Ligne directrice de l'ACOR

Le Cyberrisque pour les Regimes de Retraite

Date : 9 juin 2022

Table des matières

1. INTRODUCTION

Contexte

Les intervenants des régimes de retraite s'appuyant de plus en plus sur la technologie, l'Association canadienne des organismes de contrôle des régimes de retraite (ACOR) se penche sur le cyberrisque afin d'aider les administrateurs de régimes de retraite à assurer la sécurité de l'actif des régimes et à protéger les droits et intérêts des bénéficiaires.

Les administrateurs de régimes de retraite et leurs prestataires de services contrôlent de gros actifs financiers ainsi que des données personnelles et confidentielles, ce qui peut en faire une cible attrayante pour les criminels, les cyberattaques et la fraude. Les violations de la cybersécurité ont des conséquences considérables sur les bénéficiaires des régimes et leurs familles, ainsi qu'un préjudice à la réputation des parties concernées.

Un régime de retraite doit être administré, et ses actifs, investis par l'administrateur du régime de retraite avec la prudence, la diligence et la compétence exigées d'un fiduciaire. Des mesures doivent donc être prises afin de protéger les bénéficiaires et les actifs des régimes contre le risque de cyberattaques. Les administrateurs de régimes de retraite et leurs agents doivent être conscients qu'il s'agit d'un risque majeur et qu'ils doivent les surveiller et les gérer dynamiquement.

Le résultat de la discussion de l'ACOR sur le cyberrisque s'appuie sur les lignes directrices fondamentales de l'ACOR en matière de gouvernance des régimes (ligne directrice nº 4 de l'ACOR) et de gestion des risques (ligne directrice nº TBD de l'ACOR) en mettant l'accent sur les particularités des cyberrisques comme éléments clés dans la gestion des risques des régimes de retraite.

Un régime de retraite devrait prendre en considération la présente ligne directrice en fonction de sa taille, de la nature, de la portée et de la complexité de ses activités et de son profil de risque.

Qu'est-ce que le cyberrisque?

Le cyberrisque est le risque de perte financière, de perturbation opérationnelle ou d'atteinte à la réputation résultant d'un accès non autorisé, d'une utilisation malveillante ou non, d'une panne, d'une divulgation, d'une perturbation, d'une modification ou d'une destruction des systèmes informatiques et/ou des données qu'ils contiennent. Dans le contexte d'un régime de retraite, le cyberrisque comprend à la fois les risques internes (p. ex., des employés mécontents ou un manque de contrôles sur les accès) et les risques externes (p. ex., les hacktivistes, les activistes parrainés par l'État ou les cybercriminels).

Voici quelques exemples de cyberrisque :

- logiciel malveillant (également appelé « maliciel »);

- courriels d'hameçonnage (c.-à-d. l'acquisition de données sensibles par le biais d'une sollicitation frauduleuse, dans laquelle l'auteur se fait passer pour une entreprise légitime ou une personne de confiance);
- le piratage (c.-à-d. l'obtention d'un accès non autorisé à des réseaux, des systèmes informatiques et des appareils numériques);
- la divulgation de renseignements par inadvertance (p. ex., la fuite accidentelle de renseignements personnels concernant des membres).

Principaux points à retenir de cette ligne directrice :

- Le cyberrisque est un risque majeur pour tous les régimes, quelles que soient leur taille ou leurs caractéristiques. Il doit être régulièrement analysé et évalué afin d'assurer que des contrôles appropriés sont en place pour permettre au régime de gérer le risque. Les cyberrisques sont complexes et évolutifs et nécessitent une réaction dynamique.
- En s'acquittant de leurs responsabilités fiduciaires, les administrateurs de régimes doivent s'assurer que le régime a accès aux compétences, à l'expertise et/ou à la formation nécessaires pour comprendre et gérer le cyberrisque.
- Les rôles et les responsabilités relativement au cyberrisque doivent être clairement définis, attribués et compris, incluant toute activité déléguée à des prestataires de services tiers (et tous les sous-traitants applicables).
- Les administrateurs de régimes doivent mettre en place une stratégie pour répondre et signaler les cyberincidents.

2. L'INTÉGRATION DU CYBERRISQUE DANS LA GOUVERNANCE ET LA GESTION DES RISQUES

L'ACOR s'attend à ce que les administrateurs de régimes de retraite intègrent la gestion et la surveillance du cyberrisque dans les mêmes cadres de gouvernance et de gestion des risques utilisés que ceux utilisé pour évaluer et répondre aux autres risques importants du régime.

Considérations pour l'intégration du cyberrisque

Pour intégrer efficacement le cyberrisque, les administrateurs de régimes de retraite peuvent vouloir considérer certaines des caractéristiques qui peuvent rendre le cyberrisque difficile. Cela comprend la caractère évolutif de la technologie, des cyberpratiques et des normes sur les données, la nécessité d'une expertise et d'une formation technologiques spécialisées, ainsi que le caractère sensible des renseignements conservés par les régimes qui peuvent avoir des conséquences à long terme en cas de divulgation (p. ex., le vol d'identité) et qui pourrait entraîner une perte de confiance et un risque pour la réputation.

En intégrant le cyberrisque dans les cadres de gouvernance et de gestion des risques du régime de retraite, les administrateurs du régime doivent tenir compte de questions telles que celles présentées à l'annexe A.

Des exemples de contrôles pouvant être pertinents pour les activités de gestion du cyberrisque sont présentés à l'annexe B. Comme pour tout autre risque, les contrôles appropriés varient en fonction de la nature, de l'impact potentiel et de la probabilité du risque en question. Le processus de base de gestion de risque d'identification, de hiérarchisation, de gestion et de surveillance doit être suivi pour tous les risques, y compris le cyberrisque.

Contrats avec des tiers

Les administrateurs de régimes de retraite doivent être conscient que les attentes de l'ACOR s'appliquent lorsque les administrateurs de régimes de retraite délèguent une partie de l'administration et des placements de la caisse de retraite à des fournisseurs de services tiers. En ce qui concerne le cyberrisque, les administrateurs de régimes de retraite devraient connaître et comprendre les points suivants en ce qui concerne leurs fournisseurs de services tiers :

- Position de cybersécurité[1] et capacités de cybersécurité;
- Risques et contrôles liés aux technologies de l'information;
- Certifications et sceaux de conformité aux normes applicables;
- Processus indiquant comment et quand l'administrateur du régime de retraite serait informé d'un incident chez le tiers (et les sous-traitants s'il y a lieu), de son impact sur les bénéficiaires et les actifs du régime, et de la fréquence des mises à jour tout au long de l'incident;
- Processus permettant de fournir des mises à jour sur les cyberrisques et des conseils sur les cybermenaces aux parties concernées.

Les administrateurs de régimes de retraite doivent s'assurer que tous les fournisseurs de services tiers ont mis en place des contrôles suffisants pour protéger les données des bénéficiaires et les actifs du régime. Le cyberrisque doit être pris en compte dans la sélection d'un fournisseur de services tiers et des dispositions appropriées doivent être incluses dans les contrats.

[1] La position de cybersécurité désigne la stabilité des contrôles et des protocoles de cybersécurité permettant de prévoir et de prévenir les cybermenaces, ainsi que la capacité d'agir et de réagir pendant et après une attaque.

3. CYBERRISQUE – PLANIFICATION POUR L'INCIDENT ET LA RÉPONSE

Les cyberrisques comprennent généralement un « incident » et une « réponse ». Les administrateurs de régimes de retraite doivent construire leur cyberrésilience, c'est-à-dire leur capacité à évaluer et à minimiser le risque d'un cyberincident, mais aussi à rétablir la situation lorsqu'un incident se produit. Pour assurer une gestion efficace d'un incident, les administrateurs de régimes de retraite doivent travailler avec toutes les parties concernées (y compris les départements internes, les fournisseurs de services tiers et les employeurs) afin de déterminer :

- comment les cyberincidents seront détectés;
- la manière dont le plan se rétablira après l'incident et reprendra les opérations régulières (voir Plans de résilience); et
- quelles divulgations doivent être faites, et à qui, en ce qui concerne tout incident (voir Rapport d'incident).

Plans de résilience

La gestion des cyberrisques devrait inclure la mise en place d'un plans d'urgence résistant pour faire face aux incidents et reprendre les opérations rapidement et en toute sécurité. Les éléments essentiels d'un plan de résilience concernent généralement la continuité des activités, la reprise après sinistre et la réponse aux incidents. Un plan de résilience doit couvrir une série de scénarios et la probabilité de différents types d'incidents. Il doit préciser :

- les rôles et responsabilités de l'équipe de réponse aux incidents, y compris les responsabilités des tiers et leurs processus de réponse aux incidents;
- les ressources nécessaires pour enquêter sur le cyberincident et maintenir les fonctions essentielles (p. ex., le versement des prestations) et les processus;
- les communications en cas de crise, y compris la manière et le moment où les membres du conseil d'administration ou les fiduciaires (selon le cas) en seront informés; et,
- le processus, les seuils et les délais de notification à d'autres parties, y compris les autorités de surveillance, les forces de l'ordre (en cas de fraude), les tiers et, si nécessaire, les bénéficiaires du régime.

Les administrateurs de régimes de retraite peuvent également tirer profit de la création de divers manuels de simulation de cyberintrusion et de l'organisation régulière d'exercices de simulation avec toutes les parties concernées, les employés, les fournisseurs et fournisseur de services tiers, les compagnies de sous-traitance, etc., pour pratiquer et améliorer les capacités de gestion des cyberincidents.

Rapport d'incident

En ce qui concerne les rapports d'incidents :

- les administrateurs de régimes de retraite doivent établir clairement comment et quand les cyberincidents doivent leur être signalés, en plus des bénéficiaires du régime et des autres parties concernées;
- les administrateurs de régimes de retraite doivent déterminer si la notification d'un cyberincident à d'autres parties est requise, qu'elle soit volontaire ou prescrite par une loi, et doivent s'assurer que la notification respecte les délais prescrits;
- les bénéficiaires du régime devraient être informés de tout cyberincident ayant un impact sur leurs prestations, leurs intérêts financiers ou personnels,
- les administrateurs de régimes de retraite doivent s'assurer que les mesures prises pour atténuer l'impact de ces incidents sont communiquées aux bénéficiaires des régimes concernés

La caractère évolutif des cyberrisques

Les cyberrisques sont complexes, évoluent rapidement et nécessitent donc une réaction dynamique :

- les contrôles, les processus et les plans d'intervention doivent être régulièrement testés et révisés;
- les administrateurs de régimes de retraite doivent être régulièrement informés des cyberrisques, des incidents et des contrôles;
- les administrateurs de régimes de retraite et les autres parties concernées devraient chercher à obtenir des renseignements appropriés et une directive, sur les menaces de cybersécurité afin de rehausser la capacité du régime à répondre et se remettre des cyberincidents.

Annexe A

Pour s'assurer que les cyberrisques sont suffisamment intégrés dans le cadre de gouvernance du régime de retraite, les administrateurs de régime doivent se poser le type de questions suivantes :

- Les rôles et responsabilités concernant le plan d'action en matière de cyberrisque sont-ils clairement définis et documentés?
- Le plan inclut-il une formation, des compétences et une expertise suffisantes pour s'assurer que le cyberrisque est bien compris et géré?
- Le plan a-t-il identifié ses actifs technologiques critiques (p. ex., logiciels ou matériels), sa gestion des accès (c.-à-d. le cadre des politiques et des technologies utilisées pour authentifier l'accès des utilisateurs) et son cadre relatif à la protection des données?
- A-t-on une compréhension suffisante de l'impact potentiel d'un cyberincident ainsi que de la probabilité que différents types de violations se produisent?
- Comprend-on l'étendue de la cyberexposition du régime, y compris celle découlant des actions ou inactions de tiers?
- La gestion des cyberrisques liés aux tiers fait-elle l'objet d'une discussion avec les clients tiers (à la fois lors de la phase d'intégration et à intervalles réguliers)?

Pour s'assurer que les cyberrisques sont suffisamment intégrés dans le cadre de la gestion des risques du régime de retraite, les administrateurs de régime doivent se poser les types de questions suivantes :

- Les cyber-risques sont-ils identifiés de manière appropriée, font-ils l'objet d'un examen régulier, notamment lorsque des changements importants sont apportés dans les opérations? L'examen comprend-il des mesures permettant de suivre de manière efficace les réponses aux cyberincidents?
- Les contrôles existants sont-ils proportionnels et en nombre suffisants pour minimiser le risque d'un cyberincident ainsi que son impact potentiel?
- Le régime fait-il appel à un tiers pour évaluer régulièrement son programme de cyberrisque?
- Le régime détient-il une police de cyber-assurance appropriée et, si oui, qu'est-ce qui est couvert par l'assurance (p. ex., la réponse aux incidents)?
- Le régime a-t-il mis en place un programme officiel de sécurité de l'information pour aider à déterminer de façon appropriée les personnes, les initiatives, les politiques, etc. pour protéger les renseignements et les actifs?
- Le régime dispose-t-il d'un processus permettant de s'assurer que les tiers avec lesquels le régime détient des contrats disposent de contrôles suffisants pour faire face aux cyberrisques?

- Le plan dispose-t-il de plans d'intervention aux incidents afin de réagir rapidement et minimiser les dommages en cas de cyberincident?
- Le plan dispose-t-il d'une déclaration de tolérance au cyberrisque documentée et approuvée?

Annexe B

Voici des exemples de contrôles que les administrateurs de régimes de retraite peuvent trouver pertinents pour leurs activités de gestion des cyberrisques :

- Gérer l'accès physique, environnemental et virtuel aux systèmes et aux données.
- Augmenter la résilience et la récupération des systèmes en tirant parti de l'expertise des experts/départements des technologies de l'information.
- Établir des processus et politiques solides comme :
  - la gestion d'actifs matériels et logiciels;
  - des mises à jour régulières du matériel, des logiciels et des micrologiciels;
  - les pare-feu, les logiciels antivirus et autres outils de détection et de protection;
  - l'utilisation acceptable des appareils (y compris les appareils amovibles et personnels), du courrier électronique et de l'Internet (y compris les médias sociaux);
  - l'utilisation de mots de passe et d'autres moyens d'authentification;
  - des pratiques sécuritaires lors du travail à domicile et du travail à distance;
  - l'accès aux données, leur protection (y compris le cryptage), leur utilisation et leur transmission, ainsi que leur stockage, conformément à la législation et aux orientations en matière de protection des données;
- Développer et tester un protocole de communication qui serait activé en cas de cyberincident.
- Fournir une formation appropriée au personnel et aux administrateurs, le cas échéant. La formation doit comprendre une sensibilisation aux cyberrisques ainsi que la manière de signaler les incidents.
- Encourager les membres à adopter les meilleures pratiques en ce qui concerne les mots de passe (p. ex., les identifiants de connexion à un portail de retraite en ligne) et la sécurité de leurs données personnelles.
- Surveillance des systèmes et des réseaux pour détecter toute activité inhabituelle ou tout accès non autorisé.
- Examiner et tester régulièrement les contrôles, les processus et les plans d'intervention (par exemple, les plans de reprise après sinistre) pour s'assurer qu'ils demeurent adéquats.
- Effectuer des exercices de simulation pour tester les plans d'intervention en cas de crise et s'assurer que les personnes-ressources principales et remplaçantes comprennent leurs rôles.