PASSION AFFAIRES et technologies

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

ARS Solutions 25 ans

Décembre 2016-Janvier 2017
Vol. 3 nº 10.

En cette période de festivités, toute l'équipe d'ARS Solutions tient à vous offrir ses meilleurs vœux de succès et de bonheur.

Que la nouvelle année soit pour vous synonyme d'excellence.

Nous vous souhaitons de joyeuses fêtes et une bonne année 2017 !

Suivez-nous

2017 : où en êtes-vous avec VOTRE PLANIFICATION STRATÉGIQUE AFFAIRES-TI ?

TEMPS DE LECTURE 3:30

La nouvelle année est une bonne occasion de faire un constat de l'année précédente et de partir avec de nouvelles résolutions. Si vos TI n'ont pas été un levier pour vos affaires en 2016, il n'est pas trop tard pour y remédier en 2017 !

Sachant que les TI occupent une place importante dans les entreprises, vous aurez beaucoup à gagner en investissant dans 2 rencontres de 4 heures pour planifier 3 ans. En effet, **cela représentera probablement l'un de vos meilleurs retours sur investissement**.

Impossible de fonctionner intuitivement avec les technologies. Agir ainsi conduira l'entreprise vers un échec assuré. Par ailleurs, évitez de vous contenter d'un plan strictement technologique sans lien avec le plan d'affaires de l'entreprise. **L'arrimage Affaires-TI est la clé du succès. Il est temps que les technologies contribuent enfin à l'atteinte des objectifs d'affaires. Chaque somme investie dans les technologies, chaque projet initié, doit contribuer au succès de votre entreprise.** Dans le cas contraire, les TI ne seront pas au service de vos affaires et seront perçues comme une dépense.

SUITE À LA PAGE 2 ▼

SUITE DE LA PAGE 1 ▲

1 **La sécurité.** Depuis les 3 dernières années, le nombre de piratage informatique a connu une hausse exponentielle. Considérant que les cybercriminels seront plus actifs que jamais en 2017, ce sujet sera de loin le plus important à prendre en considération dans votre Planification Stratégique. D'ailleurs, nous avons écrit de nombreux articles à ce sujet au cours de la dernière année qui démontrent bien l'état critique de la situation. N'hésitez pas à consulter notre blogue si le sujet vous intéresse.

Avec l'augmentation de l'utilisation du Cloud, des appareils mobiles et du stockage d'information en ligne, les pirates ont désormais beaucoup plus d'opportunités de s'infiltrer et ont accès à des outils de plus en plus novateurs qui augmentent considérablement le risque pour les entreprises d'être victimes. En étant astucieux et en usant de stratégies changeantes, ils peuvent déjouer les utilisateurs les plus vigilants.

2 **La légalité des licences de vos logiciels.** Les géants tels Microsoft, Adobe, etc. sont plus que jamais actifs à auditer les entreprises, particulièrement depuis la dernière année. Ce sujet devrait être un incontournable dans votre Planification Stratégique. N'attendez pas d'être audité pour faire l'inventaire de vos licences, car si vous découvrez des licences non utilisées dans votre entreprise, vous devrez tout de même payer la facture puisqu'elles sont déjà installées... En effectuant un audit à l'avance, vous pourrez apporter les correctifs à temps, évaluer vos besoins et ainsi prendre des décisions en fonction de ce que vous êtes prêt à payer. N'oubliez pas que vous devez avoir en main tous les documents légitimes associés aux licences que vous utilisez.

3 **L'impartition. De plus en plus d'entreprises optent pour cette option.** Pourquoi? Parce que dans la plupart des cas, pour des entreprises de petite ou grande taille, il est **beaucoup plus avantageux d'impartir** les services informatiques à l'externe que d'engager une ressource à temps complet **dû au meilleur rapport coûts/bénéfices**. De plus, vous aurez accès à une équipe de gens spécialisés pour vous servir.

En tenant compte des coûts de votre temps de gestion, des coûts d'improductivité sur l'ensemble de votre entreprise, de la perte de revenu et de tous les frais qui y sont reliés, le modèle de services gérés est considéré comme étant moins dispendieux.

Si vous souhaitez vous doter d'un plan d'action, avoir une vision globale et investir dans un but précis afin d'améliorer la productivité de votre entreprise, vous adopterez une approche plus stratégique avec un modèle d'impartition.

En espérant que ces conseils puissent vous guider et vous donner quelques pistes qui vous permettront, en 2017, de faire de vos technologies un levier d'affaires!

Simon Fontaine, Président
simon.fontaine@ars-solutions.ca

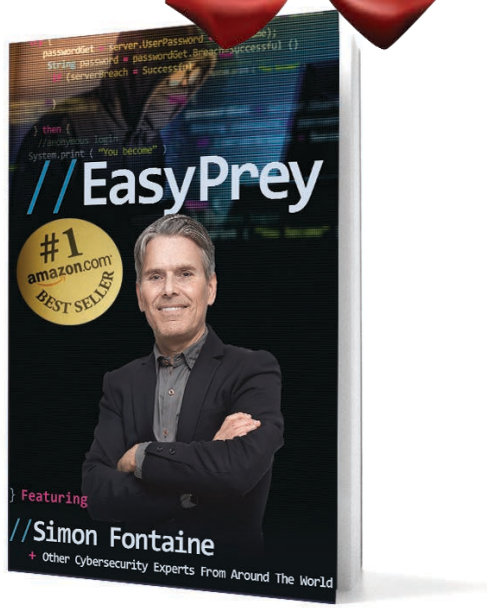
Nous rendons les entreprises plus efficaces et performantes en transforma

EASY PREY

How to protect your business from data breach, cybercrime & employee fraud

TEMPS DE LECTURE 1:00

Contactez-nous dès maintenant pour réserver votre copie GRATUITE ! info@ars-solutions.ca



Simon Fontaine, Président et cofondateur d'ARS Solutions affaires et technologies, a été sélectionné à nouveau par CelebrityPress™ - un leader en publications technologiques, pour faire équipe avec d'autres entrepreneurs de partout en Amérique du Nord afin de coécrire un second livre intitulé, "*Easy Prey – How to protect your business from data breach, cybercrime & employee fraud*".

Son chapitre qui s'intitule **"Cibler et investir judicieusement"** soutient que la façon dont la sécurité est typiquement abordée est trop générale et ne prend pas en considération ce qui est réellement important à sécuriser pour les entreprises.

La nécessité d'impliquer la direction sur la question TI et de sécuriser les éléments critiques en optant pour une approche personnalisée et non générale telle que l'industrie le suggère prend tout son sens.

À l'intérieur, vous trouverez un outil de gestion qui vous aidera à cibler les éléments essentiels à sécuriser tout en évaluant leur degré de criticité et l'impact financier associé.

La version française du chapitre écrit par Simon sera bientôt disponible !

« **Il serait important que les dirigeants prennent quelques heures et suivent les recommandations de Simon dans ce livre...**

La majorité des dirigeants que je connais ne semblent pas être préoccupés par la sécurité informatique de leur entreprise, car ils se sentent bien protégés en confiant cette tâche à leur responsable des TI. **Malheureusement, ce sentiment de sécurité pourrait se changer en cauchemar si des données importantes se perdaient.**

Cette responsabilité appartient aux dirigeants afin d'assurer la pérennité de leur entreprise. »

Jean-Pierre Lauzier
Expert-conseil en vente, mise en marché et service à la clientèle
Auteur du Best-seller : *Le Cœur aux ventes*
JPL Communications inc.

« **Simon sait trouver la façon de réduire les coûts et d'être efficace...**

Dans son chapitre, il nous démontre que **toute l'information n'a pas toujours la même valeur et ne mérite pas d'être protégée de la même façon**...

Les gestionnaires d'entreprises doivent apprendre à identifier eux-mêmes leurs informations stratégiques et ensuite s'assurer que leurs départements et sous-traitants en TI les protègent adéquatement.

Sinon, **l'entreprise voit ses procédures standardisées par des spécialistes techniques qui ne comprennent pas le modèle d'affaires et qui imposent LEUR vision, sans à la fin atteindre les objectifs de base voulus**.

Seuls les entrepreneurs peuvent faire la différence réelle entre ce qui est critique ou l'est moins. Assurez-vous de bien le communiquer à votre service TI ! »

Dominique Duchesne, ing. Adm A.
Consultant et Entrepreneur, CEB Services Conseils

TEMPS DE LECTURE 3:00

60 % des petites entreprises VICTIMES DE CYBERCRIMINALITÉ FONT FAILLITE APRÈS 6 MOIS

U.S' National Security Agency - **Il en coûte 690 000 $ à une petite entreprise pour se relever d'une cyberattaque et plus d'un million de dollars pour une moyenne entreprise.**

Sites Web piratés, fuite de données, identités volées... **Les PME sont plus que jamais dans la mire des cybercriminels...** Pourquoi? En étant peu méfiantes et souvent imprudentes, elles sont souvent vues comme des « **proies faciles** (easy prey) » par les pirates informatiques.

La cybercriminalité a connu une hausse exponentielle en 2016 et est devenue de plus en plus sophistiquée...

On dénombre que 62 % des cyberattaques sont destinées aux PME, soit environ 4 000 par jour. Et ce nombre croît rapidement, car de plus en plus d'entreprises utilisent le Cloud, les appareils mobiles et stockent de l'information en ligne. Pour contrer les menaces liées à la cybercriminalité, les dirigeants d'entreprises doivent plus que jamais mettre en place des mesures de sécurité adaptées à leurs besoins s'ils veulent assurer la continuité de leurs affaires. Malheureusement, les petites entreprises ont souvent tendance à vouloir minimiser leurs coûts dans des domaines comme la sécurité. Elles réalisent après coup que les dommages causés à leur réputation additionnés aux coûts pour se relever d'une cyberattaque surpassent largement les économies qu'elles ont cru faire.

Considérant que **75 % des organisations ont déjà subi une brèche de données au cours des 12 derniers mois**, les propriétaires de petites entreprises ont raison de s'inquiéter... Alors si vous pensiez être peu à risque parce que vous n'êtes ni une banque ou une grande entreprise comme Home Depot ou JP Morgan, détrompez-vous ! Personne n'est à l'abri.

Rappelez-vous que la plupart des brèches de données dans les entreprises sont dues au clic d'un employé, au téléchargement ou à l'ouverture d'un fichier infecté. Une formation de base peut aider à arrêter la majorité des menaces de faible niveau, mais les former n'est pas suffisant...

ACTIONS À PRENDRE POUR ASSURER LA PÉRENNITÉ DE VOS AFFAIRES :

- Ayez une politique de sécurité en place qui sera rigoureusement suivie par vos employés;
- Faites régulièrement la mise à jour de vos logiciels;
- Ayez un excellent plan de sauvegarde.
- Si vous doutez d'un lien/courriel, ne l'ouvrez pas;
- Sécurisez tous les appareils qui sont connectés à Internet;
- Vérifiez chaque support externe que vous branchez à votre réseau (clé USB, etc.);
- Cryptez vos données les plus sensibles;
- Ne déléguez pas seulement la sécurité à votre département TI; impliquez tous les employés;
- Révisez votre plan de continuité d'affaires (vous saurez quoi faire si vos systèmes sont compromis).

CAS VÉCU

LA FAILLITE POUR UNE PETITE ENTREPRISE...

Un petit détaillant de vente en ligne était loin de se douter qu'un simple clic de souris d'un employé allait conduire son entreprise à la faillite...

C'est en cliquant sur un lien d'un catalogue virtuel qui semblait tout à fait normal que le logiciel malveillant Crytowall s'est infiltré et a infecté les logiciels comptables et les comptes clients incluant les noms, adresses, numéros de carte de crédit, NAS, etc. Les logiciels et les fichiers clients ne se trouvaient pas sur l'ordinateur de l'employé, mais bien sur le réseau de l'entreprise, ce qui permis au logiciel malicieux de crypter 15 000 fichiers comptables et clients. Une demande de rançon suivit rapidement, exigeant 50 000 $ en échange d'une clé de décryptage. Comme les systèmes de sauvegarde de l'entreprise ne fonctionnaient pas depuis des mois, le virus s'avérait impossible à éliminer sans perdre des données cruciales de l'entreprise, alors la société n'avait d'autre choix que de payer. Malheureusement, la clé de décryptage ne fonctionnait pas. L'entreprise a dû cesser ses activités et c'est ainsi que 6 mois plus tard, elle ferma ses portes...

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