CPA COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

Comment sécuriser l'information confidentielle de vos clients

Un sondage mené récemment auprès de praticiens au Canada a montré que seul un faible pourcentage de CA (entre 10 % et 15 %) a toujours recours au chiffrement lors de l'envoi d'états financiers, de déclarations fiscales et d'autres informations financières par courriel à des clients[1]. Le fait d'envoyer de telles informations en texte clair peut poser un risque pour la sécurité des informations concernant le client. Un article de CAmagazine de septembre- 2012 intitulé « Comment cacheter vos courriels » contenait des explications techniques sur le cheminement des courriels, de l'expéditeur jusqu'au destinataire. Comme on l'indique dans l'article, les praticiens devraient « considérer le contenu d'un courriel comme un message sur une carte postale ». En d'autres termes, il existe un risque de violation des informations lors de transmissions en texte clair par Internet. Le présent document vise à fournir des indications aux CA en cabinet ou en entreprise sur la façon sécuritaire de transmettre de l'information aux clients ou à d'autres personnes.

1 Le sondage a été mené par l'International Innovation Network (INN). Voir **http://bit.ly/SzC9E9** pour plus de précisions

Le présent document, initialement publié par l'Institut Canadien des Comptables Agréés en 2012, a été mis à jour par les Comptables professionnels agréés du Canada.

Pourcentage des CA qui envoient de l'information confidentielle par courriel à leurs clients					
	Envoi par email	Mot de passe Parfois	Mot de passe Toujours	Chiffrement Parfois	Chiffrement Toujours
États financiers	70	29	16	14	11
Autre informations financières	77	30	13	16	10
Déclarations de revenus de particuliers	66	25	22	14	15
Déclarations fiscales d'entreprises	61	27	19	15	15

La confidentialité : une responsabilité professionnelle

Les comptables sont perçus comme des conseillers de confiance et des professionnels compétents par leurs clients et leurs employeurs, et ils doivent mettre en place des contrôles en vue de préserver la confiance de ceux qui comptent sur eux. De plus, les comptables sont tenus, en vertu de leur code de déontologie, de s'assurer que des contrôles suffisants sont en place pour protéger l'information concernant leurs clients. Selon le code de déontologie, « les membres ont un devoir de confidentialité à l'égard des informations obtenues dans le cadre de leurs relations professionnelles, d'emploi ou d'affaires [...]. Il est interdit aux membres, aux étudiants ou aux cabinets de divulguer tout renseignement confidentiel concernant les affaires d'un client, d'un ancien client, d'un employeur ou d'un ancien employeur[2]. » En résumé, les comptables ont la responsabilité de protéger les informations qui leur sont confiées.

Sur le plan de la responsabilité professionnelle, aucun praticien n'a, à ce jour, été poursuivi parce que des courriels qu'il avait envoyés auraient été interceptés par un utilisateur non autorisé. Toutefois, des comptables ont été poursuivis dans des situations où ils avaient la responsabilité de livrer à l'ARC des informations en matière d'impôt (p. ex. des demandes de crédits pour RS&DE) ou de retenues salariales, et où les informations en question se sont perdues ou sont parvenues en retard.

Au-delà de la question de la responsabilité, les praticiens devraient tenir compte de la possibilité de perdre la confiance de leurs clients. Malcolm D'Souza, de la société Les Services d'assurance des comptables agréés Inc. (Les SACA Inc.), indique que des comptables l'ont informé de cas de clients mécontents parce qu'ils avaient constaté que les informations les concernant avaient été conservées sans protection (c.-à-d. sans mot de passe ou chiffrement) sur du matériel informatique qui avait par la suite été volé.

2 Traduction d'extraits des Rules of Professional Conduct de l'ICAO. Voir aussi l'Interprétation du Conseil IC 208.

Incidences d'un manquement au devoir de confidentialité sur la réputation des CA

L'interception et la diffusion d'informations confidentielles envoyées à un client par courriel pourraient avoir des conséquences négatives pour l'ensemble de la profession. Les entreprises et les personnes qui comptent sur des CA pour obtenir des conseils sur des questions comptables, fiscales et autres pourraient avoir le sentiment que les informations les concernant ne sont pas en sécurité chez leur comptable. Les CA jouissent de la confiance de leurs clients et ils doivent faire tout leur possible pour préserver cette confiance en s'attaquant au problème de la sécurité de l'information. Autrement, le grand public pourrait ne plus faire confiance aux CA, ce qui serait néfaste pour la réputation de la marque et de la profession dans son ensemble.

Information confidentielle des clients et gestion des risques

L'établissement de contrôles de la confidentialité doit avoir lieu dès l'étape de l'acceptation de la mission par le client. Peut-être certains clients préfèrent-ils que les documents qu'ils reçoivent par courriel ne soient pas chiffrés, car ils trouvent cela plus pratique, mais ils devraient être informés des risques que cela pose. Les praticiens devraient inclure dans leur lettre de mission standard un paragraphe informant le client que les fichiers envoyés sans chiffrement peuvent être interceptés.

Au sein du cabinet, un programme complet de sensibilisation à la sécurité et à la protection des renseignements personnels devrait être mis en place afin que tous les membres du personnel qui ont accès aux systèmes du cabinet (personnel administratif, personnel professionnel, cadres, associés, contractuels, etc.) reçoivent une formation au sujet des cyber-risques associés aux courriels. Les membres du personnel devraient être informés, au moyen de séances de sensibilisation, d'avis, etc., de l'interdiction de transmettre par courriel des informations permettant d'identifier une personne (par exemple, des numéros d'assurance sociale) ou d'autres informations sensibles. Ils devraient également connaître les meilleures pratiques en matière de correspondance par courriel. Par exemple, ils devraient vérifier, avant de procéder à un envoi, s'il s'agit bien du bon document, du bon destinataire, et s'il n'y a pas de risque de transmettre involontairement des renseignements confidentiels à une personne ou entité autre que le destinataire. Il existe des outils de prévention des pertes de données pouvant être branchés aux systèmes de courriel afin de prévenir la divulgation accidentelle de types particuliers d'informations (par exemple, pour bloquer la transmission de courriels contenant des numéros d'assurance sociale ou de carte de crédit, etc.). Toutefois, les coûts de tels outils sont importants et ne sont peut-être pas à la portée des petits cabinets.

Sécurisation des documents envoyés : quelles sont les possibilités?

Bien que le courriel soit utilisé depuis des décennies, il n'existe toujours pas de norme permettant de sécuriser les échanges de courriels. Par conséquent, pour la profession, le défi consiste à déterminer quelles sont les solutions qui permettent de protéger l'information confidentielle des clients tout en étant faciles à utiliser tant pour le client que pour le cabinet.

Le logiciel de chiffrement PGP (Pretty Good Privacy) pour les courriels

Le logiciel PGP peut être utilisé pour chiffrer la totalité des courriels transmis par le personnel du cabinet à un destinataire. Ce logiciel fait appel à une infrastructure à clés publiques (ICP) pour chiffrer et déchiffrer les courriels. La clé publique du client est utilisée pour chiffrer le courriel et

son contenu, et seul ce client peut déchiffrer le courriel en question en utilisant sa clé privée[3]. Le logiciel de chiffrement PGP peut être installé dans le gestionnaire de courriels Thunderbird[4] ou acheté auprès d'un fournisseur (p. ex. Symantec[5]).

Avantages : Le PGP permet le chiffrement complet des courriels envoyés; le PGP est un protocole bien établi.

Inconvénients : Il faut passablement de travaux d'installation / de configuration pour mettre l'ICP en place (tant pour le cabinet que pour le client); le client peut éprouver des difficultés à déchiffrer les courriels.

Autres considérations : Choix du fournisseur, réputation de l'entreprise, coûts d'implantation, et autres questions liées à l'acquisition de logiciels.

Chiffrement de fichiers

Les logiciels de la suite Office, comme Microsoft Word, Excel et Adobe Acrobat, offrent souvent la possibilité de chiffrer des fichiers individuels. Pour déchiffrer le fichier envoyé, le client doit taper le mot de passe. Les praticiens peuvent aussi utiliser des logiciels de compression des données, comme le logiciel libre «7-zip», qui utilise le chiffrement AES 256 bits, pour transmettre des fichiers de n'importe quel format[6] à leurs clients.

Avantages : Le chiffrement de fichiers est gratuit et facile à utiliser pour le cabinet et pour le client.

Inconvénients : La gestion des mots de passe des clients est très exigeante. Les clients doivent recevoir leurs mots de passe dans un format sécurisé (c.-à-d. par une voie autre que le courriel, comme un texto, ou verbalement, par téléphone). Il peut aussi être nécessaire de réexpédier le fichier ou le mot de passe lorsque le client oublie le mot de passe.

Autres considérations : L'utilisation du numéro d'assurance sociale (NAS) du client comme mot de passe peut éliminer certains problèmes susmentionnés concernant la gestion des mots de passe. Toutefois, le NAS est un élément d'information sensible qui ne convient pas à l'utilisation comme mot de passe puisqu'il ne contient que des valeurs numériques. Il est préférable d'utiliser une phrase passe, qui comprend une combinaison de majuscules et de minuscules, ainsi que des valeurs numériques et des caractères spéciaux.

Services de partage de fichiers

Il y a sur le marché des fournisseurs de logiciels-services (*Software-as-a-Service/SaaS*) qui se chargent de transmettre les fichiers trop gros pour être transmis par courriel. Ces fournisseurs de SaaS peuvent également offrir des services de chiffrement. Par exemple, *yousendit.com* et *sharefile*.com (propriété de Citrix) offrent ces services. Toutefois, les praticiens doivent savoir que comme il s'agit de fournisseurs de SaaS, il faut alors conclure des accords de sous-traitance et, par conséquent, obtenir de ces fournisseurs un rapport fournissant l'assurance que les contrôles pertinents

3 http://searchsecurity.techtarget.com/definition/Pretty-Good-Privacy

4 http://lifehacker.com/180878/how-to-encrypt-your-email

5 http://www.symantec.com/content/en/us/enterprise/fact_sheets/b-pgp_desktop_email_DS_21158806.en-us.pdf

6 http://www.7-zip.org/7z.html

de l'entreprise fonctionnent efficacement. Par exemple, *yousendit.com* indique que ses centres de données font l'objet d'audits de sécurité SOC 2 Type II[7], tandis que ceux de *sharefile.com* font l'objet d'audits SSAE 16[8].

Avantages : Les services de partage de fichiers sont faciles à utiliser pour les praticiens et les clients.

Inconvénients : L'utilisateur dépend d'un tiers pour assurer la sécurité de l'information confidentielle du client. Il est possible d'accéder aux informations concernant le client sans mandat, par application de certaines lois (potentiellement à partir d'un autre pays). Il se peut que les rapports d'audit ne soient pas suffisamment détaillés pour fournir l'assurance dont le praticien a besoin.

Autres considérations : Conservation de sauvegardes locales, meilleures pratiques en matière d'impartition (p. ex. évaluation de la fiabilité du fournisseur, établissement d'ententes sur les niveaux de service, surveillance du service, évaluation des avantages relatifs du logiciel par rapport à d'autres logiciels, etc.).

Portails

Les comptables peuvent également utiliser des portails clients, comme CCH[9], Thomson Reuters[10] et d'autres[11,12]. Ces portails fournissent des sites réservés que les praticiens peuvent utiliser pour y télécharger des fichiers auxquels seul le client peut accéder. Le client peut télécharger les fichiers sur son ordinateur en toute sécurité à partir du site. Ces services, comme les services de partage de fichiers susmentionnés, sont des services fondés sur les SaaS. Par conséquent, les praticiens doivent faire affaire avec des entreprises réputées qui peuvent fournir un rapport d'audit à l'égard de leurs contrôles. Les cabinets peuvent tenir leurs propres portails, comme celui qui est offert par DOC. IT[13], mais cela exige que le cabinet ait accès à du personnel de soutien informatique pouvant maintenir et sécuriser adéquatement le serveur (p. ex. lui apporter les correctifs nécessaires, le protéger des virus et des accès non autorisés, en renforcer la sécurité, etc.).

Avantages : Les portails sont faciles à utiliser. Ils sont conçus pour être utilisés par les comptables et leurs clients.

Inconvénients : Les mises à jour sont potentiellement difficiles à effectuer (p. ex. certains portails ne contiennent pas de fonctions de maintenance, comme la possibilité de supprimer massivement des données concernant des personnes ou des entités qui ne sont plus clientes du cabinet).

7 http://www.yousendit.com/security-overview

8 http://www.sharefile.com/industries/Business/security.aspx?src=unknown&v=e&cat=1

9 http://www.cch.ca/suitecomptable/index.aspx?tid=140

10 cs.thomsonreuters.com/portals

11 L'article posté à l'adresse http://www.journalofaccountancy.com/Issues/2010/Feb/20092359.htm indique d'autres fournisseurs qui offrent ce service.

12 Avertissement—Ces exemples sont fournis à titre d'illustration seulement. L'ICCA et les auteurs du présent document n'ont effectué aucun contrôle diligent relativement à ces fournisseurs et ne soutiennent, implicitement ou explicitement, aucun fournisseur ou service mentionné dans le présent document.

13 http://www.doc-it.com/phocadownload/productinformation/docitportal.pdf

Autres considérations : Meilleures pratiques en matière d'impartition (mentionnées plus haut), besoin de ressources pour la maintenance/sécurisation des logiciels et du matériel sur place, compromis entre le coût et la facilité d'utilisation (p. ex. les solutions plus coûteuses peuvent nécessiter moins de travail ou de ressources).

Au sujet des auteurs

Malik Datardina, CA, CISA, est consultant indépendant en matière de risques informatiques et en certification de systèmes d'information. Spécialisé en gouvernance de la sécurité de l'information et en analyse de données, il agit à titre de conseiller technique auprès du Comité consultatif sur les technologies de l'information de l'ICCA.

Claudiu Popa, CISSP, CIPP, PMP, CISA, CRISC, est conseiller principal en matière de risques et chef de la direction de la société Informatica, un cabinet-conseil établi à Toronto, reconnu pour ses solutions novatrices en matière de protection des données. M. Popa est l'un des principaux consultants au Canada en matière de sécurité et de protection des renseignements personnels. Il est également auteur et agit souvent à titre de personne-ressource auprès des médias pour toutes les questions touchant au cybercrime, à la conformité et aux menaces émergentes pour les renseignements personnels des Canadiens.

Document préparé par le Comité consultatif sur les technologies de l'information de l'ICCA