PASSION AFFAIRES et technologies

Nous aidons les entreprises à transformer leurs technologies en levier d'affaires

ARS solutions 25 ans

Septembre 2017
Vol. 4 n° 7.

LES ENTENTES DE CONFIDENTIALITÉ ET DE NON-DIVULGATION

Comment protéger les informations confidentielles de l'entreprise ?

TEMPS DE LECTURE 3:30

Par Marie-Josée Lortie
Avocate, Joli-Coeur Lacasse
418 681-7007

Dans le cadre de leurs divers projets, les entreprises emploient couramment les ententes de confidentialité et de non-divulgation. En quoi consistent ces ententes et sont-elles vraiment efficaces ?

L'objet d'une entente de confidentialité et de non-divulgation est de protéger l'information confidentielle qu'une entreprise s'apprête à divulguer à une personne ou entreprise dans le cadre d'un projet d'affaires. Elle peut s'adresser à un partenaire d'affaires potentiel, à un employé, à un financier, bref, à toute personne avec qui une entreprise désire établir une relation commerciale. Cette divulgation d'informations confidentielles peut survenir à tout moment dans le cadre de négociations. Cependant, **il est prudent de penser à ce genre d'engagement dès le début de négociations avec quiconque**. Mais surtout, même si cela semble une évidence, avant de divulguer telle information.

INFORMATION CONFIDENTIELLE

L'information confidentielle est généralement de l'information qui donne une valeur au projet pour lequel elle est divulguée. Elle a une valeur intrinsèque et son utilisation non autorisée peut mettre en péril l'entreprise. Elle peut inclure des **données financières, des listes de clients ou de fournisseurs, des données techniques ou autres** qui appartiennent à l'entreprise. Il peut aussi s'agir de la propriété intellectuelle de l'organisation telle que des inventions protégées ou non par un brevet, des **connaissances**, des **procédés et autres droits intangibles**. Dans le cadre de l'acquisition d'une entreprise, elle peut couvrir une grande variété d'informations alors que dans le cadre de la vente d'un logiciel, cette information sera plus limitée. C'est pourquoi c'est une excellente raison d'avoir recours à des moyens qui vous permettront de la protéger.

SUITE À LA PAGE 2 ▼

« Dans nos rencontres d'équipe, j'ai instauré la *minute informatique*, ce qui me permet de sensibiliser notre personnel à la sécurité informatique.

De nos jours, la cybercriminalité est une réalité et nous n'avons pas d'autre choix que de nous protéger.

Je consulte toutes les informations qu'ARS m'envoie, comme les bulletins et les rapports. Par la suite, je transmets aux employés les informations pertinentes pour les sensibiliser. Ils sont de plus en plus habiles à détecter les courriels frauduleux ou représentant un risque pour la sécurité de nos systèmes.

Ce sont de bonnes habitudes que nous n'avons plus le choix de combiner à une bonne protection antivirus et antipourriel ainsi qu'à une solution de sauvegarde et de relève robuste comme celle d'ARS. »

Louyse Trudel

Agente d'administration à la direction générale, AQCS

Suivez-nous

SUITE DE LA PAGE 1 ▲

OBLIGATIONS DE CONFIDENTIALITÉ ET DE NON-DIVULGATION

Les obligations de confidentialité et non-divulgation seront plus ou moins étendues selon le projet visé. Habituellement, la partie qui reçoit l'information doit la protéger afin qu'elle ne soit pas diffusée ou transmise ou même utilisée pour une fin autre que le projet pour lequel elle est divulguée. **On prévoira souvent que la personne qui reçoit l'information ne pourra y donner accès qu'à un utilisateur qui aura été informé du caractère confidentiel de l'information et qui aura consenti à respecter ce caractère.** Idéalement, on prévoira que toute autre personne ayant accès à l'information confidentielle devra elle-même avoir signé un engagement de confidentialité et de non-divulgation. Cette mesure vise à éviter les fuites et à informer toutes les personnes qui auront accès à cette information qu'elle appartient à un tiers et qu'on ne peut en faire n'importe quoi.

UNE ENTENTE ADÉQUATE

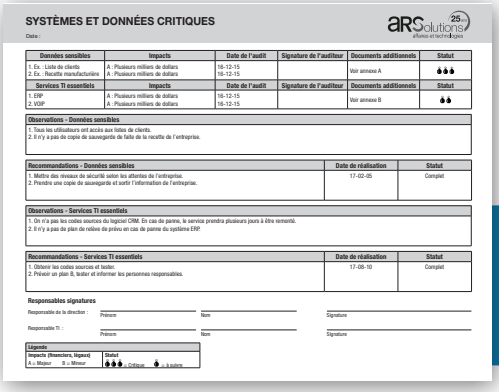
Il importe de rédiger un engagement de confidentialité de façon adéquate en tenant compte du projet pour lequel l'information sera divulguée. Avant d'entreprendre la rédaction d'un tel engagement, il faudrait d'abord se poser les questions suivantes :

- Pour quelles fins l'information doit-elle être divulguée ?
- Quelles informations nécessitent d'être protégées ?
- Pourquoi cette information doit-elle être protégée ?
- Contre qui ou quoi, doit-elle être protégée ?
- Pendant combien de temps l'information doit-elle objectivement être protégée ?

Les engagements de confidentialité et de non-divulgation sont usuels et il ne faut pas en sous-estimer l'utilité. Mais ils doivent être traités sérieusement. Leur efficacité dépendra non seulement de la rédaction qui en est faite, mais aussi des agissements de l'entreprise qui l'utilise.

Quand on dit que l'information c'est le pouvoir, c'est d'autant plus vrai que c'est la valeur de votre entreprise qui peut être en jeu.

Pour consulter l'article intégral, rendez-vous sur notre blogue *Passion affaires et technologies !* ars-solutions.ca/blogue


SYSTÈMES ET DONNÉES CRITIQUES

ARS Solutions affaires et technologies 25

Date :

Données sensibles	Impacts	Date de l'audit	Signature de l'auditeur	Documents additionnels	Statut
1. Ex. : Liste de clients 2. Ex. : Recette manufacturière	A - Plusieurs milliers de dollars A - Plusieurs milliers de dollars	16-12-15 16-12-15		Voir annexe A	♦♦♦
Services TI essentiels	**Impacts**	**Date de l'audit**	**Signature de l'auditeur**	**Documents additionnels**	**Statut**
1. ERP 2. VOIP	A - Plusieurs milliers de dollars A - Plusieurs milliers de dollars	16-12-15 16-12-15		Voir annexe B	♦♦

Observations - Données sensibles

1. Tous les utilisateurs ont accès aux listes de clients.
2. Il n'y a pas de copie de sauvegarde de faite de la recette de l'entreprise.

Recommandations - Données sensibles	Date de réalisation	Statut
1. Mettre des niveaux de sécurité selon les attentes de l'entreprise. 2. Prendre une copie de sauvegarde et sortir l'information de l'entreprise.	17-02-05	Complet

Observations - Services TI essentiels

1. On n'a pas les codes sources du logiciel CRM. En cas de panne, le service prendra plusieurs jours à être remonté.
2. Il n'y a pas de plan de relève de prévu en cas de panne du système ERP.

Recommandations - Services TI essentiels	Date de réalisation	Statut
1. Obtenir les codes sources et tester. 2. Prévoir un plan B, tester et informer les personnes responsables.	17-08-10	Complet

Responsables signatures

Responsable de la direction : Prénom Nom Signature

Responsable TI : Prénom Nom Signature

Légende

Impacts (Financiers, Légaux)	Statut
A = Majeur B = Mineur	♦♦♦ = critique ♦ = à suivre

Un outil stratégique extrêmement efficace pour votre comité de gestion

Ce guide est un document stratégique et non technique qui aborde la sécurité informatique en entreprise. **Comment cibler les informations les plus importantes et évaluer leur niveau de sécurité?**

À l'intérieur se trouve un outil de gestion stratégique extrêmement efficace qui vous sera très utile lors de vos rencontres de direction. Il est basé sur le travail que nous avons effectué avec des entreprises des secteurs manufacturiers et services professionnels de la région. Nous tenons à le partager avec la communauté d'affaires, afin d'encourager de bonnes pratiques et pour améliorer la sécurité des informations en entreprise.

TÉLÉCHARGEZ-LE DÈS MAINTENANT AU WWW.ARS-SOLUTIONS.CA/EASYPREY

Si vous ne pouvez affirmer avec 100 % de certitude que vous avez ciblé les bons éléments à sécuriser dans votre entreprise et qu'ils sont bien protégés, cet exercice est fait pour vous.

Nous rendons les entreprises plus efficaces et performantes en transforman

CYBERSÉCURITÉ : 5 questions essentielles qu'un dirigeant doit se poser

TEMPS DE LECTURE 3:15

La sensibilisation quant aux risques de la cybercriminalité est importante à tous niveaux dans une organisation. La haute direction doit jouer un rôle prédominant dans les discussions portant sur le sujet afin de s'assurer que tous les éléments mis en place pour contrer les cybercrimes soient alignés avec les besoins globaux de l'entreprise. Et comme les dirigeants sont souvent ceux qui approuvent les budgets finaux à l'interne, il est impératif qu'ils comprennent bien les avantages d'une défense proactive contre la cybercriminalité. Voici 5 questions qu'un dirigeant d'entreprise doit se poser afin de prévenir ce qui pourrait être évité.

1 Est-ce que la haute direction est informée des impacts de la cybercriminalité dans votre entreprise ?

Dans l'optique de réagir rapidement et de minimiser les dommages d'une cyberattaque, la haute direction doit être bien préparée à y faire face. Assurez-vous qu'elle détienne toutes les informations nécessaires concernant les risques et les impacts qu'implique un tel événement et qu'elle soit en mesure d'exécuter rapidement le plan d'action. Assurez-vous également d'avoir un processus de communication efficace avec les intervenants pour gérer correctement la situation.

2 Quel est le niveau de risque actuel de la cybercriminalité dans votre entreprise ?

Effectuer une évaluation des risques (audit de sécurité) en identifiant les actifs critiques et les impacts associés aux menaces vous aidera à hiérarchiser les mesures de protection et à impliquer les ressources nécessaires. Cette étape est essentielle pour comprendre jusqu'à quel point l'entreprise est exposée à des risques financiers, légaux, d'atteinte à la réputation, etc.

Pour se faire, téléchargez notre canevas « Systèmes et données critiques » au ars-solutions.ca/easyprey. Cet outil stratégique testé sur le terrain vous aidera à cibler les éléments essentiels à sécuriser et à évaluer leur degré de criticité ainsi que l'impact financier associé. Il deviendra un important cadre de référence.

Source : Herjavec group

3 Comment votre procédure en cybersécurité applique-t-elle les normes et les meilleures pratiques de l'industrie ?

Quand il est question d'une procédure de sécurité complète, satisfaire les exigences de conformité n'est pas suffisant face aux nouvelles menaces émergentes ou aux attaques de plus en plus sophistiquées. User des meilleures pratiques de l'industrie tout en mettant en œuvre des exigences de conformité permettra une réponse et une remise sur pied rapidement après un incident.

4 Combien et quel(s) type(s) de cyberincident(s) détectez-vous dans une semaine de travail ? Quel est le délai pour informer la haute direction ?

La détection d'anomalies via l'utilisation d'outils de surveillance assurera la prise en charge et la correction rapide des cyberattaques. **Des communications régulières** entre la haute direction et les responsables de la gestion des attaques permettront de diminuer les risques et les impacts sur l'entreprise. L'organisation devrait recruter des ressources spécialisées en sécurité ou envisager de l'impartir à l'externe. Si vous avez besoin d'un coup de main, nous pouvons vous aider à ce niveau.

5 À quel point votre plan d'intervention en matière de cybersécurité est-il complet ? À quelle fréquence est-il testé ?

Agir rapidement limite et prévient les dommages. **Soyez assuré de bien coordonner l'intervention dans l'ensemble de l'entreprise** (dirigeants, responsables de la sécurité informatique, contrôleur, etc.) afin de vous assurer que tous sachent quoi faire au moment opportun.

Comment cette technique éprouvée permet d'apprendre en peu de temps ce qui prend normalement des années ?

TEMPS DE LECTURE 3:00

Par quels moyens des étudiants du Missionnary Training Center *(MTC) apprennent-ils en seulement quelques semaines ce que la majorité des élèves apprennent en 3 ou 4 ans ? C'est ce que plusieurs universités ainsi que l'armée américaine ont tenté de comprendre. Ils ont analysé sa méthode et ont fait équipe avec le MTC afin d'appliquer son modèle à succès.*

LA RECETTE GAGNANTE

Le MTC utilise ce qu'on appelle **l'apprentissage basé sur le contexte**. Les étudiants commencent par réciter une phrase et travaillent sur la prononciation. Une fois qu'ils ont une compréhension de base, ils sont placés en groupe de 2 afin d'effectuer des scénarios. Les jeux de rôle représentent environ 70 % de l'apprentissage au MTC. Ils apprennent tout en exécutant et avec un professeur à leurs côtés au besoin.

La méthode du MTC :

1. Apprendre un concept
2. Pratiquer et utiliser ce concept en exécutant un scénario du monde réel
3. Être formé et obtenir de la rétrospection
4. Répéter
5. Être formé et obtenir de la rétrospection

COMMENT L'APPLIQUER ?

Si vous souhaitez un changement durable dans votre vie, vous devez cesser de vous dire « je vais essayer ». Vous devez vous commettre à le faire. L'apprentissage implique un changement permanent dans comment vous voyez les choses et agissez. Si vous souhaitez apprendre quelque chose rapidement, vous devez vous immerger immédiatement et le mettre en application. Par exemple, la meilleure façon d'apprendre l'espagnol est d'être immergé dans cette culture.

1 AYEZ UN MENTOR

Un professeur vous aidera à apprendre rapidement. Ce professeur peut même prendre la forme d'un livre ou d'un cours en ligne. Le bénéfice d'avoir une vraie personne est de pouvoir obtenir immédiatement de la rétrospection et des réponses à vos questions.

2 RÉPÉTEZ JUSQU'À CE QUE VOTRE HABITUDE DEVIENNE INCONSCIENTE

Apprendre quelque chose de nouveau repose sur votre mémoire et comment vous l'utilisez. Lorsqu'un comportement devient automatique, c'est que vous l'avez répété à maintes reprises – ce que les scientifiques appellent l'*over-learning*.

3 DÉTERMINEZ DES OBJECTIFS PRÉCIS AVEC DES DÉLAIS TRÈS STRICTS

Une fois la formation terminée, il est temps de mettre en application ce que vous avez appris. Faites-le en vous fixant de grands objectifs, vous obligeant ainsi à utiliser les connaissances que vous avez acquises. Ensuite, augmentez le niveau de difficulté de votre apprentissage et fixez-vous des échéanciers serrés.

4 SUIVEZ ET MESUREZ

Quand la performance est mesurée, elle s'améliore. Et le suivi permet une prise de conscience. Si vous ne suivez pas vos habitudes quotidiennes, comment pensez-vous pouvoir vous améliorer ?

Si vous souhaitez rapidement atteindre vos objectifs, soyez précis sur les étapes que vous devez faire pour y parvenir. N'oubliez pas de mesurer et de comptabiliser vos efforts en mettant un système clair et précis en place. Quand vous mettez tout en place pour atteindre vos buts, vous les atteindrez inévitablement !

ARS solutions affaires et technologies
6655, boul. Pierre-Bertrand, bureau 301, Québec (Québec) G2K 1M1
www.ars-solutions.ca | info@ars-solutions.ca | 418 872-4744