Renseignements à fournir en cas d'

INTRUSION INFORMATIQUE

SEPTEMBRE 2020

INSURANCE BROKERS ASSOCIATION OF CANADA

CYBERRISQUE

Ce qui devrait avoir été fait **avant** une intrusion informatique

« EN 2019,PLUS DE 28 MILLIONS DE CANADIENS ONT ÉTÉ TOUCHÉS PAR DES ATTEINTES À LA VIE PRIVÉE. » – COMMISSAIRE À LA PROTECTION DE LA VIE PRIVÉE

TYPE D'INCIDENT	NOMBRE TOTAL DE RAPPORTS
DIVULGATION ACCIDENTELLE	147
PERTE DE DONNÉES	82
VOL DE DONNÉES	54
ACCÈS NON AUTORISÉ	397
TOTAL	680

Aucun propriétaire d'entreprise ne souhaite être victime d'une intrusion informatique qui exposerait les données de ses clients ou qui porterait atteinte à sa réputation. La protection des renseignements personnels et des systèmes informatiques dont votre entreprise a besoin pour exercer ses activités devrait être en tête de vos priorités. Les exigences des lois sur la protection des renseignements personnels continuent d'évoluer.

Les exigences des lois continuent d'évoluer. Les entreprises sont maintenant tenues de consigner et de déclarer toutes les intrusions informatiques, et elles s'exposent à des amendes en cas de non-conformité.

IL FAUT **PLANIFIER, RENFORCER ET TESTER VOS SYSTÈMES INFORMATIQUES** POUR RÉDUIRE LES RISQUES D'INTRUSION INFORMATIQUE ET D'ACCÈS NON AUTORISÉ.

ATTÉNUATION DES CYBERRISQUES

RISQUE CRITIQUE

SOLUTIONS POSSIBLES

Les cabinets de courtage sont exposés à un certain nombre de risques potentiellement dévastateurs (inondations, incendies, tremblements de terre, atteintes à la vie privée, cyberattaques, etc.). Les cyberrisques sont en croissance, et la situation ira en empirant. Le Commissariat à la protection de la vie privée du Canada indique : « Depuis le 1er novembre 2018 (lorsqu'il est devenu obligatoire de déclarer les atteintes à la vie privée),
nous avons reçu 680 déclarations d'atteinte à la vie privée. C'est six fois le volume que nous avions reçu au cours de la même période un an plus tôt. Il s'agit d'une augmentation vertigineuse et plus importante que ce que nous avions prévu. » Les cabinets de courtage doivent évaluer les risques auxquels ils sont exposés et être prêts à déployer des stratégies d'atténuation pour éviter une catastrophe.

La principale exigence est la planification – un cabinet doit disposer d'un plan écrit pour répondre à chaque risque. Pour une catastrophe naturelle, discutez avec le fournisseur de votre système de gestion de courtage afin de déterminer comment vous pouvez accéder aux données si votre cabinet est fermé (un fournisseur de services d'application ou FSA) est un excellent choix). Trouvez un site secondaire à partir duquel il vous sera possible de travailler et prenez les mesures nécessaires pour que les membres du personnel puissent travailler à distance. Trouvez des sources d'alimentation de remplacement, c'est-à-dire des génératrices. Vous pouvez également conclure des ententes avec des organismes de secours.

La gestion des risques à la sécurité exige une planification encore plus poussée, planification qui tient compte de plusieurs enjeux (communications aux clients, protection de la réputation et incidence juridique). En plus d'avoir un plan qui puisse être mis en œuvre en cas d'attaque informatique, vous devez avoir des procédures de sécurité écrites qui prouvent que vous avez fait de votre mieux pour protéger les données de vos clients. Les plans écrits et mis à jour régulièrement sont essentiels pour atténuer les risques.

RESSOURCES

Gouvernement du Canada – CyberSécuritaire Canada

Gouvernement du Canada – Planification de la réponse aux urgences et catastrophes Centre canadien pour la cybersécurité

Formation en ligne du CSIO – Cyber-sécurité

Insurance Information Institute – Élaborer un plan de reprise après sinistre pour une petite entreprise (en anglais seulement)

MOTS DE PASSE UTILISÉS AU CABINET DE COURTAGE

RISQUE CRITIQUE

Une gestion inadéquate des mots de passe rend la protection des renseignements personnels extrêmement difficile. Le fait de conserver les codes utilisateur et les mots de passe par écrit ou dans un document électronique non sécurisé n'offre pas une protection adéquate.

SOLUTIONS POSSIBLES

Assurez-vous que les employés connaissent bien les meilleures pratiques en ce qui concerne la gestion des mots de passe. Une gestion efficace des *mots de passe* comprend trois aspects :

- L'utilisation des capacités de gestion des mots de passe qui sont intégrées au système de gestion de courtage, y compris la signature ou l'authentification unique.
- L'adoption d'un processus d'authentification à doubles facteurs lorsqu'un tel processus est disponible.
- L'utilisation d'une solution de signature ou d'authentification unique proposée par un tiers pour tous les autres mots de passe.

RESSOURCES

SANS Institute – Matériel de prévention des pertes de données et sensibilisation (en anglais seulement)
Broadcom – Produits de prévention des pertes de données (en anglais seulement)

SURVEILLANCE EN TEMPS RÉEL ET DÉTECTION DES INTRUSIONS INFORMATIQUES

RISQUE CRITIQUE

Il est essentiel de connaître le contenu des paquets de données qui entrent dans le réseau de l'entreprise ou qui en sortent.
Le recours à des solutions de protection contre la perte de données pour les flux de données est de plus en plus courant pour protéger l'information sensible et vérifier l'utilisation des contenus au sein d'une entreprise.

RESSOURCES

Commissariat à la protection de la vie privée au Canada – Mots de passe Gestionnaires de mots de passe 2020

SOLUTIONS POSSIBLES

Les solutions de protection contre la perte de données vont des postes de travail simples aux appareils connectés à des réseaux étendus conçus pour analyser le trafic pour les données sensibles comme les numéros de carte de crédit et d'assurance sociale. Au cours des dernières années, les solutions de logiciels-services ou de protection contre la perte de données dans le nuage ont également commencé à être proposées aux entreprises qui cherchent à confier cette fonction à un tiers ou à un fournisseur de services. Le centre de ressources à l'adresse SANS.org (en anglais seulement) fournit des renseignements sur les types de solutions de protection contre la perte de données disponibles; il faut choisir la solution qui répond le mieux aux besoins de votre entreprise.

UTILISATION DES FOURNISSEURS DE SERVICES D'APPLICATION

RISQUE CRITIQUE

Les FSA ou les systèmes exploités à partir du Web permettent d'assurer un accès en tout temps aux données du système de gestion de courtage et des autres systèmes. Ils permettent également que des sauvegardes multiples soient effectuées et que les logiciels soient mis à jour automatiquement aussitôt que les nouvelles versions sont disponibles.
Si on les compare, les ordinateurs de bureau, les ordinateurs reliés à un réseau local ou même une architecture cliente légère peuvent plus facilement être compromis en cas de dommages. Ils exigent plus d'interventions de la part du personnel pour les sauvegardes et les mises à jour et ne sont pas facilement accessibles au moyen d'un appareil mobile.

SOLUTIONS POSSIBLES

Presque tous les fournisseurs de logiciels des divers secteurs d'activité proposent des versions FSA, et souvent uniquement ces versions. Si vous utilisez un système de gestion de courtage, un comparateur de taux ou un logiciel de gestion de la relation client, vous pouvez vérifier la disponibilité des versions FSA et les prix auprès de votre fournisseur.

Un degré de diligence raisonnable doit être exercé au moment de la sélection d'un FSA : évaluez les mesures de sécurité qui sont mises en place par le fournisseur pour renforcer l'environnement informatique et réduire les risques de cyberattaques.

Remarque : Les systèmes hébergés tendent à être plus chers que les ordinateurs de bureau, car le fournisseur doit absorber certains coûts : hébergement et gestion des données, droits d'accès, mises à jour et autres mesures de sécurité. Ne pas oublier que des logiciels antivirus ou d'autres logiciels de protection devront également être installés.

RESSOURCES

Analyses de Gartner – Prévention des pertes de données (en anglais seulement)

CISCO – Évaluer les FSA (en anglais seulement)

Meilleurs logiciels antivirus (en anglais seulement)

CONCEPTION DE SITE WEB ET RÈGLES DE SÉCURITÉ

RISQUE CRITIQUE

Même si un site Web est utilisé uniquement pour fournir de l'information et même si sa conception est simple, les questions de sécurité ne doivent pas être négligées, que vous ayez conçu votre site Web vous-même ou que vous ayez fait appel à un tiers pour le faire. La sécurité de votre site Web peut être compromise de plusieurs façons : il peut, entre autres, être pris en otage et rediriger les visiteurs vers un autre site, il peut être infecté par un code malveillant ou un virus et subir une attaque par déni de service, etc.

SOLUTIONS POSSIBLES

Installez le protocole sécurisé SSL. Ce protocole ajoute le « s » dans https://, indiquant ainsi que le site est sécurisé. L'icône du cadenas s'affichera au début de l'adresse URL du site Web. L'ajout du protocole SSL est une pratique privilégiée pour la conception des sites Web, et il est requis si le cabinet accepte les paiements. Le protocole SSL empêche les navigateurs d'avertir les visiteurs que le site n'est pas sécurisé. Un avertissement de site non sécurisé pourrait éloigner existants ou potentiels.

Le protocole HTTPS est également un critère utilisé par Google pour classer votre site Web.

Utilisez des mots de passe solides pour sécuriser le compte administrateur de votre site Web et assurez-vous de toujours sauvegarder les fichiers de votre site afin de limiter les pertes qui pourraient découler de la défaillance d'un disque dur ou de la corruption de vos fichiers HTML.

RESSOURCES

Centre d'aide de Google : Sécuriser votre site à l'aide du protocole HTTPS
Pourquoi un avertissement de site non sécurisé s'affiche-t-il à l'écran (en anglais seulement)?

APPAREILS MOBILES

RISQUE CRITIQUE

L'utilisation d'appareils mobiles dans le cadre du travail expose l'entreprise à des menaces informatiques additionnelles. Ces menaces peuvent compromettre le réseau de l'entreprise et les données. Parmi les défis les plus importants auxquels une entreprise peut être confrontée, mentionnons la perte de données ou une brèche dans le système de sécurité causée par un appareil mobile volé ou perdu. Les appareils mobiles peuvent également être la cible d'attaques et de logiciels malveillants ou de rançons qui peuvent permettre à une personne de prendre votre compte ou vos données en otage.

SOLUTIONS POSSIBLES

Créez un processus d'approbation pour tous les appareils mobiles qui sont utilisés dans le cadre des activités professionnelles du cabinet. Un énoncé de la politique de l'entreprise doit être inclus dans ce processus, énoncé qui doit être lu et signé par l'utilisateur et qui doit indiquer ce qui suit.

ÉTAPES À SIUIVRE

1. L'accès à tous les appareils doit être protégé par un mot de passe.

2. Des connexions sans fil sécurisées doivent être utilisées pour transmettre les renseignements liés aux activités professionnelles – les services gratuits dans les cafés ou les aéroports ne doivent pas être utilisés.

3. Un processus de déclaration pour les appareils volés ou perdus (localisation immédiate de l'appareil ou suppression immédiate et à distance des données).

4. Les données de tous les appareils sont supprimées avant de s'en débarrasser ou de les remplacer.

5. Utilisez des disques et des cartes mémoires chiffrés.

6. Sécurisez tous les appareils mobiles, mettez les logiciels à jour et utilisez uniquement des applications de confiance.

7. Appliquez les processus d'affaires et les procédures à l'utilisation des appareils mobiles (consignation appropriée des données dans le système de gestion de courtage).

8. Appliquez la politique d'utilisation de la messagerie électronique et les meilleures pratiques aux appareils mobiles comme si les utilisateurs étaient au bureau.

RESSOURCES

Commissariat à la protection de la vie privée du Canada – Protégez vos renseignements personnels

Commissariat à la protection de la vie privée du Canada – Escroquerie d'échange de cartes SIM

CONSERVATION DES DOCUMENTS

RISQUE CRITIQUE

Plus la période de conservation des renseignements sur les clients est longue, plus le nombre de documents qui risquent d'être perdus en cas d'intrusion informatique est grand.

SOLUTIONS POSSIBLES

Conservez uniquement les renseignements dont le cabinet a besoin et seulement pendant la période requise par la loi. La législation fédérale et les organismes de réglementation provinciaux ont formulé des exigences pour les politiques de conservation des documents et l'élimination des renseignements personnels. Le cabinet devrait définir une politique de conservation des documents qui soit applicable à tous ses systèmes, et surveiller la conformité.

RESSOURCES

La gestion des risques à la sécurité des appareils mobiles (en anglais seulement)
Avantages et inconvénients de l'approche « Prenez vos appareils personnels »
Commissariat à la protection de la vie privée du Canada – Protection des renseignements personnels stockés dans vos appareils mobiles

CHIFFREMENT DE BASES DE DONNÉES

RISQUE CRITIQUE

SOLUTIONS POSSIBLES

RESSOURCES

Chiffrement de l'appareil dans Windows 10
McAfee – Le chiffrement des terminaux aide à protéger vos données (en anglais seulement)

L'utilisation de stratagèmes de plus en plus complexes et perfectionnés par les pirates informatiques et la transmission d'un volume de données de plus ne plus important par voie électronique constituent probablement le risque le plus grand auquel les entreprises sont exposées aujourd'hui.

Le respect de la réglementation provinciale en matière de protection des renseignements personnels est essentiel. La réglementation provinciale la plus stricte doit être appliquée pour la base de données clients. Utilisez les outils de chiffrement facilement disponibles comme la fonction « Activer le chiffrement de l'appareil » sous Microsoft pour chiffrer les disques durs, les dispositifs de sauvegarde et autres appareils, et empêcher que les données ne puissent être lues en cas de vol ou de perte. Assurez-vous de ne pas perdre la clé de chiffrement. Conservez-la dans un endroit sûr.

SENSIBILISATION ET ÉDUCATION

RISQUE CRITIQUE

Les employés d'un cabinet de courtage ont accès à une grande quantité de renseignements personnels qui peuvent être volés. Un des éléments les plus importants d'une politique en matière de sécurité devrait être la sensibilisation et la formation continue visant les rôles et responsabilités en ce qui concerne la protection des actifs de l'entreprise et les renseignements du client.

SOLUTIONS POSSIBLES

Définissez une politique en matière de sécurité et des procédures de notification en cas d'intrusion informatique. Expliquez-les aux nouveaux employés et passez-les en revue périodiquement avec tous les employés afin que la protection des données fasse partie intégrante de la culture du cabinet. Procédez à une évaluation annuelle de la politique en matière de sécurité et des procédures de notification en cas d'intrusion informatique. Évaluez également le niveau de sensibilisation aux menaces informatiques et toutes les responsabilités en matière de protection des renseignements personnels.

Procédez à une évaluation annuelle de la politique en matière de sécurité et des procédures de notification en cas d'intrusion informatique. Évaluez également le niveau de sensibilisation aux menaces informatiques et toutes les responsabilités en matière de protection des renseignements personnels. Des aspects de la politique en matière de sécurité et des exemples d'intrusion dans le monde où des leçons peuvent être tirées sont examinés tous les mois ou trimestres pour maintenir la sécurité et la protection des renseignements au cœur des préoccupations et témoigner du soutien et des attentes de la direction.

Établissez un calendrier de formation pour chacun des postes suivants : chef de la conformité en matière de sécurité informatique, agent de protection de la vie privée, membres de la haute direction, superviseurs, employés mobiles et tous les employés. Grâce à cette formation, les employés connaîtront leurs responsabilités et se familiariseront avec la politique du cabinet en matière de sécurité informatique et avec les énoncés relatifs à la protection des renseignements personnels.

RESSOURCES

Commissariat à la protection de la vie privée du Canada – Pour les entreprises Commissariat à la protection de la vie privée du Canada – Lois et organismes de surveillance provinciaux et territoriaux en matière de protection de la vie privée

LOIS APPLICABLES EN CAS D'INTRUSION INFORMATIQUE

RISQUE CRITIQUE

Les cabinets de courtage possèdent des données qui pourraient, en cas d'intrusion ou d'accès non autorisé, causer un préjudice grave aux personnes et organisations concernées. Le cabinet de courtage doit bien comprendre la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) ainsi que les lois applicables dans la province où le cabinet est établi et également dans toutes les provinces (ou territoires étrangers) où le cabinet exerce des activités.

SOLUTIONS POSSIBLES

- Élaborez un plan d'intervention en cas d'incident informatique. Ce plan permet de s'assurer que vous savez ce qui doit être fait, y compris les procédures à suivre, en cas d'intrusion informatique. Ce plan devrait expliquer ce qu'on entend par un incident, à quel moment et comment il doit être déclaré, et à qui (à l'interne et à l'externe, s'il y a lieu).

- La LPRPDE définit ce qui constitue spécifiquement une atteinte à la vie privée, et précise les obligations relatives à leur déclaration, ainsi que les amendes et pénalités potentielles. Le Commissariat à la protection de la vie privée du Canada (OPC) fournit un ensemble de renseignements généraux sur la LPRPDE, sur la réglementation applicable dans les provinces et sur certaines mesures à prendre en cas d'atteinte.

- De plus, les sociétés du secteur des cartes de paiement possèdent leurs propres règles en matière de sécurité et de conformité qu'elles imposent à toutes les entreprises qui acceptent, transmettent ou conservent des données sur les titulaires de cartes.

- Pour les cabinets de courtage qui exercent des activités aux États-Unis, la société Mintz-Levin présente la définition d'une atteinte aux mesures de sécurité pour chaque État ainsi que les entités couvertes, les procédures de déclaration et les amendes connexes. Il revient également au cabinet de courtage de comprendre la position du Federal Trade Commission (FTC) des États-Unis sur la protection des renseignements personnels. Les cabinets de courtage qui font souscrire des polices collectives d'assurance maladie doivent également satisfaire aux règles des lois HIPAA et HITECH des États-Unis en cas d'atteinte à la vie privée.

RESSOURCES

Commissariat à la protection de la vie privée du Canada – Pour les entreprises

Commissariat à la protection de la vie privée du Canada – Lois et organismes de surveillance provinciaux et territoriaux en matière de protection de la vie privée

Commissariat à la protection de la vie privée du Canada – Principes relatifs à l'équité dans le traitement de l'information de la LPRPDE

Commissariat à la protection de la vie privée du Canada – Ce que vous devez savoir sur la déclaration obligatoire des atteintes aux mesures de sécurité

Commissariat à la protection de la vie privée du Canada – Dix conseils pour éviter les plaintes au Commissariat

Minz-Levin – Lois en vigueur dans les États américains applicables aux obligations de déclaration en cas d'atteinte à la sécurité des données (en anglais seulement)

Règlement général sur la protection des données (RGPD) – Loi la plus stricte à ce jour dans le monde

Deloitte – Le RGPD et les organisations canadiennes

COMMUNICATION ÉLECTRONIQUE

RISQUE CRITIQUE

Dans le cas des communications électroniques, certains aspects importants doivent être pris en considération. La *Loi canadienne antipourriel* et la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) définissent les obligations à la fois pour les assureurs et les cabinets de courtage en ce qui concerne la conservation de la preuve que le consentement du client a été obtenu. Des mesures suffisantes doivent également être mises en place pour améliorer l'efficacité et la sécurité.

SOLUTIONS POSSIBLES

Assurez-vous de bien connaître et comprendre les lois fédérales et provinciales applicables aux communications électroniques. Utilisez une approche qui puise dans les meilleures pratiques et dans les normes du CSIO qui s'appliquent aux communications électroniques. Commencez par un seul processus d'affaires et une seule gamme de produits. Créez un diagramme illustrant le flux idéal de travail et les mesures de sécurité optimales pour chaque aspect. Les renseignements personnels sensibles ne doivent pas être transmis par courriel. Ils ne doivent donc jamais être inclus dans le texte d'un courriel ou dans un document joint. Intégrez plutôt dans les courriels des liens vers un site sécurisé.

RESSOURCES

Rapport consultatif du CSIO :Signature et distribution électroniques de documents d'assurance

SÉCURITÉ ET SYSTÈMES TÉLÉPHONIQUES IP

RISQUE CRITIQUE

Les réseaux convergents de voix et de données présentent une multitude d'avantages tout en permettant de faire des économies substantielles; cependant, les risques en matière de sécurité et de fraude associés à ces systèmes doivent être pris en considération. Les trois risques les plus courants sont : l'interception des appels et la protection de la vie privée, les interruptions de service et l'utilisation frauduleuse du service ou le vol.

SOLUTIONS POSSIBLES

Le respect de la réglementation provinciale en matière de protection des renseignements personnels est essentiel. La réglementation provinciale la plus stricte doit être appliquée pour la base de données clients. L'ensemble des mesures de sécurité applicables à votre infrastructure de données devient particulièrement important lors de la mise en place d'un système VoIP. Les flux de données non chiffrées des systèmes VoIP peuvent facilement être interceptés. Utilisez des protocoles de chiffrement, comme le protocole TLS. Les flux voix seront alors chiffrées comme les flux de données afin d'assurer une transmission sécurisée sur un réseau.

Pour l'installation de réseaux étendus sur les lieux de travail, l'utilisation d'un contrôleur de session en périphérie devrait être prise en considération.

RESSOURCES

VoIP-info.org – Sécurité des systèmes téléphoniques VoIP (en anglais seulement

SANS Institute – Problèmes de sécurité et mesures d'atténuation (en anglais seulement

SANS Institute – VoIP et sécurité (en anglais seulement)

DESTRUCTION DE DOCUMENTS

RISQUE CRITIQUE

Le processus de destruction des documents ne se limite pas uniquement aux dossiers papier. Il vise également les fichiers électroniques et les courriels (conservés) ainsi que les fichiers qui peuvent se trouver sur les réseaux, dans le nuage, sur les disques durs internes ou externes et sur les appareils mobiles. Les lois fédérales et provinciales exigent que les entreprises détruisent de façon appropriée les dossiers clients qui n'ont plus besoin d'être conservés. La destruction comprend le déchiquetage ou tout autre processus de modification des renseignements personnels contenus dans ces dossiers afin qu'ils soient impossibles à lire.

SOLUTIONS POSSIBLES

Établissez une politique et des processus pour guider la destruction appropriée des documents en suivant les cinq étapes suivantes :

1. Faites l'inventaire des renseignements qui sont en votre possession et déterminez à quel endroit ils se trouvent (systèmes de gestion de courtage, télécopieur, courriel, documents papier, disques durs, nuage, tiers).

2. Réduisez – consolidez les renseignements et limitez leur conservation aux endroits contrôlés et gérables.

3. Sécurisez les renseignements personnels – verrouillez les tiroirs contenant les dossiers papier, sécurisez l'accès aux serveurs, protégez les fichiers à l'aide de mot de passe, configurez les écrans de veille.

4. Identifiez – détruisez ou retirez de façon appropriée les documents ou les fichiers qui n'ont plus besoin d'être conservés.

5 Planifiez – établissez les procédures, formez les employés et surveillez le niveau de conformité.

RESSOURCE

Commissariat à la protection de la vie privée du Canada – Sécuriser les données

SYSTÈME DE GESTION DE COURTAGE ET ACCÈS À DISTANCE

RISQUE CRITIQUE

L'accès à distance offre de la souplesse; certaines étapes doivent cependant être suivies pour atténuer les risques associés à cette capacité.

Pour réduire le risque d'intrusion par les points d'accès à distance, il faut prendre en considération trois aspects importants : le processus d'authentification amélioré, la validation des points d'entrée et la sécurité des données pendant la transmission.

SOLUTIONS POSSIBLES

Utilisez un processus d'authentification rigoureux à deux facteurs. Les options disponibles pour les personnes qui travaillent à distance sont les certificats numériques, les codes transmis par message texte ou la validation des données biométriques. Évaluez la pertinence de limiter l'accès à distance pour certains systèmes. Utilisez un système de détection et de prévention d'intrusion (SDPI) entre le point d'accès à distance et votre réseau interne pour éviter les risques d'intrusion. Ce système permet de réduire le risque de transmission de logiciels frauduleux et de virus par un appareil connecté. Utilisez un réseau privé virtuel (RPV) pour sécuriser les données pendant qu'elles sont transmises par une personne qui travaille à distance.

RESSOURCE

Meilleurs logiciels de contrôle d'accès à distance (en anglais seulement)

ENVIRONNEMENT PAPIER c. ENVIRONNEMENT SANS PAPIER

RISQUE CRITIQUE

Lorsqu'un cabinet de courtage décide de privilégier un environnement de travail sans papier, plusieurs aspects doivent être pris en compte, notamment le stockage de données (sur place ou dans le nuage), la cohérence et la continuité des processus, la formation du personnel et les exigences, la conservation des documents et l'historique des communications, l'accès aux documents par l'intermédiaire du site Web des assureurs et l'accès utilisateur fondé sur le « besoin de consulter ».

SOLUTIONS POSSIBLES

Analysez les processus en vigueur et modifiez-les en fonction des nouvelles exigences du processus « sans papier ». Élaborez un bon plan de communication, formez les employés en vue de l'adoption et du respect du nouveau processus.

Déterminez l'endroit où seront stockées les données (localement sur un serveur ou dans le nuage) et assurez-vous de comprendre les vulnérabilités liées à la sécurité et les mesures de précaution à prendre pour chaque mode de stockage. Sachez que l'incidence financière de chaque option est différente, et que l'une ou l'autre des options pourrait ne pas être financièrement possible pour un cabinet de courtage. Suivez les directives des gouvernements qui s'appliquent à la conservation des documents lorsque vous décidez de passer à un environnement sans papier. La conservation de la version papier des documents pourrait ne pas être nécessaire si le cabinet de courtage a accès aux documents du client sur le site Web de l'assureur.

RESSOURCES

Les 14 conseils de CIO pour créer un bureau sans papier (en anglais seulement)

Phase 1 – Amélioration des processus pour un environnement sans papier (en anglais seulement Phase 2 – Transactions sans papier (en anglais seulement)

Article de l'Agent Council of Technology (ACT) – Création d'un plan de protection des renseignements personnels (en anglais seulement)

RESSOURCES

Les 14 conseils de CIO pour créer un bureau sans papier (en anglais seulement)

Phase 1 – Amélioration des processus pour un environnement sans papier (en anglais seulement Phase 2 – Transactions sans papier (en anglais seulement)

Article de l'Agent Council of Technology (ACT) – Création d'un plan de protection des renseignements personnels (en anglais seulement)

PROTÉGER L'INFORMATION CONFIDENTIELLE

RISQUE CRITIQUE

Les risques auxquels les cabinets de courtage sont exposés augmentent de façon importante en ce qui concerne les renseignements personnels sur la santé et les renseignements permettant d'identifier une personne. Les courtiers doivent connaître les lois qui s'appliquent à ces renseignements au Canada et dans les provinces. Ils doivent savoir quels renseignements doivent être conservés, à quel endroit ils doivent l'être et qui peut les consulter.

SOLUTIONS POSSIBLES

Effectuez une analyse du risque pour identifier les renseignements personnels sur la santé et les renseignements qui permettent d'identifier une personne et déterminez à quel endroit ils se trouvent dans votre cabinet.

Effectuez une évaluation des écarts sur le plan de la conformité. Réduisez au minimum les renseignements sur la santé des personnes qui sont conservés dans les dossiers du cabinet ou les renseignements qui permettent d'identifier les personnes. Élaborez la politique et les procédures, formez les employés et surveillez le niveau de conformité. Mettez en œuvre une politique d'accès fondée sur le « besoin de consulter ».

Assurez-vous de connaître vos obligations relatives à la **déclaration des atteintes aux mesures de sécurité.**

RESSOURCES

Commissariat à la protection de la vie privée du Canada – Pour les entreprises

Commissariat à la protection de la vie privée du Canada – Lois et organismes de surveillance provinciaux et territoriaux en matière de protection de la vie privée

Commissariat à la protection de la vie privée du Canada – Principes relatifs à l'équité dans le traitement de l'information de la LPRPDE

Commissariat à la protection de la vie privée du Canada – Ce que vous devez savoir sur la déclaration obligatoire des atteintes aux mesures de sécurité

ENVIRONNEMENT INFORMATIQUE ET TESTS

RISQUE CRITIQUE

Aucun plan n'est parfait. Vous pourriez l'apprendre à vos dépens si vos systèmes subissent une attaque informatique. Vous devez plutôt tester vos systèmes avant que l'impensable ne se produise. Des entreprises se spécialisent dans l'analyse des mesures de sécurité en utilisant les tactiques des entreprises criminelles. Ces entreprises peuvent révéler des vulnérabilités qui sont passées inaperçues pendant la conception de vos mesures de sécurité des TI, et vous aider à corriger les lacunes avant qu'elles ne soient exploitées.

SOLUTIONS POSSIBLES

Faites appel à un consultant externe pour effectuer un audit de la sécurité matérielle et technique. Utilisez l'examen des politiques et procédures pour améliorer les politiques en matière de sécurité et de collecte et conservation des données. Faites appel à une entreprise de sécurité pour effectuer un test d'intrusion de l'environnement informatique de votre cabinet. Demandez à votre professionnel des TI de vérifier la configuration de tous les appareils et d'optimiser la sécurité, et réglez votre système d'exploitation pour que les mises à jour et correctifs soient appliqués automatiquement.

RESSOURCE

InfoSecurity – Appelez les chapeaux blancs ou l'importance de confier les tests à une entreprise externe (en anglais seulement)

PLAN DE REPRISE APRÈS SINISTRE

RISQUE CRITIQUE

Ne pas envisager la possibilité que son cabinet puisse être exposé à une catastrophe peut conduire à la faillite. Selon l'organisme américain FEMA (Federal Emergency Management Agency), 90 % des petites entreprises font faillite au bout de 12 mois après une catastrophe, sauf si elles ont pu reprendre leurs activités après cinq jours. La crise créée par la covid-19 a mis en lumière les faiblesses de nombreux plans de reprise après sinistre. L'ensemble des risques auxquels les entreprises sont exposées feront probablement l'objet d'une réévaluation aux fins de planification.

RESSOURCES

Centre canadien pour la cybersécurité

Guide relatif aux tests, à la formation et aux simulations pour les plans et capacités des TI (en anglais seulement)

SOLUTIONS POSSIBLES

Décidez d'externaliser l'élaboration du plan de reprise après sinistre ou confiez cette tâche aux gestionnaires à l'interne. Lorsque le plan de reprise après sinistre a été créé, il doit être testé au moins une fois l'an à l'aide de divers scénarios de catastrophe. Testez les sauvegardes des sous-systèmes tous les trimestres. Utilisez les résultats pour raffiner le plan de reprise après sinistre. Assurez-vous que les employés reçoivent une formation adéquate en ce qui concerne le plan et qu'ils aient les outils dont ils ont besoin, en cas de sinistre, pour s'acquitter de leurs responsabilités. Un plan complet doit comprendre ce qui suit :

- Plan de communication et rôles et
- responsabilités de chacun Planification du matériel
- Plan de continuité des
- activités Vérification des sauvegardes
- Inventaire précis des actifs
- Photographies du bureau et du matériel (avant et après)
- Plan de communication avec les fournisseurs et de restauration des services

Lorsque le plan de reprise après sinistre a été créé, il doit être testé au moins une fois l'an à l'aide de divers scénarios de catastrophe. Testez les sauvegardes des sous-systèmes tous les trimestres. Utilisez les résultats pour raffiner le plan de reprise après sinistre. Assurez-vous que les employés reçoivent une formation adéquate en ce qui concerne le plan et qu'ils aient les outils dont ils ont besoin, en cas de sinistre, pour s'acquitter de leurs responsabilités.

APRÈS UNE INTRUSION INFORMATIQUE – COMMENT RÉAGIR?

RISQUE CRITIQUE

Un cabinet de courtage qui est victime d'une intrusion informatique est exposé à plusieurs risques (atteinte à la réputation, coûts imprévus pour identifier la source de l'intrusion et colmater la brèche, perte de clients et poursuite en justice et pénalités financières imposées par le Commissariat à la vie privée du Canada). Une étape importante consiste à déterminer d'abord si vous avez une obligation de déclarer l'atteinte aux mesures de sécurité. Tout manquement à cet égard pourrait se traduire par des pénalités financières et de la publicité négative, peut-être à l'échelle nationale. Le recours à un tiers pour traiter ou gérer les données ne vous décharge pas de vos responsabilités en ce qui concerne la conservation des dossiers et l'obligation de déclarer une intrusion.

SOLUTIONS POSSIBLES

1. (Arrêtez la pratique non autorisée, récupérez les données, fermez le système visé par l'intrusion, révoquez ou modifiez les codes d'accès aux ordinateurs, corrigez les faiblesses dans la sécurité matérielle ou électronique, etc.).

2. Désignez une personne pour diriger l'enquête. La personne doit avoir l'autorité et les connaissances appropriées pour effectuer l'analyse initiale et formuler des recommandations préliminaires. S'il y a lieu, une analyse plus poussée pourra être effectuée. Il faudra peut-être faire appel aux services d'un expert à l'externe.

3. Identifiez les personnes à l'interne (et peut-être à l'externe) qui doivent être mises au courant de l'incident à cette étape préliminaire. Informez les responsables, y compris la personne responsable de la conformité pour tout ce qui touche aux renseignements personnels. Assurez-vous de lire le document **Ce que vous devez savoir sur la déclaration obligatoire des atteintes aux mesures de sécurité** pour bien comprendre vos obligations.

4. Prenez soin de ne pas détruire les preuves qui pourraient servir à déterminer la cause de l'intrusion ou à prendre les mesures correctives appropriées.

RESSOURCE

Commissariat à la protection de la vie privée du Canada – Ce que vous devez savoir sur la déclaration obligatoire des atteintes aux mesures de sécurité

GLOSSAIRE

FSA

INFONUAGIQUE, NUAGE (cloud computing)

SYSTÈME DE DÉTECTION D'INTRUSION (intrusion detection system ou IDS)

SYSTÈME DE PRÉVENTION D'INTRUCTION (intrusion prevention system ou IPS)

RÉSEAU PRIVÉ VIRTUEL (RPV)

LOGICIEL SERVICE (software as a Service ou SaaS)

CONTRÔLEUR DE SESSION EN PÉRIPHÉRIQUE (session border controller ou SBC)

Un fournisseur de services d'applications est une entreprise qui fournit des services en ligne aux clients par l'intermédiaire d'un réseau, par exemple, pour accéder à un logiciel d'application (comme un logiciel de gestion de la relation client) à l'aide d'un protocole standard (comme le protocole HTTP).

Modèle informatique qui donne accès sur demande à un bassin de ressources informatiques, notamment le stockage de données et la puissance de traitement, sans gestion directe active de l'utilisateur. Le terme est généralement utilisé pour décrire les centres de traitement de données auxquels de nombreux utilisateurs ont accès sur Internet.

Système qui analyse les flux de données sur un réseau à la recherche des signatures qui correspondent à des cyberattaques connues. Système qui analyse les paquets de données en fonction du type d'attaques détecté et qui peut empêcher leur transmission.

Stratégie d'identification et de surveillance des données sensibles d'une entreprise afin qu'elles ne soient pas perdues, mal utilisées ou rendues accessibles à des utilisateurs non autorisés. Une telle stratégie permet également de respecter les exigences en matière de conformité et d'audit et d'identifier les lacunes et les anomalies aux fins d'enquête et d'intervention.

Canal de communication privé relié à l'infrastructure d'un réseau public qui permet à des utilisateurs de transmettre et de recevoir des données entre des réseaux partagés ou publics comme si les ordinateurs étaient directement connectés au réseau privé.

Logiciel standard hébergé sur les serveurs d'un fournisseur de services et généralement accessible par Internet moyennant un abonnement par opposition à un logiciel standard acheté et installé sur les ordinateurs personnels.

Dispositif permettant de protéger le réseau et les autres appareils de ce qui suit :

- Attaques malveillantes comme les attaques par déni de services ou les attaques par déni de service distribué
- Fraudes téléphoniques par l'intermédiaire de flux de données contaminées
- Protection de paquets de données mal formés
- Chiffrement de la signalisation (protocoles TLS et de sécurité pour IP) et chiffrement support

ANNEXE

Inspiré du document *How Do You Protect Your Agency's Data?*

(gracieuseté d'Agents Council for Technology (ACT). Utilisation permise.

POUR UN COMPLÉMENT D'INFO

IBACTECH@IBAC.CA