MBRCC Mortgage Broker Regulators' Council of Canada

CCARCH Conseil canadien des autorités de réglementation des courtiers hypothécaires

Conseil canadien des autorités de réglementation des courtiers hypothécaires (CCARCH)

Principes pour la préparation à la cybersécurité

Objectif

Le CCARCH est un forum où les autorités de réglementation des courtiers hypothécaires collaborent et promeuvent une plus grande cohérence réglementaire dans l'intérêt du public.

L'objectif du présent guide est de soutenir la préparation à la cybersécurité dans le secteur du courtage hypothécaire en proposant des pratiques qui permettent d'éviter les incidents de cybersécurité et d'y réagir correctement lorsqu'ils se produisent.

Les cybermenaces augmentent pour tout le monde, y compris pour le secteur du courtage hypothécaire, qui traite beaucoup de données sur ses clients. Les clients font confiance au secteur pour protéger ces données. Une gestion proactive des cybermenaces permet de se protéger contre les attaques visant à compromettre ou à voler des données électroniques.

La cybersécurité est l'application de technologies, de procédures et de mesures de contrôle pour défendre les infrastructures (systèmes, réseaux, programmes, dispositifs) et les données. Elle vise à réduire la probabilité et l'incidence des cyberattaques qui visent l'accès aux données délicates des clients et l'interruption des activités commerciales en perturbant les infrastructures essentielles et les réseaux d'entreprise.

Le présent guide respecte le principe de sécurité et de confidentialité (principe 8) du code de conduite du CCARCH. Selon ce principe : « Les personnes et les entités réglementées doivent protéger les renseignements relatifs à leurs clients et doivent utiliser et divulguer ces renseignements uniquement aux fins pour lesquelles les clients ont donné leur consentement ou si la loi l'exige. »

Les cadres législatifs fédéral et provinciaux exigent la protection des renseignements personnels. À l'échelon fédéral, la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) exige de toutes les entreprises, y compris les courtiers et les administrateurs d'hypothèques, de protéger les renseignements personnels de leurs clients. À titre d'exemple, les données personnelles recueillies doivent être protégées contre la perte, l'accès non autorisé et le vol.

Le présent guide ne crée pas de nouvelles obligations. Le CCARCH considère que le présent guide est conforme à l'ensemble des exigences, règles et normes de conduite existantes, et qu'il peut donc être interprété de manière cohérente avec celles-ci.

Approche

Le présent guide contient quatre principes qui décrivent les résultats que les entités réglementées doivent atteindre pour assurer leur cybersécurité. Il ne prescrit pas la manière dont ces principes doivent être appliqués. Cette approche fondée sur des principes offre aux entités réglementées la souplesse nécessaire pour atteindre ces résultats d'une manière adaptée à la taille et à la structure de leurs activités, et d'une manière conforme à leurs politiques et procédures de gestion des risques liés aux technologies de l'information (TI), le cas échéant.

Le guide contient à l'annexe A une liste de contrôle qui aide les entités à auto évaluer leur degré de préparation en matière de cybersécurité. L'annexe B énumère les principales normes de cybersécurité et de gestion des risques informatiques sur lesquelles s'est appuyé le CCARCH dans l'élaboration de ces principes.

Principes de préparation à la cybersécurité

Les principes qui régulent généralement la préparation des courtiers hypothécaires à la cybersécurité sont les suivants :

1. Responsabilité et ressourcement

Pour assurer la reddition des comptes, les entités réglementées doivent charger une personne de superviser le risque de cybersécurité.

La responsabilité de respecter les pratiques sécuritaires en matière de cybersécurité incombe à tous les membres de l'organisation, même ceux qui n'ont aucun rôle de supervision.

Les entités doivent disposer de suffisamment de ressources pour créer et maintenir les mesures de cybersécurité nécessaires à la protection des renseignements de leurs clients, en particulier les renseignements personnels.

Les entités réglementées sont tenues :

- D'élaborer des politiques et des procédures qui les préparent à assurer la cybersécurité.
- D'exiger des personnes chargées de superviser la cybersécurité qu'elles maintiennent leurs compétences et leur connaissance des risques de cybersécurité, notamment des moyens d'atténuer ces risques par une formation continue.
- De sensibiliser aux risques en matière de cybersécurité en conseillant le personnel et la direction (le cas échéant) sur la préparation à la cybersécurité. Il peut notamment s'agir de formations et de rappels sur les risques de cybersécurité.
- D'envisager de souscrire une assurance de responsabilité civile en matière de cybersécurité adaptée à leurs besoins.

2. Détermination et prévention des risques

Les entités réglementées sont tenues :

- De déterminer les principaux risques en matière de cybersécurité, comme la perte de renseignements sur les clients ou les problèmes d'accès aux systèmes :
  - accès accordé au personnel;
  - recours à des prestataires de services tiers;
  - sauvegarde des processus, du matériel technologique ou des installations.
- De disposer de protections appropriées pour la détection des risques « en bout de chaine », p. ex. des logiciels antivirus et des outils qui détectent les logiciels malveillants, régulièrement mis à jour.
- D'évaluer l'incidence des cyberincidents sur l'activité et veiller à ce que les risques liés à la cybersécurité fassent partie du plan de continuité des activités.
- De prendre des mesures adéquates pour minimiser la probabilité et l'incidence du risque une fois qu'il est connu, p. ex. en mettant en place dans la gestion des données des processus et des mesures de contrôle robustes qui garantissent une gestion responsable des données des clients.
- De déterminer la tolérance de l'entité aux risques relevés.

Les entités réglementées qui fournissent des services, p. ex. à des institutions financières, doivent prendre des mesures raisonnables pour comprendre et respecter leurs obligations en tant que prestataires de services tiers en matière de cybersécurité et de gestion des risques informatiques, selon le cas.

3. Surveillance, détection des incidents et intervention

Les entités réglementées doivent disposer d'un protocole de surveillance, de détection des incidents de cybersécurité et d'intervention dans le cadre de leurs politiques et procédures de préparation à la cybersécurité. L'entité doit disposer, en cas d'incident, d'un plan d'intervention qui protège les renseignements des clients et qui minimise les interruptions de service. Ce plan peut comprendre les aspects suivants :

- Suspendre certains processus opérationnels pour limiter la vulnérabilité des renseignements.
- Informer de l'incident les clients, les tiers (y compris les prêteurs hypothécaires) et les organismes de réglementation (selon la demande ou, dans certaines administrations, selon l'exigence).
- Déterminer si les critères de retour à la normale sont remplis.
- Restaurer les données, les processus et les systèmes perdus ou corrompus afin de permettre un retour à la normale.

4. Gestion par des tiers

Les entités réglementées doivent protéger les renseignements de leurs clients tout au long du processus de demande et de clôture en prenant des mesures raisonnables qui vérifient que leurs prestataires externes ont également en place des pratiques de préparation à la cybersécurité. Le secteur du courtage hypothécaire fonctionne au sein d'un écosystème de fournisseurs; la complexification et l'élargissement des réseaux augmentent le risque en matière de cybersécurité. Une gestion attentive des relations est importante pour minimiser les vulnérabilités et contribuer à la protection des renseignements des clients. La gestion des relations peut comprendre l'établissement formel par les parties de processus et de procédures qui gèrent les risques en matière de cybersécurité.

Annexe A – Liste de contrôle de la préparation à la cybersécurité

Vous trouverez ci dessous une liste de contrôle de base[1] pour la préparation à la cybersécurité. Elle ne crée pas d'exigences de conformité; cependant, les organismes de réglementation peuvent s'en servir pour évaluer le degré de préparation à la cybersécurité dans le cadre des programmes de surveillance régulière des courtiers.Elle vous aidera à relever et traiter un grand nombre des risques fondamentaux liés aux activités de courtage en prêts hypothécaires.

Non exhaustive, cette liste de contrôle ne couvre pas tous les risques potentiels en matière de cybersécurité, mais elle est utile aux entités qui n'ont pas de pratiques établies dans la préparation à la cybersécurité.

Les lacunes relevées par la liste de contrôle doivent être classées par ordre de priorité en fonction de leur incidence, de la probabilité de survenue d'un incident et des ressources disponibles.

- ☐ Avez-vous une ou plusieurs personnes qui sont chargées de gérer les risques en matière de cybersécurité?
- ☐ Avez-vous la liste de tous les appareils informatiques dont se sert votre organisme? Pour chaque appareil, notez :
  - Le type d'appareil (téléphone intelligent, tablette, ordinateur de bureau, ordinateur portatif, serveur, etc.).
  - Le numéro de modèle.
  - Le numéro de série.
  - L'utilisateur responsable de l'appareil.
  - Le système d'exploitation et les applications pertinentes installées sur l'appareil.
  - Si l'appareil est chiffré.
- ☐ Avez-vous la liste de tous les types d'enregistrements et de données électroniques conservés sur les systèmes informatiques de votre organisme (« biens électroniques ») et des endroits où ils sont stockés?
- ☐ Les biens électroniques sont-ils classés selon qu'ils contiennent l'un des éléments suivants :
  - Des renseignements d'identification?
  - Des renseignements exclusifs?
  - Des données financières délicates (p. ex., des données sur les cartes de crédit)?
  - Des données sur des opérations?
- ☐ A-t-on trouvé sur la liste des enregistrements et des données électroniques qui sont importants pour la capacité de l'organisme à fonctionner?
- ☐ Le processus de sauvegarde et de récupération des enregistrements et des données électroniques a-t-il été revu, mis à jour et mis à l'essai?
- ☐ Avez-vous des politiques et des procédures pour restreindre ou surveiller la collecte, le stockage et l'usage de données clients de nature délicate?
- ☐ Le réseau d'information de l'organisme a-t-il été cartographié (p. ex., la manière dont les ordinateurs et autres dispositifs informatiques sont connectés, les serveurs et dispositifs de stockage présents sur le réseau, la manière dont le réseau est connecté à l'internet, etc.)?
- ☐ A-t-on évalué les risques liés aux dispositifs informatiques, aux biens électroniques et à la topologie du réseau, en déterminant :
  - Les dispositifs et les biens susceptibles d'être attaqués?
  - Les voies permettant d'attaquer ces dispositifs et ces biens?
  - Les acteurs susceptibles d'attaquer l'organisme?
  - La probabilité qu'une attaque s'effectue par telle ou telle voie?
  - L'incidence qu'aurait une telle attaque?
  - La manière de réduire, voire d'éliminer, le risque de violation?

[1] Cette liste de contrôle est fondée sur les directives publiées par la Commission des services financiers et des services aux consommateurs du Nouveau-Brunswick.

- ☐ A-t-on adopté un outil de gestion à distance pour gérer les appareils informatiques de l'organisme en dehors de ses bureaux?
- ☐ A-t-on procédé à un examen des personnes qui ont accès aux biens électroniques de l'organisme de manière à leur accorder un « droit d'accès minimal[2] »?
- ☐ Offre-t-on une formation de sensibilisation à la cybersécurité aux employés, de préférence de manière continue?
- ☐ Avez-vous créé des politiques de cybersécurité pour l'organisme, ou revu de telles politiques, notamment :
    - Les pratiques exemplaires en matière de cybersécurité :
        - L'authentification multifacteur?
        - Les mots de passe?
        - Le principe du bureau dégagé?
        - L'usage d'appareils informatiques en dehors du bureau?
    - L'usage acceptable des ressources informatiques?
    - L'arrivée et le départ des employés?
    - L'usage acceptable des appareils personnels à des fins professionnelles?
    - Les tiers et fournisseurs informatiques?
    - A-t-on examiné la sécurité physique de l'organisme? Les mesures de contrôle suivantes sont elles en place pour limiter l'accès aux bureaux et aux bâtiments de l'organisme aux employés autorisés seulement, y compris l'accès par carte, les badges d'identification et les règles d'accès des visiteurs?
- ☐ L'organisme a-t-il des exigences envers les entrepreneurs indépendants ou des accords avec eux qui traitent des pratiques exemplaires en matière de cybersécurité?
- ☐ L'organisme vérifie t-il que le processus d'élimination des biens physiques (vieux matériel, documents papier, etc.) fait que tous les documents importants sont correctement détruits ou déchiquetés en fin de vie?
- ☐ A-t-on examiné l'architecture du réseau de l'organisme?
- ☐ Y a-t-il des pare feu, des détecteurs d'intrusion, des configurations de serveurs et des mécanismes de cryptage adéquats?
- ☐ A-t-on vérifié que les systèmes d'exploitation et les applications permettant le fonctionnement du réseau sont à jour, bien corrigés, et qu'un calendrier de mise à jour adéquat est en place et respecté?
- ☐ A-t-on installé un logiciel contre les virus et les programmes malveillants sur tous les appareils qui accèdent aux biens électroniques?
- ☐ Votre organisme dispose-t-il d'une bonne assurance responsabilité en matière de cybersécurité?
- ☐ A-t-on établi et mis à l'essai un plan d'intervention en cas de violation de la cybersécurité?
- ☐ A-t-on établi et mis à l'essai un plan de continuité des activités et un plan de reprise après sinistre?

[2] L'employé n'a accès qu'aux données dont il a besoin pour faire son travail, rien de plus.

MBRCC Mortgage Broker Regulators' Council of Canada

CCARCH Conseil canadien des autorités de réglementation des courtiers hypothécaires

Annexe B – Normes de cybersécurité – Autres exemples

Les principes du CCARCH dans la préparation à la cybersécurité sont élaborés par les autorités de réglementation en suivant les pratiques de pointe. Vous trouverez ci dessous quelques ressources sur lesquelles nous nous sommes appuyés pour élaborer le présent guide.

- Organisation internationale de normalisation (ISO) – ISO/IEC 27001 – Management de la sécurité de l'information
- Cadre de cybersécurité | National Institute of Standards and Technology
- Gestion du risque lié aux technologies et du cyberrisque (osfi-bsif.gc.ca) – Bureau du surintendant des institutions financières