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 permettant aux organismes canadiens de réglementation du courtage hypothécaire de collaborer et de promouvoir une plus grande cohérence réglementaire afin de servir l'intérêt public.

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

Les cybermenaces constituent un risque croissant pour tout le monde, y compris pour le secteur du courtage hypothécaire. La gestion proactive de ce risque permet de se protéger contre les attaques visant à compromettre ou à voler des renseignements électroniques.

La cybersécurité est l'utilisation de technologies, de processus et de contrôles pour défendre les infrastructures telles que les systèmes, les réseaux, les programmes, les dispositifs et les données. La cybersécurité vise à réduire la probabilité et l'impact des cyberattaques qui pourraient conduire à un accès non autorisé aux renseignements sensibles des clients et à l'interruption des activités commerciales en raison de l'interférence dans les infrastructures critiques et les réseaux d'entreprise.

Ce guide soutient le principe de sécurité et de confidentialité (principe 8) du code de conduite du CCARCH. Ce principe stipule que « les personnes et 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 fédéraux et provinciaux exigent la protection des renseignements personnels. Au niveau fédéral, la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) exige que toutes les entreprises, y compris les courtiers et les administrateurs d'hypothèques, protègent les renseignements personnels des clients. Par exemple, les données personnelles collectées doivent être protégées contre la perte, l'accès non autorisé et le vol de données.

Cette directive ne crée pas de nouvelles obligations. Le CCARCH considère que ces directives correspondent à toutes les exigences, règles et normes de conduite existantes et qu'elles peuvent donc être interprétées de manière cohérente avec celles-ci.

Approche

Ce guide contient quatre principes décrivant les résultats que les entités réglementées devraient atteindre pour assurer la préparation à la cybersécurité. Il ne prescrit pas la manière dont les principes doivent être établis. Cette approche fondée sur des principes offre aux entités réglementées la souplesse nécessaire pour atteindre les résultats d'une manière adaptée à la taille et à la structure de leur entreprise.

Le guide comprend une liste de vérification à l'annexe A pour aider les entités à évaluer leur préparation à la cybersécurité. L'annexe B énumère les principales normes de cybersécurité auxquelles le CCARCH a fait référence lors de l'élaboration de ces principes.

Principes de préparation à la cybersécurité

Les principes communs de préparation à la cybersécurité des courtiers hypothécaires sont les suivants :

1. Responsabilité et ressources

Les entités réglementées doivent nommer une personne chargée de superviser le risque de cybersécurité afin de garantir la responsabilité. La responsabilité du respect des pratiques sûres en matière de cybersécurité s'applique à toutes les personnes d'une organisation, même si elles n'ont pas de rôle de supervision.

Les entités doivent investir et affecter toutes les ressources nécessaires pour développer et maintenir des mesures de cybersécurité efficaces afin de protéger les renseignements des clients, en particulier les renseignements personnels.

Les entités réglementées doivent :

- Élaborer des politiques et des procédures de préparation à la cybersécurité.
- Exiger que les personnes chargées de superviser la cybersécurité maintiennent leurs compétences et leur compréhension des risques de cybersécurité, y compris les moyens d'atténuer ces risques par une formation continue.
- Informer sur les risques de cybersécurité en fournissant des conseils au personnel et à la direction (le cas échéant) pour assurer la préparation à la cybersécurité. Cela peut inclure des formations et des rappels sur les risques de cybersécurité.
- Envisager de souscrire une assurance responsabilité civile en matière de cybersécurité adaptée à leurs besoins.

2. Détermination et prévention des risques

Les entités réglementées doivent :

- Déterminer les principaux risques liés à la cybersécurité, comme la perte de renseignements sur les clients ou les problèmes d'accès aux systèmes :
  - L'accès accordé au personnel;
  - Le recours à des prestataires de services tiers; et
  - La sauvegarde des processus, du matériel technologique ou des installations.
- Disposer de protections appropriées pour la détection des risques de « points terminaux », telles que des logiciels antivirus et de détection des logiciels malveillants régulièrement mis à jour.
- Réaliser une évaluation de l'impact des cyberincidents sur les entreprises et veiller à ce que les risques liés à la cybersécurité fassent partie du plan de continuité des activités.
- Prendre des mesures adéquates pour minimiser la probabilité et l'impact d'un risque, une fois celui-ci établi.
- Déterminer si l'entité est à l'aise avec les risques établis (« tolérance au risque »).

Les entités réglementées sont des fournisseurs de services tiers aux institutions financières. Les entités réglementées doivent s'assurer qu'elles comprennent et respectent les attentes d'une institution financière par rapport aux prestataires de services tiers en matière de cybersécurité et, de manière générale, de sécurité des renseignements.

3. Surveillance, détection et réponse aux incidents

Les entités réglementées doivent disposer d'un protocole de surveillance, de détection et de réponse aux incidents de cybersécurité dans le cadre de leurs politiques et procédures de préparation à la cybersécurité. Les entités doivent disposer d'un plan de réponse aux incidents afin de protéger les renseignements des clients et de minimiser les interruptions de service si un incident est détecté. Les aspects de ce plan peuvent inclure ce qui suit :

- Suspendre certains processus opérationnels pour limiter la vulnérabilité des renseignements.
- Partager les renseignements pertinents sur les incidents avec les clients, les tiers (y compris les prêteurs hypothécaires) et les organismes de réglementation (qui sont demandés ou, dans certains territoires, exigés).
- Déterminer si les critères de retour à la normale ont été remplis.
- Restaurer les données, les processus et/ou les systèmes perdus ou corrompus afin de permettre un retour à la normale.

4. Gestion par des tiers

Les entités réglementées sont chargées de protéger les renseignements de leurs clients contre les cyberincidents en s'assurant que leurs prestataires de services tiers ont mis en place des pratiques de préparation à la cybersécurité. Le secteur du courtage hypothécaire fonctionne au sein d'un réseau de fournisseurs; des réseaux plus complexes et plus étendus augmentent les risques liés à la 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 inclure l'établissement formel par les parties de processus et de procédures de gestion des risques de cybersécurité.

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

Vous trouverez ci-dessous une liste de vérification de base pour la [1] préparation à la cybersécurité. Elle peut être utile pour une entité qui n'a pas de pratiques établies de préparation à la cybersécurité.

Cette liste de vérification n'est pas exhaustive et ne couvre pas tous les risques potentiels en matière de cybersécurité. Toutefois, elle devrait permettre de cibler et de traiter bon nombre des risques de base liés aux activités de courtage hypothécaire.

Toute lacune ou tout problème établi lors de l'examen de la liste de vérification doit être classé par ordre de priorité en fonction de l'impact potentiel, de la probabilité d'un incident et des ressources disponibles. Les lacunes/problèmes doivent être traités par un employé désigné dans un délai précis.

- ☐ Avez-vous une ou plusieurs personnes responsables de la gestion des risques de cybersécurité de l'organisation?
- ☐ Disposez-vous d'un inventaire de tous les appareils informatiques utilisés au sein de l'organisation? Pour chaque appareil, établissez les renseignements suivants :
  - Type d'appareil (téléphone intelligent, tablette, ordinateur de bureau, ordinateur portable, serveur, etc.)
  - Numéro de modèle
  - Numéro de série
  - Utilisateur responsable de l'appareil
  - Système d'exploitation et applications pertinentes installées sur l'appareil
  - Cryptage de l'appareil
- ☐ Disposez-vous d'une liste de tous les types d'enregistrements et de données électroniques conservés sur les systèmes informatiques de l'organisation (« actifs électroniques ») et de l'endroit où ils sont stockés?
- ☐ Les biens électroniques sont-ils classés selon qu'ils contiennent l'un des éléments suivants :
  - Des renseignements permettant d'identifier une personne?
  - Des renseignements exclusifs?
  - Des renseignements financiers sensibles (par exemple, des renseignements sur les cartes de crédit)?
  - Des données de transaction?
- ☐ A-t-on établi sur la liste les enregistrements et les données électroniques qui sont importants pour la capacité de l'organisation à fonctionner?
- ☐ Le processus de sauvegarde et de récupération des enregistrements et des données électroniques a-t-il été revu, mis à jour et testé?
- ☐ Avez-vous des politiques et des procédures pour restreindre et/ou surveiller la collecte, le stockage et l'utilisation des données sensibles des clients?
- ☐ Le réseau de renseignements a-t-il été cartographié pour l'organisation (par exemple, comment les ordinateurs et autres dispositifs informatiques sont-ils connectés? Quels sont les serveurs et les dispositifs de stockage présents sur le réseau? Comment le réseau est-il connecté à l'Internet, etc.?
- ☐ Une évaluation des risques des dispositifs informatiques, des actifs électroniques et de la topologie du réseau a-t-elle été réalisée en identifiant :
  - Les dispositifs et les actifs qui constituent des cibles d'attaque intéressantes?
  - Les vecteurs d'attaque permettant d'accéder à ces dispositifs et/ou actifs?
  - Les acteurs qui peuvent chercher à attaquer l'organisation?
  - La probabilité d'une violation par un vecteur d'attaque particulier?
  - L'impact d'une telle atteinte à la sécurité?
  - Comment atténuer, voire éliminer, les risques d'atteinte à la sécurité?

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

- ☐ Un outil de gestion à distance a-t-il été adopté pour gérer les appareils informatiques de l'organisation en dehors des bureaux de l'organisation?
- ☐ A-t-on procédé à un examen de la liste des personnes ayant accès aux actifs électroniques de l'organisation afin de garantir un droit d'accès minimal[2]?
- ☐ Une formation sur la sensibilisation à la cybersécurité a-t-elle été proposée aux employés, de préférence de manière continue?
- ☐ Avez-vous revu ou créé les principales politiques de cybersécurité de l'organisation, notamment :
  - Pratiques exemplaires en matière de cybersécurité
    - Authentification multi-facteurs
    - Mots de passe
    - Bureau bien rangé
    - Utilisation d'appareils informatiques à l'extérieur du bureau
  - Utilisation appropriée des ressources informatiques
  - Accueil et sortie des nouveaux employés
  - Utilisation acceptable des appareils personnels à des fins professionnelles
  - Tiers et fournisseurs de TI
  - La sécurité physique de l'organisation a-t-elle été revue? Les contrôles suivants sont-ils en place pour limiter l'accès physique au (x) bureau(x) / bâtiment(s) de l'organisation aux seuls employés appropriés, y compris l'accès par carte clé, les cartes d'identité et les règles d'accès des visiteurs?
- ☐ L'organisation a-t-elle des exigences pour les entrepreneurs indépendants ou des accords avec eux qui traitent des pratiques exemplaires en matière de cybersécurité?
- ☐ L'organisation vérifie-t-elle que le processus d'élimination des actifs physiques (vieux matériel, documents papier, etc.) garantit que tous les documents importants sont correctement détruits ou déchiquetés en fin de vie?
- ☐ L'architecture réseau de l'organisation a-t-elle été revue?
- ☐ Des solutions de pare-feu, des systèmes de détection d'intrusion, des configurations de serveur et des mécanismes de cryptage appropriés sont-ils en place?
- ☐ Les systèmes d'exploitation et les applications permettant le fonctionnement du réseau ont-ils été examinés pour s'assurer qu'ils sont à jour et que les corrections appropriées ont été apportées, et qu'un calendrier de mise à jour approprié est en place et suivi?
- ☐ Un logiciel anti-virus/antimaliciels à jour a-t-il été installé sur tous les appareils ayant accès aux actifs électroniques?
- ☐ Votre organisation dispose-t-elle d'une assurance adéquate pour la responsabilité en matière de cybersécurité?
- ☐ Un plan d'intervention en cas de violation de la cybersécurité a-t-il été établi et testé?
- ☐ Un plan de continuité des activités et un plan de reprise après sinistre ont-ils été établis et testés?

[2] Les employés ont uniquement accès à l'information dont ils ont besoin pour accomplir leur travail et à rien de plus.

Annexe B – Autres exemples de normes de cybersécurité

Les principes de préparation à la cybersécurité du CCARCH ont été élaborés par les régulateurs du CCARCH sur la base de pratiques de pointe. Vous trouverez ci-dessous quelques-unes des ressources que nous avons consultées pour élaborer ces orientations.

- Organisation internationale de normalisation (ISO) – ISO/IEC 27001 – Gestions de la sécurité des renseignements
- 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