Septembre 2020 • Vol. 7 n° 8

PASSION AFFAIRES *et technologies*

ARSolutions affaires et technologies

NOUS AIDONS LES ENTREPRISES À TRANSFORMER LEURS TECHNOLOGIES EN LEVIER D'AFFAIRES

« Je donne définitivement un 11/10 à ARS qui fait preuve d'une éthique professionnelle et d'une disponibilité remarquable dans notre dossier.

ARS nous avait été recommandée et **nous nous sommes sentis privilégiés de pouvoir travailler avec cette firme** qui a déjà beaucoup de clients actifs à ce jour.

L'équipe a toujours fait preuve de **disponibilité et de flexibilité** envers notre organisation compte tenu que nos délais sont souvent très courts. Nous avons effectué un exercice d'audit de sécurité et mis en place un monitoring spécialisé.

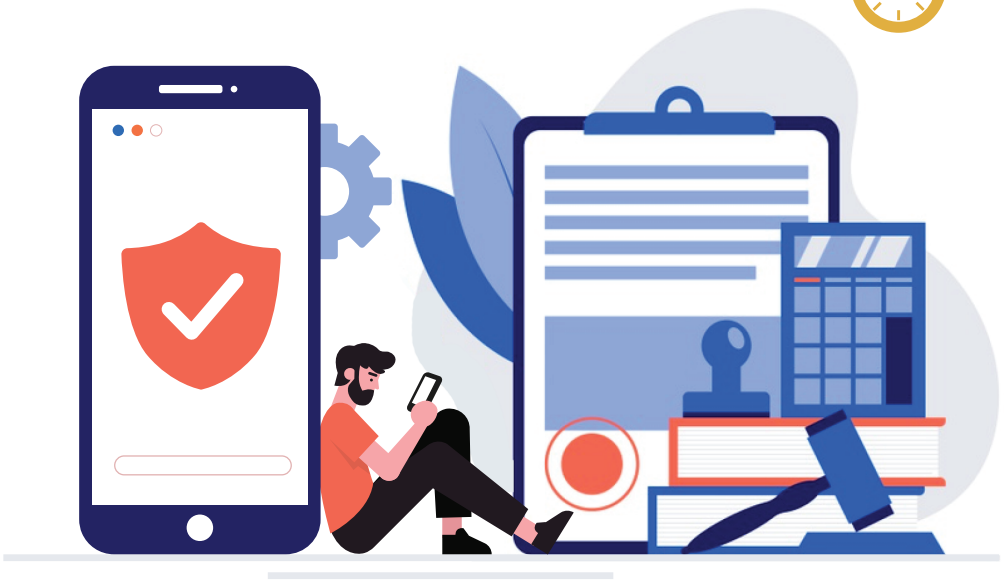
L'information nous est toujours présentée de manière claire, concise et bien vulgarisée pour faciliter la compréhension. »

Alex Bernier
Directeur général
CAUCA - Centrale 911
desservant plus de 560
municipalités au Québec

Suivez-nous

Devoirs et obligations en matière de TIC

TEMPS DE LECTURE 4:00

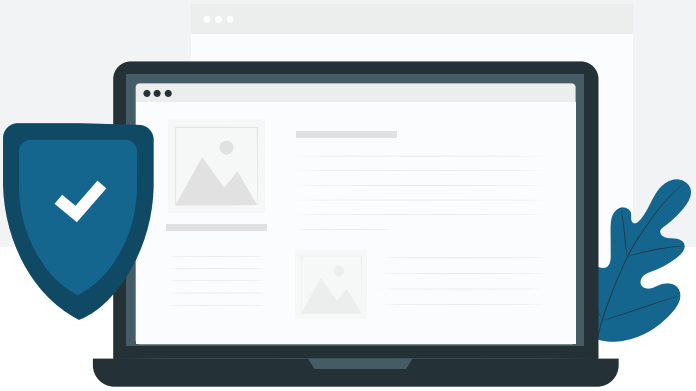


Ce que vous devez savoir en tant que dirigeant ou administrateur - Point de vue du cabinet d'avocats Therrien Couture Joli-Coeur

Grand nombre d'activités commerciales sont affectées par les technologies de l'information et des communications (TIC). Dans les entreprises, on les retrouve notamment dans les services financiers, dans les départements des communications et des ventes ainsi que dans les départements de recherche et développement. Leur importance varie selon les activités de l'entreprise. Mais, au minimum, quelle entreprise n'a pas son site Web aujourd'hui?

Les TIC sont génératrices de croissance et de création de valeur pour l'entreprise, mais leur utilisation peut aussi comporter des risques et des coûts. Et pas seulement lors de leur implantation. Les cyberattaques et la cybercriminalité, les problèmes de systèmes et les erreurs humaines en sont les principales causes. Le rapport 2019 de IBM Security et du Ponemon Institute sur les coûts des atteintes aux mesures de sécurité informatique estime que le **coût moyen d'une faille informatique au Canada s'élève à près de 5.86 M$.**

SUITE À LA PAGE 2 ▼



« En 2019, les cyberattaques malicieuses et la cybercriminalité ont été la cause de 51 % des failles informatiques. La perte de clients représente 36.2 % des coûts totaux d'une faille informatique.

Ces coûts d'une cyberattaque incluent les frais rattachés au « colmatage » de la fuite, la reconstruction des systèmes attaqués et, évidemment, la perte de clients dont la confiance aura été ébranlée.

Comme administrateur d'entreprise, **les questions d'ordre technologique devraient vous amener à vous questionner, de temps en temps, sur les stratégies de développement et d'utilisation des TIC et sur la gestion des risques qu'elles comportent.** Il s'agit d'être capable de **prévenir les risques** par la mise en place de mécanismes de protection, tout en s'assurant que l'entreprise maintienne son avantage stratégique à l'égard de ses compétiteurs par une utilisation optimale des TIC disponibles. Votre capacité à bien le faire pourrait éviter les poursuites contre l'entreprise ou, le cas échéant, vous fournir des moyens de défense plus efficaces.

La probabilité qu'une organisation ayant subi un incident de sécurité en subisse un autre dans les 2 prochaines années est de 29.6 %.

Vous devez également vous préoccuper de certains aspects légaux rattachés à l'utilisation des TIC. Ainsi, lorsque votre entreprise effectue de la vente par Internet, les informations que vous obtiendrez de vos clients doivent être protégées. Vous devez vous assurer d'obtenir les consentements adéquats à l'utilisation que vous faites des renseignements de nature personnelle. Les législations applicables à une telle protection varient d'un endroit à un autre. Le Règlement général sur la protection des données peut s'appliquer à votre entreprise.

Des modifications à la Loi canadienne sur la protection des renseignements personnels et les documents électroniques sont entrées en vigueur le 1er novembre 2018. Ces modifications ajoutent notamment de nouvelles exigences relatives au signalement obligatoire d'atteintes à la protection des données.

Le défaut de ne pas respecter ces obligations peut entraîner des frais importants pour votre entreprise, mais aussi, dans certains cas, pour ses administrateurs et dirigeants. **Comme administrateur ou dirigeant, vous avez des devoirs et responsabilités à rencontrer. Vous devez, entre autres, vous tenir informé des activités de l'entreprise. Vous avez également le devoir d'agir de bonne foi, avec compétence et diligence. Personne ne s'attend à ce que vous soyez un expert en technologie. Cependant, en vous référant aux connaissances réelles d'un expert, vous pourrez démontrer, si besoin était, que vous avez rempli ces devoirs qui vous incombent.**

Voici quelques suggestions qui vous permettront de remplir vos obligations d'administrateur prudent en matière de TIC :

1. Intégrer, si possible, au conseil d'administration, une ou des personnes ayant des connaissances technologiques qui vous aideront à mieux comprendre les enjeux, les risques et les solutions. À défaut d'intégration d'un administrateur au conseil, s'adjoindre des consultants fiables qui sauront vous conseiller adéquatement.

2. Ramener les questions technologiques au conseil d'administration de façon assez régulière afin d'en évaluer l'utilisation, la sécurité et prévenir les ennuis.

3. Déléguer une personne qui assurera le suivi de la sécurité informatique.

4. Réviser périodiquement les TIC utilisées par l'entreprise afin que celles-ci demeurent concurrentielles.

5. Se doter de règles de gouvernance en matière de TIC qui seront adaptées à votre entreprise.

Vous avez une responsabilité de comprendre et gérer les technologies qui ne cessent d'évoluer et de prendre de la place. Plus vous connaîtrez les TIC de votre entreprise, mieux vous arriverez à les contrôler.

Source : Halima Kerchi, Avocate en droit des affaires - Therrien Couture Joli-Cœur

Le SIEM comme allié de gestion

3:45 TEMPS DE LECTURE

Le SIEM (Security Information and Event Management OU Gestion de l'information et des évènements de sécurité) améliore l'ensemble des activités des entreprises et aide les dirigeants à relever leurs défis concernant la cybersécurité.

Qu'est-ce qu'un SIEM?

Au-delà d'amener un meilleur contrôle en regard à la cybersécurité, le SIEM **a une portée beaucoup plus grande en entreprise dans l'ensemble de ses opérations :** soutien légal par la traçabilité des informations et la transmission de preuves, gain de temps par des rapports de conformité automatisés prouvant votre bonne foi lors d'audits, outils d'appui aux ressources humaines en situation de litiges… **Le SIEM permet de limiter les dommages financiers et le déficit d'image de marque.** Depuis le dernier évènement de cybersécurité survenu chez le Mouvement Desjardins, les dirigeants sont maintenant concernés face aux faits des risques d'attaques qui deviennent de plus en plus importantes et de plus en plus dommageables.

À l'ère où les entreprises de toutes tailles font face aux mêmes enjeux et défis, s'adapter est un passage obligé. Un grand nombre adoptent **les nouvelles technologies comme le nuage et la mobilité** sans compter qu'on encourage l'accélération de **la transformation numérique** au Québec. Il en résulte un environnement informatique hybride, divers et complexe, jamais vu auparavant et où se côtoient plusieurs technologies. **D'où l'importance grandissante d'avoir des outils adaptés à cette nouvelle réalité.**

Basées sur l'intelligence artificielle, les solutions SIEM d'aujourd'hui **permettent à votre entreprise de réagir rapidement et avec précision** en cas de menace ou de fuite de données. Elles donnent en temps réel l'information pertinente et essentielle. Le SIEM sert à détecter les anomalies de comportement et les attaques. Il permet de détecter, de diagnostiquer et de prendre action beaucoup plus rapidement.

Anticipation de pannes

Le SIEM permet donc une meilleure anticipation des incidents aux prémices d'une attaque d'envergure et de remonter à la source de vos problèmes de sécurité AVANT que vos équipements ne tombent en panne. **Vous évitez donc les temps d'arrêt coûteux associés aux failles:**

- En détectant des logiciels malicieux ou non autorisés installés sur le réseau
- En interceptant des tentatives d'intrusions et les attaques

On met l'intelligence artificielle au service de la détection de pannes

Selon une étude approfondie menée par Osterman Research, **87 % des employés qui partent emportent des données avec eux.** Que font-ils avec cette information? Ils l'utilisent dans leur prochain emploi chez votre concurrent, la vendent à des concurrents ou deviennent un concurrent.

Réduction des coûts d'assurance en cybersécurité

Un bon contrôle par le SIEM aide à réduire les coûts d'assurance en cybersécurité. L'évaluation de vos cyberrisques est en fonction des menaces émergentes et d'autres variables en évolution. De par le SIEM, **le rapport de risques et de menaces aide à anticiper ces menaces** et permet de mettre en place un plan correctif et d'amélioration continue.

Le SIEM, un outil à l'ère de son temps

L'impact positif du SIEM sur les affaires de l'entreprise le positionne aujourd'hui comme un allié indispensable dans la conjoncture actuelle. Il devient un outil de gestion **pour la haute direction qui doit désormais prendre pleinement part à la gouvernance de la sécurité globale de l'organisation, en équipe avec son département des TI**, afin d'en assurer la viabilité financière et de **veiller à ce que les intérêts des actionnaires, des clients et des employés soient protégés.**

N'hésitez pas à nous contacter pour obtenir plus d'informations sur les bénéfices du SIEM au sein de votre entreprise.

Le travail à distance change la façon de mesurer la productivité

3:45 TEMPS DE LECTURE

En mars 2020, la plus grande expérience de travail à domicile de l'histoire a débuté. Dès que des entreprises ont déplacé l'ensemble de leur main-d'œuvre à distance, les propriétaires d'entreprises et les employés ont commencé à prendre conscience des nouvelles réalités de leur travail.

Pendant des années, on avait dit aux gens : "Il est essentiel que vous soyez au bureau", pour se rendre compte soudainement qu'être au bureau n'était pas si essentiel après tout. **Les appels de Zoom ont facilement remplacé des dizaines de réunions hebdomadaires en personne.** Les tâches manuelles, comme remplir des documents, ne pouvaient soudainement plus être effectuées de la même manière, ce qui a obligé les entreprises à accélérer leurs efforts de transformation numérique. **Des processus qui semblaient bien fonctionner dans un bureau physique ont soudain montré à quel point ils étaient dépassés et inefficaces.** Et les craintes de tous les cadres ou dirigeants de voir les employés distants ne faire que regarder Netflix et jouer à la Xbox toute la journée à la maison au lieu de travailler ont été apaisées.

Les entreprises du monde entier ont réalisé que le travail à domicile est non seulement plus efficace, mais aussi plus adapté aux souhaits et aux besoins des travailleurs d'aujourd'hui. Selon une entreprise interrogée par Forbes, ainsi que des recherches menées par Harvard Business Review, **le travail à domicile stimule la productivité de l'ensemble de l'entreprise.**

La vie des entreprises après la COVID-19 ne sera plus jamais la même. **Voici les 2 grands changements qui pourraient se produire :**

1. Les entreprises adopteront la flexibilité

Il y a 30 ans, 10 ans, voire 5 ans, il n'était pas vraiment "professionnel" de prendre un appel avec un client ou une cliente si vous n'étiez pas "au bureau".

Mais ces dernières années, et surtout ces derniers mois, **il est devenu culturellement acceptable d'être plus honnête et transparent sur votre vie personnelle en tant qu'employé ou chef d'entreprise** - tant que cela n'interfère pas avec la qualité de votre service.

Par exemple, pendant la pandémie et la nécessité de travailler à domicile, il est devenu de plus en plus courant qu'un chien aboie ou d'entendre un enfant crier lors d'une conférence téléphonique.

Mais cela ne veut pas dire que les clients vont critiquer. Au contraire, ils vont plutôt démontrer de la compréhension et de la compassion.

2. L'automatisation sera de plus en plus essentielle

De nombreuses entreprises n'ont pas réalisé à quel point elles étaient inefficaces avant que la pandémie ne frappe. Ce qui fait en sorte que que beaucoup de personnes ont ou vont perdre leur emploi en raison de l'impact économique de la pandémie. **Avec moins d'employés, les tâches manuelles doivent être remplacées par l'automatisation.** Les services d'assistance continueront à compenser les pertes de personnel par le libre-service grâce à des portails, des agents virtuels et d'autres innovations. **En combinant l'automatisation et le travail à domicile, vous obtenez des employés qui font plus de choses en moins de temps** (ce qui signifie que votre personnel est plus efficace et que vous avez besoin de moins d'employés pour effectuer le même nombre de tâches), et les frais généraux sont grandement réduits.

Dans l'automatisation des entreprises, **il existe un concept appelé "gestion du travail", qui consiste à définir l'objectif final, à déterminer ce qui doit être produit, puis à gérer toutes les tâches nécessaires à l'obtention du résultat final**. En ce moment, pendant la pandémie, c'est précisément ce que les chefs d'entreprise examinent quotidiennement. Ils sont obligés d'examiner tous leurs différents processus internes et de se demander comment ils peuvent produire les mêmes résultats qu'auparavant, mais plus rapidement, plus efficacement et avec un effectif réduit.

Et comme ces entreprises voient les améliorations apportées par l'automatisation d'un processus, elles voudront continuer à automatiser de plus en plus à l'avenir.

Source : Matt Klassen

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