PASSION AFFAIRES et technologies

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

ARS solutions 25 ans

Mai 2017
Vol. 4 n° 4.

RESPONSABILITÉS LÉGALES

des entreprises et dirigeants concernant la protection des DONNÉES PERSONNELLES AU QUÉBEC

TEMPS DE LECTURE 4:30

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

Les récents exemples d'introduction frauduleuse dans les systèmes des entreprises sont nombreux et inquiètent en raison des conséquences engendrées. Mais ces brèches informatiques peuvent également provenir de l'intérieur, d'un employé mal intentionné ou d'un sous-traitant à qui vous avez accordé l'accès à vos équipements.

Que l'on pense à la perte temporaire ou permanente de renseignements confidentiels, aux coûts engendrés par les efforts de récupération des fichiers et des systèmes, les pertes résultant de l'arrêt de production, sans compter la réputation de votre entreprise qui peut être atteinte, ce qui résultera inévitablement en la perte de clients ou de revenus.

Loi québécoise sur la protection des renseignements personnels dans le secteur privé

Au Québec, cette loi **impose aux entreprises, un certain nombre d'obligations en matière de respect de la confidentialité des renseignements personnels**. Il peut s'agir de renseignements sur des employés, des clients ou autres. Cette loi prévoit la nécessité de prendre des mesures de sécurité afin d'assurer la protection des renseignements que l'entreprise détient. L'entreprise doit aussi s'abstenir de communiquer ces renseignements à qui que ce soit. Il est important de noter que la loi étend cette responsabilité aux administrateurs et dirigeants qui ont autorisé l'accomplissement de l'acte ou qui y ont contribué.

SUITE À LA PAGE 2 ▼

VOTRE PARE-FEU EST COMPLÈTEMENT INUTILE SI...

Un **pare-feu** est un appareil qui agit à titre de «chien de garde» et veille sur votre réseau afin de détecter des accès et des activités non autorisés. **TOUTE entreprise se DOIT d'en avoir un**.

Il est complètement inutile s'il n'est pas bien entretenu et configuré correctement. Il doit être mis à jour, corrigé de façon continue et cohérente et les politiques et configurations de sécurité doivent être bien définies.

Il s'agit d'un projet assez **complexe** en soi, c'est pourquoi il est préférable d'avoir une équipe de professionnels pour s'en occuper.

Si vous avez besoin d'un coup de main, n'hésitez pas à nous contacter immédiatement au **418 872-4744**. Il nous fera plaisir de vous aider.

Suivez-nous

SUITE DE LA PAGE 1 ▲

Dans le cadre de vos activités commerciales...

Votre entreprise peut également être soumise à des ententes de confidentialité. Ces ententes prévoient généralement que l'entreprise doit assurer la protection des données et autres informations fournies dans le cadre d'un projet d'affaires. Parfois, aussi, **ces ententes prévoient des pénalités en cas de non-respect de ces obligations et même, dans certains cas, elles étendent la responsabilité aux dirigeants de l'entreprise**.

Qu'en est-il alors lorsque votre entreprise est victime de fuites qui découlent des brèches à la sécurité informatique ?

C'est généralement l'entreprise qui est appelée, au premier rang, en termes de responsabilité lorsque survient un tel problème. Mais, dans certaines circonstances, **la responsabilité de ses dirigeants pourrait aussi être retenue**. Dans un tel cas, des recours en dommages-intérêts sont possibles, même contre les dirigeants.

La responsabilité de vos administrateurs et dirigeants pourrait être en cause si, individuellement ou collectivement, ils ont permis que les renseignements protégés soient divulgués ou utilisés. Cette « permission » peut résulter de leurs agissements et cela se comprend aisément. Un dirigeant qui autorise la remise des données bancaires d'un client à un de ses fournisseurs en est un exemple. **L'omission ou la négligence d'agir peuvent aussi donner ouverture à la responsabilité.** Ce serait ainsi le cas du dirigeant d'une entreprise victime d'un rançongiciel (« *ransomware* ») qui n'aurait pas mis les logiciels de protection de l'entreprise à niveau, alors qu'il avait été informé de la faiblesse de son système de protection.

Cette même responsabilité peut aussi résulter des lacunes de gestion des employés. Ainsi, un dirigeant qui n'assure pas un suivi raisonnable des agissements de ses employés dans le cadre de leur travail peut se trouver dans une situation délicate si l'un de ses employés transmet des renseignements protégés à toute personne non autorisée à les recevoir. Ou même, si un dirigeant refuse ou néglige de mettre en place et de faire respecter une politique de confidentialité des renseignements confidentiels.

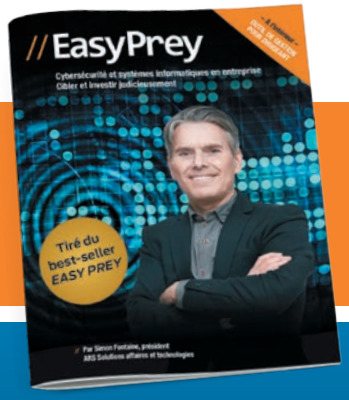
On comprendra que l'étendue de l'obligation de diligence des dirigeants, en matière de protection des renseignements, sera différente si l'entreprise gère des dossiers médicaux ou financiers ou si elle détient des secrets de fabrication que si elle est une entreprise de vente au détail. Mais le devoir de protection de l'entreprise ne doit pas être moins important lorsqu'il s'agit de la protéger adéquatement. Et ça, ça relève des dirigeants.

La protection contre les cyberattaques et contre les divulgations faites par un employé est une nécessité. Un dirigeant ne peut plus présumer que les informations détenues par l'entreprise, que ce soit sur ses employés, ses fournisseurs, ses clients, ou ses propres données financières ou ses activités, le cas échéant, n'intéresseront personne. Si ces informations sont importantes pour l'entreprise, pour quelque raison que ce soit, elles deviennent intéressantes pour toute personne malveillante qui peut être tentée de les subtiliser.

Comment pouvez-vous, comme administrateur ou dirigeant, limiter votre responsabilité en ces matières ?

En adoptant de saines mesures de sécurité. L'une des premières étapes est de se munir d'une politique visant la confidentialité des renseignements vous appartenant ou dont vous avez la garde. Celle-ci se devra d'être adaptée selon vos activités et être maintenue à jour.

De plus, des conseils sont fréquemment prodigués par des experts en sécurité informatique. Il ne faudrait pas hésiter à les consulter. Car s'il existe des domaines où le proverbe « Mieux vaut prévenir que guérir » s'applique inévitablement, c'est probablement ceux des technologies et du droit.



Un outil stratégique extrêmement efficace pour votre comité de gestion

OFFRE DE LANCEMENT !

Nous vous offrons une rencontre de 2 heures avec Simon Fontaine, coauteur de deux best-sellers en technologies pour vous aider à faire l'exercice

ET

Une validation de la sécurité des éléments ciblés comme étant essentiels

GRATUIT (valeur de 795 $)*

Cet exercice vous aidera à...

- Découvrir des informations cruciales à sécuriser dont vous n'étiez pas au courant;
- Assurer la continuité de vos affaires;
- Ramener le pouvoir vers vous, en ayant les outils requis.

Pour bénéficier de cette offre, contactez-nous au 418 872-4744 ou écrivez directement à simon.fontaine@ars-solutions.ca

Pour en savoir plus :
ars-solutions.ca/lancement

10 mythes concernant la cybercriminalité

TEMPS DE LECTURE 3:30

Les dommages liés à la cybercriminalité ont été estimés à 3 milliards de dollars en 2015 et ils devraient **doubler d'ici 2021** pour atteindre 6 milliards de dollars, selon Cybersecurity Ventures. Certaines croyances persistent à son sujet et méritent d'être démystifiées.

1 **Seulement les grandes entreprises doivent s'en préoccuper.** La cybercriminalité touche les entreprises de toutes tailles, particulièrement les PME, car elles sont souvent moins bien préparées et donc plus vulnérables.

2 **Les menaces sont surévaluées, il n'y a pas de quoi s'inquiéter.** Selon un rapport du Ponemon Institute, **62 % des cyberattaques sont destinées aux PME, soit environ 4 000 par jour**. Et ce nombre croît rapidement...

3 **Les cyberattaques proviennent toujours de l'externe.** Selon Radware, environ **(27 %) de tous les incidents sont causés par des employés à l'interne** en raison d'actions malveillantes ou accidentelles telles qu'un **clic sur une pièce jointe infectée ou sur un lien menant vers un site Web frauduleux dans un courriel**.

4 **Les entreprises sont prêtes à combattre la cybercriminalité.** 68 % d'entre elles sont mal ou non préparées et **40 % n'ont pas de plan de relève**.

5 **Tous nos postes de travail et serveurs sont équipés d'un antivirus et d'un système de cryptage de données – nous sommes bien protégés.** Inoffensifs et souvent oubliés, les appareils mobiles représentent une porte d'entrée facile et non contrôlée dans la plupart des entreprises. Même les fichiers cryptés ne sont pas à l'abri des virus...

6 **Nous avons de bons pare-feux et un réseau sécurisé, pourquoi s'inquiéter ?** 38 % des budgets en sécurité TI sont alloués à protéger les firewalls et le réseau, tandis que 18 % vont aux applications, selon F5 Network. Par contre, la réalité est que les applications sont les plus vulnérables et les plus souvent attaquées et la fréquence ainsi que la gravité des attaques sont de beaucoup supérieures à celles effectuées sur le réseau.

7 **La génération Y (née entre 1980-1999) est plus prudente.** En fait, c'est tout le contraire. Les jeunes adultes ont tendance à être moins préoccupés par leur vie privée. Ils devraient être plus alertes et conscients des dangers, mais ils sont habitués à une mentalité complètement différente où il est normal de partager sa vie privée via les médias sociaux et d'autres canaux pas nécessairement sécurisés.

8 **Des mots de passe complexes règlent le problème.** Les mots de passe forts ne sont puissants que lorsqu'ils sont combinés avec d'autres mesures, par exemple l'authentification à deux facteurs. Un gestionnaire de mots de passe devient la solution tout indiquée – sujet abordé dans l'article ***Comment retenir tous ses mots de passe*** de notre bulletin du mois d'avril.

9 **Engager de bonnes ressources en TI permettra d'être protégé.** Le manque de personnel qualifié demeure le principal problème lorsqu'il s'agit de contrer la cybercriminalité. Selon un rapport de 2016 de Trustwave, 57 % des répondants ont rapporté que d'embaucher du personnel qualifié en TI était un défi majeur et pour 35 % d'entre eux, la rétention de leur ressource était un problème. Rapportez-vous à notre article du mois d'avril : **5 raisons avantageuses d'impartir vos TI**.

10 **Il est compliqué d'acheter une police d'assurance ou ça n'existe pas.** Le marché des assurances en cybercriminalité est plein essor. Les primes brutes annuelles sont passées de 2,5 milliards de dollars en 2015 et devraient atteindre 7,5 milliards de dollars d'ici 2020 selon PWC.

Source : Darkreading

Gestion de l'anxiété et du stress au travail

TEMPS DE LECTURE 1:45

TOP 3 des meilleures applications

Il est prouvé scientifiquement que méditer apporte beaucoup de bienfaits sur la santé. Cela permet entre autres de calmer votre esprit, vous aider à mieux dormir, diminuer l'anxiété et le stress lié à votre travail.

Voici 3 applications Cloud des plus simples et efficaces qui vous aideront à adopter de bonnes habitudes.

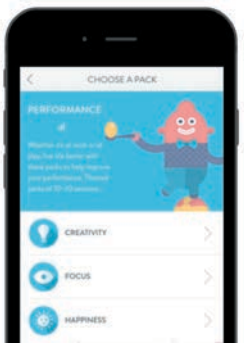
1 SIMPLE HABIT (GRATUITE)

Simple Habit est la meilleure application de méditation pour les gens occupés. Simple d'usage, elle vous aidera à réduire votre stress, à améliorer votre concentration, à mieux dormir et plus encore. Conçue par des psychologues de l'Université d'Harvard ainsi que par des experts en méditation, elle vous permettra d'explorer plus de 50 sessions gratuites sur des sujets tels l'insomnie et la préparation avant un meeting. Vous pourrez personnaliser la durée de votre session (de 1-30 minutes).
simplehabit.com

2 HEADSPACE (GRATUITE)

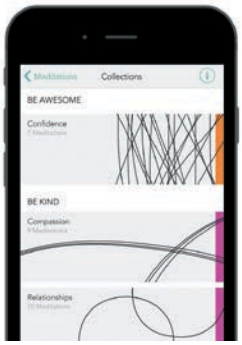
Votre entraîneur pour l'esprit

Apprenez à méditer en seulement 10 minutes par jour avec l'application Headspace – cotée 5 étoiles dans l'App Store. Vous apprendrez les bases de la méditation et découvrirez différentes techniques. À vous d'adopter celle qui vous convient. Une fois que vous aurez incorporé la méditation dans votre vie, vous voudrez la pratiquer chaque jour!
headspace.com



3 MEDITATION STUDIO (3.99$)

Cette application offre plus de 250 méditations supervisées par plus de 30 professeurs expérimentés. Il y en a pour tous les styles et besoins: diminuer le stress et l'anxiété, améliorer le sommeil, aider à réduire les douleurs chroniques, etc.
meditationstudioapp.com



Productivité et efficacité

TEMPS DE LECTURE 1:45

9 livres pour devenir un expert en productivité

Ceux qui atteignent des niveaux de productivité élevés ont quelque chose en commun: la motivation et la constance. Ils ont su développer des habitudes simples qui leur permettent d'atteindre en un an ce que d'autres mettent 10 ans à réaliser. Si vous souhaitez améliorer votre productivité, voici 9 outils pour vous aider à intégrer ou à renforcer de bonnes habitudes.

1. **THE 7 HABITS OF HIGHLY EFFECTIVE PEOPLE** – *Stephen Covey (1989)* • Apprenez 7 leçons puissantes en développement personnel.
2. **GETTING THINGS DONE** – *David Allen (2001)* • L'art de la productivité sans stress. Travaillez sereinement et faites-en plus sans multiplier vos efforts.
3. **THE 80/20 PRINCIPLE** – *Richard Koch (2007)* • Le secret pour atteindre plus avec moins en suivant le principe 80/20: 80% des effets sont le produit de 20% des causes.
4. **THE ONE THING** – *Gary Keller, Jay Papasan (2013)* • Passez à l'essentiel! Comment réussir tout ce que vous entreprenez?
5. **EAT THAT FROG!** – *Brian Tracy (2001)* • 21 bonnes façons d'arrêter de procrastiner et de faire plus de choses en moins de temps.
6. **THE POWER OF HABIT** – *Charles Duhigg (2012)* *Gagnant d'un *award* New York Times • Changez une habitude pour tout changer.
7. **POMODORO TECHNIQUE ILLUSTRATED** – *Staffan Nöteberg (2009)* • Comment organiser votre travail pour accomplir plus en moins de temps?
8. **THE WILLPOWER INSTINCT** – *Kelly McGonigal (2011)* Comment exploiter le contrôle de soi pour améliorer sa santé, son bien-être et sa productivité?
9. **WHAT THE MOST SUCCESSFUL PEOPLE DO BEFORE BREAKFAST** – *Laura Vanderkam (2013)* • Construisez des habitudes qui vous rendront plus heureux et productif (malgré la pression quotidienne).

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