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

AUTHENTIFICATION DE SÉCURITÉ POUR L'ÉCHANGE DE DONNÉES ENTRE COURTIERS ET ASSUREURS

EXPOSÉ DE POSITION NATIONALE

Les courtiers et les assureurs peuvent échanger de l'information entre eux de façon beaucoup plus efficace en utilisant des moyens électroniques que par des moyens traditionnels. Cependant, les objectifs commerciaux de ces échanges et les rôles des correspondants n'ont jamais changé; les responsabilités et rôles distincts du courtier et du souscripteur persistent. Il s'ensuit donc que les règles et les conventions en matière de sécurité relativement à l'échange de données électronique doivent refléter le modèle de fonctionnement qu'elles servent.

Les propriétaires des cabinets de courtage contrôlent les activités de leurs propres entreprises, et, en fin de compte, sont responsables des actions de leurs employés. Les assureurs confèrent le pouvoir d'engager l'assureur à chaque cabinet de courtage individuellement; en effet, les contrats entre courtiers et assureurs stipulent que les cabinets de courtage sont responsables des erreurs ou omissions commises par les membres de leur personnel et de la violation par ces derniers du pouvoir d'engager l'assureur.

Traditionnellement, les courtiers communiquaient avec les assureurs au moyen de divers outils comme les notes de service, le téléphone, ou, plus récemment, le courriel et l'EDI. Les assureurs ne décidaient pas de l'autorité qui serait conférée à chaque employé pour communiquer avec les souscripteurs ou pour transmettre les instructions d'un client; cette responsabilité a toujours incombé entièrement aux propriétaires des cabinets de courtage.

La communication d'information aux assureurs par voie électronique au moyen des services Web ne modifie pas cette responsabilité; les cabinets de courtage régissent toujours la formation et les actions de leurs propres employés et sont responsables des actions exécutées par chacune de ces personnes au nom du cabinet. Cette supervision inclut la sécurité des réseaux internes des cabinets de courtage et des systèmes de gestion de courtage, qui utilisent des noms d'utilisateur et des mots de passe individuels gérés de manière centralisé. Lorsqu'un nom d'utilisateur est supprimé ou désactivé, tout accès lié à ce nom est également enlevé, y compris la possibilité d'accéder à toute autre application dépendante qui passe par le système central du cabinet de courtage.

Des risques dangereux sont toutefois créés lorsque des individus ont directement accès aux systèmes des assureurs sans que la communication soit acheminée par le système d'un cabinet de courtage identifié. Lorsque la seule condition préalable est une connexion Internet, les personnes qui se souviennent de leurs noms d'utilisateur et mots de passe peuvent accéder aux systèmes des assureurs de n'importe où. Lorsqu'un employé quitte le cabinet de courtage, les propriétaires doivent réagir immédiatement pour annuler les mots de passe attribués à cette personne pour les systèmes de tous les assureurs, mais ils doivent souvent compter sur divers administrateurs surchargés chez les assureurs pour mener à bien cette tâche.

Outre cette possibilité élevée d'exposition aux risques, la complexité de la programmation et l'entretien continu requis pour gérer les mots de passe personnels de chaque employé du cabinet de courtage, pour les systèmes de multiples assureurs, accroît sensiblement les coûts des courtiers, et surtout des assureurs.

Par contre, une méthode d'authentification utilisant un seul mot de passe pour l'ensemble du cabinet de courtage réduit la possibilité d'abus externe par des individus et élimine de multiples niveaux de complexité et de coûts inutiles. Le système de l'assureur vérifie que le message entrant provient effectivement d'un cabinet de courtage approuvé et que l'information reçue est sanctionnée par cette firme.

Naturellement, l'expéditeur d'une communication, que ce soit un employé du cabinet de courtage ou un employé de l'assureur, doit toujours être identifiable aux fins de vérification. De plus, les cabinets de courtage doivent veiller avec diligence à ce que tous les mots de passe au niveau des utilisateurs demeurent sécuritaires et confidentiels, et que l'accès aux systèmes internes des courtiers soit immédiatement terminé pour toute personne qui cesse d'être employé par le cabinet.

L'ACAC réaffirme l'autorité des courtiers sur les activités et le personnel de leurs propres entreprises. Dans l'intérêt de l'ensemble des intervenants de l'industrie, l'ACAC s'engage à promouvoir l'utilisation la plus efficace des technologies afin de fournir le meilleur service aux consommateurs, en s'écartant des modèles de communication axés sur les portails.

L'ACAC exhorte les assureurs à prendre en considération les éléments suivants dans la conception et la construction d'interfaces électroniques avec leurs partenaires courtiers.

Principes du modèle de sécurité de l'ACAC

- Ce sont les cabinets de courtage, et non pas les individus, qui passent des contrats avec les assureurs.
- Les cabinets de courtage assument la responsabilité de la formation et des actions de leurs employés, de l'autorité qui leur est accordée et de leur accès aux ressources liées aux réseaux et aux communications.
- Les communications électroniques ne modifient pas le modèle de fonctionnement traditionnel entre les courtiers et les assureurs.
- L'authentification pour la transmission d'information par voie électronique aux assureurs peut être contrôlée de la façon la plus sécuritaire par les cabinets de courtage lorsqu'elle se situe au niveau des systèmes (c.-à-d., du système du courtier au système de l'assureur).
- L'authentification basée sur les systèmes élimine les coûts supplémentaires, la complexité et l'inefficacité inhérents aux exigences relatives aux noms d'utilisateur et aux mots de passe individuels.
- Les correspondants individuels doivent être identifiables mais n'ont pas besoin d'authentification supplémentaire.