

## DONNÉES NUMÉRIQUES ET SÉCURITÉ

### INTRODUCTION

C'est un scénario cauchemardesque. La comptable agréée marche dans le stationnement vers son automobile lorsqu'elle remarque, éparpillés sur le sol, les éclats de verre d'une des fenêtres de son véhicule. Le coeur battant, elle appuie sur le bouton de panique de son démarreur à distance, qui active le klaxon et fait clignoter les phares. Elle se précipite vers l'auto et quelques instants plus tard ses craintes sont confirmées : son portatif a disparu.

De tels scénarios se produisent tous les jours partout en Amérique du Nord. Les portatifs sont une cible de choix pour les voleurs en puissance en raison de leur grande valeur, de leur transportabilité et de la difficulté à les retracer. La plupart des voleurs sont intéressés uniquement par la valeur de l'ordinateur. Toutefois, un petit nombre sans cesse croissant de ceux-ci réalise maintenant que les données stockées dans le disque dur peuvent avoir une valeur bien supérieure à celle du portatif lui-même.

Cet article vise la sensibilisation aux problèmes de perte ou de vol d'équipement informatique ou de données numériques. Il aborde les obligations du comptable agréé relativement à la protection de la confidentialité des données des clients, aux stratégies d'atténuation des risques et aux mesures à prendre en cas de vol ou de violation de la sécurité.

### SENSIBILITÉ DES DONNÉES NUMÉRIQUES AU VOL

L'informatisation s'est avérée un outil des plus avantageux pour les comptables. La numérisation des données a permis d'offrir aux clients davantage de services, des analyses plus détaillées et approfondies ainsi qu'une prestation de service accélérée à un moindre coût. Les logiciels spécialisés simplifient la préparation des déclarations d'impôts, des états financiers et des analyses opérationnelles.

La technologie a également permis de libérer les comptables de la paperasse et de réduire la perte de documents et leurs coûts de stockage et de récupération. Au fur et à mesure que les comptables accèdent au bureau électronique, ils peuvent accéder par ordinateur à tous les renseignements pertinents de leurs clients.

Les données numériques ont également permis d'améliorer la mobilité et l'accès. Un comptable peut apporter avec lui les données d'un client dans un portatif ou un disque et être en mesure d'accéder immédiatement à l'information critique au cours de conférences avec le client, de réunions opération-

nelles avec d'autres professionnels et pour répondre aux demandes de renseignements et aux vérifications du gouvernement. Ces données permettent également au comptable de travailler à l'extérieur du bureau.

La numérisation de l'information procure de nombreux avantages mais accroît également l'exposition au vol et à la perte des données. Les données sont alors exposées à différents risques : piratage sur Internet, vol de portatif et élimination inappropriée des supports de stockage.

### OBLIGATIONS DU COMPTABLE

Les comptables ont, au plan éthique, juridique et contractuel, l'obligation de protéger la confidentialité de l'information du client. En vertu des règles de conduite professionnelle qui les gouvernent, ils doivent assurer la plus stricte confidentialité de tout renseignement confidentiel concernant les affaires de leurs clients.

Il existe également une obligation implicite, sinon expresse, pour un comptable d'assurer la confidentialité de l'information obtenue du client dans le cadre de l'exécution de son mandat.

Les comptables sont également assujettis aux lois sur la protection de la vie privée, plus particulièrement à la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) du fédéral ou à toute loi provinciale équivalente. En vertu de la LPRPDE, l'utilisation, la divulgation et la conservation de l'information sont réglementées :

« Les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles auxquelles ils ont été recueillis à moins que la personne concernée n'y consente ou que la loi ne l'exige. » (Principe 4)

L'information financière d'un client est jugée sensible en vertu de la LPRPDE. Le comptable doit donc apporter un soin accru à la protection de cette information contre toute divulgation.

De toute évidence, les comptables ont, au plan éthique, juridique et contractuel, l'obligation de protéger la confidentialité de l'information du client. Les aspects les plus importants sont peut-être ceux qui concernent les activités opérationnelles. Les clients s'attendent de leur comptable qu'il soit intègre et protège leur information financière confidentielle. La réussite de la relation professionnelle et la qualité des conseils que le comptable peut prodiguer sont étroite-

ment liées à la mesure dans laquelle le client se sent à l'aise de divulguer intégralement les renseignements qui le concernent. Toute préoccupation du client relativement à la sécurité de ses données confidentielles est susceptible de compromettre cette divulgation. En outre, toute perte subséquente de données risque de nuire à la relation comptable-client et de mener ultimement à la résiliation du contrat avec celui-ci.

Peu importe le point de vue, la protection et la sécurité de l'information du client sont d'une importance capitale pour le comptable. Malheureusement, dans le tourbillon des activités d'affaires d'aujourd'hui, on n'apporte pas toujours l'attention ou la réflexion appropriée aux problèmes liés à la sécurité des données.

## **ZONES DE SENSIBILITÉ ET MESURES DE PROTECTION**

Les aspects qui suivent sont ceux dont un comptable doit tenir compte pour assurer la protection de l'information numérique des clients :

1. Quiconque a un accès physique au support de stockage peut accéder aux données numériques. Pour assurer la protection des données, on doit envisager l'application de mécanismes tels :

- a. Des mesures de sécurité pour empêcher tout accès non autorisé aux locaux;
- b. Une protection efficace par mot de passe de l'accès aux ordinateurs qui contiennent l'information du client;
- c. Des procédures de sécurité biométriques, telle la lecture des empreintes digitales;
- d. Le chiffrement des données.

2. Les intrus de l'extérieur ne sont pas les seuls qui présentent un danger. Même le personnel et les autres employés qui ont accès aux bureaux peuvent potentiellement accéder aux données du client sans y être autorisés. En plus des mécanismes mentionnés ci-dessus, on doit envisager les mesures suivantes :

- a. Les contrats d'embauche ou les politiques en matière de personnel doivent stipuler clairement les obligations des employés relativement aux données confidentielles du client;
- b. On doit limiter l'accès des employés aux données contenues dans les fichiers auxquels ils ont accès dans le cadre de l'exécution de leur contrat. L'accès à ces fichiers doit leur être retiré à la fin du contrat;
- c. On doit analyser les pistes de vérification de l'accès aux données afin de déterminer s'il y a eu des accès non autorisés ou douteux.

3. Les réseaux dotés de point d'accès extérieurs sont exposés au piratage. On doit envisager l'application des mesures

suivantes :

- a. Utiliser un coupe-feu pour protéger les réseaux contre tout accès externe par Internet;
  - b. Utiliser un mécanisme de contrôle fort de sécurité pour les accès externes aux réseaux, y compris des mots de passe, des restrictions d'accessibilité aux données et un contrôle de la sensibilité des liens de données aux activités de piratage;
  - c. Contrôler l'accès sans fil (technologie Wi-Fi) aux réseaux de bureau;
4. Les portatifs et autres supports sortis des locaux sont exposés aux risques de vol, de perte et de piratage. On doit envisager l'application des mesures suivantes :
- a. Réduire la quantité de données stockées dans les portatifs qui sortent des locaux;
  - b. Prévoir des mesures de protection logicielles ou matérielles pour empêcher le piratage des connexions de données des portatifs ou des ordinateurs lors de l'utilisation d'accès sans fil externe (technologie Wi-Fi);
  - c. Recourir au chiffrement des données;
  - d. Prévoir des protocoles d'utilisation et de stockage des portatifs utilisés hors des locaux.
5. Un aspect de plus en plus préoccupant est l'élimination de dispositifs de vieille technologie qui contiennent des données de client. On doit envisager de recourir aux mesures suivantes :
- a. Protocoles d'élimination de supports qui peuvent contenir des données de client (ne pas oublier les supports utilisés pour la sauvegarde des données);
  - b. Destruction physique des CD-ROM, des disquettes et des disques durs;
  - c. Logiciel d'épuration pour les disques durs transformés, réattribués ou supprimés.

Cette liste n'est nullement exhaustive. Les étapes nécessaires à la protection des données dans les situations mentionnées précédemment sont au-delà de la portée de cet article. Il existe sur Internet une mine d'information qui vous offrira de l'aide pour commencer à régler ces problèmes. La meilleure méthode consiste à engager un conseiller en sécurité qui examinera vos processus, vos systèmes et vos procédures afin de maximiser la sécurité des données de client.

## **QUE FAIRE EN CAS DE VIOLATION?**

Dans le cas de perte d'information ou d'accès inappropriés par des tiers, le comptable est tenu de tout mettre en œuvre pour éviter ou réduire tout préjudice pouvant être causé à son client.

On doit signaler immédiatement à la police le vol d'équipe-

ment ou de support contenant de l'information confidentielle et remplir les rapports appropriés. Le comptable doit déterminer la nature de l'information contenue dans l'ordinateur ou le support et identifier les clients susceptibles de subir des préjudices.

L'agent responsable de la protection de la vie privée du cabinet comptable doit être informé de la situation et suivre les procédures établies initialement par l'entreprise. Ces procédures doivent prévoir d'informer le client dont les données ont été potentiellement compromises. L'agent doit intervenir le plus tôt possible afin de réduire le risque de perte découlant du vol d'identité du client ou de toute autre utilisation abusive de ses renseignements. Cette situation est particulièrement préoccupante lorsque les données en question incluent des numéros d'assurance sociale, de l'information bancaire, de l'information permettant d'identifier des actifs spécifiques, des enregistrements de sécurité ou la signature numérique du client.

On doit indiquer au client la nature exacte de l'information perdue ou volée afin de lui permettre de prendre les mesures appropriées pour se protéger dans la mesure du possible.

On conviendra que les communications avec les clients dans de telles circonstances peuvent être embarrassantes pour le comptable. Toutefois, elles sont incontournables si l'on veut minimiser les risques d'exposition du client. La perspective de devoir éventuellement communiquer avec le client dans un tel contexte devrait inciter davantage le comptable à assurer au départ la sûreté et la sécurité des données confidentielles. Cela est particulièrement motivant si l'on tient compte du grand nombre de clients différents qui conservent leurs données dans un portatif spécifique.

Les entreprises doivent prévoir un plan d'intervention en cas d'incidents semblable au modèle proposé par l'ICCA.

### **RISQUES LIÉS À LA RESPONSABILITÉ DES DONNÉES DE CLIENT**

En cas de perte ou de vol d'information, le comptable s'expose à beaucoup plus qu'au simple embarras de devoir en informer le client. Il peut éventuellement être tenu responsable de tout préjudice découlant de cette perte.

Pour définir la responsabilité, les tribunaux devront établir s'il y a eu faute professionnelle ou violation de contrat de la part du comptable. La responsabilité du comptable sera décrite en fonction des règles éthiques, de la LPRPDE, ou de toute autre loi provinciale similaire, et des obligations de common law relatives aux renseignements confidentiels. Si le comptable n'a pas pris de mesures raisonnables pour assurer la sécurité et la confidentialité des données, il sera tenu responsable des préjudices causés par la divulgation de l'information. Les préjudices dont il est question incluent les pertes découlant du vol d'identité, les coûts encourus par le

client pour réduire son exposition au vol d'identité ou à l'utilisation abusive de l'information usurpée, ainsi que tout bouleversement émotif ou embarras entraîné par la divulgation.

Le Commissaire à la protection de la vie privée du Canada a déterminé qu'une entreprise dont l'ordinateur a été volé dans l'automobile d'un de ses employés contrevenait aux dispositions de la LPRPDE. Dans ce cas précis, il a estimé que l'omission de la compagnie de respecter ses propres lignes directrices en matière de protection et de sécurité de l'information était un facteur important. Effectivement, les directives concernant l'utilisation et la sécurité des portatifs dont s'était dotée l'entreprise n'ont pas été respectées. Cette décision souligne l'importance non seulement de préparer un plan de sécurité mais également de le respecter et de surveiller les employés pour s'assurer qu'ils se conforment aux systèmes mis en place.

Il y a eu un certain nombre de cas hautement médiatisés de divulgation d'information financière confidentielle par des compagnies, des sociétés émettrices de cartes de crédit et des institutions financières qui font face à des revendications liées à la divulgation de ces renseignements. Ces entreprises s'exposent à des revendications, qu'il y ait eu ou non utilisation abusive de l'information du client. Le seul fait que cette information ait pu être potentiellement divulguée à des tiers non autorisés entraîne une possibilité de perte ou d'embarras.

### **CONCLUSION**

Les comptables manipulent quotidiennement les données sensibles de leurs clients. Ils sont tenus, au plan éthique, juridique et contractuel, de faire en sorte d'assurer la confidentialité de cette information. Ils doivent prendre des mesures pour s'assurer de conserver en lieu sûr les données du client, particulièrement les données numérisées. Cette obligation exige la mise en place de mesures de sécurité, de procédures de bureau et de systèmes appropriés. Elle requiert également que le système fasse l'objet d'une vérification de conformité et qu'il soit modifié de manière à tenir compte de l'évolution de la technologie.

La sécurité de l'information de votre client et le maintien d'une bonne relation professionnelle exige d'apporter soin et vigilance à la protection de la confidentialité de ses données.

### **À PROPOS DE L'AUTEUR**

Michael E. Girard est conseiller principal au cabinet Girard Law Office. Il est diplômé de l'Université de Windsor (1983) et a été admis à l'Association du Barreau de l'Ontario (1985). Il a complété une Maîtrise en droit (Osgoode 1998) et présenté une thèse intitulée *CyberConflicts: Jurisdiction and Choice of Law for Internet Transactions*. Sa pratique est axée sur les responsabilités professionnelles des comptables et les questions touchant la discipline, les ordinateurs et la

technologie. M. Girard a rédigé des articles et tenu des conférences sur des sujets tels la technologie, la responsabilité professionnelle, la promotion des droits et la loi sur les assurances. Il est un ex-membre de la Faculty of Computer

Education du Barreau du Haut-Canada. M. Girard est l'avocat principal du premier recours collectif lié à la loi sur la protection de la vie privée au Canada.

## RETOUR SUR L'ARTICLE « PÉNALITÉS ADMINISTRATIVES IMPOSÉES À DES TIERS »

Dans son article « Pénalités administratives imposées à des tiers : Position fiscale agressive, Faux énoncé ou exercice normal de la profession? », Keith Trussler indique que l'ICAO a refusé d'éclaircir sa position concernant l'effet de la règle de conduite professionnelle no 208. Cette déclaration exige d'autres éclaircissements et un autre contexte. L'ICAO offre effectivement des conseils à ses membres de deux manières différentes :

1) On offre aux membres (incluant ceux qui exercent la profession d'expert-comptable) un service consultatif téléphonique d'aide gratuit qui leur permet d'obtenir de l'information sur la comptabilité, les questions d'assurance et de déclaration, les préoccupations en matière de gestion des pratiques et les questions éthiques relatives aux règles de conduite professionnelle (telle la règle 208 concernant la con-

fidentialité). Les sujets sont abordés de manière informelle et les commentaires sont de nature générale. Ce service traite plus de 3 000 appels chaque année. Toutefois, chaque membre de l'Institut est responsable de s'assurer que sa propre situation est conforme aux règles et règlements. Pour les questions d'ordre juridique, on recommande aux membres de communiquer avec leur propre conseiller juridique; et

2) On conseille aux membres qui requièrent une réponse officielle concernant des situations d'ordre éthique qui les concernent de communiquer avec le comité de conduite professionnelle et de fournir par écrit les détails spécifiques de la situation. Toutefois, le comité ne donnera pas suite aux demandes « anonymes » telle celle présentée dans la situation décrite par Keith Trussler.

*Si vous préférez recevoir les futures publications de ce bulletin par courrier électronique, veuillez nous faire parvenir une note à l'adresse suivante : [carm@aica.ca](mailto:carm@aica.ca). Nous vous invitons à visiter notre site ([www.aica.ca/fr/carm\\_newsletters.aspx](http://www.aica.ca/fr/carm_newsletters.aspx)) pour consulter les numéros antérieurs de notre Bulletin de CARM et obtenir les liens d'autres outils de gestion.*

### VOTRE COMITÉ D'ASSURANCE-RESPONSABILITÉ PROFESSIONNELLE

Afin de communiquer avec votre représentant du CARP, contacter les SACA inc.

**Président** Phillip Gaunce, CA  
Halifax, NS

#### Les membres du comité

Robert Boisjoli, CA                      Gregg Clifton, CA                      Robin Elliott, FCA  
Montreal, QC                              Toronto, ON                              Vancouver, BC

Mark Gray, LLB, CA

Douglas Mundell, FCA

### Pour de plus amples renseignements :

Les SACA inc.  
277, rue Wellington Ouest, bureau 702  
Toronto (Ontario)  
M5V 3H2

#### Numéros sans frais:

Anglais: 1-800-267-4734  
Français: 1-800-268-2630  
Télécopie: (416) 204-3418

Courriel : [services@aica.ca](mailto:services@aica.ca)

CARM (Conseils de l'assurance responsabilité pour les membres) est un bulletin d'information publié par les SACA Inc. pour les membres souscripteurs au régime d'assurance responsabilité professionnelle. Il s'adresse aux membres de l'ICCA assurés en vertu du programme d'assurance-responsabilité professionnelle; il vise à attirer l'attention des membres sur la prévention des sinistres et la gestion du risque dans l'exercice de leurs activités professionnelles.

Le bulletin CARM traite de façon concise un certain nombre de questions complexes. Il est recommandé au lecteur de faire appel à des professionnels de la comptabilité, du droit ou de toute autre discipline pertinente avant de poser quelque geste que ce soit sur la seule foi des renseignements contenus dans ce bulletin. Bien qu'on ait déployé tous les efforts raisonnables pour s'assurer de l'exactitude des informations énoncées dans ce bulletin, aucun individu ni organisme ayant participé à la préparation ou à la distribution du bulletin n'accepte d'être tenu responsable, sur le plan contractuel ou délictuel, de son contenu ou des conséquences découlant de son utilisation. Editrice - Kathleen Aldridge.