Le crime économique gagne du terrain, mais vous pouvez le combattre

36 %
Un peu plus du tiers des organisations canadiennes ont déclaré avoir été victimes de crimes économiques.

38 %
Plus du tiers des organisations canadiennes sondées se sont récemment intéressées à une possibilité d'affaires sur un marché caractérisé par un risque élevé de corruption.

47 %
Près de la moitié des répondants canadiens ont affirmé que la perception du risque de cybercriminalité s'est accrue au sein de leur organisation.

pwc

www.pwc.com/ca/fr/crimesurvey

En dépit des efforts des organisations, des autorités réglementaires et de tous les professionnels qui luttent contre la fraude, le crime économique persiste. Cette tendance présente des occasions non seulement de mieux gérer les risques de fraude et de corruption, mais aussi d'améliorer le positionnement stratégique des organisations.

Table des matières

3 *Introduction*

5 *Le portrait général de la situation*

9 *Faire des affaires à l'échelle mondiale*

9 Pleins feux sur le trafic d'influence et la corruption, le blanchiment d'argent et les lois sur la concurrence et antitrust

11 Un gros plan sur le trafic d'influence et la corruption

14 *Pleins feux sur la cybercriminalité*

14 Notre monde est un vaste réseau : Les avantages et les risques ne sont pas prêts de disparaître

19 *D'autres types de fraudes*

19 La fraude liée à l'approvisionnement : Plus la tentation est grande, plus la menace s'acroît

21 La fraude comptable : Une menace qui persiste

22 Le détournement d'actifs : Le plus répandu des crimes économiques

23 *Le fraudeur*

23 Interne ou externe

29 *La perception du crime économique*

29 Les organisations s'attendent à ce que la fraude persiste

32 *Contactez-nous*

La sophistication et l'ampleur croissantes du crime économique font que ce type de crime constitue une préoccupation grandissante pour les chefs de direction.

Introduction

Le sondage Global Economic Crime Survey 2014 (« le sondage ») mené par PwC a confirmé qu'en dépit des efforts des organisations, des autorités réglementaires et de tous les professionnels qui luttent contre la fraude, le crime économique persiste. Le crime économique peut attaquer vos processus opérationnels, entacher l'intégrité de vos employés et ternir votre réputation. C'est pour toutes ces raisons que le rapport de cette année se concentre sur la manière dont ce crime peut vous affecter et sur ce que vous pouvez faire pour le combattre.

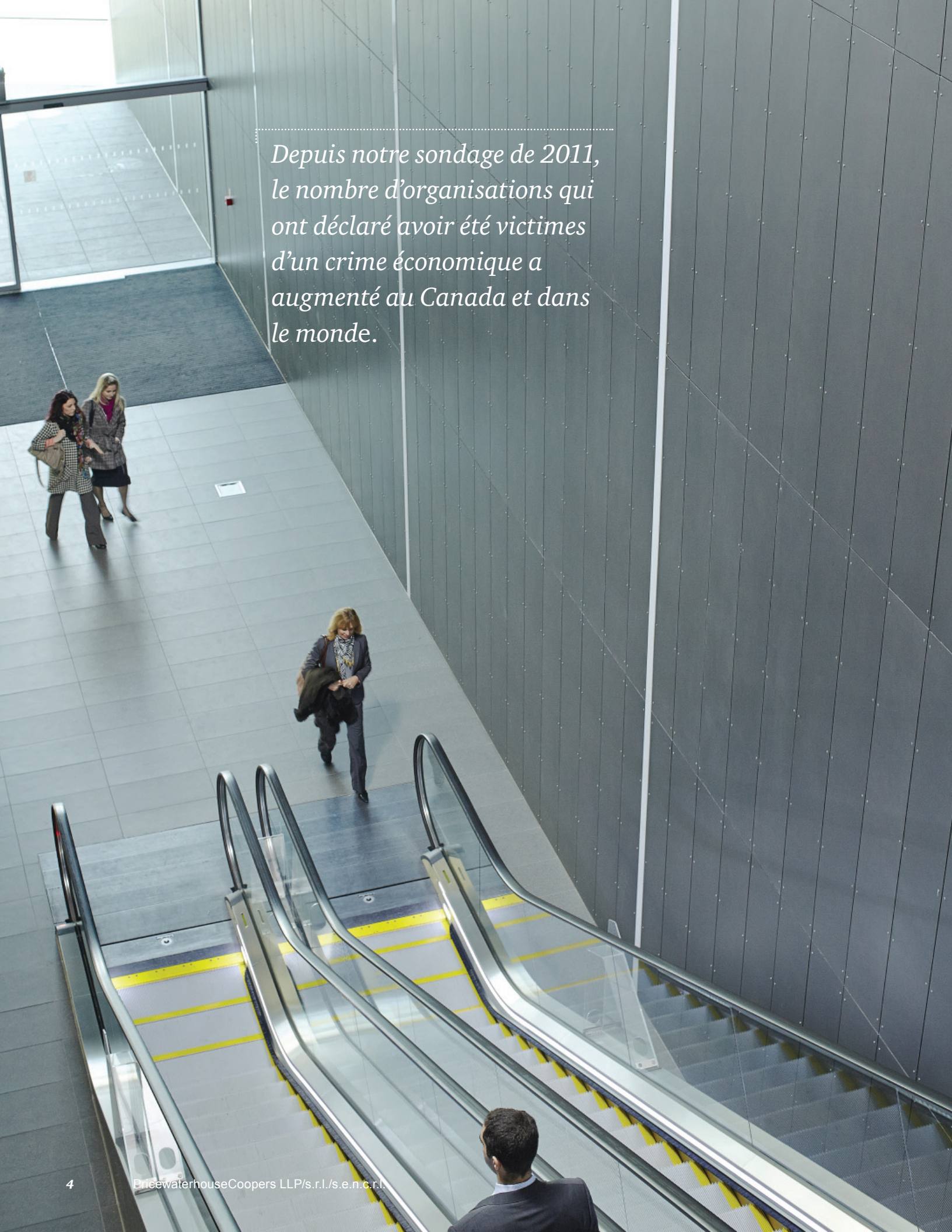
Comme les virus, le crime économique est une menace à facettes multiples en mutation constante; il se dissimule de manière opportuniste au sein des tendances de fond qui touchent chaque organisation et attaque les organisations là où elles sont le plus vulnérables.

La cybercriminalité ne cesse de prendre de l'ampleur et devient de plus en plus sophistiquée, et des catégories de crimes économiques parfois occultées – comme la fraude liée à l'approvisionnement ou la fraude relative aux ressources humaines – remontent vers les premières places sur la liste des menaces, en compagnie d'autres catégories comme le détournement d'actifs, le trafic d'influence et la corruption, le blanchiment d'argent et la fraude comptable.

La sophistication et l'ampleur croissantes du crime économique font que ce type de crimes constitue une préoccupation grandissante pour les chefs de direction. Plus de la moitié des dirigeants de organisations qui ont participé à notre « Enquête mondiale 2014 menée auprès des chefs de direction » ont déclaré que le trafic d'influence et la corruption les inquiétaient ou les inquiétaient fortement.

Cette année, au lieu d'agiter le « drapeau rouge » de la mise en garde, nous nous concentrons sur les thèmes – et les stratégies – suggérés par les résultats de notre sondage, parce qu'il se cache au sein des tendances et des menaces mondiales des opportunités stratégiques – non seulement de bien gérer les risques, mais aussi d'assurer la réussite des organisations et de leur donner un avantage concurrentiel.

Ce rapport présente une comparaison entre les résultats du sondage canadien de 2014, ceux du sondage canadien de 2011 et ceux du sondage mondial de 2014. Il établit la position du Canada par rapport au reste du monde en matière de crimes économiques.



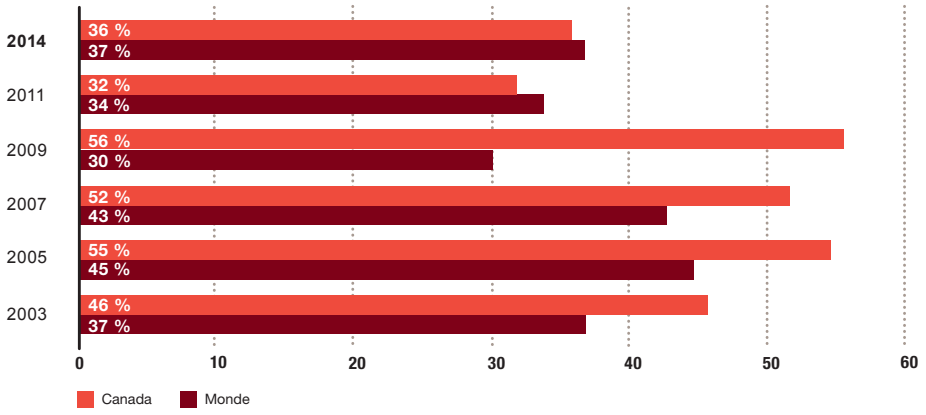
Depuis notre sondage de 2011, le nombre d'organisations qui ont déclaré avoir été victimes d'un crime économique a augmenté au Canada et dans le monde.

Le portrait général de la situation

Les résultats de notre sondage de 2014 indiquent que 36 % des organisations canadiennes (37 % à l'échelle mondiale) ont déclaré avoir été victimes d'un crime économique au cours de la période visée par le sondage. La figure 1 montre que, depuis notre sondage de 2011, le nombre d'organisations qui ont déclaré avoir été victimes d'un crime économique a augmenté au Canada (4 %) et dans le monde (3 %). Le sondage de cette année confirme que le crime économique reste une réalité incontournable pour les organisations, et ce, peu importe où elles sont situées dans le monde.

Depuis le sondage mené en 2011 par PwC, moins de crimes économiques ont été signalés au Canada qu'ailleurs dans le monde. Cette tendance pourrait s'expliquer par le fait que les organisations canadiennes sont plus diligentes que les autres à mettre en œuvre des programmes antifraudes robustes, comprenant des mesures d'évaluation des risques de fraude et la mise en place de systèmes de dénonciation, ce qui réduit les occasions de commettre des fraudes et renforce la capacité de l'organisation de les détecter. Cependant, cette augmentation globale du nombre de crimes économiques est troublante, car le nombre de crimes signalés risque d'être inférieur à la réalité.

Figure 1 : Organisations ayant déclaré une fraude

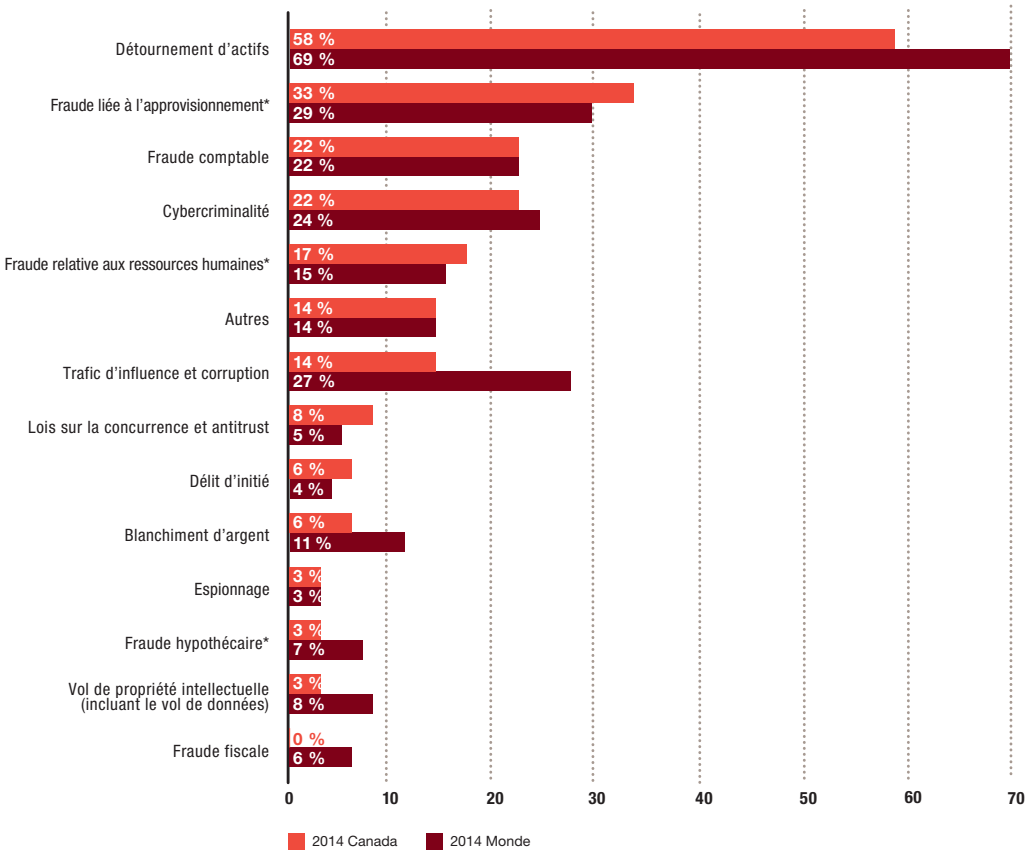


Les types de crimes économiques

Le crime économique prend diverses formes, chacune ayant ses propres caractéristiques, menaces et conséquences stratégiques. La figure 2 montre les différents types de crimes économiques déclarés par les répondants canadiens. Le crime le plus courant est le détournement d'actifs, soit le vol de biens de l'organisation (y compris les actifs monétaires ou en espèces ou les fournitures et le matériel) par des personnes (p. ex., des employés ou des dirigeants) de l'organisation. Le détournement d'actifs est cité par 58 % des organisations canadiennes qui disent avoir été victimes d'un crime économique au cours de la période visée par le sondage. La fraude liée à l'approvisionnement (33 %), une nouvelle catégorie ajoutée à notre sondage, est la seconde catégorie la plus courante. Viennent ensuite la cybercriminalité et la fraude comptable (toutes deux à 22 %).

En plus de la fraude liée à l'approvisionnement, nous avons ajouté deux nouvelles catégories de crimes économiques à notre sondage de 2014 : la fraude relative aux ressources humaines et la fraude hypothécaire.

Figure 2 : Types de crimes économiques



* Les répondants pouvaient sélectionner ces catégories de crimes économiques pour la première fois lors de notre sondage de 2014.

Le préjudice financier

Bien qu'il soit difficile de mesurer le coût financier d'un crime économique, plus de un répondant canadien sur dix ayant indiqué qu'un crime économique a affecté leur organisation pendant la période visée par le sondage ont déclaré des pertes de plus de 5 millions $ US (figure 3).

Par ailleurs, à l'échelle mondiale, le pourcentage de répondants qui ont déclaré que leur organisation avait subi des pertes de plus de 100 M$ US a doublé depuis notre dernier sondage, passant de 1 % à 2 %. Ces pertes élevées sont peut-être attribuables à l'augmentation des cas de trafic d'influence et de corruption déclarés – des fraudes qui peuvent s'avérer particulièrement coûteuses pour les organisations qui en sont victimes, en raison des amendes découlant des infractions à la réglementation, des frais juridiques et des coûts liés aux mesures correctives.

Figure 3 : Pertes financières

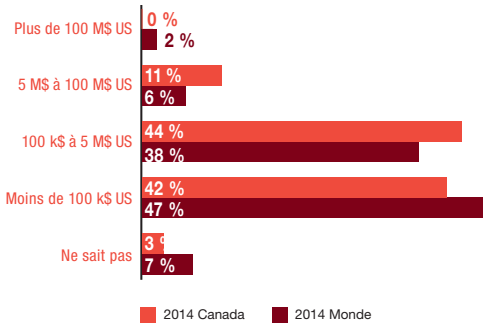
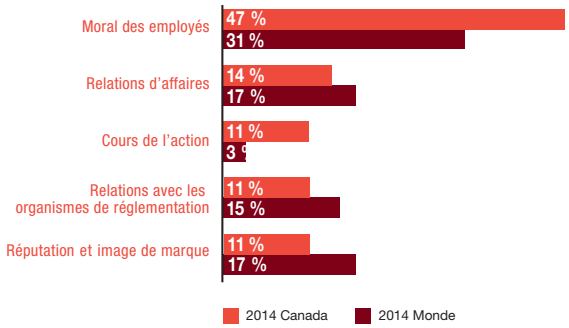


Figure 4 : Dommages indirects – une incidence notable sur les activités commerciales



Les dommages indirects : difficiles à évaluer, difficles à ignorer

Les pertes économiques ne sont pas les seuls problèmes auxquels les organisations sont confrontées dans leur combat contre la fraude. Les répondants canadiens ont indiqué que les préjudices non financiers les plus graves entraînés par la fraude sont, entre autres, les dommages indirects causés au moral des employés (47 %), les incidences négatives sur les relations d'affaires (14 %) ainsi que sur la réputation et l'image de marque (11 %). La figure 4 donne des détails additionnels sur les dommages indirects importants déclarés pas les organisations.

Lorsqu'on prend en considération les dommages indirects, le coût réel d'une fraude peut avoir des conséquences à long terme. Il est certes difficile d'attribuer une valeur purement financière aux dommages, mais une chose est claire : si une fraude affecte l'embauche, la rétention des employés, les relations d'affaires et la réputation, elle aura des effets sur l'état des résultats – même si elle n'y est pas présentée comme une « fraude ». Les employés d'aujourd'hui sont très motivés par des facteurs non financiers, comme l'atmosphère de travail d'équipe et la certitude que l'organisation qui les emploie est une organisation où il fait bon travailler. L'attention négative des médias ou la perception que l'activité criminelle est tolérée peuvent altérer le moral des employés ou leur perception de leur employeur.

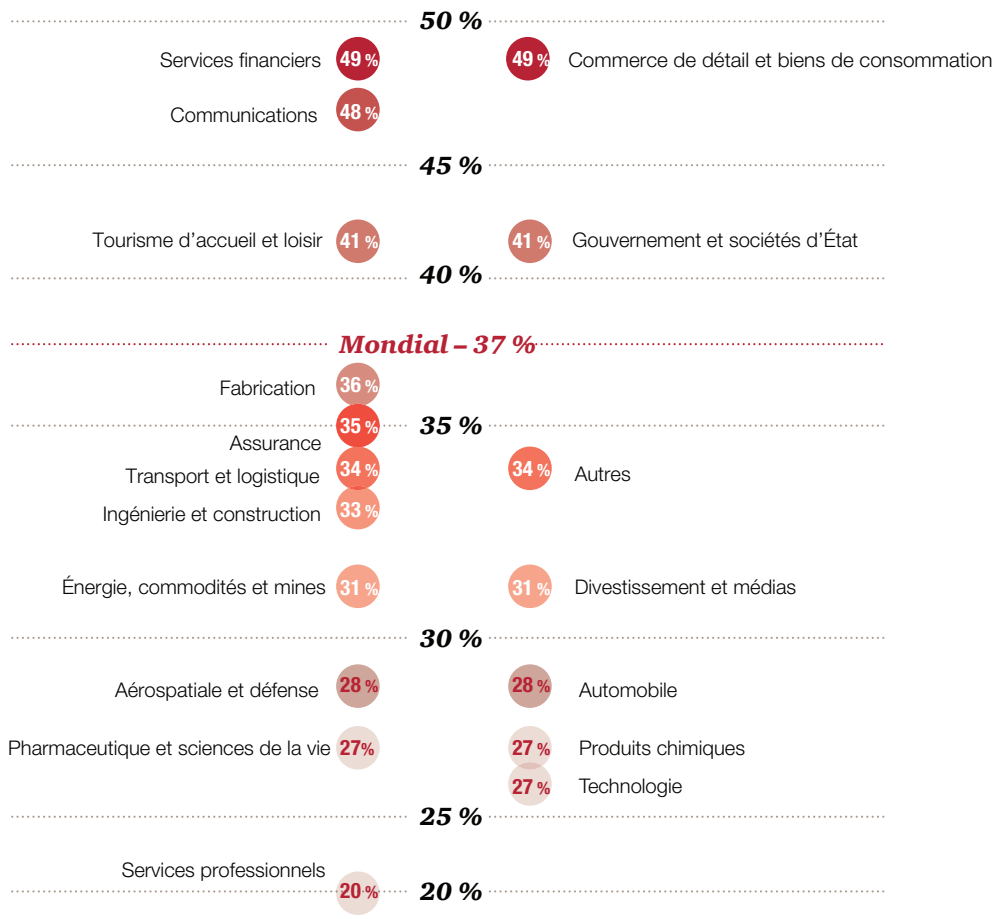
Dans une proportion de 11 %, les répondants canadiens ont estimé que la réputation et l'image de marque de leur organisation avaient été ternies considérablement par suite d'un crime économique. Toutefois, comme ces éléments sont souvent étroitement associés à l'avantage concurrentiel d'une organisation et que plusieurs années sont souvent nécessaires pour les rétablir, il est important de ne pas sous-estimer les répercussions des dommages indirects.

L'analyse des crimes économiques selon les industries

À l'échelle mondiale, trois industries sont davantage frappées par les crimes économiques : les services financiers, le commerce de détail et les biens de consommation, ainsi que les communications. Dans les services financiers, les cas relativement nombreux de cybercriminalité et de blanchiment d'argent font monter les niveaux de fraude. Sans surprise, les cas de détournement d'actifs sont relativement importants dans l'industrie du commerce de détail et des biens de consommation. Il en est de même dans l'insdustrie des communications.

La figure 5 présente les résultats obtenus par industrie, à l'échelle mondiale.

Figure 5 : Types de crimes économiques déclarés par industrie



% des répondants qui ont été victimes d'un crime économique au cours de la période visée par le sondage

Comme le démontre la figure 5, nous avons constaté une forte concentration d'industries où les organisations ont signalé des fraudes dans une proportion de 27 % à 36 %. Bien que ces pourcentages soient inférieurs à la moyenne mondiale de 37 %, nombre de ces industries – en particulier celles de l'énergie, des commodités et des mines, de l'ingénierie et de la construction ainsi que du transport et de la logistique – sont plus exposées aux crimes économiques tels que le trafic d'influence et la corruption ou la fraude liée à l'approvisionnement.

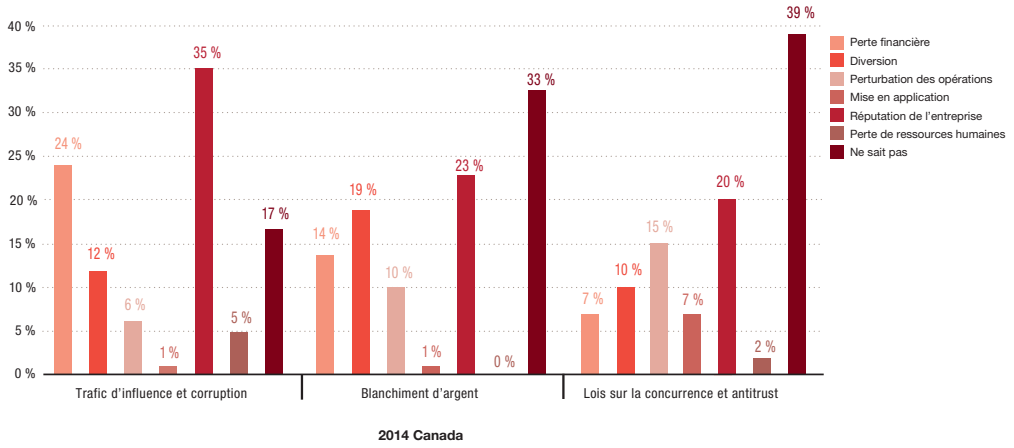
Pleins feux sur le trafic d'influence et la corruption, le blanchiment d'argent et les lois sur la concurrence et antitrust

Certaines formes de crimes économiques peuvent entraîner beaucoup plus de risques que d'autres; c'est le cas du trafic d'influence et de la corruption, du blanchiment d'argent et des comportements anticoncurrentiels. Ces trois crimes sont sanctionnés par les pouvoirs publics et visés par des normes de plus en plus rigoureuses, de mieux en mieux appliquées et des peines de plus en plus sévères. Dans un monde interdépendant, ces crimes représentent des dangers particuliers pour les organisations multinationales.

Si le détournement d'actifs peut s'apparenter à un vol à la tire ou à un cambriolage, une violation grave d'une loi anticorruption comme la Loi sur la corruption d'agents publics étrangers (« LCAPE ») au Canada ou la Foreign Corrupt Practices Act (« FCPA ») aux États-Unis – qui peut donner lieu à de fortes amendes et grandement affecter une organisation – s'apparente à une agression systémique contre l'organisation.

Outre qu'elles donnent lieu à des amendes élevées et même à des poursuites criminelles, ces violations peuvent être considérées comme un problème organisationnel plus vaste et avoir des répercussions très négatives – allant de l'atteinte à la réputation aux pertes financières, en passant par une perturbation coûteuse des opérations et la perte de compétences inestimables au sein du personnel.

Figure 6 : Incidences sur les organisations du trafic d'influence et de la corruption, du blanchiment d'argent et des lois sur la concurrence et antitrust



En ce qui concerne la corruption et le trafic d'influence, le blanchiment d'argent et les lois sur la concurrence et antitrust, les répondants canadiens considèrent que l'atteinte à la réputation de l'organisation est la répercussion la plus grave (respectivement 35 %, 23 % et 20 % de ces répondants – figure 6). Les autres répercussions déclarées par les répondants canadiens sont discutées ci-dessous, et ce, de manière disctincte pour chacun de ces trois types de crimes économiques :

- **Le trafic d'influence et la corruption :** les pertes financières se classent en deuxième position avec 24 % des voix des répondants canadiens, suivies de la diversion causée par les mesures d'application de la loi et de la réglementation (12 %), de la perturbation des opérations (6 %), de la perte de ressources humaines (5 %) et de la mise en application de politiques, de procédures et d'outils de conformité (1 %).
- **Le blanchiment d'argent :** la diversion causée par les mesures d'application de la loi et de la réglementation se classe en deuxième position avec 19 % des voix des répondants canadiens, suivie des pertes financières (14 %), de la perturbation des opérations (10 %) et de la mise en application de politiques, de procédures et d'outils de conformité (1 %).
- **Les lois sur la concurrence et antitrust :** la perturbation des opérations se classe en deuxième position avec 15 % des voix des répondants canadiens, suivie de la diversion causée par les mesures d'application de la loi et de la réglementation (10 %), des pertes financières et de la mise en application de politiques, de procédures et d'outils de conformité (chacune avec 7 % des réponses) et de la perte de ressources humaines (2 %).

La quantification des pertes

Il est important de prendre la mesure du coût financier associé au trafic d'influence et à la corruption, au blanchiment d'argent et aux comportements anticoncurrentiels. Comme nous l'avons mentionné précédemment dans ce rapport, ces types de crimes économiques ne sont pas les plus fréquents (figure 2). Néanmoins, les résultats de notre sondage démontrent que leur coût peut être considérable. Plus précisément :

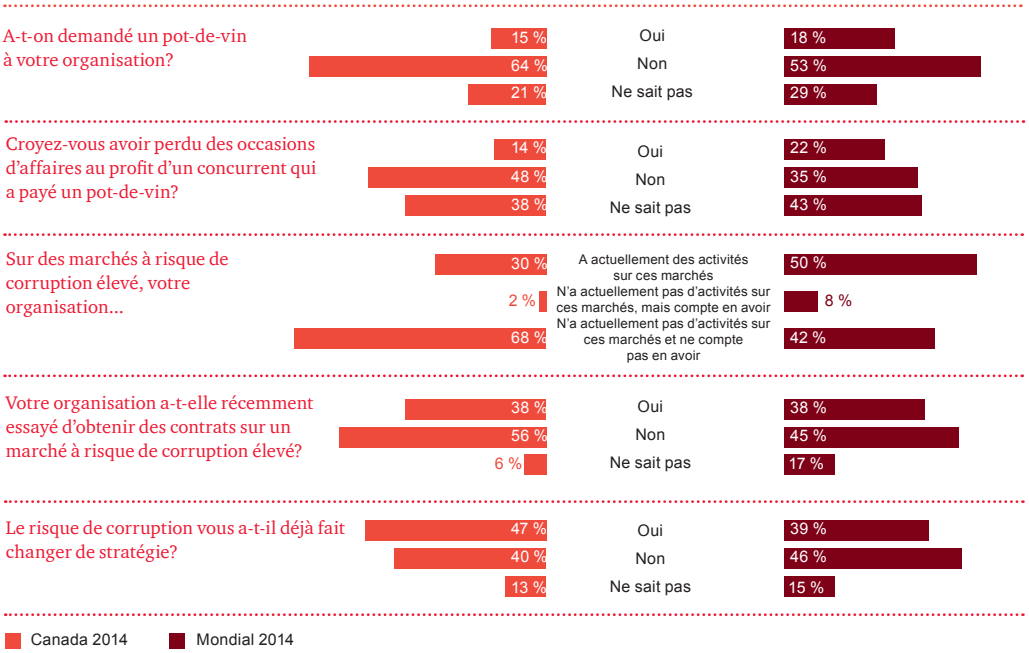
- **Le trafic d'influence et la corruption :** 13 % des répondants canadiens ont déclaré des pertes supérieures à 100 000 $ US et 4 % d'entre eux, des pertes oscillant entre 5 millions $ US et 100 millions $ US;
- **Le blanchiment d'argent :** 4 % des répondants Canadiens ont fait état de pertes comprises entre 100 000 $ US et 1 million $ US;
- **Les lois sur la concurrence et antitrust :** 4 % des répondants ont fait état de pertes de plus de 100 000 $ US et 1 %, de pertes comprises entre 5 millions $ US et 100 millions $ US.

Lorsque nous leur avons demandé de classer les risques de trafic d'influence et de corruption, de blanchiment d'argent et d'infractions aux lois sur la concurrence et antitrust associés aux affaires conduites à l'échelle mondiale, la majorité des répondants canadiens (60 %) a jugé que le trafic d'influence et la corruption sont les éléments qui présentent le niveau de risque le plus élevé.

Un gros plan sur le trafic d'influence et la corruption

Chaque région du monde a déclaré un nombre élevé de cas de trafic d'influence et de corruption. Même si le Canada ne figure pas parmi les pays ayant déclaré les plus hauts taux de corruption, plusieurs données intéressantes méritent d'être signalées. La figure 7 présente ces données.

Figure 7 : Trafic d'influence et corruption – leurs incidences sur l'organisation



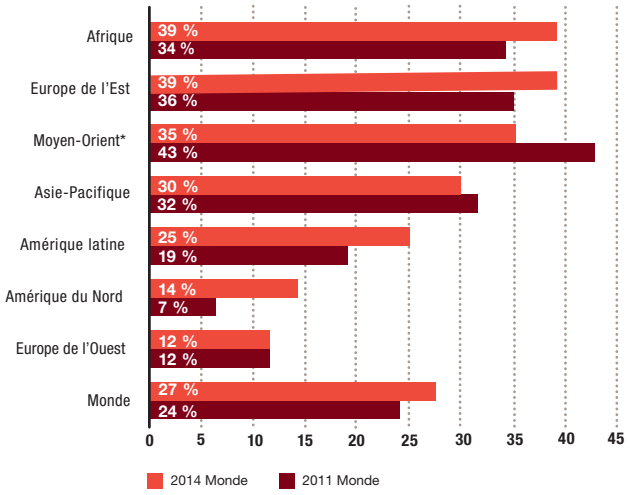
La figure 7 démontre que globalement, les répondants canadiens ont signalé moins de demandes de pots-de-vin (15 %) que les répondants à l'échelle mondiale (18 %). Elle démontre également que 14 % des répondants canadiens estiment avoir perdu une occasion d'affaires au profit d'un concurrent qui a payé un pot-de-vin.

Les résultats de notre sondage révèlent également que 50 % des organisations multinationales estiment évoluer sur des marchés affichant un risque élevé de corruption, alors que ce pourcentage tombe à 30 % pour les organisations canadiennes. Cet écart important suggère que les organisations canadiennes pourraient ne pas être préparées ou avoir suffisamment confiance dans leurs procédures et contrôles anticorruption pour faire affaires sur des marchés à risque élevé. En ayant évité les marchés à risque élevé plus souvent que les organisations multinationales, les organisations canadiennes pourraient avoir perdu des occasions de générer des revenus sur des marchés où il est possible d'atténuer le risque de fraude en appliquant un programme de gestion des risques de fraude approprié.

Pendant le sondage, 38 % des répondants canadiens ont mentionné qu'une occasion d'affaires s'était récemment présentée pour leur organisation sur un marché caractérisé par un risque élevé de corruption. Parmi ces répondants, 47 % ont modifié leur plan d'affaires du fait d'un risque de corruption et 40 % ne l'ont pas fait. Les 13 % restants ignoraient s'ils l'avaient fait ou non, ce qui est préoccupant étant donné les conséquences de la corruption précédemment discutées dans ce rapport. Ces statistiques devraient inciter les membres de la direction et des conseils d'administration à dresser un programme de gestion des risques de fraude, surtout quand l'organisation s'aventure sur un marché très risqué. Cela dit, parmi les 47 % des répondants qui ont modifié leur plan d'affaires, 78 %, ont indiqué avoir mis en œuvre des contrôles diligents supplémentaires. La stratégie ayant recueilli le plus d'appui en deuxième lieu (33 %) consistait à se retirer purement et simplement du marché, ce qui, ici aussi, pourrait s'être traduit par la perte d'une occasion d'affaires et des revenus correspondants.

Nous croyons que l'une des raisons du nombre élevé de cas de trafic d'influence ou de corruption qui ont été rapportés pourrait être la tendance générale au transfert de richesse des pays développés d'Occident vers les pays émergents en expansion rapide du Sud et de l'Est. La figure 8 présente les cas de trafic d'influence et de corruption déclarés par les répondants à l'échelle mondiale, et ce, par région.

Figure 8 : Trafic d'influence et corruption déclarés par région



* Le Moyent-Orient était inclus dans la région Asie-Pacifique en 2011.

Comme le révèle la figure 8, davantage de cas de trafic d'influence et de corruption ont été déclarés dans les régions comme l'Afrique, l'Europe de l'Est et le Moyen-Orient. Bon nombre de ces pays ou régions pourraient avoir une attitude culturelle différente face à la fraude et à la corruption, être moins réglementés et soumis à une application de la réglementation plus aléatoire, ce qui hausse le profil de risque de ce type de crimes économiques. Si d'autres régions comme l'Amérique du Nord (14 %) et l'Europe de l'Ouest (12 %) se situent dans le bas de l'échelle pour les cas déclarés de trafic d'influence et de corruption, cela est grandement attribuable à l'influence des mesures d'application de la loi déployées par leur gouvernement respectif.

Comme les cas de trafic d'influence et de corruption font souvent l'objet de poursuites par les autorités au-delà des frontières, les organisations doivent être conscientes des risques importants que comportent les activités exercées dans les régions en expansion rapide, même si les pratiques et les coutumes de ces régions sont plus laxistes.

Le trafic d'influence et la corruption – l'atténuation des risques

Peu importe votre industrie ou les régions où votre organisation exerce ses activités, il existe des moyens de diminuer le risque de trafic d'influence et de corruption. Voici les quatre sphères que nous proposons de cibler en priorité :

1) **La direction doit donner l'exemple.** Bien que le respect des lois soit l'affaire de tous, l'exemple doit venir d'en haut, ce qui suppose une bonne compréhension des lois anticorruption, un message clair et cohérent affirmant que le trafic d'influence et la corruption ne sont pas tolérés et l'affectation de ressources suffisantes pour lutter contre ces menaces.

2) **L'évaluation des risques.** L'organisation et son environnement de conformité étant en évolution constante, il est essentiel de faire des évaluations périodiques des risques et de s'assurer que les risques identifiés antérieurement ont été mitigés.

3) **L'environnement de contrôle.** Pour lutter efficacement contre les risques de corruption, il faut un plan de communication solide et des procédures internes vigilantes de mise en application. Il faut donc non seulement prévoir un code de conduite écrit et former le personnel en conséquence (notamment sur des questions de conformité délicates comme les cadeaux et les divertissements), mais aussi un système de contrôles pour surveiller les transactions douteuses. Finalement, il faut se rappeler que le degré de conformité d'une organisation se mesure par rapport à son maillon le plus faible. Les partenaires commerciaux, les fournisseurs et les autres tiers doivent aussi être contrôlés et surveillés afin de bien gérer le risque de faire des affaires dans des pays plus exposés à la corruption.

4) **L'évaluation de l'efficacité.** Les programmes d'évaluation des risques et des contrôles ne suffisent pas à assurer le respect de la loi. Il faut également des contrôles diligents, des visites périodiques par la direction des lieux à risque élevé, des rapports de conformité adressés au conseil d'administration, un suivi sur la ligne de dénonciation, un suivi sur les cas potentiels de fraude et de corruption signalés et des audits des partenaires commerciaux. De plus, tous ces éléments doivent être réévalués régulièrement dans le cadre d'un programme interne de conformité.

En ayant évité les marchés à risque élevé plus souvent que les organisations multinationales, les organisations canadiennes pourraient avoir perdu des occasions de générer des revenus sur des marchés où il est possible d'atténuer le risque de fraude en appliquant un programme de gestion des risques de fraude approprié.

Notre monde est un vaste réseau
Les avantages et les risques ne sont pas prêts de disparaître

La cybercriminalité, aussi appelée crime informatique, est un crime économique commis à l'aide d'un ordinateur et d'Internet.
Ce genre de crime comprend la transmission de virus, le téléchargement illégal de contenus, l'hameçonnage et le détournement de domaine ainsi que le vol de renseignements personnels tels que des renseignements sur les comptes bancaires. Cette définition ne comprend pas les types courants de fraudes dans lesquelles un ordinateur est utilisé comme accessoire pour frauder. Elle n'inclut que les crimes économiques dans lesquels un ordinateur, Internet et d'autres appareils électroniques jouent un rôle de premier plan et non accessoire dans la perpétration du crime.

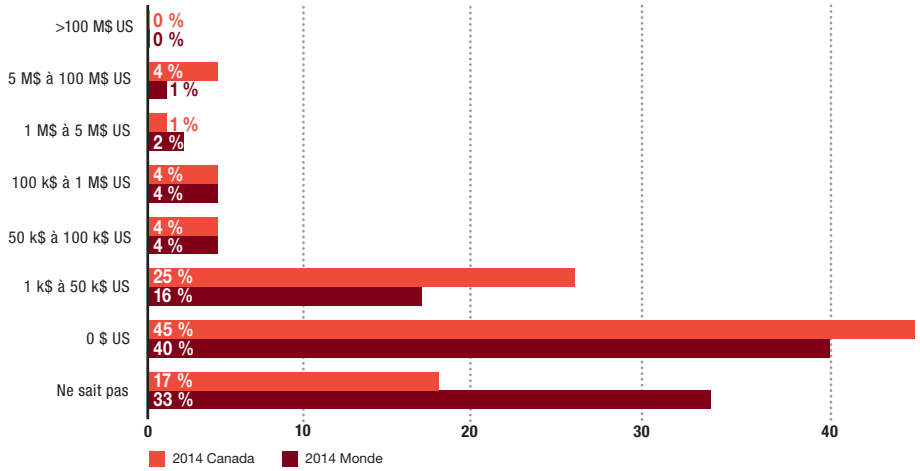
Selon notre sondage de 2014, la cybercriminalité continue de se classer parmi les principaux crimes économiques, derrière le détournement d'actifs et la fraude liée à l'approvisionnement (figure 2). L'avancée de la technologie dans les organisations, l'essor spectaculaire des médias sociaux et la dépendance des organisations à la connectivité ont contribué à la prolifération de la cybercriminalité dans notre société.

La connectivité et la facilité d'accès ont leur côté sombre – cela permet à des criminels décidés, qui maîtrisent parfaitement les technologies, de perpétrer leurs méfaits à l'insu de leurs victimes. Comme ces criminels agissent dans l'ombre, il peut arriver que des organisations ne s'aperçoivent qu'elles ont été attaquées que longtemps après que le mal a été fait. C'est pour cela que la fraude électronique est un des crimes économiques les plus dangereux.

Le coût que vous pouvez évaluer

Notre sondage de 2011 avait été le premier de notre série à révéler que la cybercriminalité était une très grave menace pour les organisations. Le sondage de cette année confirme l'impact important et constant de ce genre de crimes sur les organisations; près de un répondant sur quatre a rapporté que son organisation a été victime de la cybercriminalité (figure 2) – et plus de 5 % d'entre eux ont rapporté des pertes financières de plus de 1 million $ US (figure 9).

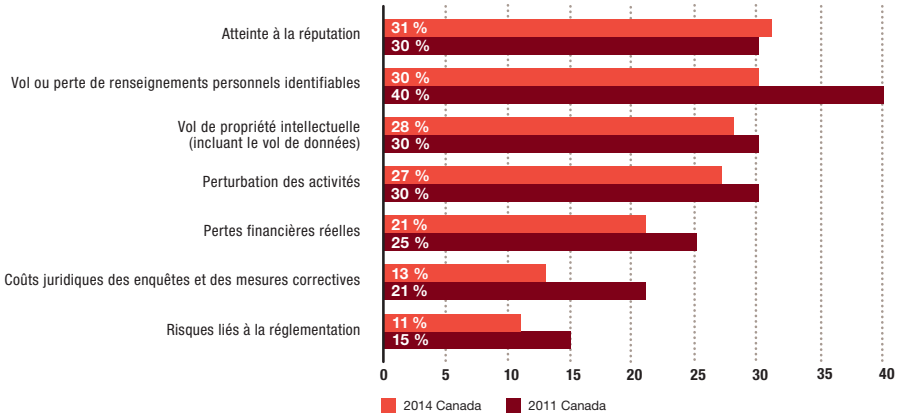
Figure 9 : Cybercriminalité : pertes estimées



Le coût qui fait peur aux organisations

Les résultats de notre sondage confirment les répercussions financières évidentes de la cybercriminalité. Toutefois, comme l'illustre la figure 10, les plus grandes craintes des répondants canadiens à l'égard de la cybercriminalité sont l'atteinte à la réputation (31 %) et les conséquences que pourraient avoir le vol ou la perte de renseignements personnels identifiables (30 %). Ils considèrent les coûts potentiels associés à ces risques plus dangereux que les pertes financières qu'ils pourraient subir en raison de la cybercriminalité (21 %).

Figure 10 : Coût qui préoccupe les organisations

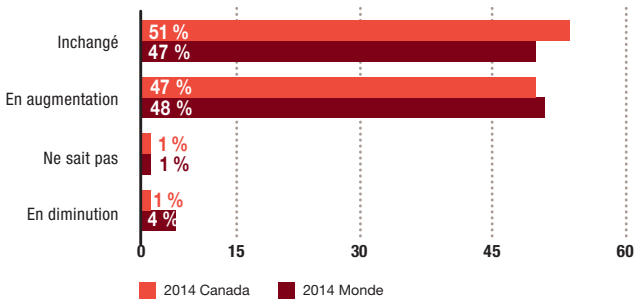


Les résultats de notre sondage soulignent que les organisations sont conscientes que les conséquences indirectes de la cybercriminalité leur font courir un risque beaucoup plus important que les pertes financières associées à ce type de fraude. Par exemple, une attaque lancée sur un réseau de jeux vidéo, qui cause une fuite de renseignements personnels peut éroder la confiance des clients, provoquer des interruptions de service et faire baisser le nombre d'utilisateurs. Tout cela peut causer un préjudice financier à l'organisation. Il est important de souligner que même s'il est parfois impossible d'évaluer sur le champ les conséquences financières de la cybercriminalité, cela n'en diminue pas nécessairement la gravité. Il est rare qu'une attaque n'ait qu'une seule conséquence; les implications peuvent être beaucoup plus graves dans le futur.

La perception de l'avenir de la cybercriminalité

Il ressort de notre sondage que les organisations continuent de prendre la menace de la cybercriminalité très au sérieux puisque 47 % des répondants canadiens estiment que leur perception du risque associé à ce type de crime économique s'est accrue au cours de la période visée par le sondage. Seulement 1 % de ces mêmes répondants ont indiqué que leur perception de ce risque avait diminué. Globalement, les résultats de notre sondage détaillés dans la figure 11, illustrent la crainte croissante des organisations à l'égard de la cybercriminalité au Canada et ailleurs dans le monde, et la nécessité de demeurer à l'affût des menaces qui font leur apparition ou

Figure 11 : Perception des risques associés à la cybercriminalité



sont en émergence.

L'ignorance peut coûter cher

Qu'environ un quart des répondants déclarent que leur organisation a été victime de la cybercriminalité est assez inquiétant, mais il faut savoir qu'un pourcentage important d'organisations en ont peut-être été victimes à l'insu de leur répondant. La situation est donc très alarmante.

Le tableau se complique encore, car il arrive souvent que des organisations décident de ne pas déclarer les cas de cybercriminalité qu'elles ont détectés. À part les violations touchant certains domaines réglementés, comme le vol d'identité, peu de dispositions réglementaires exigent que ces crimes soient déclarés. Il peut y avoir des raisons impérieuses, liées à la concurrence – dans le cas, par exemple, d'un vol de propriété intellectuelle important – de garder le silence sur de telles pertes pour éviter les embarras publics ou les critiques.

Supposons qu'un document confidentiel sur la planification d'une offre de service soit volé par des cybercriminels et utilisé par un rival pour remporter cette offre, l'organisation propriétaire du document va-t-elle déclarer ce vol? Les organisations se protègent-elles bien contre de tels crimes et si un crime est découvert, comment en évaluer la perte?

En résumé, la plus grande partie des dommages causés par ce genre d'attaques n'est pas révélée, parce qu'elles ne sont pas détectées, parce que les pertes sont difficiles à évaluer ou parce que les victimes n'en parlent pas. Il est évident que ce genre de flou opérationnel fait courir des risques aux organisations qui dépendent de plus en plus de la technologie et de la propriété intellectuelle, et ce, dans un environnement qui valorise la transparence.

Un environnement dans lequel il est plus facile de voler un actif incorporel vital que d'estimer la valeur, de déclarer ou même de détecter une perte est un environnement dangereux.

L'intégrité des données est menacée

Les données recueillies et conservées par de nombreuses organisations contiennent souvent des renseignements privés, ce qui donne aux criminels la possibilité de voler des données qu'ils peuvent utiliser à toutes sortes de fins; par exemple, pour accéder à des comptes financiers et voler de l'argent.

Les organisations d'aujourd'hui dépendent largement de la technologie et de la connectivité informatiques ce qui amplifie les conséquences des cyberattaques qui affectent la propriété intellectuelle, l'avantage concurrentiel, la stabilité opérationnelle, la conformité à la réglementation et la réputation, sans compter l'intégrité des données. Les données, en tant qu'actif, n'ont pas toutes la même valeur et elles continuent de croître à un rythme extraordinaire. Assurer le plus haut degré de protection à toutes les données n'est ni réaliste ni possible. La perte de certains types de données peut être simplement gênante, alors que la perte d'autres peut détruire des pans entiers d'une organisation.

Vos données sensibles circulent et sont utilisées probablement dans tout l'écosystème de vos affaires, ce qui étend considérablement le domaine à surveiller et à protéger. Aujourd'hui, l'intégrité et la stabilité de votre organisation dépendent plus que jamais de ceux qui ont accès à votre réseau de données.

Une conséquence involontaire de l'accès universel à la technologie dans les organisations a été de créer des vulnérabilités qui sont exploitées par les ennemis – ce qui accroît fortement le degré d'exposition des organisations et les incidences négatives possibles. Parmi les exemples, citons le vol d'informations de recherche et de développement, la reproduction rapide de produits ou de procédés, l'accès à des renseignements stratégiques ou sur les clients et la perturbation de la stabilité opérationnelle. Ces adversités minent la rentabilité à long terme et l'avantage concurrentiel de l'organisation.

Les dirigeants et les conseils d'administration des organisations ne peuvent plus se contenter de considérer les cyberattaques comme un problème de technologie; celles-ci concernent aujourd'hui l'organisation dans son ensemble. Cela doit commencer en haut de l'échelle : les hauts dirigeants doivent intégrer la cybercriminalité dans leur programme d'activités et évaluer leur tolérance face à ce risque.

La cybercriminalité est un problème humain, pas un problème technologique

Même parmi les organisations généralement conscientes des différents types de menaces informatiques dont elles pourraient être victimes, beaucoup ne comprennent pas très bien les capacités des criminels, les cibles qu'ils peuvent viser et la valeur que peuvent avoir ces cibles. Les organisations cherchent à mettre des données critiques à la disposition de la direction, des employés, des fournisseurs et des clients sur toutes sortes de plates-formes – y compris sur les plates-formes à risque élevé comme les téléphones portables ou l'informatique en nuage – parce que les avantages économiques et concurrentiels semblent si intéressants.

Il est intuitivement facile de comprendre les avantages de la disponibilité des données, et personne ne s'attend à ce que les organisations réduisent leurs volumes de données numériques. Cependant, alors qu'une quantité grandissante de données est accessible sur un nombre sans cesse croissant de plates-formes, il est évident que les données les plus importantes continueront d'être attaquées, et que le coût des atteintes à la sécurité augmentera.

Aujourd'hui, le réseau est le centre nerveux du monde des affaires et il est en constante évolution. Les adversaires sophistiqués en profitent pour s'attaquer à toutes les nouvelles faiblesses. Les organisations doivent donc se maintenir au niveau des forces qui les menacent. En définitive, la cybercriminalité n'est pas un problème technologique; c'est un problème humain qui concerne la stratégie et les processus.

Les mesures de protection contre les cyberattaques

- **Mobiliser le chef de la direction** – le chef de la direction et le conseil d'administration doivent être sensibilisés aux menaces informatiques et comprendre les risques et les possibilités du cyberespace.
- **Réévaluer** – réévaluer la fonction sécurité et l'état de préparation de l'organisation en cas de crime informatique. Contrairement aux crimes économiques traditionnels, les crimes informatiques évoluent rapidement en raison des avancées technologiques entraînant constamment de nouveaux risques, ce qui contraint l'organisation à adapter continuellement ses procédures.
- **Sensibiliser** – les organisations doivent bien connaître le monde informatique actuel et en émergence. Ainsi, elles pourront prendre des décisions et des mesures éclairées en fonction de leurs priorités.
- **Créer une équipe d'intervention en cas de cyberincidents** – une équipe d'intervention rapide et efficace s'assure, dès le signalement d'un incident n'importe où dans l'organisation, que celui-ci fait l'objet d'un suivi, qu'il est évalué en fonction des risques et que les dirigeants de l'organisation en sont informés.
- **Former tous les employés** – toute organisation doit implanter une culture de « cybersensibilisation » et communiquer à l'ensemble du personnel les politiques, les procédures et les protocoles appropriés.
- **Les organisations doivent adopter une approche plus active et transparente à l'égard de la cybercriminalité** – prendre des mesures en poursuivant les auteurs de crimes informatiques au moyen de poursuites judiciaires et communiquer publiquement les mesures prises par l'organisation contre les menaces et les incidents.

La fraude liée à l'approvisionnement
Plus la tentation est grande, plus la menace s'accroît

Comme nous l'avons mentionné précédemment, cette année nous avons ajouté la fraude liée à l'approvisionnement – une conduite illégale d'un employé, d'un propriétaire, d'un fournisseur ou d'un dirigeant relativement à l'achat de services, de marchandises ou de biens pour le compte d'une organisation, souvent pour son enrichissement personnel – comme nouvelle catégorie de crimes économiques dans notre sondage.

De façon générale, lorsqu'une organisation s'adresse à un tiers pour se procurer des services, des marchandises ou des biens, il y a risque de fraude liée à l'approvisionnement. Il nous est apparu que deux facteurs seraient à l'origine de cette catégorie de crimes.

Premièrement, comme le soulignait récemment notre « Enquête mondiale 2014 menée auprès des chefs de direction », nous assistons à une interdépendance accrue des entités commerciales – par l'externalisation d'éléments de la chaîne de valeur, l'achat de matières et une dépendance accrue à l'égard de fournisseurs.

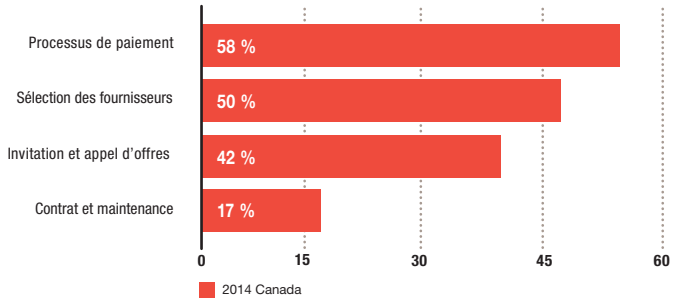
Deuxièmement, depuis que les économies nationales se sont relevées de la crise économique récente, les pratiques d'embauche semblent avoir changé. En effet, les mesures à court terme prises post-crise, comme le remplacement d'un personnel permanent occupant des postes internes par des ressources externes plus malléables et adaptables sont restées en place dans bien des cas, les organisations étant plus enclines à externaliser certaines tâches. Ces changements dans les pratiques d'embauche exposent les organisations à des problèmes de séparation des tâches dans le processus d'approvisionnement.

Le niveau élevé de cas de fraude lié à l'approvisionnement signalés – 33 %, catégorie dépassée uniquement par le détournement de biens (figure 2) – a surpassé nos prévisions. Cela pourrait s'expliquer en partie par le lien entre la fraude liée à l'approvisionnement et le trafic d'influence et la corruption. Dans nos sondages précédents, les commissions secrètes, les trucages d'offres et autres agissements similaires étaient peut-être englobés dans la catégorie trafic d'influence et corruption. Il n'empêche que ce deuxième rang mérite d'être souligné.

La nature des fraudes liées à l'approvisionnement

La figure 12 montre que les répondants canadiens ont indiqué que la fraude liée à l'approvisionnement se produit essentiellement au cours du processus de paiement (58 %), de la sélection des fournisseurs (50 %) et de l'appel d'offres (42 %).

Figure 12 : La fraude liée à l'approvisionnement – zones à risque



En adoptant quelques stratégies, les organisations pourraient non seulement réduire la fraude liée à l'approvisionnement, mais aussi simplifier leur processus d'appel d'offres et de sélection des fournisseurs.

Le processus d'achat et d'approvisionnement sous attaques

Comme il a été mentionné, les appels d'offres et la sélection des fournisseurs constituent un terrain de prédilection pour la fraude. Une personne du service des achats ou de l'approvisionnement peut être de connivence avec un fournisseur qui souhaite décrocher un contrat auprès de l'organisation. L'initié communique des informations sur le processus d'appel d'offres, comme les montants avancés par les concurrents, afin d'avantager le soumissionnaire qu'il privilégie. À l'inverse, l'initié peut approuver un prix inutilement élevé.

La facilité avec laquelle le processus d'achat et d'approvisionnement peut être attaqué est illustrée par le processus d'approvisionnement du secteur public. Ce secteur peut être amené à faire d'importants achats de matériel de pointe sur une longue période et devoir s'adresser à un marché où il existe un nombre limité de fournisseurs ayant la taille voulue pour soumissionner. En matière de services, les organisations du secteur public sollicitent régulièrement des soumissions portant sur une foule de responsabilités de moindre importance comme l'entretien du matériel, les services de logement et de restauration ou le soutien logistique.

Dans des environnements non soumis à la concurrence et souvent opaques, ces soumissions sont fréquemment l'occasion de fraude liée à l'approvisionnement. Nous avons assisté à plusieurs scandales retentissants dans de tels environnements au cours des dernières années et nous nous attendons à en voir davantage dans les années à venir.

La riposte

Il est pour le moins paradoxal qu'au moment où des politiques de lutte contre le trafic d'influence et la corruption sont mises en œuvre dans bien des organisations – souvent du fait de la pression exercée par la haute direction, attentive aux lois anticorruption publicisées comme la LCAPE –, il existe beaucoup moins de programmes de formation sur la prévention de la fraude liée à l'approvisionnement, qui y est étroitement associée.

Et pourtant, la formation sur la prévention de la fraude liée à l'approvisionnement est sans doute beaucoup moins complexe et coûteuse, les facteurs de risque étant plus simples et plus faciles à cerner.

En adoptant quelques-unes des stratégies suivantes, les organisations pourraient non seulement réduire la fraude liée à l'approvisionnement, mais aussi simplifier leur processus d'appel d'offres et de sélection des fournisseurs :

- S'assurer que l'organisation demande des soumissions cachetées qui seront ouvertes devant un groupe de personnes. Cette façon de procéder assure un meilleur contrôle sur l'intégrité des soumissions et du processus d'appel d'offres;
- Instaurer une séparation des fonctions au sein des services des achats et de l'approvisionnement pour s'assurer que plusieurs personnes participent au processus;
- Envisager de faire appel à différents fournisseurs pour différents projets. Par exemple, le fait de soumettre régulièrement les fournisseurs à un examen ou à un appel d'offres leur indique qu'ils devront se mesurer aux prix du marché. En outre, le donneur d'ouvrage prend ainsi connaissance des prix et des services qu'on trouve sur le marché.

La fraude comptable
Une menace qui persiste

La fraude comptable a toujours été l'un des crimes économiques les plus fréquemment signalés dans notre sondage. Depuis 2005, ce crime est signalé par plus de 20 % des répondants à l'échelle mondiale qui ont été victimes d'un crime économique.

Cette année n'a pas fait exception. Du côté canadien, 22 % (figure 2) des répondants ont déclaré avoir été victimes d'une fraude comptable, tout comme les 22 % (figure 2) recensés à l'échelle mondiale.

Les états financiers représentent un baromètre fondamental de la situation financière de l'organisation, et le point de départ traditionnel des analyses sur lesquelles s'appuient les décisions de crédit, les attributions de contrats et la mobilisation de capitaux sur les marchés publics. La fraude comptable – notamment la préparation d'états financiers trompeurs ou altérés – peut mener des banques, des prêteurs, des fournisseurs et des investisseurs à prendre des décisions risquées et mal fondées. En raison de l'utilisation systématique des états financiers et des données financières dans le cadre des activités commerciales, ce type de crime économique a des répercussions sur de nombreux processus d'affaires.

Le détournement d'actifs
Le plus répandu des crimes économiques

Le détournement d'actifs est de loin le crime économique le plus répandu, 58 % des organisations canadiennes répondantes qui ont signalé un cas de fraude en ayant été victimes (figure 2). Ce pourcentage est presque le double du taux de la fraude liée à l'approvisionnement, soit le deuxième crime économique en importance ayant été signalé. Bien que l'incidence de ce type de fraudes soit inférieure à celle de la cybercriminalité ou du trafic d'influence et de la corruption, l'ampleur de la menace est telle que les organisations doivent se montrer vigilantes.

Des disparitions mystérieuses

Tout le monde a entendu parler de choses qui disparaissent mystérieusement. Cet euphémisme pour parler du détournement d'actifs met généralement en cause l'un des processus de gestion fondamentaux : la distribution, la logistique ou le stockage.

Prenons une organisation de vente au détail à l'échelle mondiale qui possède des entrepôts pour stocker sa marchandise. Cette marchandise passe non seulement entre les mains de membres du personnel, mais aussi de plusieurs organisations tierces, ce qui crée plusieurs points de vulnérabilité le long de la chaîne logistique et de la distribution. Le procédé malhonnête peut se résumer au fait pour un employé de quitter le travail en emportant avec lui un article ou donner lieu à des agissements plus alambiqués comme classer au rebut de la marchandise en parfait état pour ensuite la revendre.

Le détournement d'actifs comprend aussi le vol d'argent par suite d'un détournement de fonds, souvent entre les mains d'une autorité chargée de garder des sommes d'argent en dépôt. Un exemple des nombreux stratagèmes associés au détournement d'actifs est le report différé dans les comptes de clients (« lapping »). Cette fraude consiste à voler de l'argent dans le compte d'un client et à combler le découvert avec de l'argent reçu d'un autre client. Les criminels ont de multiples façons de couvrir leurs crimes – comme de subtiliser de petites sommes afin de ne pas éveiller les soupçons.

La lutte contre le détournement d'actifs

Comme ce type de fraudes se passe surtout dans les environnements où règne la confiance, le meilleur conseil qu'on puisse donner à une organisation est de mettre en place de saines procédures de gestion :

- **Connaître son employé** : procéder à des contrôles préalables à l'embauche et tenir compte des résultats.
- **Connaître son fournisseur** : tout comme les employeurs font des vérifications des antécédents des employés ayant accès à des actifs de valeur, l'organisation devrait procéder à des vérifications de ces fournisseurs éventuels.
- **Séparer les tâches** : s'assurer que plusieurs personnes participent à tout processus qui débouche sur la distribution de fonds ou de marchandises, ce qui complique la tâche du fraudeur, qui souhaite passer inaperçu.

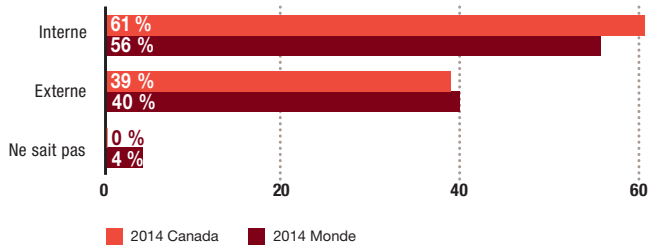
À la lecture de la présente liste de fraudes courantes et de risques auxquels les actifs d'une organisation sont exposés, il est important de se rappeler qu'un plan de gestion des risques de fraude bien conçu permet d'avoir recours à plusieurs contrôles pour prévenir différents types de fraudes. Ainsi, en instaurant par exemple des contrôles liés à la séparation des fonctions dans toute l'organisation, il serait possible de prévenir le détournement d'actifs en limitant les occasions pour les employés de quitter les lieux en emportant de la marchandise, tout en prévenant la fraude liée à l'approvisionnement par un processus d'appel d'offres scindé.

Interne ou externe

Qui commet la fraude? L'ennemi sous vos yeux

Dans la lutte contre le crime économique, comme dans tout combat, il est un besoin essentiel : connaître l'ennemi. Nous avons demandé aux répondants dont l'organisation a été victime d'un crime économique d'où provenaient les principaux auteurs des fraudes commises les plus graves. Comme le montre la figure 13, 61 % des répondants canadiens ont indiqué que le fraudeur provenait de l'intérieur de l'organisation, et 39 %, qu'il s'agissait de quelqu'un de l'extérieur.

Figure 13 : D'où provenait le fraudeur?



L'avantage, lorsque les pertes dues à la fraude sont majoritairement imputables à des personnes de l'intérieur – sur qui l'on peut théoriquement exercer une certaine surveillance – est que le renforcement des politiques, des processus et des contrôles internes peut réduire le risque. Ce n'est pas toujours le cas lorsque le fraudeur vient de l'extérieur.

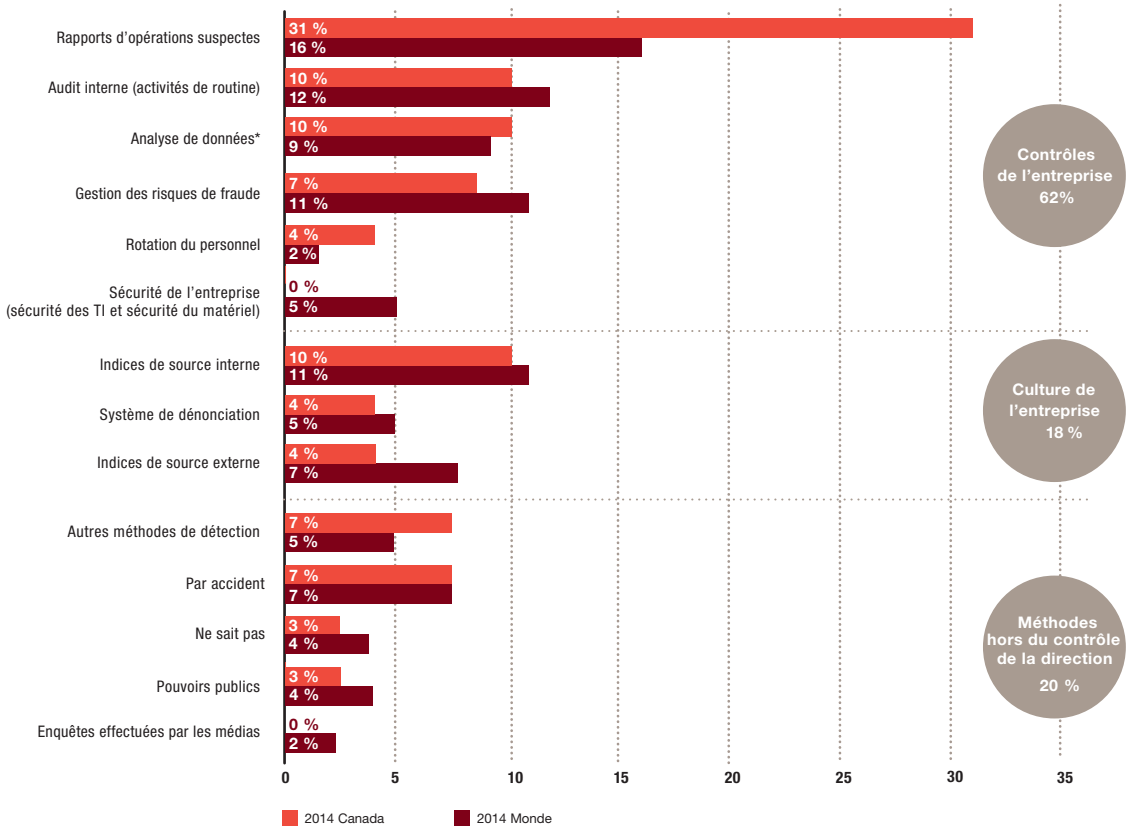
Une proportion de 31 % des fraudes déclarées par les répondants canadiens ont été détectées grâce à des rapports d'opérations suspectes

Détecter la fraude

Comment empêcher un crime économique de survenir – ou, à tout le moins, intervenir pendant qu'il est perpétré?

Les méthodes de détection de la fraude se classent normalement dans l'une de ces trois catégories : les contrôles de l'organisation, la culture de l'organisation et les méthodes hors du contrôle de la direction. La figure 14 présente les méthodes grâce auxquelles les organisations sondées ont détecté des fraudes graves. Son contenu révèle, entre autres, qu'une proportion de 31 % des fraudes déclarées par les répondants canadiens ont été détectées grâce à des rapports d'opérations suspectes.

Figure 14 : Méthodes de détection de la fraude



*L'analyse de données a été ajoutée comme catégorie dans le sondage de 2014.

Le fraudeur interne

Les spécialistes évoquent souvent le « triangle de la fraude » – ces trois éléments souvent réunis lorsqu'il y a acte frauduleux : la motivation, l'occasion et la rationalisation.

Près des trois quarts (73 %) des répondants canadiens ont indiqué que l'occasion ou la possibilité de commettre le crime était l'élément qui avait le plus contribué à la perpétration d'un crime économique par un acteur interne dans leur organisation. Si cela peut à première vue sembler décourageant, il faut savoir que, des trois éléments susmentionnés, l'occasion est celui sur lequel l'organisation a le plus de contrôle. Par conséquent, même si les employés peuvent subir des pressions diverses et trouver des motifs de commettre un méfait, si l'organisation limite les occasions qu'ils ont de passer à l'acte, elle pourrait réussir à empêcher l'engrenage frauduleux de se mettre en marche.

Même si la motivation et la rationalisation varient d'une fraude à l'autre, nous pouvons tout de même dresser un profil du fraudeur interne. Nous avons demandé aux répondants qui ont désigné un acteur interne comme le principal responsable d'un crime économique quels étaient le rang hiérarchique, l'âge, le sexe, l'ancienneté et le niveau d'études de celui-ci. Les figures 15 et 16 présentent les résultats.

Figure 15 : Fraudeur interne (membre du personnel)

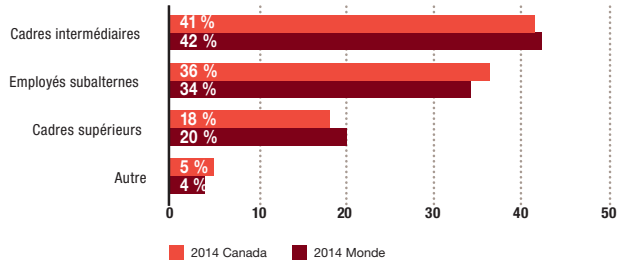
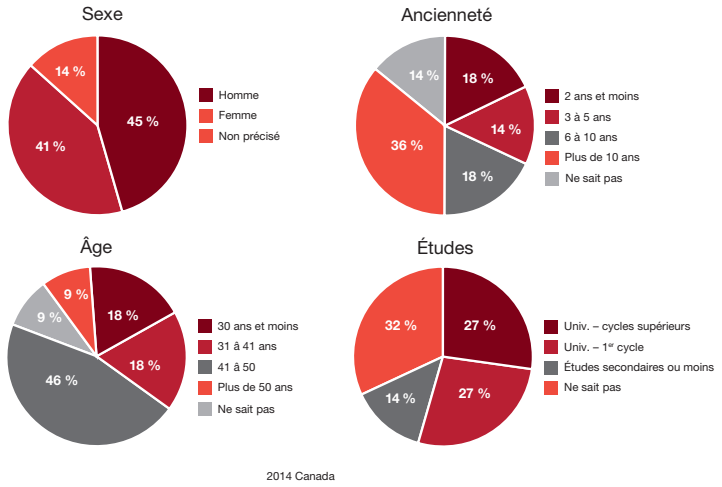


Figure 16 : Profil du fraudeur interne



Les résultats canadiens de 2014 esquissent le profil du fraudeur interne : un homme (45 %) ou une femme (41 %) d'âge moyen qui a fait des études universitaires et qui travaillait dans l'organisation depuis plus de 10 ans occupant, le plus souvent, un poste de cadre intermédiaire.

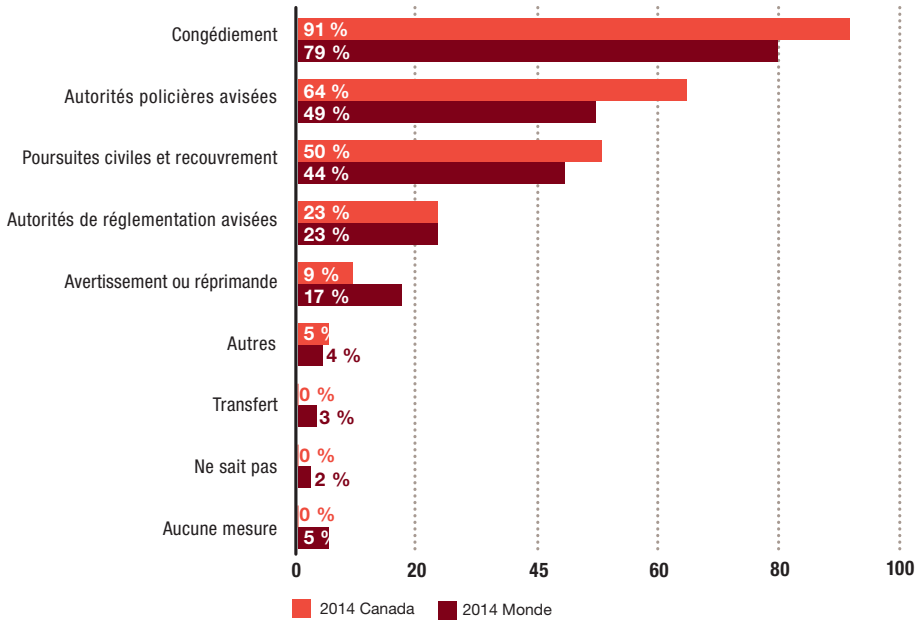
Il importe de noter que les fraudeurs internes tendent à avoir une longue ancienneté et à commettre des crimes complexes. Même si les résultats canadiens montrent que les cadres supérieurs (18 % – figure 15) commettent moins de crimes économiques que les employés subalternes (36 % – figure 15), ces crimes ont tendance à être plus complexes et à impliquer des montants plus élevés. Par ailleurs, le fait que les fraudes complexes soient plus difficiles à détecter pourrait également expliquer que les crimes économiques commis par des cadres supérieurs ne soient pas détectés aussi souvent que ceux imputables à des cadres intermédiaires ou à des employés subalternes.

Confronter le fraudeur interne

Le sondage de cette année confirme que les organisations continuent de réagir énergiquement à la fraude interne, plus de 90 % des répondants disant congédier les fraudeurs démasqués. Globalement, la figure 17 traduit l'importance des mesures prises contre les fraudeurs internes – congédiement, appel aux autorités policières, poursuite civile, avis aux autorités de réglementation, etc. – par rapport à 2011.

Selon les statistiques, aucune organisation canadienne n'ignorait les mesures à prendre contre les fraudeurs internes ou n'a rien fait. Voilà qui devrait servir d'avertissement aux fraudeurs internes en devenir : s'ils se font prendre, ils en paieront le prix.

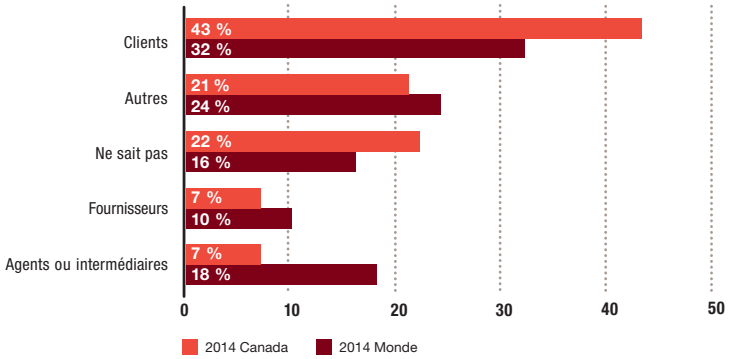
Figure 17 : Mesures prises à l'encontre des fraudeurs internes



Le fraudeur externe

La presque majorité (43 % – figure 18) des organisations canadiennes désigne les clients comme les fraudeurs externes les plus courants.

Figure 18 : Fraudeur externe (rôle)

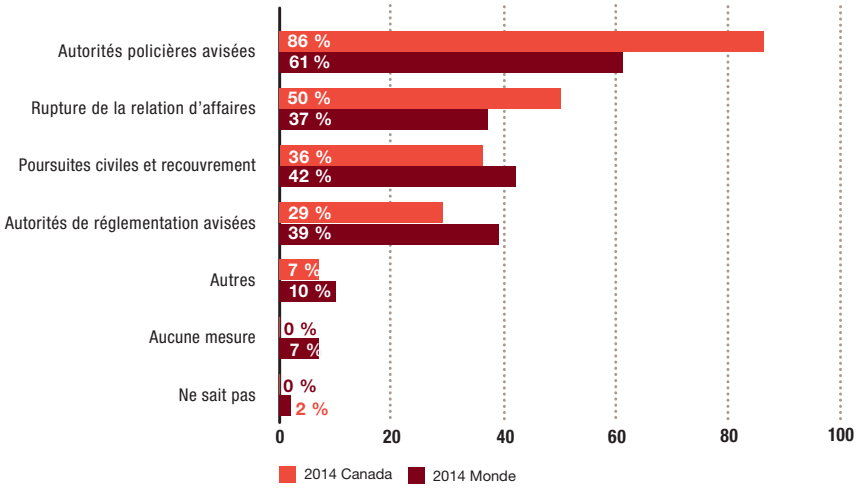


Mesures prises à l'encontre des fraudeurs externes

À l'échelle canadienne, la mesure la plus courante prise à l'encontre des fraudeurs externes est le signalement aux autorités policières (86 % – figure 19). Selon ce résultat, les organisations canadiennes sont plus susceptibles d'informer la police si le fraudeur provient de l'extérieur (le taux est de 64 % si le fraudeur est interne – voir la figure 17). De multiples facteurs expliquent la diversité des mesures prises à l'encontre des fraudeurs externes, notamment le fait que le congédiement ne soit pas une option dans ces cas.

De nombreuses difficultés entravent les enquêtes portant sur des fraudes, que celles-ci aient été commises par un fraudeur interne ou externe. Entre autres, la capacité d'effectuer une enquête approfondie sur les allégations de fraude fait souvent défaut aux organismes d'application de la loi. Il est donc important que les organisations victimes de fraude aient un protocole d'enquête adéquat en place, afin de mener elles-mêmes des enquêtes complètes avant de se tourner vers les autorités.

Figure 19 : Mesures prises à l'encontre des fraudeurs externes

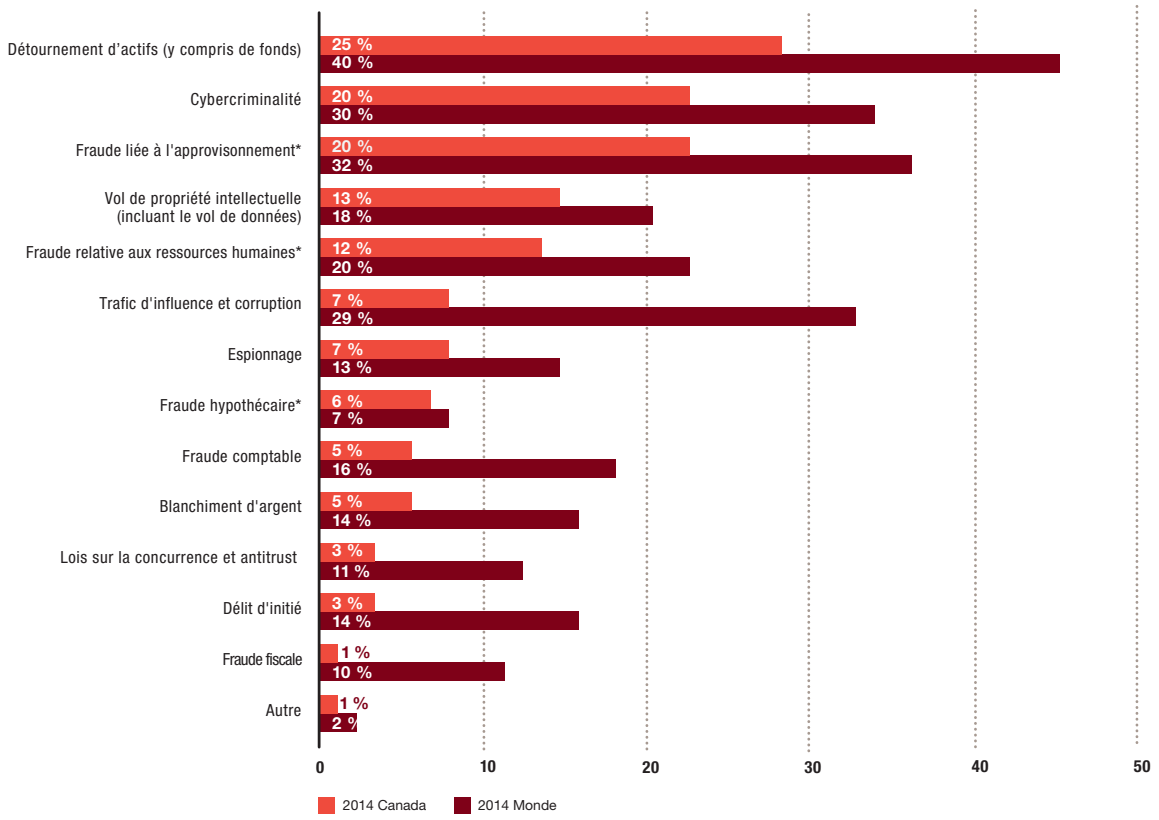


Près du tiers (30 %) des répondants canadiens ont déclaré que leur organisation n'avait pas procédé à une évaluation du risque de fraude pendant la période visée par le sondage.

Les organisations s'attendent à ce que la fraude persiste

La figure 20 illustre les menaces de fraude économique auxquelles les organisations estiment qu'elles seront exposées au cours des 24 prochains mois. Une proportion de 25 % des répondants canadiens pensent que leur organisation est susceptible de subir un détournement d'actifs et 20 % de ceux-ci classent ex æquo, à la deuxième place, la cybercriminalité et la fraude liée à l'approvisionnement.

Figure 20 : Perception de la fraude au cours des 24 prochains mois



* Les répondants pouvaient sélectionner ces catégories de crimes économiques pour la première fois lors de notre sondage de 2014.

Malgré la persistance des crimes économiques et la perception que le risque de fraude est accru, 30 % des répondants canadiens ont affirmé que leur organisation n'avait pas procédé à une évaluation du risque de fraude pendant la période visée par le sondage. Lorsqu'on leur a demandé les raisons pour lesquelles leur organisation n'avait pas procédé à cette évaluation :

- 53 % ont affirmé que cette évaluation leur semblait présenter peu de valeur;
- 17 % ne savaient pas exactement en quoi consistait une évaluation du risque de fraude;
- 7 % ont cité le coût comme raison principale;
- 7 % ignoraient la raison pour laquelle l'évaluation du risque de fraude n'avait pas été effectuée.

Lorsque les dirigeants s'intéressent vivement à la fraude dans leur organisation et infligent des sanctions disciplinaires sévères à ses auteurs, ils donnent le ton qui convient. Les résultats du sondage de 2014 démontrent que le ton donné par la direction en matière d'éthique combiné à un environnement de contrôle interne solide constitue le meilleur moyen de dissuader les comportements répréhensibles et d'accroître la probabilité de détecter les activités frauduleuses.

Les organisations qui accordent beaucoup d'importance à l'intégrité – là où la haute direction joint le geste à la parole – et mettent en œuvre un programme antifraude complet et bien communiqué sont moins susceptibles d'être victimes de crimes économiques.

Mettre en œuvre un programme efficace de lutte contre la fraude

Lorsqu'ils évaluent et examinent leur programme antifraude, les dirigeants devraient songer à demander à des professionnels des conseils sur les programmes de conformité et de prévention et de détection des fraudes; l'organisation doit également s'assurer que les lignes directrices et les pratiques de lutte contre la fraude reflètent l'évolution du climat économique, et que les mesures prises tiennent compte des lois et de la culture établies par les autorités compétentes de chaque territoire, sur le marché mondial.

À notre avis, les principaux contrôles antifraudes devraient comprendre les suivants :

1. Gouvernance – surveillance par le comité d'audit et le conseil d'administration;
2. Évaluation du risque de fraude;
3. Code d'éthique et de conduite;
4. Mécanismes de signalement des incidents;
5. Protocole d'enquête (y compris les rapports sur les opérations suspectes);
6. Protocole de mise en œuvre de mesures correctives;
7. Politiques et procédures d'embauche et de promotion;
8. Évaluation et tests de la direction.

Les organisations qui accordent beaucoup d'importance à l'intégrité – là où la haute direction joint le geste à la parole – et mettent en œuvre un programme antifraude complet et bien communiqué sont moins susceptibles d'être victimes de crimes économiques.

Contactez-nous

Équipe de juricomptabilité

Steven P. Henderson
Leader national, Services de juricomptabilité
Toronto
416 941-8328
steven.p.henderson@ca.pwc.com

Lori-Ann Beausoleil
Leader nationale, Services conseils en juricomptabilité
Toronto
416 687-8617
lori-ann.beausoleil@ca.pwc.com

Peter Vakof
Leader, Solutions technologiques en juricomptabilité
Toronto
416 814-5841
peter.vakof@ca.pwc.com

Calgary

Krista A. Mooney
Directrice principale
403 509-7336
krista.a.mooney@ca.pwc.com

Halifax

Paul F. Bradley
Associé
902 491-7436
paul.f.bradley@ca.pwc.com

James A. Pomeroy
Vice-président
902 491-7416
james.a.pomeroy@ca.pwc.com

London

Chris Gray
Vice-président
519 640-8011
chris.gray@ca.pwc.com

Montréal

Marie-Chantal Dréau
Associée
Montréal
514 205-5407
marie-chantal.dreau@ca.pwc.com

Benoit Legault
Vice-président
514 205-5682
benoit.legault@ca.pwc.com

Ottawa

Kas Rehman
Associé
613 755-4328
kas.rehman@ca.pwc.com

Chantal Amyot
Directrice principale
613 755-4355
chantal.amyot@ca.pwc.com

Jason Armstrong
Directeur principal
613 755-8743
jason.r.armstrong@ca.pwc.com

Steve Malette
Vice-président
613 755-5979
steven.m.malette@ca.pwc.com

Toronto

Sarah E. MacGregor
Associée
416 814-5763
sarah.e.macgregor@ca.pwc.com

Harm Atwal
Directrice principale
416 869-2330
harm.k.atwal@ca.pwc.com

Jeff Bowen
Directeur principal
416 869-2472
jeff.r.bowen@ca.pwc.com

H. Ray Haywood
Directeur principal
416 814-5801
h.ray.haywood@ca.pwc.com

Roberto Israel
Directeur principal
416 814-5740
roberto.r.israel@ca.pwc.com

Kelly Ohayon
Directrice principale
416 814-5843
kelly.ohayon@ca.pwc.com

Lloyd Wilks
Directeur principal
416 687-8115
lloyd.wilks@ca.pwc.com

Winnipeg

Jeffrey Johnson
Associé
204 926-2441
jeffrey.b.johnson@ca.pwc.com

Dave Johnson
Vice-président
204 926-2423
dave.a.johnson@ca.pwc.com

Kyla Kramps
Vice-présidente
204 926-2434
kyla.kramps@ca.pwc.com

www.pwc.com/ca/fr/crimesurvey

Pour voir une copie de nos rapports, numérisez ce code RQ avec une application lisant les codes RQ à l'aide de votre téléphone intelligent ou de votre tablette.

La valeur selon vous

Nous mettons l'accent sur quatre domaines : certification, conseils, transactions et services fiscaux. Cependant, nous sommes d'avis que les produits et services standards ne sont pas toujours la solution appropriée. La façon dont nous utilisons nos connaissances et notre expérience dépend de ce que vous recherchez. PwC Canada compte plus de 5 700 associés et employés, d'un océan à l'autre. Que vous soyez un client ou un membre de l'une de nos équipes, nous cherchons à approfondir nos relations avec vous et à créer de la valeur dans tout ce que nous faisons. Pour commencer, nous aimerions faire connaissance avec vous. Vous parlez et nous vous écoutons. Ce que vous nous direz déterminera comment nous utiliserons notre réseau mondial composé de plus de 184 000 personnes dans 157 pays — ainsi que leurs relations, leurs contacts et leur savoir-faire — pour vous aider à obtenir la valeur que vous recherchez. Pour plus de renseignements, consultez la page suivante : www.pwc.com/ca/fr.

Ces renseignements sont fournis à titre d'information seulement et n'ont pas pour objet de remplacer les conseils d'un professionnel.

© PricewaterhouseCoopers LLP/s.r.l./ s.e.n.c.r.l., une société à responsabilité limitée de l'Ontario, 2014. Tous droits réservés. PwC s'entend du cabinet canadien, et quelquefois du réseau mondial de PwC. Chaque société membre est une entité distincte sur le plan juridique. Pour obtenir de plus amples renseignements, visitez notre site Web à l'adresse : www.pwc.com/structure.
3350-03-0214