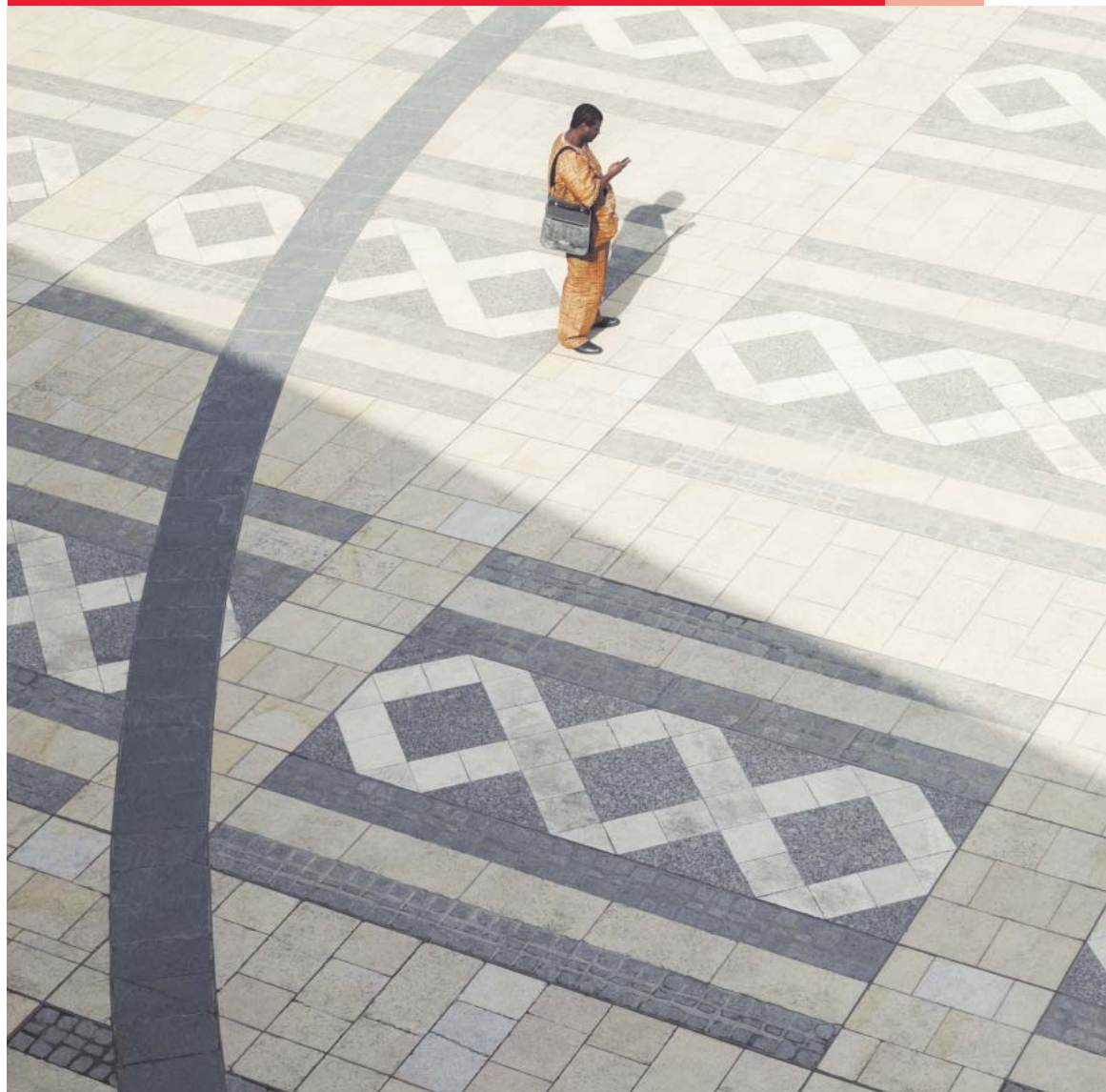


# **Sondage** *Global Economic Crime Survey 2011* Pleins feux sur la cybercriminalité La perspective canadienne

*Près de 4 000 répondants  
provenant d'entreprises  
de 78 pays dressent un  
tableau de la criminalité  
économique à l'échelle  
mondiale.*

*Novembre 2011*





---

# *Table des matières*

Introduction	2
Pleins feux sur la cybercriminalité	3
La fraude, le fraudeur et le fraudé	7
Comment PwC peut vous aider	15
Personnes-ressources	16

# Introduction

Le sondage *Global Economic Crime Survey 2011* mené par PwC continue de fournir des informations sur l'état de la criminalité économique dans le monde. Bien que nous ressentions peu à peu les effets d'une reprise à la suite du ralentissement économique mondial qui a eu une incidence notable sur les résultats du sondage mené en 2009, il ressort clairement des résultats de cette année que les parties prenantes doivent continuer de gérer les risques de fraude avec diligence, puisqu'aucune entreprise ni aucun secteur d'activités ne sont à l'abri.

*Les résultats de notre sondage de 2011 indiquent que 32 % des entreprises canadiennes sondées ont déclaré avoir été victimes d'un délit économique au cours des 12 derniers mois.*

Notre sondage de 2011 met en lumière la menace grandissante que constitue la cybercriminalité dans un monde où l'Internet et les technologies interconnectées sont omniprésents, ce qui rend les entreprises vulnérables au risque d'attaques par des criminels du monde entier. Le sondage examine l'importance et les répercussions de la cybercriminalité ainsi que la manière dont elle influe sur les entreprises du monde entier.

Les résultats de notre sondage de 2011 indiquent que 32 % des entreprises canadiennes sondées (34 % à l'échelle mondiale) ont déclaré avoir été victimes d'un délit économique au cours des 12 derniers mois, ce qui représente une diminution de 24 % par rapport aux résultats de notre sondage de 2009. Parmi les entreprises qui ont subi un délit économique dans le monde, près d'une entreprise sur quatre affirme avoir été victime de cybercriminalité au cours des 12 derniers mois, et 39 % des répondants à l'échelle mondiale ont indiqué avoir davantage conscience des menaces liées à la cybercriminalité. Le rapport canadien de cette année est divisé en deux grandes parties, soit :

- **la cybercriminalité** – prise de conscience du délit, de son incidence sur les entreprises et mesures à prendre pour en gérer les risques;
- **la fraude, le fraudeur et le fraudé** – les types de fraudes commis, les auteurs de ces fraudes, les méthodes de détection et les mesures de remédiation prises par les entreprises pour y faire face.

## La cybercriminalité se classe parmi les quatre principaux crimes économiques.

# Pleins feux sur la cybercriminalité

Aux fins de notre sondage, nous avons défini la cybercriminalité comme suit :

*Un délit économique commis à l'aide d'ordinateurs et d'Internet. Cela inclut notamment la transmission de virus, le téléchargement illégal de fichiers, le hameçonnage<sup>1</sup> et le détournement de domaine<sup>2</sup>, ainsi que le vol de renseignements personnels tels que des renseignements sur les comptes bancaires. On ne parle de cybercriminalité que si un ou des ordinateurs et l'Internet jouent un rôle de premier plan, et non accessoire, dans la perpétration du délit.*

1 Le hameçonnage est une tentative d'obtention de renseignements tels que des noms d'utilisateurs, des mots de passe et des renseignements sur les cartes de crédit en se faisant passer pour un organisme fiable dans une communication électronique.

2 Le détournement de domaine est une attaque perpétrée par un pirate informatique dans le but de rediriger les visiteurs d'un site Web vers un faux site Web.

La cybercriminalité est-elle simplement un moyen utilisé par un fraudeur pour commettre un acte illégal ou est-ce un délit économique à part entière? Les

entreprises doivent-elles prendre des mesures spécifiques, en plus des autres moyens de prévention et de détection des fraudes afin d'en gérer le risque? Notre sondage examine ces enjeux de plus près. Les principaux objectifs du sondage de 2011 relativement à la cybercriminalité consistaient à savoir :

- si l'incidence de la fraude liée à la cybercriminalité a augmenté au cours des dernières années;
- d'où proviennent les risques de fraudes liés à la cybercriminalité;
- quelles sont les mesures adoptées par les entreprises pour prévenir et détecter ce type de fraude.

### **Cybercriminalité : la prochaine vague**

Selon notre sondage de 2011, la cybercriminalité se classe parmi les quatre principaux crimes économiques, tout juste derrière le détournement de biens, la fraude comptable, le trafic d'influence (« pot-de-vin ») et la corruption. Certaines raisons parmi les suivantes pourraient expliquer l'apparition de la cybercriminalité parmi les principaux types de délits économiques :

- des cas récents de cybercriminalité ont davantage retenu l'attention des médias, ce qui a accru la sensibilisation à ce type de délit économique. Les entreprises pourraient ainsi avoir mis en place des contrôles supplémentaires pour détecter et déclarer ce type de crime économique;

- les répondants pourraient avoir reclassé certains types de délits plus traditionnels en délits informatiques, puisque cette catégorie fait son apparition pour la première fois dans le sondage en tant que catégorie distincte;
- les organismes de réglementation y consacrent une plus grande attention;
- il se peut que les avancées technologiques facilitent la perpétration de délits informatiques.

### **La menace est-elle uniquement externe?**

Au cours des 12 derniers mois, 38 % des entreprises canadiennes (39 % à l'échelle mondiale) estiment que leur perception des risques encourus par leur entreprise à l'égard de la cybercriminalité s'est accrue. Cela illustre bien l'importance croissante de la cybercriminalité dans le monde et de la nécessité de demeurer à l'affût des menaces de cybercriminalité qui font leur apparition ou sont en émergence.

Plus de la moitié (57 %) des répondants canadiens (46 % à l'échelle mondiale) croient que la principale menace liée à la cybercriminalité dans leur entreprise est d'origine externe, tandis que 9 % d'entre eux (13 % à l'échelle mondiale) considèrent qu'elle est plutôt d'origine interne, et 19 % (29 % à l'échelle mondiale) croient que les principales menaces sont tant internes qu'externes.

# La plus grande crainte des répondants canadiens concernant la cybercriminalité est le vol ou la perte de renseignements d'identification personnelle.

## D'où provient la menace?

Parmi les répondants canadiens qui croient que les principales menaces liées à la cybercriminalité sont d'origine externe, 53 % (51 % à l'échelle mondiale) ont déclaré que les menaces proviennent à la fois du Canada et d'ailleurs. Les cinq premiers pays étrangers visés figurent au graphique 1 ci-après.

Graphique 1 : Classement des cinq premiers pays désignés comme sources probables de cybercriminalité

(Par ordre alphabétique)

États-Unis

Hong Kong (et Chine)

Inde

Nigéria

Russie

Ces données illustrent le caractère mondial de la cybercriminalité et le fait que les frontières géographiques traditionnelles n'offrent aucune protection contre ce fléau.

Parmi les répondants qui pensent que la principale menace liée à la cybercriminalité est d'origine interne, le service le plus visé au sein d'une entreprise est celui des technologies de l'information avec 53 % des répondants à l'échelle mondiale jugeant qu'il s'agit d'un secteur à risque élevé.

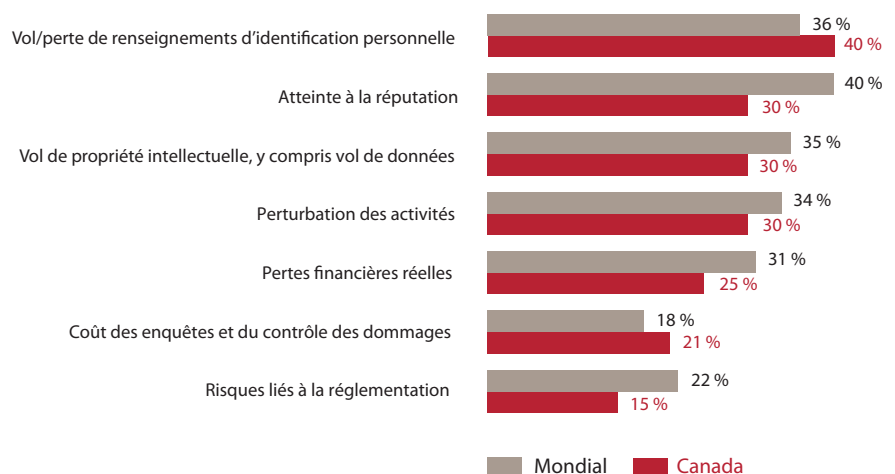
## Quelle est la grande crainte des entreprises?

Le graphique 2 démontre que la plus grande crainte des répondants canadiens concernant la cybercriminalité est le vol ou la perte de renseignements d'identification personnelle, suivi de l'atteinte à la réputation, le vol de propriété intellectuelle et la perturbation des activités de l'entreprise. Les risques liés à la réglementation et les coûts engagés pour la réalisation des enquêtes et le contrôle des dommages semblent de moindre importance, ce qui pourrait indiquer que les entreprises admettent la nécessité de se protéger contre la cybercriminalité et d'enquêter sur des incidents qui y sont liés.

## Avez-vous les moyens d'y faire face?

Lorsqu'il s'agit de prévention et de détection de la cybercriminalité, 60 % des répondants au Canada et ailleurs dans le monde estiment qu'ils possèdent les ressources à l'interne pour prévenir et détecter les délits informatiques, traduisant ainsi un certain niveau de confiance dans l'infrastructure des technologies de l'information (TI) de leur entreprise. Il est primordial que les entreprises continuent de mettre l'accent sur l'amélioration ou la modification de leurs ressources en matière de prévention de la cybercriminalité pour faire face aux nouveaux risques liés à la cybercriminalité à mesure qu'ils apparaissent. Par contre, seuls 36 % des répondants canadiens (40 % à l'échelle mondiale) pensent avoir accès à des ressources internes pour mener des enquêtes sur les délits informatiques, et

Graphique 2 : Craintes liées à la cybercriminalité (2011)





*Soixante-dix pour cent des répondants canadiens ont déclaré ne pas surveiller de près l'utilisation des sites de médias sociaux (comme Facebook ou Twitter) par leurs employés.*

47 % des répondants canadiens (39 % à l'échelle mondiale) ont déclaré avoir accès à des enquêteurs spécialisés en solutions technologiques juricomptables. Il est crucial que les entreprises mettent en place une équipe d'intervention en cas d'incidents informatiques qui sera chargée d'établir des mécanismes et des politiques de réponse efficaces et de s'assurer que toute menace de cybercriminalité est traitée efficacement, que ce soit à l'interne ou par l'entremise d'experts externes.

En cas d'incident lié à la cybercriminalité, 53 % des répondants canadiens (65 % à l'échelle mondiale) ont déclaré avoir consulté des experts à l'extérieur de l'entreprise et 51 % des répondants, tant au Canada qu'ailleurs dans le monde, ont rapporté l'incident aux autorités chargées de l'application des lois.

Parmi les répondants du monde entier qui ont déclaré avoir consulté des experts externes, 40 % ont indiqué avoir recours à des experts de façon régulière ou proactive, alors que 48 % ont dit ne consulter un expert qu'en cas d'incident avéré, ou de façon plus réactive.

### **Garder un œil sur les sites de médias sociaux**

Soixante-dix pour cent (70 %) des répondants canadiens (60 % à l'échelle mondiale) ont déclaré ne pas surveiller de près l'utilisation des sites de médias sociaux (par exemple, Facebook, Twitter, etc.) par leurs employés. Parmi les répondants qui surveillent de près l'utilisation des sites de médias sociaux, la majorité d'entre eux mettent en place des mesures telles que :

- la surveillance du trafic électronique interne et externe, y compris les activités sur le Web;
  - la référence à un code de conduite dans les contrats de travail;
  - la mise en place de programmes de formation à l'intention des employés sur l'utilisation adéquate d'Internet.
- Étant donné l'utilisation croissante des médias sociaux par les employés, il devient de plus en plus important pour les entreprises de prendre en considération :
- la diminution de la productivité des employés;
  - l'utilisation inappropriée d'Internet par les employés (par exemple, le jeu, la pornographie, etc.);
  - la fuite d'informations confidentielles de l'entreprise;

- l'exposition des infrastructures de l'entreprise à des attaques informatiques; et
- l'éventualité d'un litige.

### **Réduire les risques**

Quarante-neuf pour cent (49 %) des répondants canadiens (42 % à l'échelle mondiale) ont indiqué n'avoir reçu aucune formation aux fins de sensibilisation à la sécurité sur Internet au cours des 12 derniers mois. Pour gérer la menace grandissante que constitue la cybercriminalité, il est essentiel que l'entreprise comprenne bien l'environnement cybernétique actuel et émergent et que les dirigeants comprennent les risques et les possibilités du monde cybernétique. Alors que le mode de formation le plus répandu était la communication par courriel/affichage/bannière dans 42 % des cas (40 % à l'échelle mondiale) et la formation par ordinateur dans 17 % des cas (22 % à l'échelle mondiale), la majorité des répondants ont considéré que ces méthodes étaient les moins efficaces, jugeant plutôt que les événements « fondés sur des rapports humains » tels que les présentations, les réunions d'équipe et les ateliers sont les méthodes de formation les plus efficaces.

**Quarante-neuf pour cent des répondants canadiens ont indiqué n'avoir reçu aucune formation aux fins de sensibilisation à la cybersécurité au cours des 12 derniers mois.**

### **À qui incombe la responsabilité ultime de la gestion de la cybercriminalité au sein d'une entreprise?**

Interrogés sur la responsabilité globale de la prévention de la cybercriminalité au sein d'une entreprise, la majorité des répondants ont déclaré que cette responsabilité incombait aux hauts dirigeants, soit 43 % (54 % à l'échelle mondiale) des répondants estimant qu'elle revenait au chef des technologies de l'information et 34 % (21 % à l'échelle mondiale), au chef de la direction et au conseil d'administration.

Lorsqu'il s'agit des risques auxquels leur entreprise est exposée en raison de la cybercriminalité, 21 % des répondants (15 % à l'échelle mondiale) ont déclaré que les cadres supérieurs et les membres du conseil d'administration procèdent à l'examen des risques liés à la cybercriminalité chaque année, tandis que 23 % des répondants canadiens et étrangers n'examinent ces risques que de façon occasionnelle. Ces constatations confirment la culture plus « réactive » indiquée dans les résultats du sondage. Il est essentiel que les responsables de la gouvernance liée aux questions de cybercriminalité adoptent une approche plus proactive quant à la menace que représente la cybercriminalité, fassent une priorité de la lutte contre cette menace et demandent l'aide de professionnels pour évaluer et renforcer la détection et la prévention de la cybercriminalité et en fassent l'une des principales composantes de leur programme antifraude.

### **Quelles mesures les entreprises doivent-elles adopter pour se protéger contre les attaques cybernétiques?**

- **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 monde cybernétique.
- **Réévaluer** – réévaluer la fonction sécurité et l'état de préparation de l'entreprise en cas de délit informatique. Contrairement aux délits économiques traditionnels, les délits informatiques évoluent rapidement en raison des avancées technologiques entraînant constamment de nouveaux risques, ce qui contraint l'entreprise à adapter continuellement ses procédures.
- **Sensibiliser** – les entreprises doivent bien connaître le monde informatique actuel et en émergence. Ainsi, des décisions et des mesures à la fois éclairées et priorisées pourront être prises.
- **Créer une équipe d'intervention en cas d'incidents cybernétiques** – celle-ci devra agir avec rapidité et agilité. Une équipe d'intervention cybernétique s'assure, dès le signalement d'un incident n'importe où dans l'entreprise, que cet incident fasse l'objet d'un suivi, qu'il soit évalué en fonction des risques, que les dirigeants de l'entreprise en soient informés et qu'il soit trié.
- **Former tous les employés** – toute entreprise doit implanter une culture de « cybersensibilisation » et communiquer à l'ensemble du personnel les politiques, les procédures et les protocoles appropriés.
- **Les entreprises doivent adopter une approche plus active et transparente à l'égard de la cybercriminalité** – prendre des mesures en poursuivant les auteurs de délits informatiques au moyen de poursuites judiciaires et communiquer publiquement les mesures prises par l'entreprise en ce qui a trait aux menaces, aux incidents et aux mesures prises.

Pourcentage des répondants canadiens qui indique que le chef des technologies de l'information est responsable de la prévention de la cybercriminalité

**43 %**

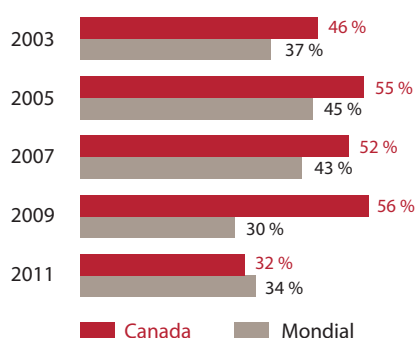
Pourcentage des répondants canadiens qui indique que le chef de la direction est responsable de la prévention de la cybercriminalité

**34 %**

*Bien que, dans le passé, les délits économiques déclarés aient été plus nombreux au Canada qu'ailleurs dans le monde, les résultats de 2011 font état d'une baisse du nombre de ces délits.*

## La fraude, le fraudeur et le fraudé

Graphique 3 : Entreprises ayant déclaré une fraude (de 2003 à 2011)



Répondants victimes d'un délit économique au cours des 12 derniers mois (2009 et 2011) et au cours des 24 derniers mois (2003, 2005 et 2007)

### Les entreprises savent-elles à quoi elles s'exposent?

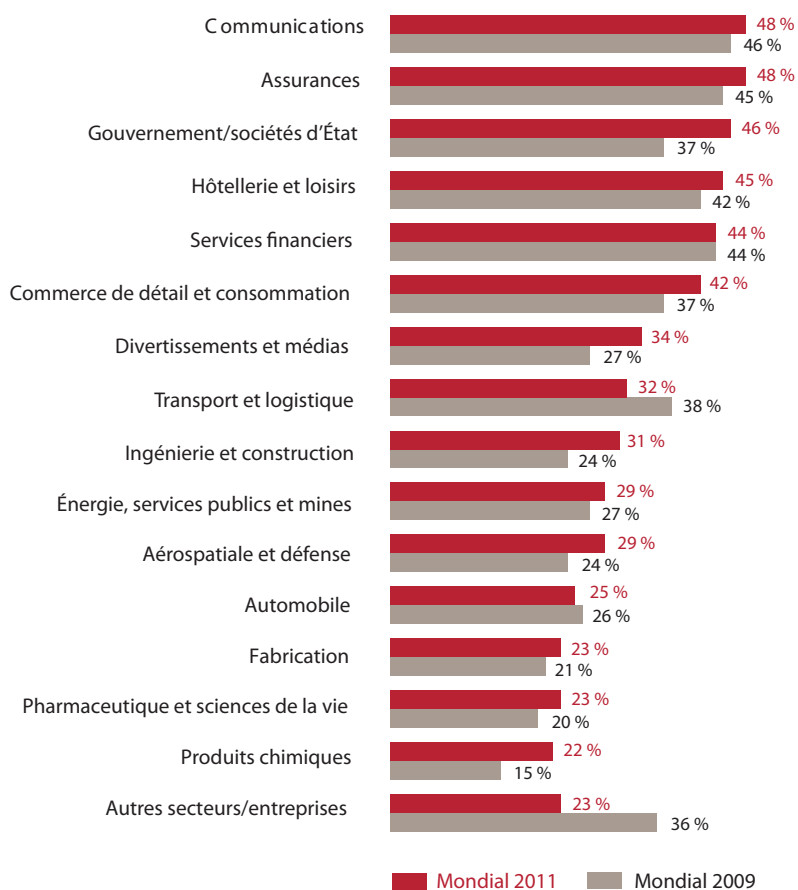
Les résultats de notre sondage de 2011 indiquent que 32 % des entreprises canadiennes (34 % à l'échelle mondiale) ont déclaré avoir été victimes d'un délit économique au cours des 12 derniers mois. Il s'agit d'une diminution de 24 % par rapport aux résultats du sondage de 2009. Le graphique 3 démontre le pourcentage d'entreprises ayant déclaré une fraude de 2003 à 2011, tant d'une perspective canadienne que mondiale.

Bien que, dans le passé, les délits économiques déclarés aient été plus nombreux au Canada qu'ailleurs dans le monde, les résultats de 2011 font état d'une baisse du nombre de ces délits. Cette baisse pourrait s'expliquer par le fait que les entreprises canadiennes se montrent plus diligentes dans la mise en œuvre de programmes antifraude robustes, y

compris l'évaluation des risques de fraude et la mise en place de systèmes de dénonciation, ce qui favorise une augmentation de la sensibilisation à la fraude, réduit les occasions de commettre des fraudes et accroît la capacité de l'entreprise à détecter les fraudes. La baisse du nombre de fraudes déclarées pourrait également s'expliquer par la reprise de l'économie canadienne plus vigoureuse qu'ailleurs dans le monde au cours des deux dernières années. En effet, en période de ralentissement économique, l'environnement de contrôle de l'entreprise favorise une grande capacité de détection des fraudes, ce qui n'est pas toujours le cas en période de reprise. Enfin, cette baisse du nombre de délits déclarés pourrait aussi indiquer que ce sont des fraudes plus complexes, comme la cybercriminalité ou la collusion entre les parties, qui sont commises, lesquelles sont par essence plus difficiles à détecter.



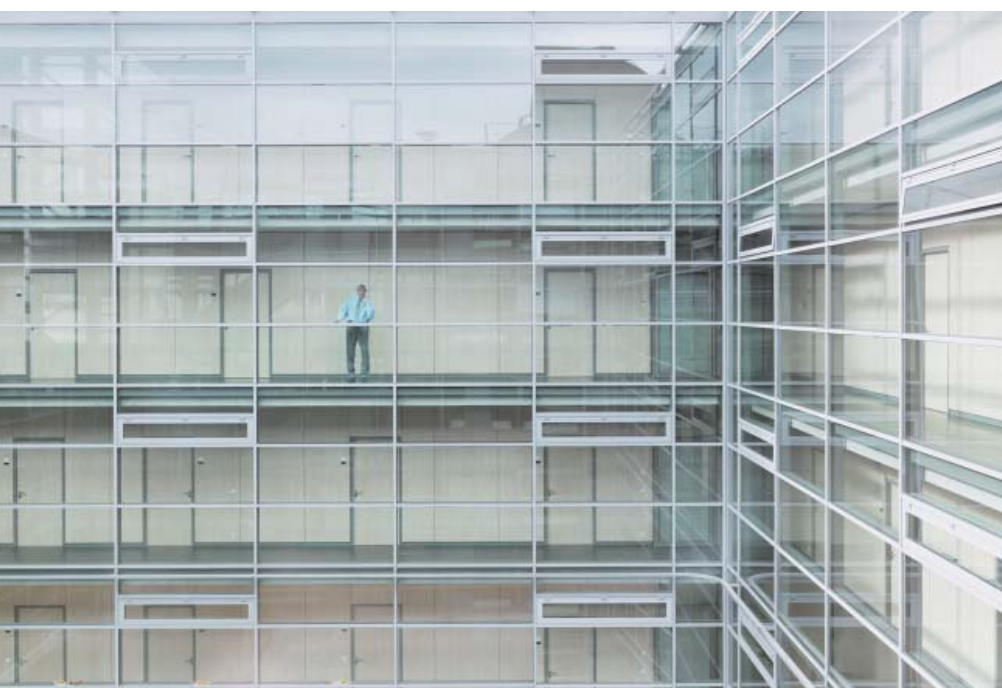
Graphique 4 : La fraude par secteur d'activités (% des fraudes déclarées)



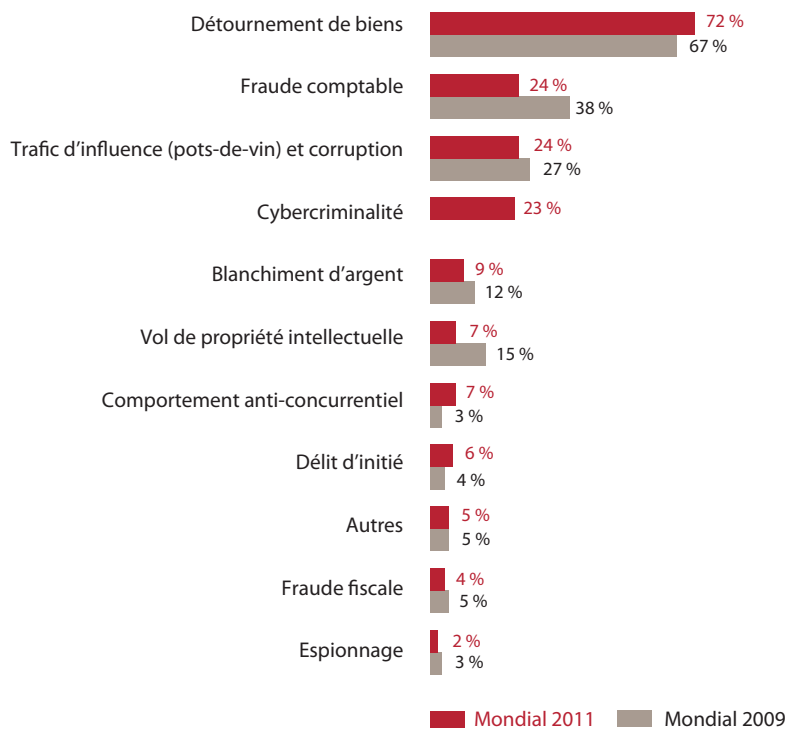
**Certains secteurs sont-ils davantage exposés à la fraude?**

Le crime économique est présent dans tous les secteurs d'activité à l'échelle mondiale, comme l'illustre la comparaison, au graphique 4, des résultats actuels avec ceux de notre sondage de 2009.

Les secteurs des communications et des assurances demeurent au sommet du classement pour ce qui est du nombre de fraudes déclarées. On observe cependant que la fraude dans le secteur public a augmenté de 9 % par rapport aux résultats de notre sondage de 2009, ce qui place ce secteur parmi les cinq premières cibles de la criminalité économique.



Graphique 5 : Types de délits économiques † ††



† Nota : un grand nombre de répondants ont subi plusieurs de ces types de délits économiques.

†† Dans nos sondages précédents sur la criminalité économique, lorsque l'on demandait aux répondants s'ils avaient fait l'objet de cybercriminalité, le taux de réponse était très bas et statistiquement non significatif. Conséquemment, nous avons regroupé ces résultats dans la catégorie « Autres types de fraudes » dans nos sondages précédents considérant l'augmentation de la menace liée à la cybercriminalité, nous avons mis l'accent sur la cybercriminalité cette année et l'avons réintroduite à la question concernant les types de fraudes, dans le cadre d'une question aux répondants, à savoir s'ils avaient été victimes de cybercriminalité au cours des 12 derniers mois.

### Quels sont les types de délits économiques visés?

Les délits économiques peuvent revêtir diverses formes. Le graphique 5 montre les différents types de délits économiques déclarés par les répondants du monde entier ayant subi des délits économiques au cours des 12 derniers mois.

Le délit le plus courant déclaré par les entreprises interrogées à l'échelle mondiale est le détournement de biens, soit le vol de biens de l'entreprise (y compris les actifs monétaires/espèces ou les fournitures et le matériel) par les dirigeants, les fiduciaires ou les employés pour leur bénéfice personnel. Viennent ensuite la fraude comptable ainsi que le trafic d'influence (les pots-de-vin) et la corruption. Soixante-douze pour cent (72 %) des entreprises interrogées à l'échelle mondiale qui ont été victimes de délits économiques au cours des 12 derniers mois ont subi un détournement de biens, ce qui constitue une hausse de 5 % par rapport aux résultats de notre sondage de 2009.

La non complexité de ce type de fraude peut expliquer le fait que le détournement de biens soit plus fréquent que d'autres types de fraudes, ce qui le rend plus facile à commettre par des personnes à de nombreux échelons de l'entreprise.

Vingt-quatre pour cent (24 %) des entreprises interrogées à l'échelle mondiale ont été victimes de fraude comptable, en baisse de 14 % par rapport à notre sondage de 2009. Ce type de fraude inclut les manipulations comptables, les méthodes d'emprunt ou de financement frauduleuses, les demandes de crédit frauduleuses et les opérations non autorisées ou malhonnêtes. Les éléments suivants pourraient expliquer cette baisse, soit :

1. les entreprises peuvent avoir mis en place des contrôles plus serrés pour dissuader les fraudeurs potentiels;
2. notre sondage de 2009 avait révélé une hausse brusque du nombre de fraudes comptables par rapport à notre sondage de 2007, ce qui résultait peut-être du fait que les entreprises devaient lutter pour survivre en période difficile et que leur direction subissait des pressions au point de manipuler leurs états financiers. Il semble qu'il y ait moins de raisons et/ou de pressions aujourd'hui;
3. il se peut que les entreprises ne détectent pas avec précision les délits économiques en raison des réductions d'effectifs en matière de prévention de la fraude survenues au sein des entreprises partout dans le monde depuis notre dernier sondage.

Un quart des entreprises ayant déclaré des crimes économiques à l'échelle mondiale ont indiqué le trafic d'influence (pots-de-vin) et la corruption. Le trafic d'influence (pots-de-vin) et la corruption constituent une forme de crime économique dont la fréquence n'a cessé d'augmenter de croître dans nos sondages jusqu'en 2007, avant d'amorcer une légère baisse depuis notre sondage de 2009. Les entreprises hésitent probablement à déclarer cette forme de crime économique en raison du renforcement de la couverture médiatique, de l'application des lois en matière de réglementation et de criminalité, y compris de lourdes sanctions appliquées ces dernières années.

Le Canada s'est engagé publiquement à lutter contre le trafic d'influence (pots-de-vin) et la corruption dans le cadre de la Loi sur la corruption d'agents publics étrangers. Il est important que les entreprises canadiennes qui prennent de l'expansion sur les marchés émergents comprennent cette loi et la manière dont elle régit leurs interactions avec les fonctionnaires étrangers.

## Treize pour cent des répondants à l'échelle mondiale ont indiqué qu'au cours des 12 derniers mois, leur entreprise a choisi de ne pas pénétrer un nouveau marché ou a renoncé à saisir une nouvelle possibilité d'affaires à cause des risques de corruption.

Treize pour cent des répondants à l'échelle mondiale ont indiqué qu'au cours des 12 derniers mois, leur entreprise a choisi de ne pas pénétrer un nouveau marché ou a renoncé à saisir une nouvelle possibilité d'affaires à cause des risques de corruption.

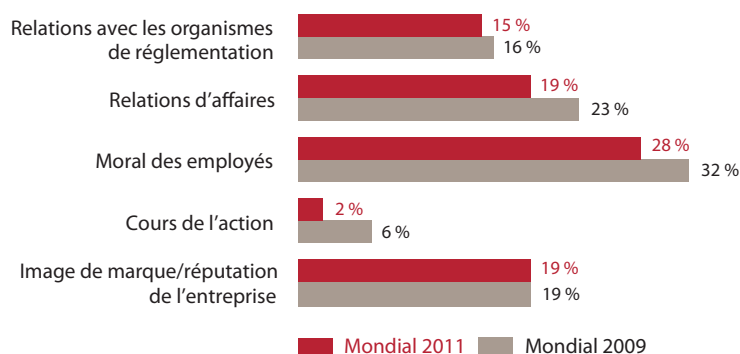
Ce chiffre pourrait indiquer que les entreprises ont conscience des conséquences de la corruption de fonctionnaires étrangers et de l'incidence de la corruption sur leur réputation et sur leurs projets de croissance et d'expansion. Il sera intéressant de vérifier, dans de futurs sondages, si cette réticence à pénétrer de nouveaux marchés en raison de la corruption subsistera, alors que les entreprises poursuivent leur expansion à l'échelle mondiale.

La cybercriminalité est une nouvelle catégorie de crime économique figurant dans les résultats de notre sondage de 2011. Les résultats de notre sondage montrent que 23 % des répondants à l'échelle mondiale en ont subi les conséquences.

### **Combien coûte la fraude et quels en sont les dommages indirects?**

Bien qu'il soit difficile de mesurer l'incidence financière d'un crime économique, près d'un répondant à l'échelle mondiale sur dix ayant subi une fraude au cours des 12 derniers mois a déclaré des pertes de plus de 5 millions \$US. Parmi les entreprises victimes de trafic d'influence (versement de pots-de-vin) et de corruption, près d'une entreprise sur cinq a subi en moyenne des pertes de plus de 5 millions \$US.

Graphique 6 : Dommages indirects



Au-delà des pertes directes, notre sondage s'est également penché sur les dommages indirects subis par les entreprises, notamment les dommages causés à l'image de marque ou à la réputation de l'entreprise, au cours de l'action, au moral des employés, aux relations d'affaires et aux relations avec les organismes de réglementation. Le graphique 6 nous renseigne sur les entreprises qui ont déclaré avoir subi des dommages indirects importants dans le monde entier.

L'incidence des pertes indirectes attribuable à la fraude peut être difficile à quantifier. C'est le cas, par exemple, du moral des employés, dont 28 % des répondants à l'échelle mondiale ont estimé qu'il a été fortement affaibli par suite d'un crime économique. L'expérience montre qu'un événement qui mine le moral des employés peut se traduire par des pertes additionnelles pour l'entreprise, puisque la performance peut diminuer et donner lieu à certains comportements répréhensibles. La réputation de l'entreprise a été considérablement atteinte par un crime économique dans 19 % des cas pour les répondants à l'échelle mondiale en 2009 et en 2011. Comme la réputation d'une entreprise est souvent étroitement associée à son avantage concurrentiel et que plusieurs années sont souvent nécessaires pour rétablir une réputation ternie, il est important de ne pas sous-estimer les répercussions des dommages indirects.

*Près d'un répondant à l'échelle mondiale sur dix ayant subi un crime économique au cours des 12 derniers mois a déclaré des pertes de plus de 5 millions \$US.*

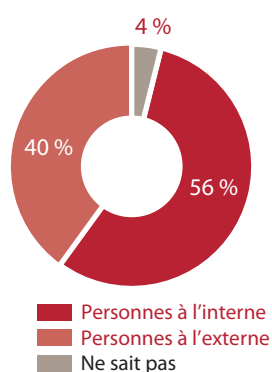
### Qui sont les fraudeurs?

Selon notre sondage de 2011, 56 % des entreprises du monde entier victimes d'un crime économique au cours des 12 derniers mois ont indiqué que les fraudeurs étaient des personnes à l'interne, soit des employés, tandis que 40 % ont affirmé qu'il s'agissait principalement de personnes à l'externe (graphique 7).

Vu l'importance des cas de fraudes commises par des employés, les entreprises doivent améliorer leurs contrôles internes et démontrer une meilleure connaissance des profils des fraudeurs. Les résultats de notre sondage de 2011 indiquent que le fraudeur interne type est un homme (77 %) âgé entre 31 ans et 40 ans (43 %), titulaire d'un diplôme universitaire de premier cycle (37 %) et possède entre trois et cinq ans d'ancienneté au sein de l'entreprise (30 %).

Le graphique 8 montre que, selon les entreprises interrogées à l'échelle mondiale en 2011 qui ont subi un délit économique perpétré par un employé, 39 % des fraudeurs étaient des employés subalternes, 41 % étaient des cadres intermédiaires et 18 % étaient des cadres supérieurs.

Graphique 7 : Relation du fraudeur avec l'entreprise (à l'échelle mondiale, 2011)

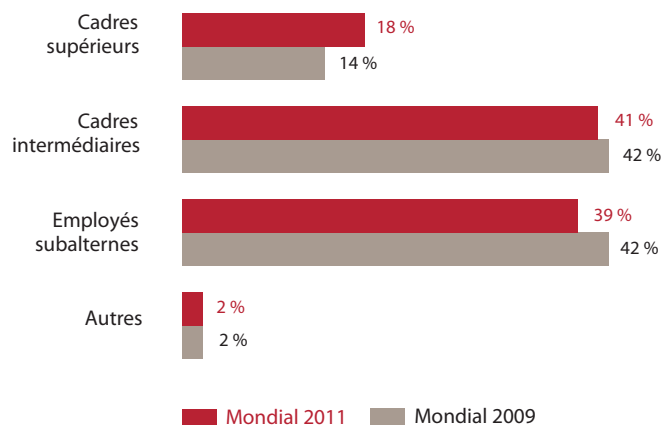


Il est important de noter que, même si les résultats de notre sondage mondial indiquent que les cadres supérieurs commettent moins de délits économiques que les employés subalternes, ces délits ont tendance à être plus complexes et plus importants sur le plan financier. Par ailleurs, le fait que les fraudes complexes sont plus difficiles à détecter pourrait également expliquer que les délits économiques commis par les cadres supérieurs ne soient pas détectés aussi souvent que ceux commis par des cadres intermédiaires ou des employés subalternes.

Parmi les entreprises ayant subi des délits économiques à l'échelle mondiale principalement commis par des parties externes, 35 % ont identifié les clients comme étant les fraudeurs les plus courants, 18 % ont désigné les agents ou les intermédiaires et 17 % ignoraient qui était coupable de ces délits.

*Cinquante-six pour cent des entreprises à l'échelle mondiale victimes d'un crime économique au cours des 12 derniers mois ont indiqué que les fraudeurs étaient des personnes à l'interne.*

Graphique 8 : Profil des fraudeurs internes



### Quel sort les entreprises réservent-elles aux fraudeurs?

Les réponses obtenues à l'échelle mondiale en 2011 concernant les mesures disciplinaires prises à l'encontre des fraudeurs internes révèlent que, dans la majorité des cas (77 %), les fraudeurs ont été congédiés. Dans 44 % des cas, les autorités chargées de l'application des lois ont été informées et dans 40 % des cas, des poursuites civiles ont été engagées contre les fraudeurs.

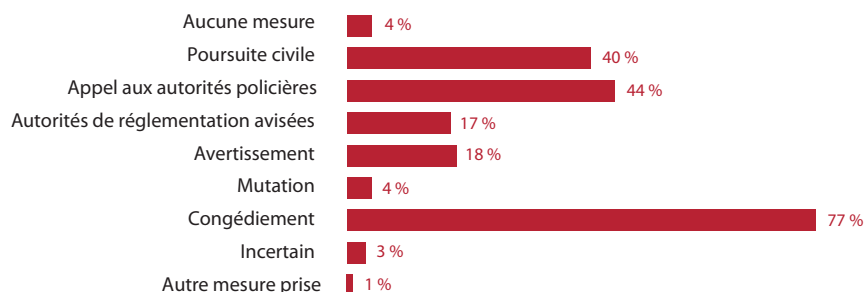
Le besoin d'instaurer des protocoles d'enquête robustes et adéquats pour obtenir des preuves est plus grand. De tels protocoles permettront à une entreprise d'optimiser le recouvrement et de prévenir d'éventuelles pertes à l'avenir.

### Comment les entreprises détectent-elles une fraude?

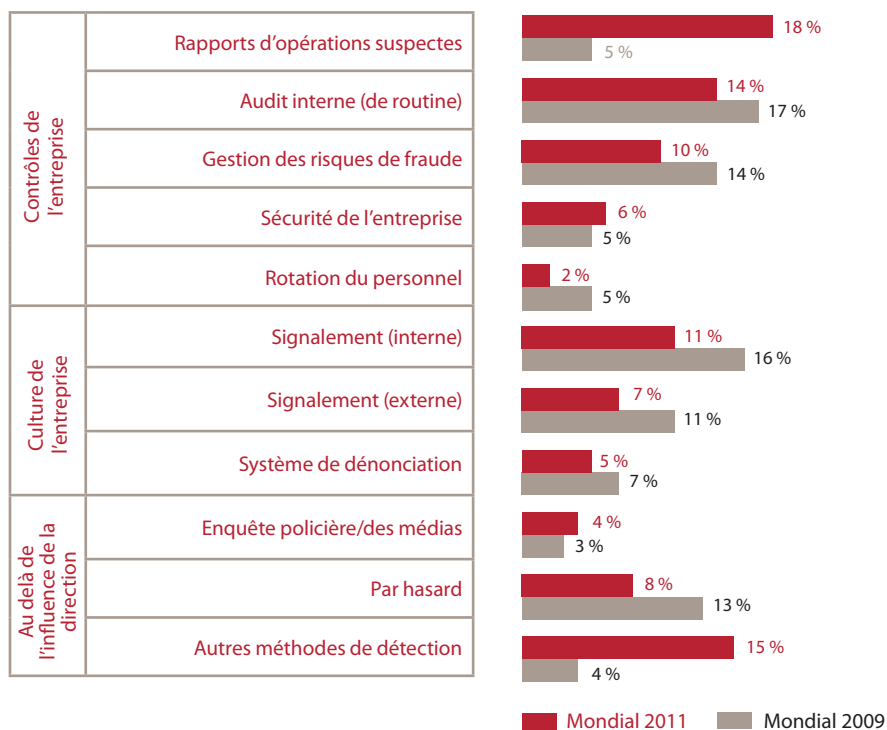
La détection de la fraude fait référence aux méthodes utilisées par les entreprises pour déterminer si un délit économique a été commis. Le graphique 10 présente les diverses méthodes de détection de la fraude.

Notre sondage révèle que 18 % des crimes économiques déclarés par les répondants à l'échelle mondiale ont été détectés grâce à des rapports d'opérations suspectes, soit une hausse de 13 % par rapport à 2009 (5 %). Les rapports d'opérations suspectes font appel à l'utilisation d'analyses prévisionnelles de données afin de repérer, dans les données financières, des irrégularités qui pourraient découler d'activités frauduleuses.

Graphique 9 : Mesures prises à l'encontre des fraudeurs internes (Mondial 2011)



Graphique 10 : Méthodes de détection

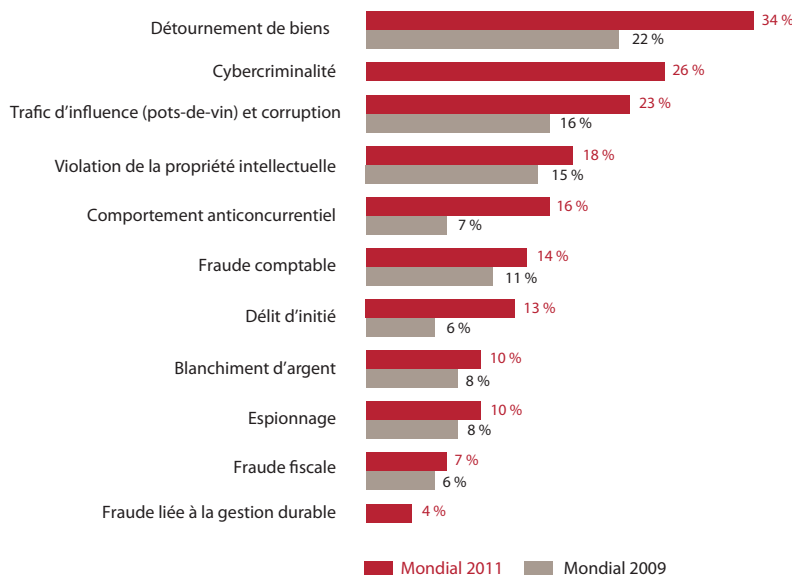


En 2011, 23 % des entreprises à l'échelle mondiale victimes de délits économiques au cours des 12 derniers mois ont détecté une fraude grâce à un système de dénonciation ou à des indices fournis par des sources internes ou externes, ce qui constitue une diminution de 11 % par rapport à 2009 (34 %). Ce résultat laisse supposer qu'il y a moins de délits économiques; cependant, il peut aussi laisser entendre que les employés sont réticents à l'idée de dénoncer leurs collègues et leurs clients, ou que la communication entre les services de l'entreprise est défaillante et qu'aucun suivi n'est fait à la suite des rapports d'irrégularités. Les entreprises doivent s'assurer que leurs employés sont informés de l'existence de ces systèmes, qu'ils sont à l'aise d'utiliser la ligne d'assistance des dénonciations et qu'ils ont une meilleure compréhension de leur obligation de déclarer des délits économiques, ainsi que des conséquences en cas de manquement. Les employés doivent également être assurés que la direction de leur entreprise prend au sérieux les dénonciations pour qu'ils aient l'assurance qu'ils peuvent avoir confiance dans les mécanismes de dénonciation prévus aux fins de signalement des fraudes, que les signalements de fraudes restent confidentiels et qu'ils soient traités de façon appropriée.

En plus des rapports d'opérations suspectes et de la culture de l'entreprise, 32 % des fraudes détectées avaient été signalées au moyen des activités de contrôle des entreprises interrogées, notamment l'audit interne, la gestion des risques de fraude, la sécurité d'entreprise et la rotation du personnel.

D'après les résultats de notre sondage de 2011, la mise en place d'un processus de gestion des risques de fraude s'est avérée moins efficace comme méthode de détection qu'en 2009, avec une baisse des fraudes, qui sont passées de 14 % à 10 % à l'échelle mondiale. La diminution des fraudes détectées grâce à la gestion des risques de fraude pourrait être attribuable, par exemple, à une plus grande utilisation des analyses prévisionnelles de données. Les entreprises qui misent sur une approche organisationnelle croisée de détection des fraudes, pour l'ensemble de leurs activités, englobant une culture de respect de l'éthique, des contrôles robustes

Graphique 11 : Perception de la fraude † † †



† Nota : un grand nombre de répondants ont subi plusieurs de ces types de délits économiques.

† † Dans nos sondages précédents sur la criminalité économique, lorsque l'on demandait aux répondants s'ils avaient fait l'objet de cybercriminalité, le taux de réponse était très bas et statistiquement non significatif. Conséquemment, nous avons regroupé ces résultats dans la catégorie « Autres types de fraudes » dans nos sondages précédents considérant l'augmentation de la menace liée à la cybercriminalité, nous avons mis l'accent sur la cybercriminalité cette année et l'avons réintroduite à la question concernant les types de fraudes, dans le cadre d'une question aux répondants, à savoir s'ils avaient été victimes de cybercriminalité au cours des 12 derniers mois. La fraude liée à la gestion durable a été incluse comme catégorie de fraude pour la première fois dans le sondage de cette année.

et une communication transparente, ont plus de chances de détecter les comportements frauduleux – en d'autres termes, « cherchez et vous trouverez ».

### Les entreprises prévoient plus de fraudes à l'avenir

Le graphique 11 illustre les menaces perçues de fraude économique telles qu'elles ont été exprimées dans nos sondages de 2009 et de 2011. À l'échelle mondiale, 34 % des répondants pensent que leur entreprise est susceptible de subir un détournement de biens au cours des 12 prochains mois, soit une augmentation de 12 % par rapport aux résultats de notre sondage de 2009. Vingt-six pour cent des répondants à l'échelle mondiale estiment qu'ils sont susceptibles d'être victimes de cybercriminalité, ce qui laisse penser que les entreprises sont de plus en plus conscientes de la menace réelle que représente la cybercriminalité.

Malgré l'existence d'activités frauduleuses et la perception de risques de fraude accrus, 29 % des répondants à l'échelle mondiale ont affirmé que leur entreprise n'avait pas procédé à une évaluation des risques de fraude et 12 % ignoraient si une telle évaluation avait eu lieu au cours des 12 derniers mois. Lorsqu'on leur a demandé les raisons pour lesquelles leur entreprise n'avait pas procédé à une évaluation des risques de fraude au cours des 12 derniers mois :

- 36 % des répondants à l'échelle mondiale ont affirmé que cette évaluation présentait peu de valeur;
- 30 % ont indiqué ne pas savoir exactement en quoi consistait le processus d'évaluation des risques de fraude;
- 20 % ignoraient la raison pour laquelle l'évaluation des risques de fraude n'avait pas été effectuée.

Lorsque les dirigeants s'intéressent vivement aux risques de fraude dans leur entreprise et infligent des sanctions disciplinaires sévères à leurs auteurs, ils donnent le ton qui convient. Les résultats du sondage de 2011 démontrent que le ton donné par la direction en matière d'éthique combiné à un contrôle interne solide constituent le meilleur moyen de dissuader les comportements répréhensibles et d'accroître la probabilité de détecter les activités frauduleuses. Les entreprises 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 articulé sont beaucoup moins exposées aux délits économiques.

### ***Mettre en place d'un programme antifraude efficace***

Lorsqu'ils évaluent et examinent leur programme antifraude, les dirigeants devraient songer à demander conseil à des professionnels en la matière sur la conformité, ainsi que les programmes de prévention et de détection des fraudes. L'entreprise doit également s'assurer que les

lignes directrices et les pratiques antifraude reflètent le climat économique changeant et que les mesures prises tiennent compte des lois et de la culture établies par les autorités compétentes pour chaque territoire sur le marché mondial.

Nous croyons que les principales mesures de contrôle antifraude doivent inclure les éléments suivants :

1. la gouvernance – la surveillance par le comité d'audit et le conseil d'administration;
2. des évaluations des risques de fraude;
3. un code de conduite et d'éthique;
4. des mécanismes de déclaration des incidents;
5. un protocole d'enquête (incluant des rapports d'opérations suspectes);
6. un protocole de remédiation;
7. des politiques et des procédures d'embauche et de promotion;
8. une évaluation et des contrôles de la direction.

*Les entreprises 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 beaucoup moins exposées aux délits économiques.*



# Comment PwC peut vous aider

PwC peut vous aider à contrer tous les types de crimes économiques et à mener des enquêtes financières avec rapidité, doigté et discrétion. Le crime économique est une menace réelle et sérieuse pour la stabilité d'une entreprise. Pour contrer la fraude et les irrégularités financières, il faut non seulement du savoir-faire, mais aussi de la rapidité, du doigté et de la discrétion. Nous sommes conscients de la nécessité de mettre un terme aux activités illégales, tout en assurant la sécurité des actifs et la protection de la réputation de votre entreprise, la prévention des récidives et l'élaboration d'une solution qui causera le moins de perturbations possible dans les activités courantes de votre entreprise. Nous offrons notamment les services suivants :

- les enquêtes de fraudes;
- la juricomptabilité;
- la gestion des risques de fraude;
- les enquêtes sur la cybercriminalité et les services de juricomptabilité informatique;
- le dépistage électronique;
- l'analyse de données;
- la vérification des antécédents et les recherches au sujet d'entreprises;
- les enquêtes sur le blanchiment d'argent;
- et les services liés au recouvrement d'actifs.

Le réseau international de professionnels des Services Enquête et juricomptabilité de PwC réunit une grande diversité de compétences et de connaissances, notamment en matière d'enquêtes, de juricomptabilité, de solutions technologiques juricomptables, de sécurité de l'information et de mise en application des lois et de la réglementation. Nous possédons les compétences techniques, les connaissances et l'expérience pratique nécessaires pour mener des enquêtes sur des fraudes commises par les cols blancs et fournir des conseils en matière de gestion et de réduction des risques incluant des façons d'identifier et d'analyser les failles en matière de sécurité.

Les cabinets du réseau PwC fournissent des services de certification, de fiscalité et de conseils dans divers secteurs d'activité afin d'apporter une valeur ajoutée à leurs clients. Dans les 154 pays où sont répartis les cabinets membres du réseau PwC, plus de 161 000 personnes mettent en commun leurs idées et leur expérience pour trouver des solutions, présenter de nouvelles perspectives et donner des conseils pratiques.

La diversité de nos profils et de nos compétences vous sera utile dans vos enquêtes et vos projets en juricomptabilité, quelle que soit la taille de votre projet.

Pour plus de renseignements, veuillez consulter notre site : <http://www.pwc.com/ca/fr/crimesurvey>.

# Personnes-ressources

## Équipe nationale des Services Enquête et juricomptabilité



**Steven Henderson**  
Leader national, Services  
Enquête et juricomptabilité  
416 941-8328  
steven.p.henderson@  
ca.pwc.com



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



**Kas Rehman**  
Leader national – Secteur  
public, Services  
Enquête et juricomptabilité  
613 755-4328/514 205-5171  
kas.rehman@ca.pwc.com



**Paul Bradley**  
Associé délégué, Services  
Enquête et juricomptabilité  
902 491-7436  
paul.f.bradley@  
ca.pwc.com



**Jason Armstrong**  
Directeur principal,  
Services  
Enquête et juricomptabilité  
613 755-8743  
jason.r.armstrong@  
ca.pwc.com



**Harm Atwal**  
Directrice principale,  
Solutions technologiques  
en juricomptabilité  
416 869-2330  
harm.k.atwal@  
ca.pwc.com



**Marie-Chantal Dréau**  
Vice-présidente, Services  
Enquête et juricomptabilité  
514 205-5407  
marie-chantal.dreau@ca.  
pwc.com



**Chris Gray**  
Vice-président, Services  
Enquête et juricomptabilité  
519 640-8011  
chris.gray@ca.pwc.com



**Ray Haywood**  
Leader, Services Enquête et  
juricomptabilité, Région du  
Grand Toronto  
416 814-5801  
h.ray.haywood@  
ca.pwc.com



**Dave Johnson**  
Vice-président, Services  
Enquête et juricomptabilité  
204 926-2423  
dave.a.johnson@  
ca.pwc.com



**Kyla Kramps**  
Vice-présidente, Services  
Enquête et juricomptabilité  
204 926-2434  
kyla.kramps@ca.pwc.com



**Sarah MacGregor**  
Directrice principale,  
Services  
Enquête et juricomptabilité  
416 814-5763  
sarah.e.macgregor@  
ca.pwc.com



**Steven Malette**  
Vice-président, Services  
Enquête et juricomptabilité  
613 755-5979  
steven.m.malette@  
ca.pwc.com



**Krista Mooney**  
Directrice principale,  
Services  
Enquête et juricomptabilité  
416 941-8290  
krista.a.mooney@  
ca.pwc.com



**James Pomeroy**  
Vice-président, Services  
Enquête et juricomptabilité  
902 491-7416  
james.a.pomeroy@  
ca.pwc.com



**Nikki Robar**  
Vice-présidente, Services  
Enquête et juricomptabilité  
902 491-7453  
nikki.l.robear@ca.pwc.com



**Lloyd Wilks**  
Directeur principal,  
Solutions technologiques  
en juricomptabilité  
416 687-8115  
lloyd.wilks@ca.pwc.com

La présente publication est conçue exclusivement à des fins d'information générale et ne constitue nullement un conseil professionnel. Il est recommandé de ne prendre aucune mesure fondée sur l'information contenue dans cette publication avant d'avoir obtenu l'avis d'un professionnel. Aucune déclaration ni garantie (explicite ou implicite) ne sont données quant à l'exactitude et à l'exhaustivité de l'information contenue dans cette publication, et, dans la mesure prévue par la loi, PricewaterhouseCoopers n'accepte ni n'assume aucune responsabilité ni obligation relativement aux conséquences de gestes posés ou non posés, par vous ou une autre personne, sur la foi de l'information contenue dans cette publication, ou relativement à toute décision fondée sur cette information.

© 2011 PwC. Tous droits réservés. Toute diffusion ultérieure du présent rapport requiert l'autorisation préalable de PwC. « PwC » s'entend de la marque sous laquelle les sociétés membres de PricewaterhouseCoopers International Limited (PwCIL) exercent leurs activités et offrent leurs services. Ensemble, ces sociétés forment le réseau PwC. Chaque société du réseau est une entité distincte sur le plan juridique, qui n'agit pas à titre de mandataire de PwCIL ni de toute autre société membre. PwCIL ne fournit pas de services aux clients. PwCIL n'est pas responsable des actes ou des omissions de la part de ses sociétés membres, et n'a aucune obligation à cet égard. PwCIL n'a aucun contrôle sur l'exercice du jugement professionnel au sein de ses sociétés et ne peut les lier de quelque manière que ce soit.

