INSURANCE BROKERS ASSOCIATION OF CANADA
ASSOCIATION DES COURTIERS D'ASSURANCES DU CANADA

PRISE DE POSITION NATIONALE SUR L'AUTHENTIFICATION DES DONNÉES ÉCHANGÉES ENTRE COURTIERS ET ASSUREURS

Il est beaucoup plus efficient pour les courtiers et les assureurs d'échanger des informations par voie électronique qu'en ayant recours aux méthodes traditionnelles. L'objet commercial de ces échanges et les rôles des parties à la correspondance n'ont toutefois jamais changé; les rôles distincts et les responsabilités respectives du courtier et de l'assureur demeurent les mêmes. Il est donc essentiel que les règles et les protocoles de sécurité visant les échanges de données par voie électronique reflètent le modèle économique sous-jacent.

Les dirigeants de cabinets de courtage gèrent leurs propres activités et sont responsables en dernier ressort des actions de leurs employés. Un assureur confère à chaque cabinet de courtage le pouvoir d'engager sa responsabilité, et les contrats entre courtiers et assureurs précisent clairement que les cabinets de courtage sont responsables des erreurs ou des omissions de leurs employés, ou de leurs manquements en ce qui concerne les obligations relatives au pouvoir d'engager la responsabilité de l'assureur.

Les courtiers communiquent avec les assureurs par divers moyens, par exemple les notes écrites et le téléphone ou, plus récemment, les courriels et les échanges de données par voie électronique. Les assureurs n'attribuent pas à un employé particulier le pouvoir de correspondre avec les souscripteurs ou de transmettre les instructions du client; depuis toujours, c'est aux dirigeants du cabinet de courtage qu'incombe la responsabilité de désigner cet employé.

Le fait que les données soient transmises aux assureurs par voie électronique par l'intermédiaire d'un site Web ne modifie en rien cette responsabilité. Un cabinet de courtage continue de superviser la formation et les actions de ses employés et est responsable des décisions qui sont prises en son nom. Cette supervision s'étend à la sécurité des réseaux internes et des systèmes de gestion du cabinet de courtage qui repose sur des identifiants utilisateurs et des mots de passe individuels contrôlés de façon centralisée. Lorsque l'identifiant d'un utilisateur est supprimé ou désactivé, cet utilisateur perd tous ses accès, y compris aux applications liées auxquelles le système central de la société de courtage donne accès.

Il existe toutefois des risques importants lorsqu'une personne peut accéder directement aux systèmes d'un assureur sans passer par le système de gestion du cabinet de courtage dûment identifié. S'il suffit d'avoir une connexion Internet pour accéder au système d'un assureur, quiconque disposant d'un identifiant et d'un mot de passe peut donc ouvrir une session sans peine dans ce système, peu importe où il se trouve. Lorsqu'un employé quitte ses fonctions, les dirigeants du cabinet de courtage doivent s'assurer d'annuler sans délai les mots de passe de cet employé pour chacun des assureurs, mais ces annulations demandent souvent l'intervention des administrateurs de système surchargés.

Outre l'exposition potentielle à ce risque important, la complexité de la tâche de programmation et les activités de maintenance continues requises pour la gestion des mots de passe individuels des nombreux employés du cabinet de courtage pour les divers assureurs entraînent des coûts non négligeables à la fois pour les courtiers et (particulièrement) pour les assureurs.

L'adoption d'une méthode d'authentification fondée sur un mot de passe unique attribué au cabinet de courtage permettrait de réduire le risque d'une utilisation à mauvais escient par des parties externes, et éliminerait plusieurs couches de complexité et de coûts inutiles. Le système de l'assureur pourrait vérifier que le message entrant provient bel et bien d'un cabinet de courtage autorisé et que l'information reçue est bel et bien approuvée par le cabinet

Il va sans dire que l'expéditeur d'une communication, qu'il s'agisse d'un employé du cabinet de courtage ou de l'assureur, devra demeurer identifiable aux fins de l'audit. De plus, le cabinet de courtage devra prendre les mesures nécessaires pour assurer la sécurité et la confidentialité de tous les mots de passe des utilisateurs, et veiller à ce que l'accès aux systèmes internes soit supprimé sans délai lorsqu'un employé quitte ses fonctions.

L'ACAC souligne de nouveau le pouvoir dont disposent les cabinets de courtage pour gérer leurs propres activités et leur personnel. Pour servir l'intérêt de tous les acteurs du secteur de l'assurance, l'ACAC est déterminée à promouvoir une utilisation efficace de la technologie pour mieux servir les clients, et l'abandon des modèles de communication qui privilégient l'utilisation d'un portail.

L'ACAC invite les assureurs à prendre en considération les facteurs suivants lorsqu'ils conçoivent et établissent des interfaces électroniques avec les courtiers partenaires.

Principes du modèle de sécurité de l'ACAC

- Les contrats avec les assureurs doivent être conclus au nom des cabinets de courtage et non de leurs employés.
- Les cabinets de courtage assument la responsabilité de la formation et des actions de leurs employés, du pouvoir qui leur est conféré et de leur accès aux réseaux et ressources de communication.
- Les modes de communication électroniques ne modifient en rien le modèle d'affaires traditionnel entre courtiers et assureurs.
- L'authentification des données transmises par voie électronique aux assureurs peut être contrôlée de façon plus sécuritaire par les cabinets de courtage lorsqu'elle s'effectue à partir du système (c.-à-d. du système de gestion du cabinet de courtage au système de l'assureur).
- L'authentification au niveau du système de gestion réduit les coûts, la complexité et l'inefficience inhérents aux mesures de sécurité fondées sur des identifiants utilisateurs et des mots de passe.
- Les parties à la correspondance doivent être identifiables, mais ne devraient pas faire l'objet d'une authentification supplémentaire.