de la gestion des incidents et ne crée des risques supplémentaires, compte tenu de la communication de renseignements de nature délicate. Le besoin en ressources et la coordination associés à ces signalements pourraient s'avérer particulièrement contraignants pour les plus petits régimes.

Les administrateurs de régimes, en leur qualité de fiduciaires, sont déjà tenus de mettre en place des cadres de gouvernance, de gestion des risques et de gestion des données appropriés qui englobent les risques liés aux technologies de l'information et à la gestion de données confidentielles ou personnelles, y compris lorsqu'elles font l'objet d'une délégation ou d'entente de service avec des tiers.

Par ailleurs, le préavis ne traite pas de la communication au BSIF de renseignements délicats qui ne relèvent pas de son pouvoir de réglementation (p. ex., lorsque l'incident concernant un risque lié aux

technologies de l'information ne se limite pas au régime de retraite et à ses participants, mais qu'il touche également la sécurité et la gestion de l'information au sein de l'organisation). Certains des indicateurs présentés dépassent le champ d'application de la *Loi sur les normes de prestation de pension* du Canada (LNPP) et peuvent ne pas avoir d'incidence réelle sur les participants au régime.

L'absence de confidentialité relativement aux renseignements demandés par le BSIF (par exemple, dans le cadre d'une demande de signalement en vertu de la LNPP, de la *Loi sur l'accès à l'information* du Canada ou de la *Loi sur la protection des renseignements personnels* du Canada) pourrait entraîner la divulgation inappropriée de renseignements sur la cause, la nature et l'état des incidents – une situation incohérente avec la gouvernance et les pratiques de gestion des risques de l'administrateur d'un régime de retraite.

La proposition relative à la transmission de renseignements délicats à une boîte de courriel centrale du BSIF ne cadre pas avec des pratiques prudentes de gestion des risques.

Exemples d'incidents à signaler

La LNPP n'oblige pas les régimes de retraite à mettre en place un portail en ligne. Par conséquent, à moins d'un problème concernant les versements aux participants ou la confidentialité ou l'intégrité des données, il n'est pas nécessaire de signaler un incident en lien avec le portail d'un régime de retraite. En outre, les serveurs des employeurs sont exclus du champ d'application de la LNPP (dans la mesure où ils ne sont pas liés au fonctionnement des RRF).

Une atteinte majeure aux outils technologiques ou à la cybersécurité d'un tiers touchant les données d'un régime ou les fonds d'une caisse de retraite doit généralement être signalée par le tiers en question, en vertu de la LPRPDE ou des exigences actuelles des IFF en matière de signalement. En fait, le tiers pourrait ne fournir à l'administrateur du RRF que des détails limités au sujet de la violation des données.

Un message d'extorsion reçu par un employeur ne s'inscrit pas non plus dans le champ d'application de la LNPP, sauf si un RRF est impliqué.

Les exemples d'incidents à signaler devraient faire l'objet de précisions, et le champ d'application devrait se limiter aux incidents liés à la technologie ou à la cybersécurité qui affectent les serveurs de l'administrateur d'un régime de retraite ou d'un fournisseur tiers, qui sont susceptibles d'avoir des répercussions importantes sur le versement des rentes ou la confidentialité ou l'intégrité des données et qui n'ont pas à être signalés autrement par une IFF ou en vertu de la LPRPDE.

Formulaire de rapport d'incident

Nous suggérons d'éliminer le Rapport d'incident et de déterminer plutôt les principes selon lesquels une RRF devrait signaler au BSIF un incident lié à la technologie ou à la cybersécurité :

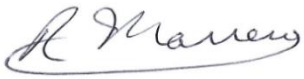
- S'assurer que les RRF disposent de plans de résilience appropriés en cas d'incident touchant les outils technologiques ou la sécurité informatique en les documentant dans leurs cadres de gouvernance;

dans le cas rare d'un RRF autonome (entité juridique distincte du promoteur du régime), le BSIF pourrait prendre d'autres mesures pour vérifier le plan de résilience

- Lorsqu'un incident concernant un RRF doit être signalé en vertu de la LPRPDE, signaler l'incident au BSIFà condition que les renseignements personnels transmis au BSIF le soient de manière appropriée
- Les RRF doivent aviser le BSIF de tout incident signalé à l'ensemble des participants qui n'a pas été résolu en temps opportun
- Le BSIF doit revoir les exigences en matière de signalement pour les IFF afin de s'assurer que les questions relatives aux RRF sont traitées adéquatement (p. ex., une atteinte aux systèmes de garde de biens ou aux systèmes de paiement ayant une incidence sur les bénéficiaires).

Nous vous remercions de votre attention et restons à votre disposition si vous avez besoin d'aide supplémentaire.

Cordialement,



Ric Marrero
Chef de la direction
ACARR