Organismes canadiens de réglementation en assurance

Préparation à la cybersécurité

Préambule

Si les intermédiaires en assurance réglementés (les « intermédiaires ») peuvent avoir recours à la technologie pour recueillir, stocker et utiliser de l'information pour les besoins de la vente ou du service après vente de produits d'assurance, ils sont également responsables de la protéger contre tout accès non autorisé.

La présente publication fournit aux intermédiaires de l'information d'ordre général sur les pratiques de cybersécurité dans le but de protéger les renseignements confidentiels, d'accroître leur résilience aux incidents de cybersécurité et de répondre adéquatement à ceux-ci. Bien qu'il existe des pratiques de cybersécurité et des mécanismes de contrôle du risque pouvant s'appliquer à tous, certains d'entre eux doivent être mis en œuvre d'une façon qui convient à la taille et à la structure de l'organisation.

On entend par cybersécurité les pratiques visant à protéger la confidentialité, l'intégrité et l'accessibilité des données sur les activités, le personnel et la clientèle de l'organisation qui se trouvent dans ses systèmes informatiques. Toute défaillance dans ces protections constitue un « cyberincident ». Ce dernier peut être le fait d'une erreur humaine, du mauvais fonctionnement d'un système ou d'une intrusion délibérée, comme une cyberattaque. Pour prévenir les cyberincidents susceptibles de compromettre les renseignements sur les clients ou mener à leur vol ainsi qu'atténuer leurs conséquences sur les intermédiaires et leurs clients, il est primordial de mettre en place les mesures appropriées de façon proactive.

Étant donné l'accroissement des cyberincidents, et particulièrement des cyberattaques, il importe que tous les intermédiaires évaluent leurs données et systèmes technologiques afin de cerner les données pouvant intéresser les cybercriminels ainsi que les systèmes qui sont vulnérables à ces attaques. Ils devraient passer en revue leurs pratiques en matière de cybersécurité et prendre les mesures indiquées pour traiter ou atténuer les risques identifiés.

Les intermédiaires devraient envisager de faire appel à un professionnel en cybersécurité qui pourra leur venir en aide dans l'examen de leurs pratiques actuelles et leur prodiguer des conseils adaptés à leurs besoins. Ils devraient également faire en sorte que les mesures de cybersécurité en place soient conformes aux lois applicables en matière de protection des renseignements personnels.

Les intermédiaires devraient suivre l'évolution de l'environnement de la cybersécurité et songer à contracter une assurance responsabilité civile en matière de cyberrisque pour les aider dans leur préparation à la cybersécurité.

---

[1] **Définition d'intermédiaire en assurance réglementé :** Le terme « intermédiaire » reçoit un sens large qui peut varier selon les définitions applicables dans les différents territoires du Canada. Il englobe les experts en sinistre, les agents, les courtiers et les représentants, ainsi que les entités qui distribuent des produits et des services d'assurance, dont les agences générales et les tiers administrateurs. Il s'applique également à toutes les méthodes de distribution, y compris par Internet.

Préparation à la cybersécurité

La préparation à la cybersécurité requiert des intermédiaires qu'ils élaborent une stratégie adaptée à leur organisation et aux risques propres à leurs activités. Se trouvent ci dessous des suggestions pour les aider à y arriver.

1. Faire de la cybersécurité une priorité

La préparation à la cybersécurité implique d'établir au sein de l'organisation une culture de cybersécurité et de rendre disponibles l'expertise appropriée et les ressources nécessaires.

Organisation

- Confier à quelqu'un la responsabilité de surveiller les risques de cybersécurité de l'organisation et de faire rapport sur ceux-ci, et veiller à ce qu'il reçoive le soutien et les ressources nécessaires, y compris l'accès à un professionnel en cybersécurité pour obtenir de l'aide et des conseils, au besoin.
- Élaborer des politiques et des procédures relatives aux pratiques en matière de cybersécurité qui doivent être suivies par tous les membres de l'organisation.
- Veiller à ce que tous les membres de l'organisation soient informés de leurs rôles et responsabilités en regard des politiques et des procédures en matière de cybersécurité.
- Sensibiliser et former périodiquement tous les membres de l'organisation sur les bonnes pratiques en matière de cybersécurité, la prévention des cyberincidents et la réponse à ceux-ci.
- Instaurer une approche d'intervention en cas de cyberincident qui rend tous les membres de l'organisation à l'aise de faire un signalement. L'objectif devrait être axé sur la compréhension et la résolution du cyberincident aussi rapidement et efficacement que possible.
- Se renseigner sur la mesure dans laquelle l'assurance responsabilité civile en matière de cyberrisque peut aider dans la préparation à la cybersécurité. Une telle assurance, si elle est raisonnablement accessible, pourrait aider l'organisation à identifier les risques, à faciliter sa préparation, à lui donner accès à des ressources technologiques et à s'acquitter des coûts associés aux interventions en cas de cyberincident.

Individu

- Assister aux formations sur la cybersécurité, ainsi que comprendre les politiques et procédures de l'organisation en la matière, et y adhérer.
- Être à l'affût des cybermenaces, comme les courriels, textos ou appels téléphoniques douteux.

2. Savoir quels renseignements sur les clients et quelles technologies doivent être protégés

Pour déterminer les mesures de cybersécurité devant être prises pour mieux intervenir en cas de cyberincident, il est fondamental de savoir les renseignements sur les clients que détient l'organisation dans le cadre de ses activités, et la façon dont ils sont stockés.

Organisation

- Recenser tous les appareils informatiques utilisés dans le cadre des activités de l'organisation, en consignant ce qui suit :
    - le type d'appareil utilisé (par exemple, un ordinateur de bureau, un ordinateur portable, une tablette, un téléphone intelligent, une montre intelligente ou une clé USB) et des détails à son sujet (l'utilité, le modèle, le numéro de série, etc.);
    - les fonctions des utilisateurs (par exemple, administrateurs, membres du personnel des services informatiques, salariés, intermédiaires, etc.).
- Savoir les renseignements que détient l'organisation sur support électronique ainsi que l'endroit où ils sont stockés, et prendre en considération l'importance de disposer de copies de sauvegarde et de les stocker dans des centres de sauvegarde, y compris le stockage infonuagique.
- Établir le niveau de sensibilité des renseignements détenus par l'organisation et leur importance pour son fonctionnement.
- Comprendre les façons d'accéder aux dossiers électroniques et aux données par l'intermédiaire du réseau de l'organisation, notamment ce qui suit :
    - les appareils, logiciels ou applications qui sont branchés au réseau de l'organisation (par exemple, les appareils informatiques, les imprimantes, les routeurs et les serveurs), et la façon dont ils sont branchés;
    - la connexion du réseau de l'organisation à Internet;
    - les dossiers ou données électroniques accessibles au moyen du réseau de l'organisation, et l'identité des personnes y ayant accès.

Individu

- N'utiliser les appareils fournis par l'organisation qu'à des fins professionnelles autorisées et ne permettre à personne d'autre de les utiliser ou d'accéder au réseau, aux dossiers électroniques ou aux données de l'organisation.
- Éviter d'accéder au réseau de l'organisation au moyen d'appareils personnels ou, si une telle pratique est permise, le faire en observant rigoureusement les politiques et procédures établies.
- Se garder d'accéder à des renseignements sensibles au moyen d'un réseau Wi-Fi public ou non sécurisé. Le recours à un réseau privé virtuel (VPN) pourrait constituer une solution plus sûre.

3. Identifier les cyberrisques découlant des activités de l'organisation ou de leur impartition à des tiers fournisseurs de services

Afin de déterminer les mesures de cybersécurité devant être prises pour mieux intervenir en cas de cyberincident, il est crucial d'identifier les risques pertinents liés à la confidentialité, à l'intégrité et à l'accessibilité des renseignements sur les clients, les risques technologiques associés à l'accès accordé au personnel, à l'équipe de direction ou à des tiers fournisseurs de services, ou le risque d'une cyberattaque.

Organisation

Risque lié à l'organisation

- Analyser continuellement le risque de cyberincidents auquel sont exposés les appareils informatiques, les dossiers électroniques et les réseaux de l'organisation, estimer la probabilité de ces incidents et en comprendre l'incidence sur les activités.

- Passer en revue régulièrement l'identité des personnes ayant accès aux appareils informatiques, aux dossiers électroniques et aux données de l'organisation, puis déterminer les accès dont ils ont besoin dans le cadre des activités, tout en retirant ceux qui ne sont plus nécessaires.

Risque lié aux tiers fournisseurs de services

- Évaluer les pratiques en matière de cybersécurité des tiers fournisseurs de services, les intermédiaires étant responsables des services qu'ils leur impartissent.

- Vérifier les antécédents des tiers fournisseurs de services par un contrôle des références, des recherches sur le Web ou d'autres moyens, puis confirmer qu'ils ont mis en place des pratiques appropriées en matière de cybersécurité qui cadrent avec celles de l'intermédiaire avant de conclure tout accord avec eux.

    - S'assurer que l'accord conclu avec des tiers fournisseurs de services tient compte du caractère confidentiel des renseignements sur les clients ainsi que de la sécurité des systèmes informatiques et des réseaux de l'organisation.
    - Les contrats devraient traiter du partage des responsabilités en matière de cybersécurité entre le tier fournisseurs et l'organisation dans la prestation des services.
    - Intégrer un plan d'intervention en cas de cyberintrusion avec le tiers dans le contrat pour contrer les cyberattaques, y inclure des points de contact chez le tiers et élaborer un plan coordonné avec lui.
    - Exiger des tiers qu'ils informent immédiatement l'organisation de tout cyberincident impliquant un accès non autorisé aux renseignements sur les clients ou aux systèmes de l'organisation.

- Dans le cadre de la stratégie d'atténuation des risques, surveiller périodiquement l'état de préparation des tiers à la cybersécurité.

Individu

- Informer le responsable de la surveillance de la cybersécurité au sein de l'organisation de tout accès dont vous n'avez pas besoin.

- Adhérer aux politiques et aux procédures de l'organisation relativement aux interactions avec le personnel du tiers fournisseur de services qui encadre l'accès accordé aux systèmes informatiques de l'organisation ou aux renseignements qu'elle détient sur les clients.

4. Mettre en place des mesures de cybersécurité adéquates

Il est indispensable de prendre des mesures appropriées pour prévenir ou atténuer adéquatement les cyberrisques identifiés, comme la surveillance des menaces ou des accès non autorisés aux renseignements sur les clients et l'ajustement de la stratégie de cybersécurité en conséquence.

Organisation

- Exercer un contrôle sur l'accès aux dossiers électroniques, aux données et au réseau de l'organisation :
  - Resserrer ou surveiller la collecte, le stockage, le transfert et l'utilisation de données sensibles des clients, y compris restreindre ou interdire l'utilisation d'appareils externes, comme les clés USB.
  - Limiter et surveiller le nombre de salariés ayant un accès privilégié aux réseaux et aux renseignements de l'organisation, tout en veillant à circonscrire cet accès au strict nécessaire pour que le personnel puisse faire son travail.
  - Ne fournir qu'au personnel autorisé les moyens d'accéder aux locaux de l'organisation, y compris cartes d'accès, cartes d'identité et cartes d'accès pour les visiteurs.
  - Surveiller le réseau pour y détecter tout trafic inhabituel ou accès non autorisé.
  - Mettre en œuvre l'authentification multifactorielle pour plus de sûreté.
- Assurer la destruction ou le recyclage sécuritaire des appareils informatiques, des dossiers électroniques et des données.
- Cataloguer les renseignements sur les clients et en créer une copie de sauvegarde pour en faciliter la récupération au cas où ils seraient perdus ou grandement endommagés.
- Veiller à ce que les systèmes d'exploitation et les réseaux de l'organisation soient à jour et aient reçu les correctifs appropriés, et qu'un calendrier de mise à jour soit en place et respecté.
- Tester les systèmes informatiques et les réseaux de l'organisation pour détecter les vulnérabilités.
- Étudier la possibilité de contracter une assurance responsabilité civile en matière de cyberrisque pour accroître la résilience de l'organisation en cas de cyberattaque et lui donner accès à des ressources techniques.

Individu

- Comprendre que l'individu est la première ligne de défense contre les cyberincidents et, par conséquent, toujours être attentif aux actions posées et des causes potentielles de cyberincidents.
- Adhérer aux politiques et aux procédures de l'organisation ainsi qu'aux pratiques de cybersécurité dans le cadre des activités quotidiennes, notamment les suivantes :
  - veiller à ce que les appareils et applications soient toujours à jour;
  - créer un mot de passe complexe et unique pour chaque appareil ou application, et le garder secret;
  - verrouiller les appareils quand ils ne sont pas utilisés;

- ne pas utiliser les appareils professionnels à des fins personnelles;
- se garder d'envoyer des renseignements personnels ou sensibles par texto ou par courriel;
- ne pas télécharger d'applications sur les appareils professionnels sans l'autorisation de l'organisation;
- s'abstenir d'utiliser les appareils professionnels pour consulter des sites Web peu sûrs ou n'ayant pas trait au travail;
- éviter de cliquer sur des liens ou des pièces jointes d'origine inconnue ou douteuse.

5. Détecter les cyberincidents et intervenir

Il est essentiel d'avoir un plan de détection, d'évaluation et d'intervention en cas de cyberincident afin de veiller à ce que le personnel, l'équipe de direction et les fournisseurs de services soient informés des mesures à prendre pour détecter les cyberincidents ou intervenir lorsqu'ils surviennent.

Organisation

- Investir dans des systèmes de détection d'intrusion et mettre en place une surveillance périodique, comme des systèmes antivirus et la journalisation des actions.

- Rédiger un plan d'intervention en cas de cyberincident afin de protéger les renseignements sur les clients, de réduire au minimum les interruptions de service, de faciliter l'atténuation des cyberincidents et de documenter ces derniers (voir l'exemple de plan ci-après).

- Constituer une équipe d'intervention formée de membres du personnel et membres de la direction afin de traiter les cyberincidents et de demander une expertise externe, au besoin. Son objectif est de réduire au minimum l'incidence d'un cyberincident et le temps d'intervention nécessaire.

- Élaborer un protocole de communication pour guider l'équipe d'intervention dans son évaluation de l'information qu'elle pourrait devoir communiquer aux intervenants, aux tiers, aux autorités de réglementation ou aux organismes d'application de la loi, et faire qu'elle soit transmise efficacement et en temps opportun. Les intermédiaires devraient connaître leur obligation de déclarer les cyberincidents ou de prendre toute autre mesure conformément aux lois applicables en matière de protection des renseignements personnels.

- Mettre à l'essai le plan d'intervention en cas de cyberincident pour tester son l'efficacité et y apporter les ajustements nécessaires.

- Chercher la cause profonde du cyberincident, évaluer le risque que celui-ci se reproduise et mettre en œuvre des mesures pour éviter ou empêcher que la situation se répète.

Individu

- Comme la cybersécurité est l’affaire de tous, il importe d’être au fait de tout acte pouvant entraîner un cyberincident et d’en faire le signalement sans tarder.

- Détecter de façon proactive les cybermenaces et cyberincidents potentiels, signaler toute activité douteuse et suivre les procédures de l’organisation. Par exemple :

    - informer le personnel responsable de la cybersécurité de l’organisation;
    - mettre l’appareil hors tension;
    - noter la date et l’heure du cyberincident, les programmes qui étaient utilisés et la description de l’incident.

Éléments à inclure dans un plan d'intervention en cas de cyberincident

Investigation	Mener une enquête sur la nature et l'ampleur du cyberincident, et ses répercussions sur l'organisation et les clients.
Atténuation	Prendre des mesures d'atténuation, comme la suspension de l'accès aux renseignements sur les clients ou à la technologie touchés. Il faut notamment relever les vulnérabilités, les corriger, restaurer les systèmes concernés ou les renseignements perdus, puis mettre en place des mesures de protection.
Évaluation	Évaluer si le cyberincident rend inaccessibles les renseignements sur les clients ou la technologie pendant une longue période, et si elle déclenche le plan de continuité des activités.
Communication	Prendre contact avec les personnes touchées par le cyberincident ainsi que les autorités de réglementation ou les organismes d'application de la loi compétents, et déterminer les étapes à suivre pour réduire les torts causés à ces intervenants.
Documentation	Consigner les étapes nécessaires à la détection du cyberincident et à l'intervention, tout en veillant à préserver les preuves et la documentation traitant de l'analyse de l'incident. Indiquer le moment auquel les systèmes ont été entièrement remis en service et la cybermenace n'était plus présente.