

Titre de la séance : Pratiques exemplaires en matière de protection des données sensibles et de réaction aux violations de la vie privée

Animateurs/Panélistes :

Jonathan Batty, Directeur de la conformité et avocat, Élections Ontario

Beth DeWitt gestionnaire du service aux entreprises et chef du personnel, Gestion des risques technologiques, Deloitte

Boris Perron, Analyste-Enquêteur, Commission d'accès à l'information du Québec

Patricia Kosseim avocate générale principale, Commissariat à la protection de la vie privée du Canada

Peter Gzowski directeur général adjoint des élections, Élections Nouvelle-Écosse

Date et heure : Mardi le 10 décembre, 13 h 45

Rapporteur : Rosalie Readman

Résumé de la séance

La séance a débuté par une discussion générale portant sur les cas d'atteinte à la vie privée et l'attention médiatique qu'ils génèrent, ainsi que sur la question de savoir si l'adoption de nouvelles technologies par les organisations accroît les risques auxquels elles s'exposent.

Les organisations doivent placer la protection des renseignements au cœur de leur réflexion s'ils veulent être aptes à gérer d'éventuelles situations critiques en termes de perte de renseignements. Selon les témoignages du panel de discussion, la préparation et l'anticipation sont la clé du succès en terme de protection des données sensibles. Les organismes doivent se préparer soigneusement à ce genre de possibilité. Bien entendu, il est important d'établir des processus permettant de minimiser les risques de pertes d'informations, mais cela n'est pas suffisant. Les organismes doivent également préparer des processus de gestion de pertes de renseignements pour contrôler la situation, limiter les dommages et réussir à préserver la confiance du public.

En termes d'évolution dans le domaine de la protection des données sensibles, les panélistes soulignaient une tendance vers l'instauration d'une divulgation obligatoire en cas de pertes (ce processus est actuellement volontaire au niveau fédéral au Canada). Les panélistes ont également remarqué chez les citoyens un grand souci pour la préservation de la vie privée bien que ces derniers aient un taux de confiance mitigé envers les institutions et leur capacité à parvenir à cet objectif.

Il a été soulevé dans cette discussion que les cas d'atteinte à la vie privée se produisent souvent dans des contextes où les organisations entreprennent des projets temporaires, en dehors de leurs activités régulières.

En ce qui a trait à la préparation de processus permettant de gérer la perte de renseignement confidentielle, une panéliste a présenté un plan d'action très

complet, en quatre étapes. Dans un premier temps, il faut être en mesure de freiner l'hémorragie, savoir qui s'occupera de l'enquête et penser à qui devra être au courant de la fuite à l'interne. Dans un deuxième temps, il faut faire un état des lieux pour connaître l'ampleur et la nature de la violation et anticiper les impacts sur les personnes affectées par cette perte. Ceci peut par exemple nécessiter la collaboration de spécialistes d'enquête.

Dans un troisième temps, il est nécessaire de prévoir de quelle façon et quand seront averties les personnes visées par la perte. Sera-t-il question d'une diffusion dans les médias ou d'un processus plus individualisé, par exemple? Les personnes visées devraient-elles être informées rapidement? Quelles actions devrait-on leur dire d'entreprendre? Y a-t-il d'autres personnes de l'externe qui doivent être informées, telles qu'un Commissaire de protection à la vie privée ou les autorités policières?

Dans un quatrième temps, il faut réexaminer les systèmes et les processus initialement prévus en termes de protection des renseignements pour apporter les correctifs et prévoir d'autres fuites.

Les panélistes ont aussi soulevé qu'il peut être utile de contacter les différentes agences et commissions à qui incombe, dans le cadre de leur compétence, la protection de la vie privée dans le but d'obtenir des conseils au sujet des procédures et des meilleures pratiques.

Finalement, les panélistes ont également fait ressortir l'importance de la pratique des processus instaurés en matière gestion de pertes de renseignements. En ce sens, une simulation permettra de réellement mettre à l'épreuve la préparation de la mise en place et d'identifier les ressources avec lesquelles travailler tant à l'intérieur de l'organisme en cause que chez les organismes régulateurs en matière de protection des renseignements.

Par-dessus tout, il est ressorti de la séance que la meilleure façon de se prémunir contre les cas d'atteinte à la vie privée est d'inclure des principes de respect de la vie privée dès la conception des processus où seront traitées des informations. Pour les organisations, l'implantation de tels principes s'avère rentable sachant que la résolution des cas d'atteinte à la vie privée est souvent coûteuse en temps comme en ressources. Enfin, hormis ces soucis matériels, les panélistes ont discuté des importantes conséquences négatives que peuvent générer de tels cas sur le moral d'une agence ainsi que sur la confiance que porte le public à son travail.

Les participants ont également échangé au sujet des organismes auxquels peuvent s'adresser les citoyens afin de bénéficier de services de surveillance en matière de crédit et de vol d'identité. En voici quelques exemples :

Equifax – www.consumer.equifax.ca
All Clear – [www. Allclearid.com](http://www.Allclearid.com) (USA)
Experian – www.experian.com (USA)