

Avis de sécurité

Client : Gestionnaire de XYZ

Participants : Cet avis à été rédigé par René W. Vergé Avocat et Christophe Jolivet avec l'aimable participation de Patrick Boucher et Dominique Dubé.

Date de la demande : 27 mai 2011

Date de l'avis : 12 juillet 2011

Priorité : 3 (basse)

Demande n° : 03-2011

Objet : **Doit-on permettre l'utilisation de www.Dropbox.com aux employés de XYZ?**

Demande/Contexte

www.Dropbox.com est un service de stockage et de partage de fichiers en ligne (photos, vidéos, fichiers de tout format) proposé par Dropbox Inc. sur Internet.

Par ailleurs, Dropbox :

- permet la synchronisation des fichiers stockés sur différents ordinateurs;
- fonctionne de manière transparente (les sauvegardes et synchronisations sont automatiques);
- le site web permet d'accéder à une copie des fichiers, mais également à leurs versions successives et à une copie des fichiers détruits.

La version gratuite permet de stocker jusqu'à 2 Go de données, extensibles à 10 Go grâce au parrainage (2 Go + 8 Go à raison de 250 Mo par parrainage); le filleul reçoit lui aussi 250 Mo, et des versions payantes permettent de stocker 50 ou 100 Go.

On découvre également que « *Pour aller (beaucoup) plus loin dans l'utilisation de Dropbox, rendez-vous sur : <http://wiki.Dropbox.com/> . Vous y apprendrez, entre autres, à personnaliser votre Dropbox, prendre le contrôle de votre PC à distance, synchroniser une clé USB (toujours utile si vous n'avez pas de connexion Internet), synchroniser vos mots de passe, etc. ».*

Objectif et portée

L'objectif est donc d'évaluer les risques associés au fait d'autoriser l'utilisation des services offerts par Dropbox à l'ensemble des employés de XYZ. Nous devons nous assurer que le fait d'autoriser le personnel à utiliser les services de Dropbox ne mette pas en péril la sécurité des informations corporatives et, par le fait même, la réputation de l'organisation.

Problématique

Actuellement, nous ne bloquons pas l'accès aux services de Dropbox dans notre système de filtrage Internet.

Il semblerait que Dropbox ait eu à donner des explications sur sa sécurité auprès de la FTC (Federal Trade Commission)¹. Cette controverse est confirmée par : <http://www.webactus.net/actu/9988-securite-Dropbox/>

¹ <http://www.infos-du-net.com/actualite/18468-Dropbox-Stockage-Securite.html>

Cet avis n'a pas pour but de fournir des conseils techniques, organisationnels et juridiques aux lecteurs. Ces derniers ne devraient pas prendre action sur la foi des renseignements qu'il contient, sans d'abord se faire conseiller à l'égard de leur situation spécifique. Il nous fera plaisir de fournir, sur demande, toute information additionnelle.

En effet, initialement « Tous les fichiers stockés sur Dropbox étaient chiffrés (AES256) et inaccessibles sans mot de passe » est devenu « Tous les fichiers stockés sur Dropbox sont chiffrés (AES256) ». Cela laisse donc penser que désormais, **on peut accéder à nos fichiers sans forcément avoir notre mot de passe** et encore pire, notre accord... puisqu'il est sous-entendu lorsque l'on accepte ces conditions... ».

De plus, son utilisation nécessite d'installer un petit logiciel permettant de faire la synchronisation entre les fichiers locaux (poste de travail de l'employé) et ceux distants (serveurs de Dropbox). Nous ne contrôlons pas ce petit logiciel.

Classification des actifs concernés

Rappelons que les informations corporatives pouvant être déposées chez Dropbox peuvent être de nature stratégique, confidentielle (comprenant des renseignements personnels), car nous n'avons pas les moyens de filtrer le contenu des fichiers transigeant en sortie sur nos liens Internet.

Identification des vulnérabilités

Une mauvaise compréhension par les employés du caractère stratégique et confidentiel (y compris des renseignements personnels) de certains documents corporatifs qu'ils décideraient de déposer sur Dropbox, combinée au niveau faible de sensibilité des employés face à la sécurité de l'information et le fait que Dropbox induirait en erreur ses utilisateurs au sujet de sa sécurité².

Utilisation grandissante pour faciliter le partage de documents des utilisateurs de I-Pad. En effet, n'ayant pas de clé USB, l'une des façons de transférer facilement des documents du réseau à son I-Pad est via Dropbox.

Le 20 juin 2011, Dropbox fait "manchette". En effet, durant quatre heures, le site web [Dropbox ne vérifiait plus vos mots de passe](#). Il était alors possible **d'accéder à n'importe quel compte**.

Source : <http://fr.canoe.ca/techno/internet/archives/2011/06/20110621-132712.html>

Identification des menaces

Les menaces sont directement liées au site web et aux employés exploitant la solution (site web sur lequel nous n'avons malheureusement aucun contrôle). Nous évaluons cette menace comme étant moyenne.

À noter que, pour avoir la fonction de synchronisation, il est nécessaire d'installer un petit logiciel en local sur le poste - logiciel dont on n'a pas le contrôle non plus (code source).

On peut lire également que « **Cela devrait en plus attirer les hackers**³ maintenant qu'ils savent que le service permet de récupérer les fichiers, d'autant plus que Dropbox est de plus en plus utilisé. ». Nous évaluons cette menace comme étant élevée.

Évaluation de la probabilité de risque

Compte tenu que depuis 1 an, le service gagne en popularité, Dropbox sera de plus en plus utilisé et visé comme mentionné précédemment. La probabilité qu'un document corporatif contenant des informations stratégiques ou confidentielles soit déposé sans l'accord de XYZ est élevée, à mesure que le temps passe sans prendre position.

² <http://www.cnetfrance.fr/news/Dropbox-induisait-en-erreur-sur-la-confidentialite-des-donnees-et-le-cryptage-39760824.htm>

³ <http://www.webactus.net/actu/9988-securite-dropbox/>

Cet avis n'a pas pour but de fournir des conseils techniques, organisationnels et juridiques aux lecteurs. Ces derniers ne devraient pas prendre action sur la foi des renseignements qu'il contient, sans d'abord se faire conseiller à l'égard de leur situation spécifique. Il nous fera plaisir de fournir, sur demande, toute information additionnelle.

IDENTIFICATION DES MESURES DE SÉCURITÉ EN PLACE ACTUELLEMENT

D'ORDRE TECHNOLOGIQUE	D'ORDRE ORGANISATIONNEL
Aucune	Le niveau faible des employés au caractère stratégique et confidentiel (comprenant des renseignements confidentiels) de certaines informations corporatives.

Évaluation des risques actuels

Compte tenu du niveau faible de sensibilité au regard de l'information stratégique et confidentielle des employés, de son utilisation grandissante à l'interne, considérant la propriété américaine des serveurs hébergeant le service Dropbox, nous considérons qu'il est probable qu'une divulgation d'information stratégique ou confidentielle puisse se matérialiser par l'utilisation de Dropbox.

On peut noter également que « Christopher Soghoian⁴ a soulevé des questions quant à la sécurité des transactions de l'informatique dans les nuages et a fait valoir que les fournisseurs de services d'informatique dans les nuages ont eu tendance à délaissé les solutions éprouvées en matière de sécurité. Pour appuyer ses arguments, il souligne que les fournisseurs de services d'informatique dans les nuages pourraient (et devraient) à tout le moins utiliser les moyens courants de cryptage utilisés par les banques et les détaillants en ligne pour protéger leurs flux de données, mais que la plupart ne le font pas actuellement. Quant à la sécurité de l'entreposage, comme l'indique Doctorow, si les applications de l'informatique dans les nuages étaient conçues de manière à défendre les intérêts des utilisateurs plutôt que d'accroître l'efficacité des modèles opérationnels, les données seraient massivement cryptées »

...« Dans tous les cas, non seulement les données d'une personne sont à risque dans l'infrastructure d'informatique dans les nuages, mais il est possible que cette personne ne prenne jamais conscience de l'atteinte ».

Aspects légaux :

D'un point de vue légal, afin de déterminer si nous devons permettre ou non l'utilisation de DropBox aux employés de XYZ, les points suivants doivent être pris en considération :

1 - Les lois et les règlements applicables à XYZ

XYZ étant un organisme public provincial, la « Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels » s'applique. Selon l'article 63.1 de cette loi, XYZ doit prendre des mesures de sécurité raisonnables pour assurer la protection des renseignements personnels (RP).

De plus, l'article 70.1 de cette même loi mentionne que l'organisme ne peut communiquer des RP à l'extérieur du Québec à moins que ces derniers bénéficient d'une protection équivalant à celle prévue à la présente loi. Les entreprises privées trouveront l'équivalent à l'article 17 de la « Loi sur la protection des renseignements personnels dans le secteur privé ».

Les articles 6, 25 et 26 de la « Loi concernant le cadre juridique des technologies de l'information » imposent également des obligations, en matière de sécurité des RP, applicables aux organismes publics et privés ainsi qu'aux fournisseurs de services impliqués dans l'utilisation, le traitement, la communication et la conservation des RP en question.

S'il n'en était que de ces articles, XYZ pourrait probablement considérer l'externalisation du stockage et du traitement de ses renseignements personnels à l'extérieur de sa juridiction. Par contre, selon l'article 67.2 de la « Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels », XYZ ne peut communiquer un RP

⁴ http://www.priv.gc.ca/information/pub/cc_201003_f.cfm

à un sous-traitant, sans le consentement de la personne concernée, à moins d'avoir indiqué dans le contrat de sous-traitance certaines obligations spécifiques du sous-traitant.

De plus, selon l'article 63.2 de cette même loi, XYZ doit également mettre en œuvre les mesures édictées par règlement. Selon la section IV du « *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels* », XYZ doit informer son Comité sur l'accès à l'information et la protection des RP de tout système ou service qui conserve des RP. Cette section du règlement mentionne également une série de mesures qui doivent être mises en place dans ces circonstances pour assurer la protection des RP.

Dans le cas de DropBox, XYZ ne conclut pas un contrat d'entreprise avec ce fournisseur de service, dans lequel elle pourrait négocier des clauses particulières concernant la protection des renseignements personnels. Ce sont les employés eux-mêmes qui adhèrent au contrat et ils ne peuvent le modifier. Les exigences imposées par ces articles de loi ne seraient donc pas respectés dans les circonstances, si des documents comportant des RP étaient communiqués et stockés chez DropBox.

2 - La nature des informations

Qu'en est-il des autres types d'informations (information stratégique, administrative, opérationnelle ou autres)? Rien dans la législation canadienne et québécoise n'interdit de façon générale l'externalisation de la communication, du stockage et du traitement de l'information des organisations publiques ou privées, à l'extérieur du Québec ou du Canada, en autant que des mesures de sécurité adéquates ou équivalentes soient mises en place.

Par contre, compte tenu de la nature des opérations de XYZ, il est fort probable que des RP se retrouvent dans une multitude de documents, sinon la majorité des documents traités par XYZ. Donc, même en permettant uniquement le stockage d'information ne contenant pas des RP, le risque est quand même très élevé que des RP se retrouvent stockés chez DropBox.

3 - Le contrat présentement conclu

Comme la plupart des contrats sur Internet, par le biais desquels on s'engage avec un simple clic, nous sommes en présence d'un contrat d'adhésion. Dans un contrat d'adhésion, les termes du contrat sont imposés par une partie à l'autre. Dans notre cas, DropBox impose ses termes à l'utilisateur et ce dernier ne peut que les accepter ou refuser d'adhérer au service.

À l'heure actuelle, les contrats avec DropBox sont conclus personnellement par des individus qui n'ont pas nécessairement l'autorisation de conclure un contrat, au nom de XYZ, à l'insu de cette dernière. Bien entendu, la situation serait différente si un contrat d'entreprise était conclu directement entre XYZ et DropBox. XYZ aurait alors exprimée sa volonté d'externaliser ses données chez ce fournisseur de services et serait consciente de ses droits et obligations et des risques qu'elle encourt.

4 - La législation applicable aux données stockées chez DropBox

L'externalisation du stockage de données aux États-Unis soulève beaucoup de controverse et d'hésitation. Cela est dû en partie par la multitude de lois fédérales et étatiques concernant la vie privée, la divulgation en cas d'incident et les exigences en matière de sécurité, peut importe où se trouvent les données. Les données ne reçoivent pas le même niveau de protection si elles sont stockées sur un poste de travail, sur un serveur chez un fournisseur de services ou en transit entre les deux. De plus, ces lois ont souvent reçu des interprétations différentes et parfois inconsistantes par les tribunaux.

Par contre, notons que l'article 17 de la « *Loi sur la protection des renseignements personnels dans le secteur privé* », ainsi que l'article 70.1 de la « *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements*

Cet avis n'a pas pour but de fournir des conseils techniques, organisationnels et juridiques aux lecteurs. Ces derniers ne devraient pas prendre action sur la foi des renseignements qu'il contient, sans d'abord se faire conseiller à l'égard de leur situation spécifique. Il nous fera plaisir de fournir, sur demande, toute information additionnelle.

personnels » ne doivent pas être interprétés de façon à interdire l'externalisation de services à l'étranger, même si elle inclut la communication de RP, sujet à l'application des lois de la juridiction hôte. L'important étant de s'assurer que des mesures de sécurité adéquates et équivalentes sont mises en œuvre pour assurer la protection des RP confiés au fournisseur de service.

5 - La sécurité de l'environnement et des données chez DropBox

Étant donné que les services de DropBox sont offerts par le biais de la nuagique (*cloud computing*), et que cet environnement n'est pas accessible, la façon d'évaluer l'existence de mesures de sécurité adéquates est par le biais du contrat conclu avec DropBox. Une analyse détaillée de ce contrat, en date du mois de juin 2011, révèle que les mesures de sécurité suivantes doivent être déployées par DropBox:

- Chiffrement des données sur les serveurs (AES-256);
- Chiffrement des données en transit (SSL) entre le poste de travail de l'utilisateur et les serveurs de DropBox et vice-versa;
- Contrôle d'accès à trois niveaux (utilisateur, invités et public);
- Utilisation d'Amazon S3 pour le stockage de données (répartition dans plusieurs centres de données et sécurité physique des sites de niveau militaire);
- Protection contre les problèmes de sécurité réseau (DDOS, HDM et reniflage de paquets, etc.) chez DropBox et Amazon;
- Copies de sauvegarde redondantes des données dans plusieurs sites;
- Les employés de DropBox ont uniquement l'autorisation d'accéder aux métadonnées (noms de fichiers et emplacements), pas au contenu des fichiers eux-mêmes;
- Les informations contenues dans le profil de l'utilisateur ne sont utilisées qu'à des fins de support, de maintenance et d'amélioration des services et leur confidentialité est maintenu en tout temps;
- L'utilisateur peut également utiliser sa propre application pour chiffrer ses données sur les serveurs de DropBox.

Il est également important de noter les termes suivants présents au contrat de DropBox :

- DropBox ne revendique aucun droit de propriété sur les données stockées sur ses serveurs;
- DropBox n'a aucune obligation de surveiller l'utilisation du site, des services, du contenu et des fichiers, mais peut le faire pour la bonne marche du site, pour s'assurer du respect des conditions d'utilisation, pour se conformer à la législation en vigueur ou pour satisfaire l'exigence d'un tribunal ou d'une organisation gouvernementale;
- DropBox n'est pas responsable des activités effectuées à l'aide du mot de passe de l'utilisateur, autorisées ou non;
- DropBox n'est responsable d'aucune façon de la fidélité, exhaustivité, justesse, légalité, ou applicabilité des données stockées sur ses serveurs;
- Les services de DropBox sont proposés tels quels, sans garantie, et DropBox n'est responsable d'aucune façon des dommages causés ou de la perte de données découlant de l'utilisation du site;
- DropBox peut mettre fin aux services ou au compte d'un utilisateur en tout temps, avec ou sans justification et préavis;
- DropBox peut supprimer sans préavis les fichiers d'un compte gratuit inactif pendant 90 jours.

Conclusion légale

Cet avis n'a pas pour but de fournir des conseils techniques, organisationnels et juridiques aux lecteurs. Ces derniers ne devraient pas prendre action sur la foi des renseignements qu'il contient, sans d'abord se faire conseiller à l'égard de leur situation spécifique. Il nous fera plaisir de fournir, sur demande, toute information additionnelle.

Mêmes si les mesures de sécurité mises de l'avant par DropBox sont adéquates, voir supérieures à celles utilisées par la majorité des organisations, les 3 premiers points nous portent à conclure que XYZ ne devrait pas permettre, à l'heure actuelle, le stockage de son information chez DropBox, tant pour les renseignements personnels que pour les autres types d'informations.

En fait, l'efficacité de ce genre d'interdiction repose grandement sur la sensibilisation et la responsabilisation du personnel de XYZ. Que ce soit simplement par inadvertance ou de façon intentionnelle, il existe une multitude de façons de transmettre de l'information sensible à l'extérieure de l'organisation.

Le jour où XYZ décidera d'offrir à ses employés la possibilité d'utiliser un tel service, elle devrait négocier elle-même un contrat avec le fournisseur en s'assurant que les conditions et les mesures appropriées sont prévues.

1. Recommandations générales

Considérant que l'ensemble des employés sont très peu sensibilisés au fait de ne déposer aucune information corporative ailleurs que sur le réseau interne dans leurs répertoires de travail sécurisés;

Considérant le contournement possible aux règles;

Considérant les lois provinciales et canadiennes concernant la protection des renseignements personnels auxquelles XYZ doit se conformer et;

Considérant les termes de sa politique de sécurité, **nous recommandons de ne pas autoriser l'utilisation de www.Dropbox.com. Cette restriction ne devrait pas s'appliquer uniquement à DropBox, mais à tous les services semblables de stockage de fichiers en ligne, peu importe leur emplacement géographique.**

1.1. RECOMMANDATIONS SPÉCIFIQUES - MESURES ADDITIONNELLES

De manière plus spécifique, et afin d'atténuer au maximum les risques, nous recommandons :

D'ORDRE TECHNOLOGIQUE	D'ORDRE ORGANISATIONNEL
De bloquer dans notre système de filtrage Web le type de service Cloud auquel Dropbox appartient.	Nous recommandons de sensibiliser (via un communiqué) l'ensemble des employés à ne pas utiliser d'autres sites de partage gratuit de fichiers, en rappelant qu'il est strictement interdit de téléverser ⁵ des fichiers corporatifs, quel que soit leur niveau de classification du document sur des infrastructures n'appartenant pas à XYZ.

ÉVALUATION DES RISQUES RÉSIDUELS

Compte tenu des vulnérabilités et menaces identifiées, nous considérons que les risques résiduels seront faibles, dans le cas où sont mises en place les mesures additionnelles recommandées ci-dessus.

1.2. MESURES COMPENSATOIRES

Dans la mesure où XYZ souhaite vraiment utiliser Dropbox, nous recommandons :

D'ORDRE TECHNOLOGIQUE	D'ORDRE ORGANISATIONNEL
Faire apparaître une fenêtre informant l'utilisateur qu'il est	Nous recommandons de sensibiliser (via un communiqué)

⁵ http://www.granddictionnaire.com/BTML/FRA/r_Motclef/index800_1.asp

Cet avis n'a pas pour but de fournir des conseils techniques, organisationnels et juridiques aux lecteurs. Ces derniers ne devraient pas prendre action sur la foi des renseignements qu'il contient, sans d'abord se faire conseiller à l'égard de leur situation spécifique. Il nous fera plaisir de fournir, sur demande, toute information additionnelle.

<p>interdit d'exporter des informations corporatives et qu'il est aussi interdit de transmettre des renseignements personnels en dehors du réseau.</p> <p>Lui indiquer que les données corporatives doivent être alors chiffrées à l'aide d'un logiciel tel Truecrypt avant d'être téléchargées vers Dropbox.</p> <p>Mettre un contrôle en place des utilisateurs pour cibler la sensibilisation par service et direction.</p>	<p>l'ensemble des employés à ne pas utiliser ce type de service, sauf en cas de grande nécessité, en rappelant qu'il est strictement interdit de téléverser des fichiers corporatifs sensibles sur des infrastructures n'appartenant pas à XYZ.</p> <p>S'assurer que la haute direction de XYZ accepte ou négocie (si possible) les conditions d'utilisation de Dropbox pour ses employés dans le cadre de leur travail.</p> <p>S'assurer que les usagers acceptent les conditions d'utilisation de Dropbox.</p>
--	---

ÉVALUATION DES RISQUES RÉSIDUELS DANS LE CAS DE LA MISE EN PLACE DES MESURES COMPENSATOIRES

Compte tenu des vulnérabilités et menaces identifiées, nous considérons que les risques résiduels seront moyens, dans le cas où sont mises en place les mesures compensatoires en force.

Cet avis n'a pas pour but de fournir des conseils techniques, organisationnels et juridiques aux lecteurs. Ces derniers ne devraient pas prendre action sur la foi des renseignements qu'il contient, sans d'abord se faire conseiller à l'égard de leur situation spécifique. Il nous fera plaisir de fournir, sur demande, toute information additionnelle.