

Prévention des fraudes

« L'ingéniosité représente la seule façon de limiter les fraudes à l'interne, affirme James Hunter, président de KPMG Forensic. S'il y a une possibilité de vol, de tromperie, d'enrichissement injuste, soyez assurés que des personnes malhonnêtes sauteront sur l'occasion. »

Et cela peut coûter cher. Selon l'Association des examinateurs certifiés de fraude, le coût moyen d'une fraude envers une petite entreprise est de 97 000 \$, sans compter les coûts indirects tels que la perte de réputation ou de clientèle. Et cela se produit plus souvent que vous ne le croyez.

« Vous seriez certainement très étonné de l'importance de la fraude au sein des petites et moyennes entreprises, déclare Jay Stark, vice-président, Lutte antifraude à RBC Banque Royale. Dans des études menées récemment, plus de 50 % des répondants ont indiqué avoir été victimes de fraude. »

Plusieurs facteurs expliquent le fait que les petites et moyennes entreprises soient particulièrement exposées au

risque. « Elles n'ont pas nécessairement le budget pour s'équiper d'un système de détection, dit M. Hunter, ou bien elles n'ont pas établi de contrôles internes. Et elles fonctionnent davantage sur le principe de la confiance. Cela ouvre la porte à la fraude. »

Un peu de prévention

Les deux hommes s'accordent sur le fait qu'une entreprise, quelle que soit sa taille, dispose de plusieurs mesures de prévention, à commencer par une bonne compréhension des divers types de fraude.

« Il y a d'abord la fraude à l'interne, explique M. Stark. Cela comprend par exemple le vol de biens et de chèques par des employés, ou encore la modification des salaires et des comptes d'approvisionnement. Ensuite, on retrouve la fraude à l'externe, comme la fraude sur chèque, la fraude commerciale et le vol de renseignements confidentiels. »

Pour M. Stark, la réduction de la fraude à l'interne commence par un rigoureux contrôle préalable à l'emploi,



ce qui comprend une vérification des antécédents criminels, de crédit et de faillite, des recherches dans les médias et auprès des tribunaux ainsi qu'un suivi des références fournies à propos de l'emploi et de la formation.

Étant donné que la plupart des fraudes sont découvertes à l'interne (au moyen d'un informateur ou par accident), la culture d'entreprise joue également un rôle clé. « Dans une grande entreprise, vous pourriez mettre en place une ligne téléphonique de dénonciation, suggère M. Hunter. Dans une petite entreprise, vous devez favoriser un environnement dans lequel un employé se sentira à l'aise de faire part de ses soupçons à la haute direction. »

Pour tout ce qui est lié à l'argent, les experts en fraude conseillent aux propriétaires de petites entreprises de « ne jamais quitter l'argent des yeux ». M. Hunter insiste sur le fait que le propriétaire ou le chef de la direction doit faire preuve de vigilance. « Cela signifie de garder l'œil sur le chéquier. Assurez-vous de savoir où vont les entrées et les sorties d'argent. Et si la taille de votre entreprise le permet, séparez les responsabilités. »

Par exemple, il peut s'agir d'avoir une personne responsable de la réception du courrier et une autre personne chargée du contrôle des comptes clients.

Il est également payant de protéger vos chèques contre le vol et la falsification. « La première chose à faire, selon M. Stark, est de réduire le nombre de chèques libellés en passant à un mode de paiement électronique lorsque cela s'avère possible. De plus, les chèques que vous utilisez devraient être assortis de caractéristiques de sécurité spéciales. Enfin, gérez vos stocks de chèques. Cela signifie d'observer une constance dans les couleurs, les polices et les styles d'impression. » Il recommande également d'utiliser un service de vérification des décaissements, un processus de rapprochement de chèques offert par la plupart des institutions financières et qui permet de repérer les chèques contrefaits, dupliqués ou dont le montant a été augmenté avant que le chèque soit encaissé.

Outre la protection des liquidités et des chèques, M. Stark mentionne que les petites et moyennes entreprises doivent se préoccuper de plus en plus de la

protection des renseignements privés des clients et de l'entreprise, surtout si celle-ci est en pleine croissance. « Le plus important est d'exercer un contrôle sur votre entreprise au moyen de politiques et procédures appropriées en ce qui a trait à l'utilisation des renseignements et des technologies de l'information, » conclut-il.

Signaux d'alarme

Si vous craignez que votre entreprise ait été compromise, M. Stark et M. Hunter proposent certains signaux d'alarme à considérer. Il peut s'agir de changements soudains dans les résultats financiers sans explication évidente : ventes faisant un bond vers le haut ou vers le bas, marge de profit qui semble avoir été réduite. Ou encore, si un employé semble vivre nettement au-dessus des moyens que lui procure son emploi. « Vous devez vous demander d'où vient l'argent, dit M. Hunter. N'ignorez pas l'évidence. Si quelque chose cloche, l'explication ne réside pas nécessairement dans la fraude, mais vous devez vérifier, car ce pourrait être le cas. »

Autrement dit, mieux vaut prévenir que guérir.

Pour obtenir des ressources et des conseils utiles qui vous permettront d'atteindre vos objectifs d'affaires, rendez-vous au www.rbc.com/conseilsentreprise.



RBC Banque Royale®

Ce document est présenté uniquement à des fins d'information et n'est pas conçu pour fournir des conseils précis. Veuillez consulter votre conseiller personnel avant de mettre en place une stratégie.

© Marques déposées de la Banque Royale du Canada. RBC et Banque Royale sont des marques déposées de la Banque Royale du Canada.
VPS55192

33117 (11/2009)