CPA COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

Gestion efficace des risques liés aux TI pour les petites entreprises

Une petite entreprise tire quelques leçons sur la gestion des risques liés aux TI

Même si les projecteurs sont le plus souvent braqués sur les grandes sociétés cotées, les petites entreprises du secteur privé comptent pour beaucoup dans l'économie canadienne. Elles représentent en effet 98,2 %[1] de toutes les entreprises au Canada. Comme la majorité des entreprises actuelles, les petites s'en remettent largement aux technologies de l'information (TI) pour soutenir leurs activités de soutien administratif et d'exploitation, gonfler leur présence dans l'offre de produits et de services concurrentiels auprès des clients locaux, ou accéder aux marchés mondiaux. Par conséquent, la gestion des risques liés aux TI est essentielle à leur survie et à leur succès. Nombreux sont les petits entrepreneurs qui ont adopté les technologies, mais certains ont encore des choses à apprendre sur les risques qu'elles comportent. Nous vous présentons Gabriel Schmidt, propriétaire fictif d'une petite entreprise, qui traverse une crise relative aux TI et qui en retire certaines leçons qui lui seront profitables.

Gabriel Schmidt est un entrepreneur prospère qui a investi toute sa passion dans son entreprise, EPI Inc., pour l'amener à un chiffre d'affaires annuel de 2,5 millions de dollars. EPI, de son nom complet Équipement de protection incendie, fabrique de l'équipement de sécurité spécialisé pour les pompiers. Gabriel a lancé son entreprise il y a cinq ans, et a maintenant 15 employés. L'entreprise a connu une croissance rapide, et lui-même s'est hissé récemment dans la liste des 250 meilleurs entrepreneurs canadiens, compilée par une populaire revue d'affaires. Il avait très hâte au dîner de gala organisé par cette revue, au cours duquel on

1 Industrie Canada, statistiques relatives aux petites entreprises—rapport d'août 2013 : **www.ic.gc.ca/eic/site/061.nsf/fra/02804.html**

devait lui remettre un prix devant tous ses pairs. Après une bonne année de dur labeur, il envisageait même de partir en vacances dans les Caraïbes avec sa femme. Alors que Gabriel était perdu dans ses pensées, il fut ramené à la réalité par un appel urgent de son directeur de l'exploitation, Carlos Santos, qui voulait le voir immédiatement.

Lorsque Carlos lui eut expliqué le motif de l'urgence, l'optimisme de Gabriel a commencé à s'évaporer. Les principaux serveurs de l'entreprise avaient planté tôt ce matin-là. Les serveurs nécessaires à toutes les activités—y compris la fabrication, les achats, les finances et le service à la clientèle—étaient tous tombés en panne. Il n'était même plus possible d'envoyer ou de recevoir un courriel. Carlos et son équipe avaient travaillé toute la journée à résoudre les problèmes.

Gabriel a demandé à Carlos quel était son plan pour restaurer les systèmes. Les données avaient certainement été sauvegardées et pourraient être chargées dans de nouveaux serveurs, et l'entreprise serait de nouveau sur les rails en quelques heures.

Carlos lui a révélé qu'il était possible que les données n'aient pas été sauvegardées. Le contractuel en TI qui s'occupait des serveurs avait quitté EPI le mois précédent parce qu'on ne lui avait pas accordé l'augmentation tarifaire qu'il avait demandée. On venait tout juste de lui trouver un remplaçant, mais celui-ci ne commençait que la semaine suivante.

Gabriel était sans voix. Comment était-il possible que toutes les données et opérations informatiques de l'entreprise se soient soudainement envolées? Les questions se sont mises à affluer dans sa tête :

- Pourquoi les serveurs étaient-ils tombés en panne? À cause d'un virus? D'une cyberattaque d'un concurrent? Depuis la publication de l'article sur son entreprise dans la revue d'affaires, beaucoup de gens l'avaient appelé pour le féliciter, dont certains concurrents. Pouvaient-ils tremper dans cette affaire?
- Était-il possible que le nouveau stagiaire venant du collège d'informatique ait manipulé les serveurs, intentionnellement ou non?
- Était-il possible que le contractuel mécontent ait corrompu les fichiers du serveur? EPI n'avait pas modifié les mots de passe d'accès à distance aux systèmes depuis le départ du contractuel le mois dernier.
- Et qu'en était-il des sauvegardes? Pourquoi le service de l'exploitation ne s'était-il pas assuré que les sauvegardes se faisaient régulièrement et de manière appropriée?
- Le personnel n'avait-il pas préparé un plan de continuité des activités pour EPI? Gabriel ressentait une certaine culpabilité à cet égard. Il avait entendu parler de l'importance d'avoir un plan de continuité des activités lors de la dernière conférence pour les petites entreprises à laquelle il avait assisté, mais il avait été si occupé qu'il n'avait pas soulevé cette question auprès de son service de l'exploitation.

- Comment allait-il poursuivre ses activités, faire ses suivis auprès des clients, payer ses employés?
- Comment EPI allait-elle compiler les données financières nécessaires aux fins fiscales, calculer les cotisations au régime d'indemnisation des accidentés du travail ou préparer le rapport périodique exigé par sa banque dans la clause restrictive de son contrat de prêt?

Gabriel avait besoin d'aide. Il voulait savoir quoi faire pour régler le problème immédiat, et quoi faire pour éviter ce genre de crise à l'avenir.

Gabriel savait que le cabinet d'expertise comptable et de services-conseils du coin, RRJL, comptait des CPA versés dans le domaine des technologies. Il a donc appelé les gens de ce cabinet, leur a raconté son histoire et leur a demandé de l'aide.

Le cabinet lui a affecté ses deux meilleurs conseillers. Après examen de la situation, ceux-ci ont rencontré Gabriel pour lui soumettre les recommandations suivantes.

Recommandations immédiates

1. Rencontrer les principaux employés concernés afin de recueillir le maximum d'informations sur ce qui s'était possiblement passé, et pour déterminer les répercussions immédiates de la situation sur EPI, autant à l'interne qu'à l'externe.

2. Faire appel à une équipe spécialisée dans les TI pour examiner les serveurs d'EPI et déterminer s'il était possible d'extraire ou de recréer les données. L'équipe devrait travailler avec le fournisseur des serveurs et des logiciels pour connaître les solutions possibles. Si l'extraction des données n'était pas possible, il serait alors nécessaire de recréer les enregistrements des opérations à partir de la dernière sauvegarde utilisable et de toute piste papier existante. Le cas échéant, l'équipe de services-conseils décrirait les étapes à suivre dans une note distincte.

3. Si les serveurs et systèmes devaient redevenir fonctionnels, il faudrait appliquer certaines mesures pour gérer les risques présents. Ces mesures comprendraient le maintien des systèmes hors ligne pour éviter tout accès de l'extérieur, une analyse antivirus, la modification des mots de passe de tous les points d'accès et, finalement, la restauration prudente de la connectivité, une fois que l'on serait suffisamment assuré que les systèmes et les données ont été restaurés et mis à l'essai et qu'ils fonctionnent comme prévu.

4. Au besoin, élaborer un plan de communication pour informer les parties concernées de l'incident et des mesures qui ont été prises à cet égard, afin qu'elles sachent qu'EPI avait la situation bien en main.

Réponse du fournisseur des serveurs

Gabriel a communiqué avec le fournisseur des serveurs, qui lui a envoyé immédiatement des techniciens pour résoudre le problème. Heureusement, les techniciens ont été en mesure de trouver une solution. Ils ont découvert que les serveurs avaient été configurés pour créer une sauvegarde automatique chaque nuit sur un lecteur distinct. Auparavant, ces données auraient été sauvegardées sur des supports amovibles et conservées hors site. Une fois que l'on pourrait déterminer l'heure à laquelle les dernières bonnes données avaient été sauvegardées, il serait possible de les isoler et de les récupérer.

Après enquête, il a été établi que les données étaient intactes jusqu'à 22 h 17 la veille. Les serveurs ont alors été restaurés en fonction de cette heure. Puisqu'il n'y avait pas eu de transactions pendant la nuit, le personnel d'EPI a pu saisir les activités de la journée, notées sur papier, dans les systèmes rétablis. Gabriel a poussé un soupir de soulagement.

Conseils pour l'avenir

Gabriel voulait maintenant prendre proactivement certaines mesures pour éviter qu'un tel incident se reproduise. Il a demandé à l'équipe de services-conseils de RRJL de lui indiquer quels étaient les risques liés aux TI auxquels son entreprise était exposée, et les mesures qu'il devait prendre pour mieux gérer et atténuer ces risques.

Les conseillers lui ont fourni une liste des sept principaux enjeux dont il devait s'occuper pour gérer les risques liés aux technologies. Ils ont ajouté une réserve à leurs recommandations, en précisant que les stratégies suivantes ne pouvaient garantir qu'aucun autre incident ne se produirait à l'avenir. Par contre, ils allaient aider Gabriel et EPI à atténuer davantage les risques et à être mieux préparés pour affronter un incident le cas échéant. Gabriel a expressément demandé à l'équipe de services-conseils de lui soumettre des recommandations simples et réalisables, que les membres de son personnel et lui-même pourraient facilement comprendre.

Sept principaux enjeux et recommandations

Les conseillers ont soumis les enjeux suivants à Gabriel, accompagnés des risques potentiels qu'ils présentent et de leurs répercussions possibles pour EPI et d'autres petites entreprises. Ils lui ont aussi soumis des recommandations ou solutions possibles pour atténuer ces risques.

1. Établir un plan de continuité des activités

L'enjeu : Comme on l'a constaté lors de la panne des serveurs, EPI n'avait pas de plan de reprise après sinistre approprié quant aux TI pour maintenir son fonctionnement. Le service de l'exploitation n'avait peut-être pas les connaissances voulues pour élaborer et tenir à jour un plan de reprise après sinistre tenant suffisamment compte des besoins de l'entreprise en matière de disponibilité des systèmes. Il est possible aussi qu'il ait mal planifié les mesures visant à assurer la disponibilité des systèmes.

Les risques : L'entreprise pourrait ne pas être en mesure de poursuivre ses activités en cas de défaillance des systèmes, pour l'une ou l'autre des raisons suivantes[2] :

- défaillance du matériel;
- panne de courant ou défaillance des télécommunications;
- défaillance d'une application ou corruption de la base de données;
- erreur humaine, sabotage ou grève;
- logiciels malveillants;
- piratage ou autres attaques par Internet;
- agitation sociale ou attaques terroristes;
- incendie;
- catastrophes naturelles.

Les solutions : Pour rédiger son premier plan de reprise après sinistre, EPI aurait avantage à embaucher un professionnel qui l'aiderait à définir ses besoins et à élaborer des procédures qui pourraient être rapidement mises en œuvre. Celles-ci devraient comprendre un cycle de sauvegarde des principaux systèmes et données. Une fois ce premier plan élaboré, le service de l'exploitation d'EPI pourrait le tenir à jour à l'interne. La personne responsable de l'exécution de chacune de ces procédures devrait être spécifiquement désignée, et un cadre supérieur devrait vérifier périodiquement si elles sont appliquées et tenues à jour. EPI pourrait envisager de confier les processus de sauvegarde à un fournisseur de services en nuage externe, qui serait en mesure de sauvegarder les données par Internet. La planification de la continuité des activités n'incombe pas seulement aux employés responsables des systèmes; pour qu'elle fonctionne, les employés clés de tous les secteurs de l'entreprise doivent s'engager dans une certaine mesure à cet égard.

2. Assurer une gestion efficace des fournisseurs de TI

L'enjeu : Les petites entreprises ont tendance à trop se fier à des contractuels ou à des fournisseurs externes pour s'occuper des fonctions de TI et assurer le soutien à cet égard. C'est ce qui est arrivé à EPI.

Les risques : Avec de telles ententes, il existe parfois un risque que l'on définisse mal, dans le contrat, les attentes, les niveaux de service à respecter ainsi que les politiques et les normes qui permettront de répondre aux exigences de l'organisation. Le contrat doit prévoir une protection advenant que le fournisseur développe un logiciel expressément pour ses clients et qu'il cesse de le prendre en charge ou qu'il mette fin au contrat, sans que le client dispose du logiciel original (code source) pour être en mesure de prendre le relais. Si les nouveaux contrats ne passent pas sous la loupe d'un professionnel, l'entreprise peut se retrouver coincée avec un fournisseur dont elle ne pourra se débarrasser facilement en mettant fin au contrat. Si l'on dépend exagérément de certains contractuels ou si on leur accorde une trop grande confiance, il y a un risque, advenant le départ d'un contractuel, que l'entreprise ne dispose pas de ressources suffisantes ou suffisamment formées en TI pour soutenir les activités jusqu'à l'embauche

2 www.sans.org/reading-room/whitepapers/recovery/introduction-business-continuity-planning-559 (en anglais seulement)

d'un remplaçant. Il est aussi possible que l'on comprenne mal ce que les contractuels font et ne font pas. Un fournisseur peut aussi se voir accorder un plein accès à distance sans que des contrôles appropriés de l'accès et des changements soient en place.

Les solutions : Les mesures pouvant être mises en œuvre sont les suivantes :

- Avant de signer le contrat vous liant au fournisseur, faites-le vérifier par un avocat spécialisé en la matière.
- Définissez vos attentes en matière de prestation de services et déterminez si le fournisseur pressenti peut satisfaire à ces attentes, y compris en ce qui a trait aux contrôles internes requis.
- Vérifiez les références, et si le fournisseur peut répondre à vos attentes en matière de service.
- Si vous faites appel à un travailleur autonome, assurez-vous que votre personnel de surveillance à l'interne a les connaissances nécessaires pour surveiller son travail, et qu'il serait en mesure de le remplacer temporairement si votre fournisseur devait mettre fin à son contrat.
- Gardez une liste de contractuels de remplacement, que vous pourrez utiliser si le contractuel principal vous fait faux bond.
- Mettez en place des contrôles appropriés pour surveiller l'accès à distance à vos systèmes.

3. Gérer de façon active la sécurité des données

L'enjeu : EPI n'a peut-être pas les moyens de mettre en œuvre des mécanismes de protection des données appropriés, ou connaît peut-être mal ce type de mécanismes.

Les risques : La gestion des risques liés à la sécurité des données devrait porter notamment sur la perte, l'affichage ou la publication accidentelle de données, la destruction ou le vol intentionnel ou non intentionnel de données, la perte de propriété intellectuelle et le non-respect des exigences des autorités de réglementation. Les coûts rattachés à la gestion de ces risques doivent être évalués par rapport à leur incidence directe sur les résultats et les flux de trésorerie de l'entreprise.

Les solutions : Il est utile de consulter un professionnel qui examinera où vous en êtes en matière de sécurité et qui vous aidera à exploiter les caractéristiques de sécurité déjà comprises dans vos logiciels et dans votre réseau actuels. La mise en œuvre de mécanismes de protection sera d'autant plus efficace que vous aurez élaboré des politiques et des normes minimales qui fourniront une orientation quant au niveau de sécurité recherché; là encore, il pourrait être utile de demander l'aide ponctuelle d'un professionnel pour ce faire. Une autre solution possible consiste à externaliser la surveillance de la sécurité, ce qui pourrait être plus rentable que l'embauche ou la formation d'une personne à l'interne en tant que conseiller en sécurité. En outre, il est prudent de communiquer les attentes définies dans votre politique en établissant un programme annuel général de formation et de sensibilisation en matière de sécurité.

Enfin, vous devez penser à équilibrer les contrôles techniques de la sécurité et la robustesse de vos processus d'affaires et contrôles d'examen, afin de détecter et de corriger tout événement échappant aux contrôles techniques.

4. Veiller à mettre à jour les contrôles antivirus et antimaliciels

L'enjeu : EPI n'a peut-être pas investi dans des logiciels antivirus et antimaliciels appropriés ou, si elle l'a fait, elle a peut-être négligé de faire les mises à jour voulues.

Les risques : Si un maliciel ou un virus s'insinue dans les systèmes, il y a risque de perte, de vol ou de corruption des données.

Les solutions : Acquérir et installer les programmes antivirus d'un fournisseur reconnu (McAfee, Norton) qui exécuteront des processus de prévention et de détection des virus et aviseront EPI de toute mise à jour à faire. Il est important qu'un membre du personnel d'EPI ait la responsabilité de s'assurer que les mises à jour sont effectuées et que les frais de maintenance sont ajustés en fonction du nombre d'utilisateurs.

5. Contrôler l'accès aux systèmes

L'enjeu : EPI n'a pas suffisamment d'employés ou de contractuels à sa disposition pour assurer une séparation appropriée des tâches et pour contrôler les utilisateurs qui ont un accès privilégié aux systèmes.

Les risques : Une augmentation du risque d'erreurs de traitement, de fraude et de perte de données.

Les solutions : Des contrôles efficaces doivent être mis en place afin qu'il soit nécessaire d'obtenir les autorisations appropriées lors de toute nouvelle demande d'accès aux systèmes, et que des mesures immédiates soient prises pour supprimer les droits d'accès des personnes qui n'en ont plus besoin. De plus, des examens doivent être menés régulièrement pour s'assurer que seuls les employés et les contractuels actuels et autorisés ont accès aux systèmes. L'accès aux données et aux fonctions des systèmes ne doit être accordé qu'aux personnes qui en ont besoin pour faire leur travail. Des journaux doivent être conservés quant à certaines activités clés, comme les tentatives de connexion qui ont échoué (trois essais ou plus), les activités des utilisateurs ayant des droits d'accès privilégiés, l'utilisation de certaines commandes clés (ajout d'utilisateurs, modification des droits d'accès) et la mise à jour de certains fichiers essentiels (paie, dossiers des employés, numéros de carte de crédit). Ces journaux doivent être examinés régulièrement par une personne étrangère à ces fonctions, ou par des pairs dont les fonctions sont similaires. Si cette séparation des tâches n'est pas possible, il faut envisager de créer des codes d'utilisateurs spéciaux pour les activités menées sur une base périodique seulement, afin qu'il soit plus facile de journaliser et d'examiner les accès supplémentaires, ou confier les activités de surveillance de la sécurité à un cabinet externe. Envisagez de consulter un professionnel pour vous aider à élaborer les lignes directrices entourant la séparation des tâches.

6. Tenir compte des cybermenaces

L'enjeu : On ne sait pas ce qui a causé la défaillance des serveurs d'EPI, mais les menaces à la cybersécurité ne peuvent être exclues. Devant la couverture médiatique des cyberattaques, la plupart des chefs de la direction prudents cherchent activement à comprendre les incidences que pourraient avoir de telles attaques sur leur propre organisation.

Les risques : Vous vous demandez peut-être s'il existe vraiment des menaces du fait que vous avez une petite entreprise et qu'il y a bien d'autres entreprises plus imposantes et plus intéressantes à viser que la vôtre. Cela dit, vous devez savoir que votre petite entreprise peut être considérée comme une cible facile ou comme une occasion d'utiliser un réseau non protégé pour atteindre vos clients et fournisseurs.

Les solutions : Envisagez de consulter un conseiller professionnel en sécurité pour vous aider à comprendre qui sont les adversaires potentiels de votre entreprise et les menaces qu'ils peuvent représenter, y compris les menaces propres à votre secteur. L'exercice en question s'étend au-delà de vos systèmes financiers, et porte sur les différents points d'accès à vos systèmes par l'intermédiaire d'Internet, de votre site Web, de vos divers emplacements physiques, de vos clients et des partenaires présents dans votre chaîne d'approvisionnement. Vous jugerez peut-être utile aussi d'examiner la robustesse des contrôles de sécurité de tout partenaire d'affaires qui a accès à vos systèmes, car ce peut être une voie d'attaque. Une fois cet exercice fait, vous saurez au moins où investir vos ressources limitées pour assurer votre sécurité.

7. Adopter une stratégie mûrement réfléchie pour atténuer les risques liés aux TI

L'enjeu : Nombre de petites entreprises croient qu'elles ont du succès en raison justement de leur taille et de leur souplesse, et parce qu'elles ne sont pas ralenties par la bureaucratie et les politiques formelles. Les propriétaires de ces entreprises estiment qu'ils peuvent gérer toutes les activités efficacement et garder le cap grâce à leur propre engagement et à leur sens des affaires, qui les ont si bien servis jusqu'à présent.

Les risques : Le risque que pose cette façon informelle d'aborder l'atténuation des risques liés aux TI tient au fait que le propriétaire ne peut pas être un spécialiste dans tous les domaines. Il se peut que le personnel ne soit pas au courant des risques et, sans un plan en bonne et due forme pour élaborer des contrôles d'atténuation et en informer le personnel, l'entreprise s'expose à la perte de données, à l'indisponibilité de ses systèmes, à des erreurs dans le traitement des opérations ainsi qu'à des attaques venant de l'intérieur comme de l'extérieur.

Les solutions : À mesure qu'elles croissent et gagnent en complexité, les entreprises doivent s'attarder à comprendre quels sont les risques liés aux TI, à élaborer leurs stratégies d'atténuation et à les consigner de manière à pouvoir les communiquer et les expliquer au personnel. En plus de ce registre de base des risques liés aux TI, chaque entreprise doit établir et communiquer certaines prises de position clés sur la

façon dont elle gérera les risques au moyen de politiques et de procédures simples que les membres du personnel peuvent comprendre et suivre, et dont la surveillance sera assurée par le propriétaire et les cadres.

Conclusion

En tant que propriétaire d'une petite entreprise, Gabriel a appris à la dure qu'il devait être vigilant dans sa compréhension et sa gestion des risques liés aux TI. Il a été chanceux cette fois-ci, car les choses se sont bien terminées, mais s'il ne prête pas dûment attention aux risques liés aux TI, il pourrait finir par compromettre le succès obtenu au prix de tant d'efforts. S'il suit les recommandations qu'on lui a données, il pourra mieux gérer les risques auxquels son entreprise s'expose en matière de TI.

Au cours de sa discussion avec les conseillers de RRJL, Gabriel s'est rendu compte qu'il aimerait aborder d'autres domaines des TI avec eux une fois ses problèmes immédiats résolus : prise de certaines décisions concernant de nouveaux systèmes, élaboration d'une stratégie de TI s'harmonisant avec la stratégie de l'entreprise et respect de la réglementation relative à la technologie, comme les exigences en matière de protection des renseignements personnels.

Préparation : Robert Reimer, CPA, CA et Jodie Lobana, CPA, CA