www.pwc.fr

La fraude en entreprise : tendances et risques émergents

6e édition « Global Economic Crime Survey 2011 »

pwc

Sommaire

La fraude gagne du terrain 3
Des modes de détection plus efficaces 3
Quels sont les secteurs d'activité et les entreprises les plus touchés ? 6
Une baisse notable de la fraude comptable 8
La cybercriminalité : l'émergence d'un nouveau risque 9
La cybercriminalité : un risque de fraude atypique 10
Face à ce nouveau risque, les dispositifs de prévention et de contrôle doivent être adaptés 11
Qui sont les fraudeurs ? 12
Quelles sont les sanctions encourues par le fraudeur ? 14
Le coût de la fraude et les dommages collatéraux 15
Quelles perspectives pour les années à venir ? 16
Conclusion 17
Description de la population ayant répondu à notre enquête 18
Quelques définitions 20

édito

Nous avons le plaisir de vous présenter l'édition 2011 de notre étude mondiale sur la fraude en entreprise. Réalisée avec la collaboration de la *London School of Economics,* notre enquête repose sur des questionnaires collectés entre fin juillet et mi-septembre 2011 auprès de 3 877 entreprises dans 78 pays.

Notre étude apporte une analyse unique sur l'évolution des thèmes généraux relatifs à la fraude dans le monde et, en particulier en France, tout en s'inscrivant pleinement au cœur des préoccupations des entreprises. Nous avons choisi, à l'occasion de notre étude 2011, de porter une attention particulière au risque émergent que représente la cybercriminalité puisque dorénavant celle-ci figure au quatrième rang des fraudes dont les entreprises sont le plus victimes dans le monde.

Par ailleurs, il ressort de notre étude 2011 que les entreprises ont franchi une nouvelle étape dans leur lutte contre la fraude. Elles sont aujourd'hui de plus en plus souvent dotées de dispositifs d'identification des transactions inhabituelles qui leur permettent d'être plus efficaces dans la détection de la fraude. De ce fait, les entreprises dans le monde ont déclaré plus de fraudes que lors de notre étude précédente (34 % contre 30 %), il en est de même pour les entreprises françaises (46 % contre 29 %).

Enfin, toutes les entreprises sont touchées par la fraude, quel que soit leur secteur d'activité ou leur taille. Toutefois, notre étude montre qu'il existe encore de fortes disparités entre les grandes entreprises et celles de taille plus réduite. Ainsi, plus d'une grande entreprise sur deux (54 %) déclare avoir été victime d'une fraude au cours des douze derniers mois, alors que ce rapport est de moins d'une sur quatre (17 %) pour les plus petites entreprises.

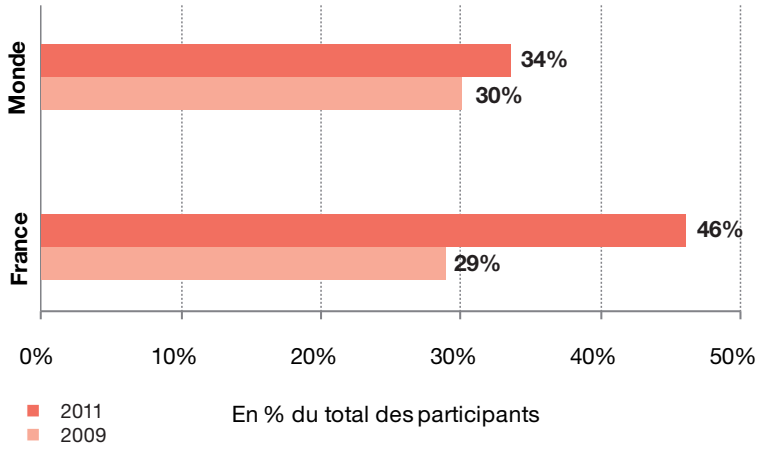
Depuis dix ans maintenant, PwC rassemble les témoignages des entreprises sur leur expérience et leur perception du risque de fraude. Nous espérons que cette nouvelle étude 2011 vous aidera à progresser dans votre compréhension de ce sujet complexe et dans votre lutte contre la fraude.

Dominique Perrier **Jean-Louis Di Giovanni**

La fraude gagne du terrain

La fraude demeure un enjeu majeur pour les entreprises puisqu'une entreprise sur trois interrogée dans le monde (34 %) dit avoir été victime d'une fraude au cours des douze derniers mois, près d'une entreprise sur deux en France (46 %). Ces résultats marquent une progression de la fraude par rapport à notre précédente étude de 2009 de respectivement + 4 points dans le monde et de + 17 points en France.

Fraudes reportées par les entreprises



Un niveau plus élevé de fraudes reportées ne signifie pas nécessairement que l'entreprise est davantage touchée par la fraude. Cela peut aussi signifier que l'entreprise la détecte mieux. En effet, une fraude n'est recensée qu'à partir du moment où elle a été détectée.

En ce sens, notre étude 2011 met en évidence une évolution notable dans la manière dont les entreprises détectent aujourd'hui les fraudes, tant au niveau mondial qu'en France.

Des modes de détection plus efficaces

Depuis 2005, nous analysons de quelle manière les entreprises découvrent les fraudes dont elles sont victimes. Nous distinguons trois modes de détection qui sont : les dispositifs de prévention et de contrôle de l'entreprise, la culture d'entreprise et les modes de détection en dehors de l'influence de l'entreprise comme le hasard par exemple.

Depuis 2009, les dispositifs de prévention et de contrôle constituent le mode de détection le plus efficace. Une fraude sur deux est détectée grâce à ces dispositifs dans le monde (61 % en France).

Toutefois, il est intéressant de noter l'évolution qu'ont connue les différents modes de détection depuis notre étude de 2005 :

- En 2005, les modes de détection en dehors de l'influence de l'entreprise étaient le principal mode de détection (33 %) permettant de découvrir une fraude puisque la sensibilité de l'entreprise au risque de fraude était encore limitée ou considérée comme un sujet difficile à aborder.

- En 2007, le fait que les entreprises focalisent leurs efforts sur certains aspects gravitant autour de la culture d'entreprise (code de conduite, code éthique, y compris les systèmes d'alerte), permet à ce mode de détection d'identifier 43 % des fraudes qui nous ont été signalées lors de cette étude.

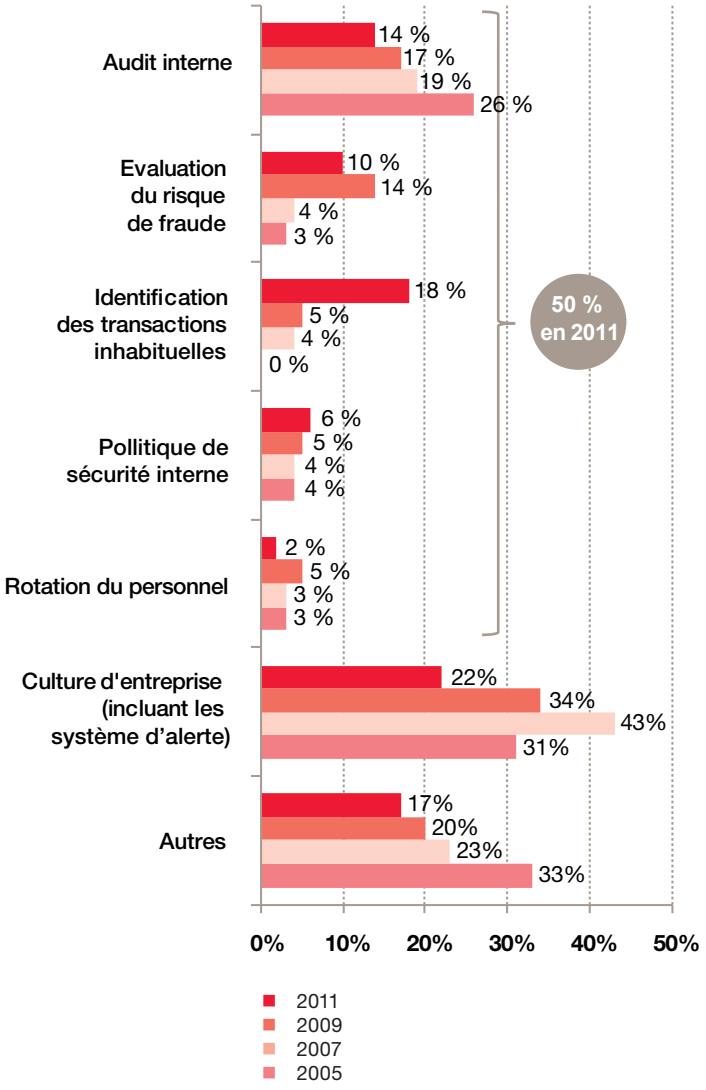
- En 2009, nouvelle évolution, puisque les entreprises se livrent dorénavant à des évaluations de leurs risques de fraude et sont amenées, à cette occasion, à en découvrir. En effet, il ressort de notre étude 2009 que ce moyen d'identification connait, à cette époque, une variation particulièrement importante en passant de 4 % à 14 % des fraudes qui nous ont alors été reportées.

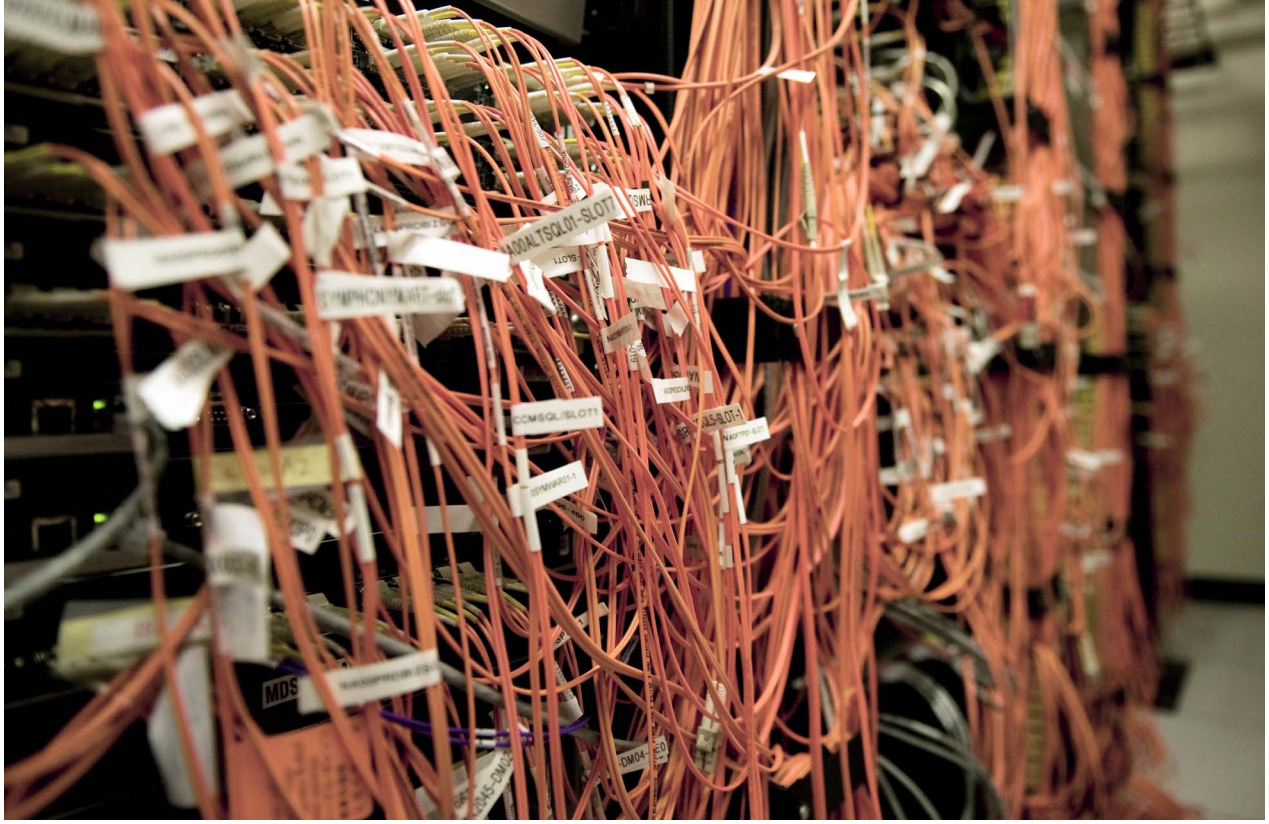
- Enfin en 2011, et dans le prolongement de cette réflexion sur le risque de fraude, les entreprises décident de lutter plus en amont contre la fraude et ce, à l'aide de moyens détectifs consistant à identifier des transactions présentant un caractère inhabituel. Aujourd'hui une fraude sur cinq est découverte de cette façon.

Concomitamment, il apparait que de moins en moins de fraudes sont découvertes par l'audit interne à l'occasion de ses missions périodiques ce qui est logique car dorénavant le risque de fraude est traité plus en amont.

Il ressort clairement depuis notre dernière étude que les entreprises ont franchi une nouvelle étape dans leur démarche de lutte contre la fraude en développant des contrôles automatisés d'identification des transactions inhabituelles. La mise en œuvre de ces contrôles permet aujourd'hui de raccourcir le délai nécessaire pour identifier une fraude et en conséquence de réduire le coût qui y est associé.

Modes de détection

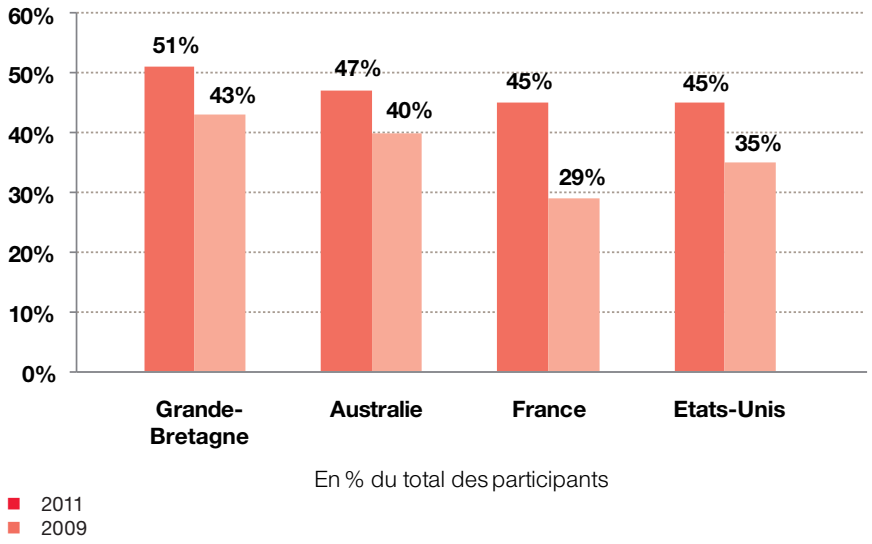




Par ailleurs, notre étude 2011 révèle une corrélation entre le niveau de fraudes reportées et l'importance prise par les systèmes automatisés dans les modes de détection. Ainsi, au Royaume-Uni et aux Etats-Unis, deux pays qui se classent dans le peloton de tête des pays ayant déclaré le plus de fraudes en 2011, c'est respectivement une fraude sur deux ou une fraude sur trois qui a été détectée grâce à des systèmes automatisés contre, rappelons le, une sur cinq dans le monde.

En France, les systèmes automatisés de détection de la fraude ont permis en 2011 de détecter plus d'une fraude sur trois ce qui est à comparer à moins d'une sur cinq en 2009. La France rejoint ainsi le peloton des bons élèves de la détection. De ce fait, le niveau de fraudes reportées en France en 2011, bien qu'en forte progression, est cohérent avec celui des pays leaders dans la détection de la fraude.

Fraudes reportées dans certains pays leaders de la détection

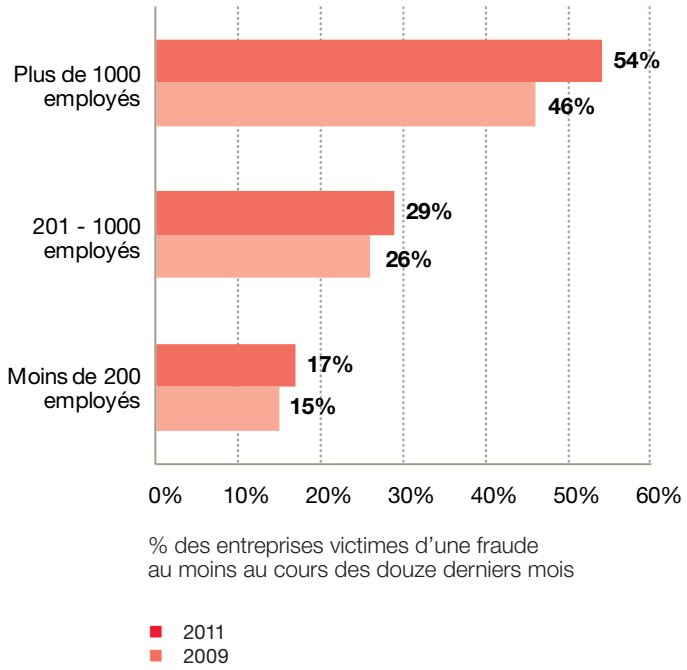


Quels sont les secteurs d'activité et les entreprises les plus touchés ?

Comme les années précédentes, nous constatons que tous les secteurs d'activités sont touchés par la fraude même s'il existe des disparités marquées selon les secteurs. Ainsi, certains secteurs le sont plus que d'autres au rang desquels nous trouvons le secteur des télécommunications qui déclare dans 48 % des cas avoir subi au moins une fraude au cours des douze derniers mois. Il en est de même pour le secteur des assurances (48 %) et celui de la banque (44 %). Comme nous le verrons ci-après, pour ces deux derniers secteurs, les fraudes externes dépassent, en valeur relative et de manière parfois significative, les fraudes internes.

Il est intéressant de noter que le secteur public (y compris les entreprises dans lesquelles l'Etat détient une participation) entre à la troisième place du classement des secteurs les plus touchés par la fraude (6e place en 2009). Ce constat nous parait être la conséquence du renforcement des contrôles et de la lutte contre la fraude dans ce secteur dans un contexte de rigueur économique.

Fraudes reportées selon la taille des entreprises



Notre étude 2011 met de nouveau en évidence une corrélation importante entre la taille de l'entreprise et l'occurrence de la fraude. En effet, il ressort qu'une entreprise de plus de mille employés sur deux (54 %) a été victime d'une fraude au cours des douze derniers mois, soit une progression de huit points par comparaison à 2009, ce chiffre atteignant même 67 % pour la France.

Ce pourcentage tombe à moins d'une entreprise sur trois (29 %) pour les structures comprenant de 200 à 1000 employés et à moins d'une sur cinq (17 %) pour les structures de moins de 200 employés. Bien que l'on constate également une progression sensible pour les entreprises de taille plus réduite allant de +2 à +3 points par rapport à 2009, ces dernières identifient un nombre de fraudes bien inférieur à celui constaté auprès des grandes entreprises.

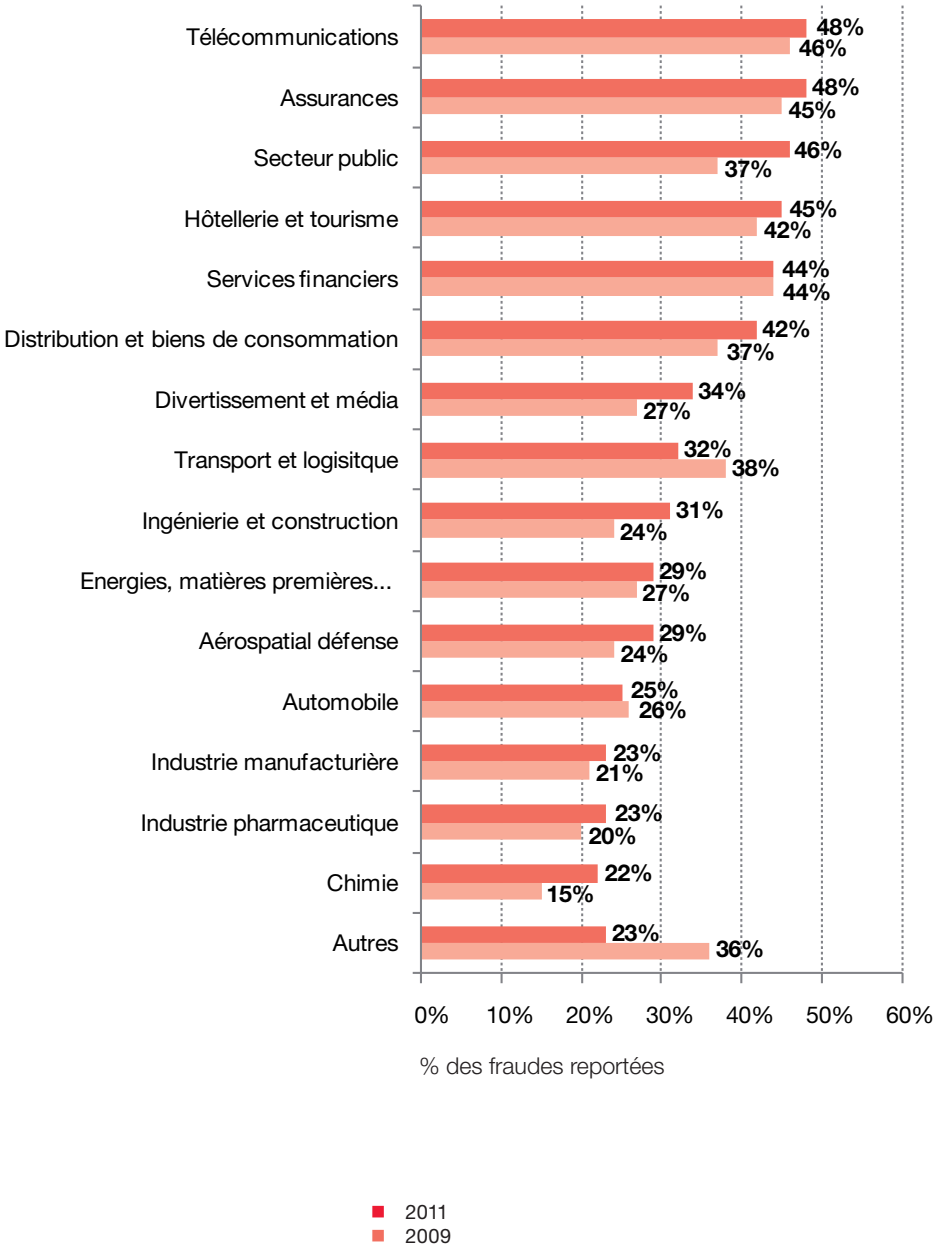
Cette situation ne signifie pas que les entreprises de taille plus réduite sont épargnées par la fraude. En effet, si les opportunités pour commettre un acte frauduleux sont plus nombreuses dans les grandes entreprises (organisations complexes, processus et systèmes interconnectés), les grandes entreprises sont aussi celles qui sont les mieux armées pour lutter contre la fraude.

Cette évolution doit, à notre avis, être mise en regard des résultats obtenus à l'occasion de la mise en place de systèmes détectifs visant à identifier les transactions inhabituelles qui sont généralement développés par des structures de plus grande taille.

De même, une fois encore, notre étude montre une corrélation entre la mise en œuvre d'une évaluation du risque de fraude et la découverte d'une fraude. En effet, il apparaît que parmi les entreprises évaluant le risque de fraude plus d'une fois par trimestre, 60 % ont détecté au moins une fraude au cours des douze derniers mois alors que ce pourcentage tombe à 28 % pour les entreprises qui ne se sont jamais livrées à ce type d'analyse. Il est donc possible de déduire de ces statistiques que la partie cachée de la fraude reste importante et qu'il existe, en particulier, un foyer potentiel de fraudes non détectées dans les entreprises de plus petite taille puisque les trois quart des sociétés ne mettant jamais en œuvre d'évaluation du risque de fraude sont des entreprises de moins de 1000 employés.

Malgré la corrélation démontrée entre la mise en œuvre régulière d'une évaluation du risque de fraude et la détection d'une fraude, 36% des entreprises demeurent toujours sceptiques et perçoivent encore ce type d'analyse comme à faible valeur ajoutée, ce qui va à l'encontre même des résultats de notre étude 2011.

Fraudes reportées par secteur d'activité



Une baisse notable de la fraude comptable

Conformément aux différentes définitions disponibles à la fin de cette étude, la fraude économique peut prendre de multiples formes qui sont principalement les détournements d'actifs, la fraude comptable ou bien la corruption.

Notre étude 2011 révèle cette année une baisse notable des fraudes comptables puisque 24 % des entreprises au niveau mondial disent avoir été affectées par ce type de fraude contre 38 % lors de notre dernière étude en 2009. Une baisse similaire a été constatée en France puisque ce même pourcentage passe de 33 % à 18 % des fraudes déclarées au cours des douze derniers mois.

Il convient de rappeler qu'en 2009, les fraudes comptables avaient fortement augmenté, ce qui avait été analysé, à l'époque, comme étant la résultante des pressions (internes et externes) plus importantes subies par les entreprises pour atteindre leurs objectifs financiers en temps de crise. Il n'est pas exclu non plus, qu'au cours de cette période de crise, les entreprises, à la recherche de résultat, aient aussi passé leurs comptes au « peigne fin » ce qui à l'époque, a certainement permis de découvrir plus de fraudes comptables voire, par la suite, de mettre en place des contrôles dissuasifs pour lutter contre ce type de fraude et décourager les fraudeurs potentiels.

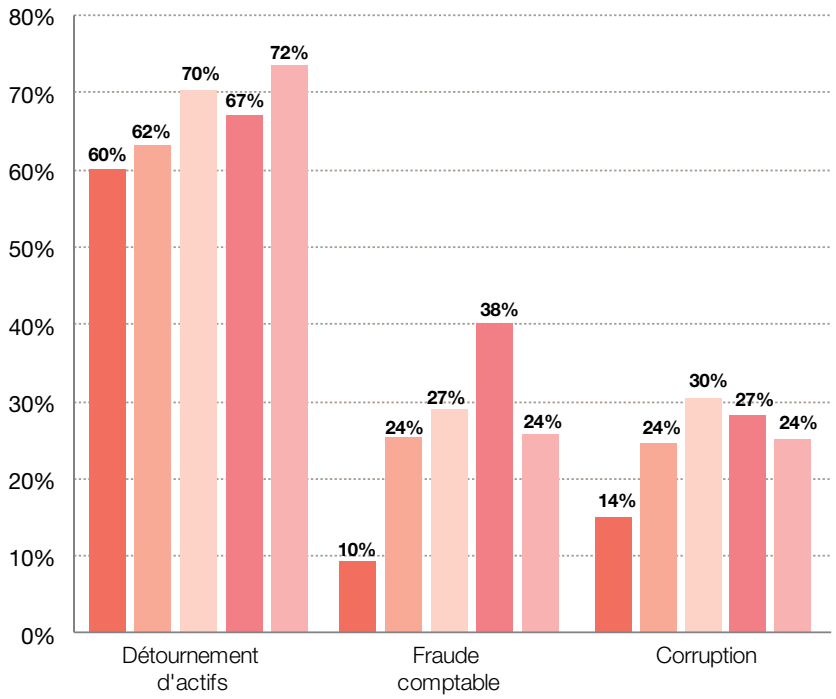
Par ailleurs, une fois encore, le détournement d'actifs demeure la fraude la plus répandue puisque 72 % des entreprises interrogées dans le monde nous indiquent avoir été victimes de cette catégorie de fraude au cours de ces douze derniers mois (80 % en France). Il est à noter que ce type de fraude, qui a souvent une incidence limitée sur les comptes des entreprises, est, de par sa nature, la plus difficile à prévenir mais en revanche la plus facile à identifier.

Enfin, la corruption est, au sein de notre étude, la troisième catégorie de fraude la plus rencontrée au niveau mondial avec 24 % des entreprises interrogées. Ce pourcentage est en recul par rapport à nos précédentes études (moins six points par rapport à 2007). Ce phénomène peut s'expliquer par la pression médiatique née de cas avérés qui ont conduit les entreprises à plus de vigilance sur ce sujet.

Il est également vraisemblable que les effets de l'arsenal législatif de lois qui ont été votées pour lutter contre la corruption depuis le début des années 2000 aient aussi contribué à ce recul du fait de leur application plus systématique.

Il n'en demeure pas moins qu'il existe de fortes disparités d'un pays à l'autre. En Europe de l'Ouest, 12 % seulement des entreprises ont reporté des cas de corruption dans le cadre de notre étude 2011. Ce risque affecte néanmoins tous les pays dès lors que les entreprises travaillent avec des agents publics étrangers dans des pays émergents ou font appel à des intermédiaires.

Fraudes reportées par les entreprises (2003-2011)



La cybercriminalité : l'émergence d'un nouveau risque

Grande nouveauté de notre étude 2011, la cybercriminalité fait son entrée au quatrième rang dans le classement mondial des principales catégories de fraude avec 23 % des entreprises qui nous disent avoir été victime d'un acte de cybercriminalité au cours des douze derniers mois, juste derrière la fraude comptable et la corruption.

Aucune définition universelle de la cybercriminalité n'existe et de nombreuses personnes considèrent que cette notion recouvre en réalité des agissements beaucoup plus larges. A titre d'exemple, certains peuvent considérer que le cas d'un responsable des ventes sauvegardant sur une clef USB les bases de données ventes et marketing de son ancien employeur alors qu'il s'apprête à rejoindre un concurrent relève, entre autres, de la cybercriminalité. Dans ce cas particulier, la cybercriminalité n'est pas forcément vue comme un délit en soi mais plutôt comme un moyen utilisé pour réaliser un acte de criminalité économique.

Dans notre étude 2011, la cybercriminalité a été définie de la manière suivante :

> ***"La cybercriminalité, également appelée criminalité informatique, consiste en la réalisation de délits commis à l'aide d'équipements informatiques et d'Internet. Parmi les exemples classiques de cybercriminalité, il est possible de citer la diffusion de virus informatiques, le téléchargement illégal, les actes de phishing, le vol d'informations personnelles telles que des données bancaires. Cette définition exclut les cas de fraude plus classiques où le fraudeur s'appuie sur un ordinateur ou tout autre équipement électronique pour commettre son acte sans que cela constitue l'élément principal du schéma de fraude."***

Lors de nos précédentes études, le nombre d'entreprises qui déclaraient avoir été victimes de cybercriminalité était non significatif d'un point de vue statistique. Par le passé, ces résultats ont par conséquent été intégrés au sein de la catégorie regroupant les autres types de fraude. Il est donc légitime de chercher à comprendre pourquoi la cybercriminalité apparaît aujourd'hui comme la quatrième catégorie de fraude la plus rencontrée par les entreprises au cours des douze derniers mois.

En premier lieu, l'exposition médiatique de plus en plus marquée autour d'exemples frappants d'actes de cybercriminalité a joué certainement un rôle important dans la sensibilisation des entreprises au risque de cybercriminalité. La prise de conscience résultant de cette médiatisation pourrait avoir conduit les entreprises à renforcer leur environnement de contrôle afin de mieux détecter les actes de cybercriminalité les concernant et, par conséquent, à en relever de plus nombreux.

Par ailleurs, l'ambiguïté entourant la définition de la cybercriminalité, précédemment soulignée et le focus fait cette année dans le cadre de cette étude, pourraient également avoir conduit certains répondants à catégoriser quelques types de fraudes « classiques » en actes de cybercriminalité parce qu'ils ont été commis à l'aide d'un ordinateur ou d'équipements électroniques par exemple.

Enfin, nous assistons de plus en plus à une vraie professionnalisation de la cybercriminalité. En effet, l'entreprise n'est plus uniquement confrontée à un hacker isolé qui se lance un défi visant à s'introduire dans tel ou tel système d'information mais aussi à de véritables réseaux organisés dont le seul objectif est financier ce qui, in fine, a vraisemblablement contribué à l'augmentation de la cybercriminalité au cours de ces deux dernières années.

Ainsi, les résultats de notre étude montrent clairement que la cybercriminalité est considérée comme une menace en nette croissance puisqu'une entreprise sur deux ayant été victime d'un acte de cybercriminalité au cours des douze derniers mois, considère à l'avenir que ce risque est en augmentation.

La cybercriminalité : un risque de fraude atypique

La cybercriminalité est un risque de fraude atypique comparé aux autres types de fraude plus conventionnels. Par référence au « Triangle de la fraude » de Donald Cressey, les trois éléments déclenchants du risque de cybercriminalité, à savoir la motivation, l'opportunité et la rationalisation de l'acte, peuvent être analysés de la manière suivante.

La motivation : les systèmes informatiques centralisent et agrègent de nombreuses données et constituent donc naturellement une cible tentante pour qui s'intéresse à ces informations parfois insuffisamment protégées qui, par ailleurs, sont susceptibles d'être utilisées à des fins lucratives.

L'opportunité : la criminalité informatique est généralement caractérisée par un rapport gains / risques largement supérieur aux délits classiques. Ainsi, il apparaît que :

- grâce aux systèmes informatiques, des vols peuvent être commis sans déplacer le bien dérobé et l'espace n'est finalement plus une barrière ;
- l'obtention d'habilitations normalement attribuées à des tiers permet de contourner certains contrôles, de la même manière que dans un schéma de collusion ;
- la cybercriminalité n'a pas de barrière géographique et offre souvent la possibilité d'agir de manière furtive tout en masquant son identité ce qui rend difficile sa détection, mais aussi l'arrestation et la poursuite des auteurs ;
- la coopération internationale des régulateurs en la matière se heurte souvent à certains obstacles qui n'existent pas dans le cas d'un délit commis localement.

La rationalisation de l'acte : les personnes commettant des actes de cybercriminalité peuvent facilement se représenter leurs actions comme étant « virtuelles » et donc bien moins graves qu'un délit classique. En agissant ainsi, certains fraudeurs occultent également le caractère délictuel de leurs actes, poussés par une forme de curiosité ou en percevant leurs actions sous un aspect ludique.

Face à ce nouveau risque, les dispositifs de prévention et de contrôle doivent être adaptés

Comme nous l'avons vu, les entreprises sont de plus en plus préoccupées par les risques grandissants liés à la cybercriminalité. Et pourtant, notre étude montre une insuffisance des mesures permettant de prévenir la matérialisation de ces risques, les entreprises semblant encore privilégier une approche réactive plutôt que proactive face à la menace d'être confrontées à un acte de cybercriminalité.

Ainsi, au niveau mondial, une entreprise sur quatre déclare qu'elle n'a aucun dispositif de prévention et de détection des risques de cybercriminalité sachant que 42 % des répondants déclarent ne pas avoir les compétences en interne pour investiguer les actes de cybercriminalité.

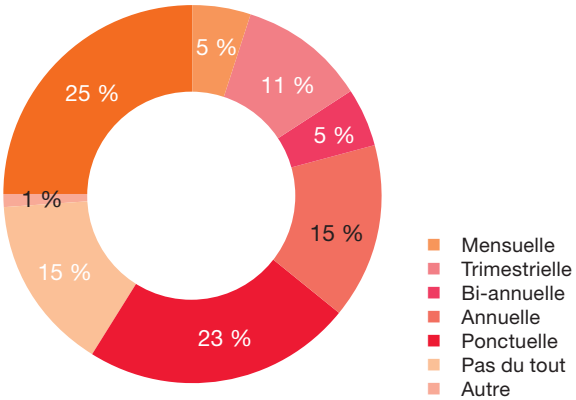
Historiquement, la gestion des risques de cybercriminalité a souvent été catégorisée comme étant une problématique dépendant purement de la fonction informatique, engendrant ainsi un fossé de communication entre les responsables de la sécurité informatique et les responsables métier.

Notre dernière étude spécifique à la sécurité des systèmes d'information montre d'ailleurs que désormais, les entreprises reconnaissent qu'avant d'être un sujet technique, la gestion de la sécurité informatique est avant tout un enjeu métier primordial.

Pourtant, notre étude fait ressortir que plus d'une entreprise sur deux déclare que le Directeur des Systèmes d'Information est, in fine, propriétaire des risques de cybercriminalité. Seulement, une entreprise sur cinq (5 % en France) déclare ainsi que cette responsabilité est, in fine, du ressort de la Direction Générale ou du Conseil d'Administration.

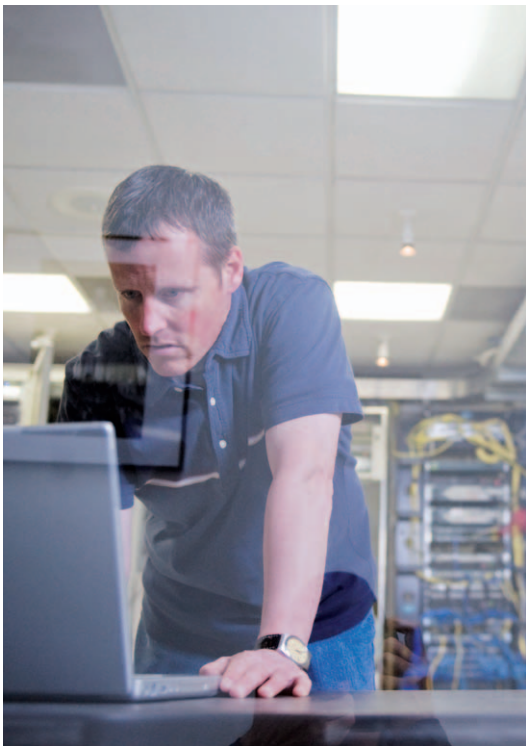
Dans ces conditions il n'est pas surprenant que les Directions Générales et les Conseils d'Administration ne réalisent pas régulièrement une revue du risque de cybercriminalité : seulement 36 % des répondants (29 % en France) déclarent que des revues de ce type sont réalisées, au sein de leurs entreprises, au moins une fois par an.

Fréquence de revue des risques de cybercriminalité par la direction



En % du total des participants

Le niveau de maturité des entreprises en matière de gestion de la cybercriminalité semble donc encore pouvoir bénéficier d'une certaine marge de progression.



Qui sont les fraudeurs ?

Pour se prémunir contre le risque de fraude, il est nécessaire que l'entreprise identifie qui sont les fraudeurs et d'où ils viennent (interne ou externe), pour mieux cibler les éventuelles faiblesses dans leur dispositif de lutte contre le risque de fraude.

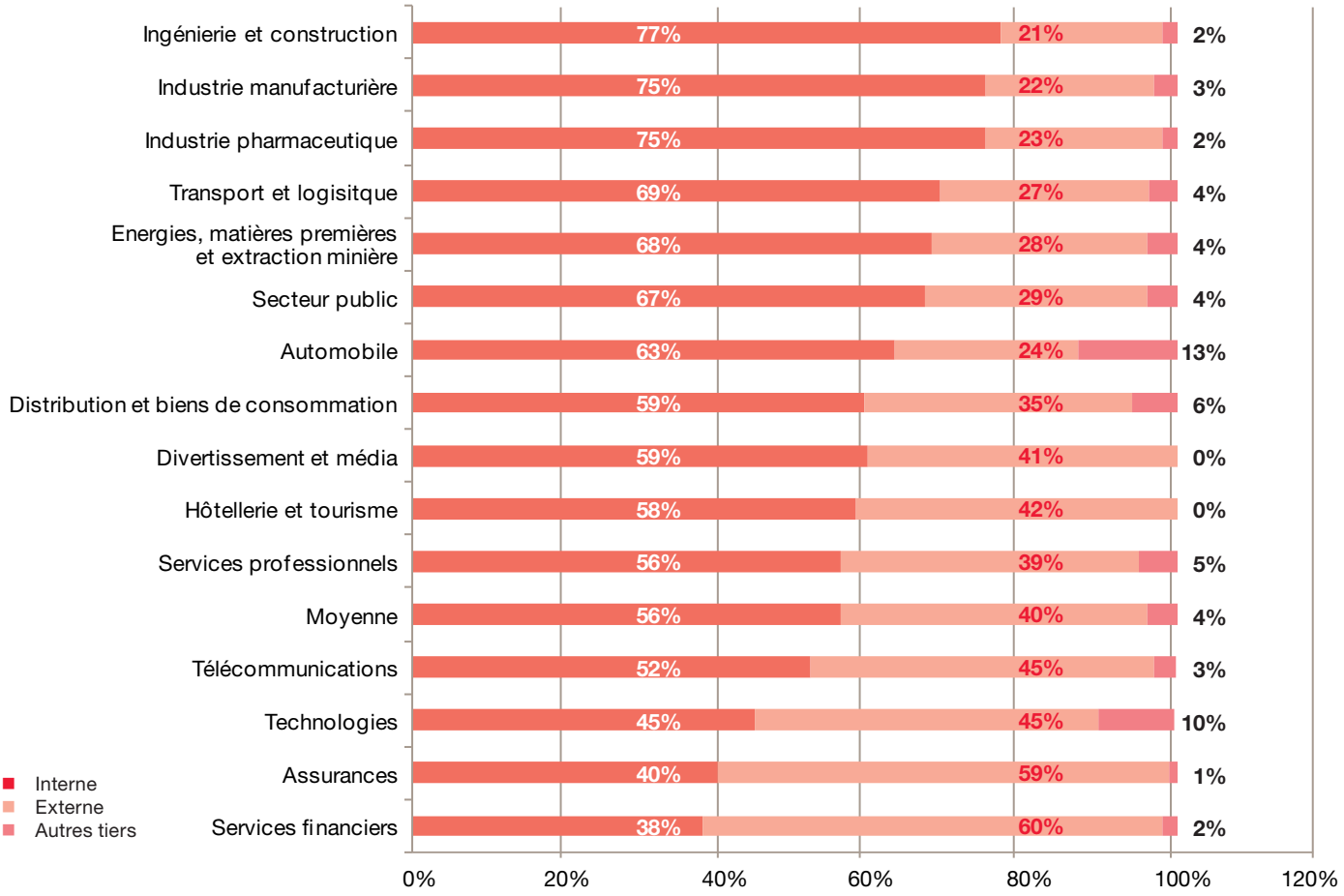
Les entreprises qui ont été victimes d'au moins une fraude au cours des douze derniers mois nous ont indiqué à 56 % qu'elles avaient été commises par un fraudeur interne (53 % en 2009) et à 40 % par un fraudeur externe (44 % en 2009). Comme lors de nos précédentes études, le pourcentage relativement élevé des fraudes externes s'explique par le fait que les secteurs des services financiers et des assurances sont fortement représentés au sein de notre échantillon mondial, et ont déclaré, de par la nature même de leur activité, un pourcentage élevé de fraudes externes.

Toutefois, et comme il est possible de le constater dans l'analyse complète par secteur d'activité, la fraude interne demeure largement prépondérante dans la très grande majorité des différents secteurs d'activité.

À propos des fraudes externes, il est intéressant de noter que dans près d'un cas sur cinq, les entreprises déclarent ne pas savoir qui en est l'auteur, soit une progression de 15 points par rapport à notre étude précédente ce qui est à mettre, à notre avis, en regard de l'augmentation constatée au niveau de la cybercriminalité et des difficultés rencontrées à identifier ce type de fraudeur.

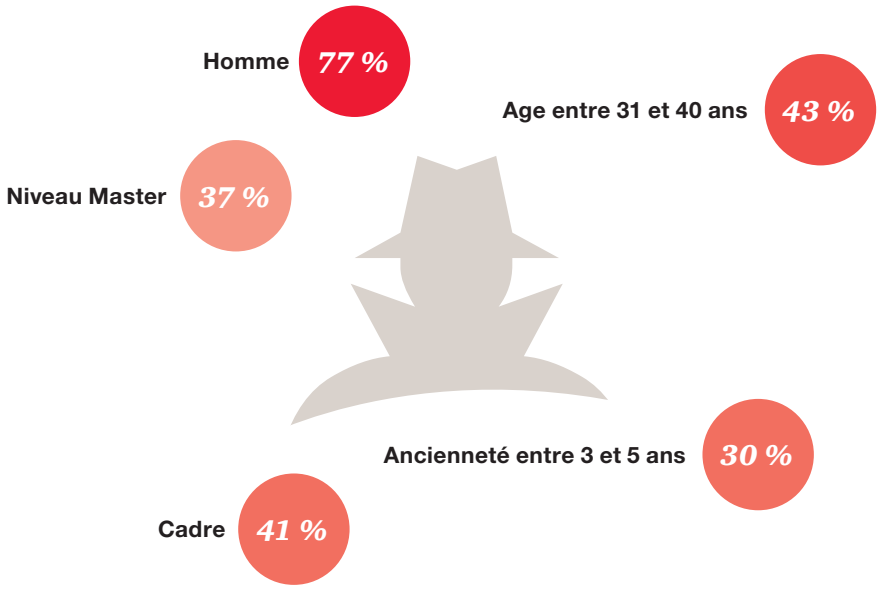
Il est à noter qu'au cas particulier de la cybercriminalité, seulement 13 % des entreprises considèrent que la menace est exclusivement interne à l'entreprise et qu'elle se situe plus particulièrement au niveau du département informatique à hauteur de 53 %. Cette analyse ne nous semble pas refléter la réalité, plus particulièrement pour ce qui concerne l'origine interne de la menace qui, au regard de notre expérience, nous semble sous-évaluée.

Fraude interne / fraude externe par secteur d'activité



Le fraudeur interne est un homme, dans 77 % des cas, majoritairement âgé de 31 à 40 ans et disposant de trois à cinq ans d'ancienneté dans l'entreprise. Les cadres sont les principaux auteurs des fraudes commises au niveau mondial (41 %) suivis de très près par les employés (39 %). Il est toutefois intéressant de noter qu'en Europe de l'Ouest et en France, le fraudeur est majoritairement plus âgé puisqu'il se situe dans la tranche d'âge allant de 41 à 50 ans et dispose de davantage d'ancienneté dans l'entreprise soit plus de 10 ans. Il convient de ne pas oublier un point important qui n'est pas directement issu de notre étude mais de notre expérience sur le terrain : le fraudeur est généralement une personne sympathique. Ce point, associé aux caractéristiques du fraudeur en Europe de l'Ouest, rendent ce dernier difficilement soupçonnable.

Portrait robot du fraudeur



En % des fraudes reportées

En ce qui concerne le cyber fraudeur, c'est un employé dans 85 % des cas, qui dispose de moins de cinq ans d'ancienneté au sein de l'entreprise dans 51 % des cas et est âgé de moins de 40 ans dans 65 % des cas. Ce profil est cohérent avec la nature même de ce type de fraude qui implique que le fraudeur soit familier des nouvelles technologies.

Quelles sont les sanctions encourues par le fraudeur ?

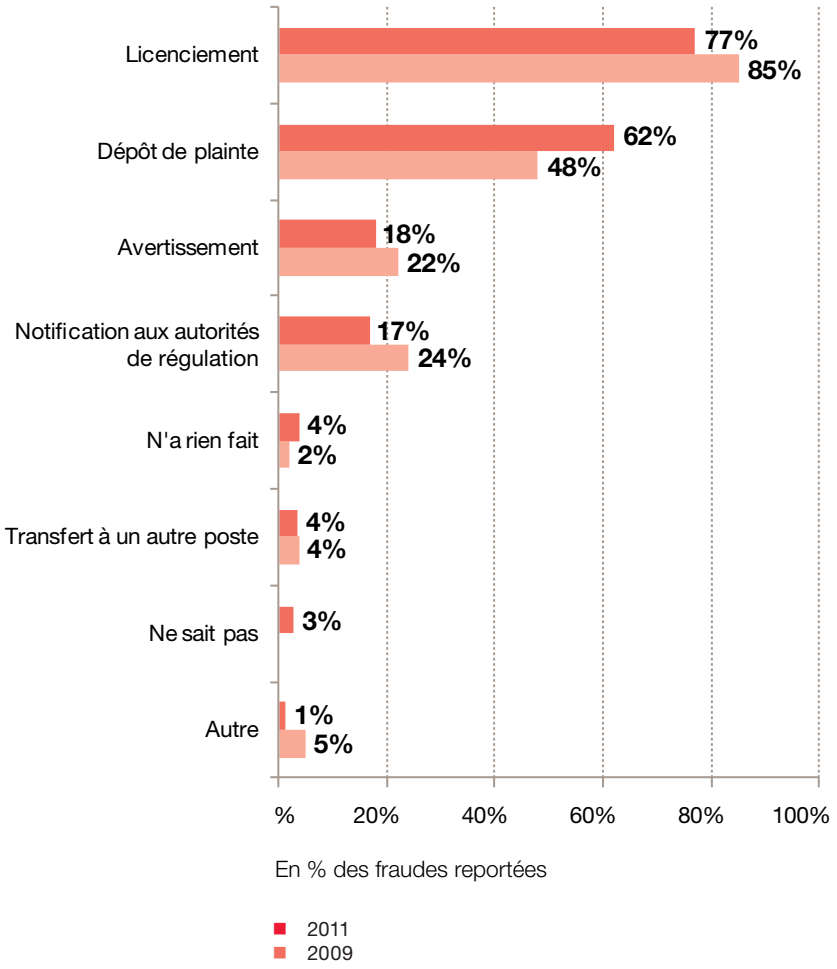
La réaction de l'entreprise à l'égard du fraudeur est, à notre avis, essentielle. Il ne faut pas laisser impuni ce type de comportement et délivrer un message fort de « tolérance zéro » aux fraudeurs potentiels qui conduira, in fine, à réduire d'autant le risque global de fraude au sein de l'entreprise.

En cas de fraude interne, notre étude 2011 montre que la sanction la plus couramment employée est le licenciement du fraudeur. En effet, celui-ci intervient dans 77 % des cas au niveau mondial et s'accompagne dans 62 % des cas d'un dépôt de plainte (au pénal ou au civil). Il ressort de notre étude, des pourcentages globalement similaires pour la France par rapport à ceux relevés au niveau mondial puisque le licenciement intervient dans 76 % des cas.

Bien que les entreprises soient de plus en plus conscientes de la nécessité de l'exemplarité des sanctions, il reste inquiétant de constater que dans 4 % des cas de fraude interne, l'organisation n'a pas sanctionné le fraudeur ou que le fraudeur a simplement été transféré à un autre poste, ou encore que dans 18 % des cas, un simple avertissement lui a été adressé.

Or, l'entreprise doit dissuader les fraudeurs potentiels de passer à l'acte. En effet, dans une entreprise, vous trouverez toujours, mais de façon plus ou moins marginale, des personnes qui frauderont et d'autres qui ne frauderont jamais et ce, quelles que soient les circonstances. À côté de ces deux populations, va se trouver la grande majorité des employés qui seront susceptibles de frauder dès lors que l'entreprise ne les dissuadera pas de le faire au regard des procédures mises en place et des sanctions encourues. C'est là que réside le véritable enjeu pour les entreprises.

Sanctions prises à l'égard des fraudeurs



Le coût de la fraude et les dommages collatéraux

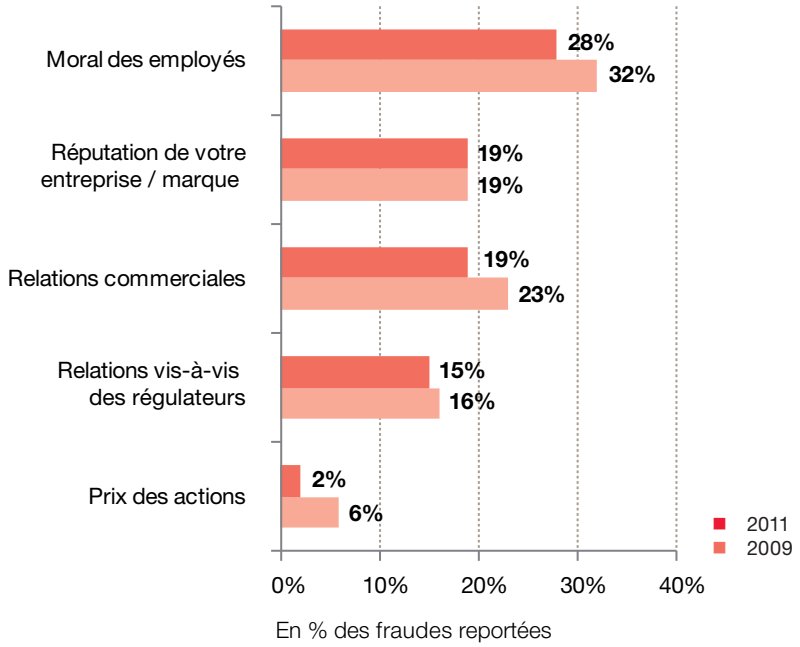
Près d'une entreprise sur dix dans le monde ayant déclaré avoir été victime d'au moins une fraude au cours des douze derniers mois, a signalé des

pertes de plus de cinq millions de dollars. Néanmoins, et comme nous l'avons vu précédemment, le coût moyen direct de la fraude est disparate en fonction de la nature des fraudes perpétrées. Ainsi, une entreprise sur cinq dans le monde ayant déclaré avoir été victime de corruption signale un préjudice de plus de cinq millions de dollars.

Il est intéressant de noter que dans la pratique, il existe généralement une corrélation entre le coût de la fraude et la position hiérarchique de celui qui la commet. En effet, plus cette position sera élevée plus le coût de la fraude sera important.

Par ailleurs, l'incidence des fraudes n'est pas seulement limitée au coût financier. La découverte d'une fraude peut avoir d'autres conséquences collatérales affectant plus particulièrement le moral des employés (28 %). En effet, les personnes qui connaissaient le fraudeur se sentent trahies. De plus, voir associé le nom de son entreprise à ce type d'affaire dans les médias est souvent très démotivant. Puis viennent, parmi les autres dommages collatéraux, la réputation de l'entreprise (19 %) et les relations commerciales avec les tiers (19 %). Dorénavant, certaines grandes entreprises se livrent à des contrôles systématiques avant de débuter une relation commerciale avec un nouveau fournisseur en vérifiant, par exemple, que ce tiers n'a jamais été condamné dans le cadre d'une affaire frauduleuse ou une problématique de corruption.

Dommages collatéraux



Au cas particulier de la cybercriminalité, tant dans le monde qu'en France, plus d'une personne interrogée sur trois se dit très préoccupée par les effets qu'un acte de cybercriminalité peut avoir sur la réputation de son entreprise. Tandis qu'il s'agit de l'effet jugé le plus préoccupant au niveau mondial, en France, cet aspect se positionne juste après le risque de vol ou de perte de données personnelles.

Quelles perspectives pour les années à venir ?

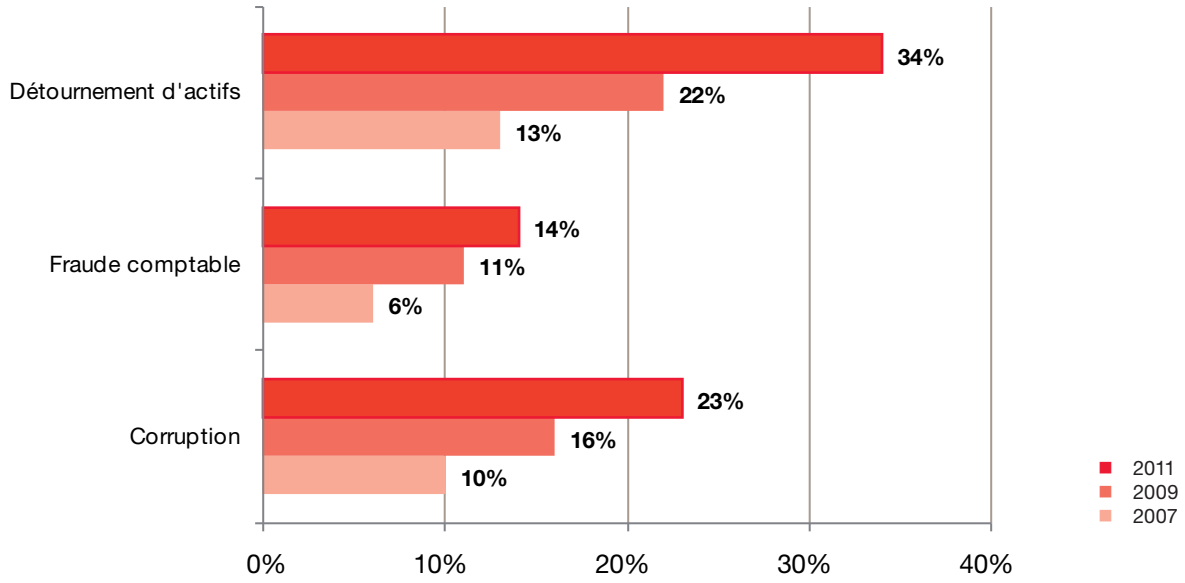
Depuis 2001, date de notre première étude, les entreprises n'ont cessé de progresser dans leur perception du risque de fraude. Ainsi, elles sont de plus en plus conscientes du risque qu'elles encourent.

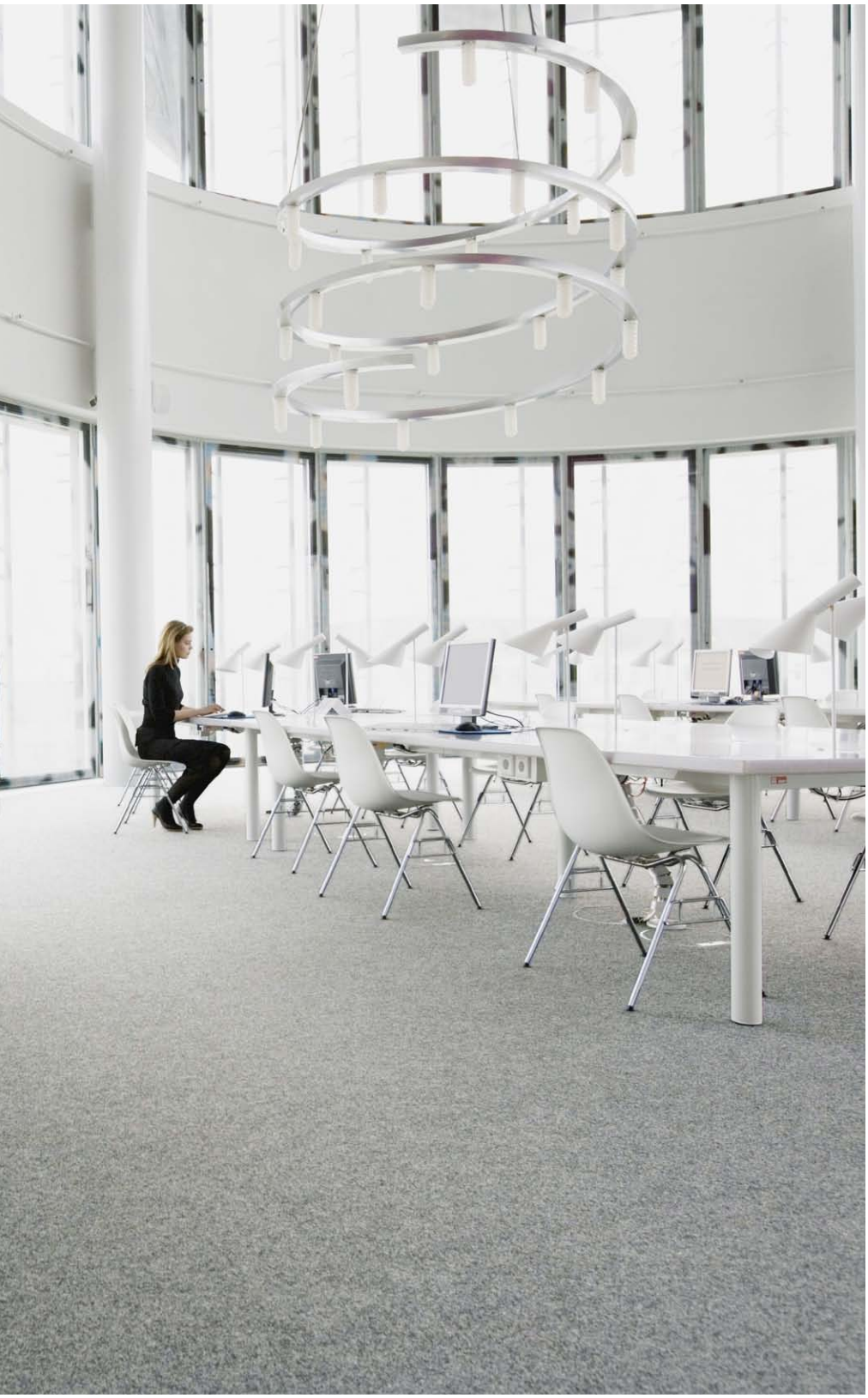
Dans le monde, 24 % des entreprises ayant participé à notre étude 2011 anticipent qu'elles seront victimes dans les douze prochains mois d'au moins un des trois principaux types de fraude alors qu'elles n'étaient que 16 % en 2009.

En France, 50 % des entreprises estiment qu'elles seront victimes d'un détournement d'actifs dans les douze mois qui viennent alors qu'elles n'étaient que 35 % en 2009 et qu'elles ont été 37 % à être réellement victimes de ce type de fraude en 2011.

Au cas particulier du risque émergent de cybercriminalité, 24 % des entreprises estiment qu'elles en seront victimes dans les douze prochains mois (32 % en France). Il est intéressant de constater que ces pourcentages sont au-delà de ceux attendus pour les fraudes comptables (14 %) et la corruption (23 %).

Evolution de la perception du risque de fraude (2007-2011)





Conclusion

Depuis 2001, date de notre première étude, les entreprises françaises n'ont cessé de progresser dans la lutte contre la fraude.

Elles sont de plus en plus conscientes du risque puisque 50 % d'entre elles estiment qu'elles seront victimes d'un détournement d'actifs dans les douze mois qui viennent.

Comme nous l'avions préconisé dans notre précédente édition, elles sont de plus en plus nombreuses à développer des systèmes de prévention et de détection des transactions inhabituelles. Elles se situent dorénavant dans le peloton de tête en matière de détection aux côtés des entreprises anglo-saxonnes.

Toutefois, face à l'émergence de la cybercriminalité, un effort particulier est à réaliser en matière de prévention de ce type de fraude. Cela suppose l'intégration des actions de sécurité des systèmes d'information dans la démarche de la lutte contre la fraude et une meilleure compréhension et appropriation de ce type de risque au niveau de la direction générale.

La poursuite et la généralisation de ces actions sont essentielles à la lutte contre la fraude car la dissuasion contribue fortement à la réduction du risque de fraude.

Description de la population ayant répondu à notre enquête

Notre sixième étude mondiale sur la fraude économique en entreprise a été réalisée entre fin juillet et mi-septembre 2011 en collaboration avec la London School of Economics. 3877 réponses ont été recueillies auprès de 78 pays sur la base de questionnaires complétés sur un site internet dédié. Il a aussi été demandé aux participants de préciser dans quel type d'entreprise ils travaillaient et le pays dans lequel ils se trouvaient.

Zone / Pays en nombre de participants	2011
Asie & Pacifique	**796**
Australie	79
Corée du Sud	-
Hong Kong (et Chine)	22
Inde	106
Indonésie	84
Japon	73
Malaisie	93
Nouvelle Guinée	1
Nouvelle-Zélande	93
Pays du Moyen-Orient*	127
Philippines	-
Singapour	18
Taïwan	2
Thaïlande	79
Vietnam	19
Afrique	**260**
Afrique du Sud	123
Angola	1
Botswana	1
Ghana	29
Kenya	91
Libéria	5
Namibie	2
Nigéria	3
Sierra Leone	-
Soudan	1
Swaziland	1
Tunisie	2
Zambie	1
Amérique du Sud et Centrale	**483**
Argentine	77
Bolivie	3
Brésil	115
Chili	1
Colombie	1
Equateur	11
Mexique	174
Pérou	17
Venezuela	84

*Les pays du Moyen-Orient incluent des participants de Jordanie, du Koweït, d'Oman, d'Arabie Saoudite, du Qatar, de Bahreïn et des Emirats Arabes Unis.

Zone / Pays en nombre de participants	2011
Amérique du Nord	**209**
Canada	53
Etats-Unis	156
Europe de l'Ouest	**1317**
Allemagne	38
Andorre	1
Autriche	8
Belgique	84
Chypre	5
Danemark	116
Espagne	85
Finlande	61
France	112
Grande-Bretagne	178
Grèce	92
Hollande	41
Irlande	80
Italie	127
Luxembourg	3
Norvège	67
Portugal	-
Suède	79
Suisse	140
Europe Centrale et de l'Est	**804**
Bulgarie	58
Croatie	1
Estonie	1
Hongrie	85
Lituanie	7
Moldavie	1
Montenegro	1
Pologne	79
République Tchèque	84
Roumanie	76
Russie	126
Serbie	14
Slovaquie	84
Slovénie	48
Turquie	55
Ukraine	84
Pas de pays spécifié	**8**
TOTAL	**3877**

Secteur des entreprises participantes	2011
Services financiers	18%
Industrie manufacturière	12%
Distribution et consommation	8%
Energie, matières premières et extraction	7%
Services professionnels	6%
Ingénierie et construction	5%
Secteur public	5%
Assurances	5%
Industrie pharmaceutique	5%
Technologies	5%
Automobile	4%
Transport & logistique	4%
Télécommunications	3%
Divertissement et medias	3%
Chimie	2%
Hôtellerie et loisirs	2%
Aérospatial et défense	1%
Education	1%
Alimentaire	1%
Santé	1%
Construction	1%
Autres secteurs	1%

Type d'entreprises participantes	2011
Cotées en bourse	51%
Secteur privé	36%
Gouvernement et secteur public	10%
Autres	3%

Taille des entreprises participantes	2011
Jusqu'à 200 employés	32%
De 201 à 1.000 employés	29%
Plus de 1.000 employés	38%
Ne sait pas	1%

Fonction occupée par les participants à notre enquête	2011
Direction générale et financière	46%
Audit interne	16%
Gestion des risques	6%
Conformité et contrôle	5%
Département de sécurité	4%
Département juridique	4%
Systèmes d'information	4%
Conseiller / consultant	3%
Opérations et production	3%
Marketing	2%
Ressources humaines	1%
Fiscalité	1%
Service clients	1%
Recherche et développement	1%
Achats	1%
Autres	2%

Quelques définitions

- **Fraude :** acte intentionnel réalisé par un salarié (fraude interne) ou un tiers (fraude externe) de manière à retirer un avantage généralement financier selon un procédé illicite.

- **Détournement d'actifs :** transfert illégal d'un bien du patrimoine de l'entreprise à celui d'un salarié, d'un tiers ou d'une autre entreprise.

- **Fraude comptable :** manipulation intentionnelle des comptes dans le but d'en donner une image plus flatteuse. Ne procure pas nécessairement au fraudeur un gain financier personnel.

- **Corruption :** acte d'offrir, donner, recevoir ou solliciter quelque chose de valeur pour influencer une décision ou obtenir un avantage généralement financier.

- **Cybercriminalité :** également appelée criminalité informatique, consiste en la réalisation de délits commis à l'aide d'équipements informatiques et d'Internet. Parmi les exemples classiques de cybercriminalité, il est possible de citer la diffusion de virus informatiques, le téléchargement illégal, les actes de phishing, le vol d'informations personnelles telles que des données bancaires.
  Cette définition exclue les cas de fraude plus classiques où le fraudeur s'appuie sur un ordinateur ou tout autre équipement électronique pour commettre son acte sans que cela constitue l'élément principal du schéma de fraude.

Litiges et Investigations. Une offre de services complète de PwC

Le département Litiges et Investigations de PwC France, créé en 1999, est intégré au sein d'un réseau mondial de 1.500 experts, dont 570 en Europe. Ses interventions consistent à évaluer les impacts financiers de situations de crise et à accompagner ses clients dans la mise en œuvre de solutions permettant de limiter leurs risques de pertes. La gestion des litiges, y compris pour faire suite à une transaction, les investigations comptables, financières et technologiques ainsi que l'assistance à la gestion des sinistres sont les différents domaines d'expertise du département Litiges et Investigations.

Gestion des litiges

- Accompagnement de l'entreprise, en collaboration avec ses avocats, dans l'évaluation des impacts financiers du litige, dans l'analyse des problématiques comptables et financières, dans la définition de la stratégie à adopter d'un point de vue financier et dans l'identification des documents clés devant être sauvegardés pour être produits.

- Participation au débat contradictoire et/ou témoignage dans le cadre de procédures amiables, contentieuses et arbitrages.

Litiges post-acquisition

- Assistance de l'entreprise lors de la revue des états financiers définitifs utilisés pour la détermination du prix de cession définitif, élaboration ou revue critique d'avis d'objections et mise en place d'un suivi documenté d'une garantie de passif et de sa mise en jeu.

- Intervention en qualité d'expert indépendant ou d'expert auprès d'une des parties.

Investigations/Investigations technologiques

- Recherches et mise en évidence d'irrégularités pouvant avoir été commises au sein d'une société.

- Reconstitution des schémas d'opérations frauduleuses, collecte des preuves en vue d'éventuelles poursuites judiciaires et évaluation des incidences financières.

- Extraction des données numériques en respectant les procédures légales et récupération des données effacées, corrompues ou protégées.

- Analyse et conseil dans le cadre de programmes de prévention du risque de fraude y compris l'identification des vulnérabilités existantes et exploitables au sein d'un système d'information.

Assistance à la gestion de sinistres

Détermination, évaluation et suivi des demandes d'indemnisation auprès d'un assureur, réassureur ou captive, suite à une analyse détaillée de la couverture offerte par la police d'assurance, ainsi que de la nature et des circonstances exactes du sinistre.

Les informations contenues dans le présent document ont un objet exclusivement général et ne peuvent en aucun cas être utilisées comme un substitut à une consultation rendue par un professionnel. En tout état de cause, en aucun cas la responsabilité de PricewaterhouseCoopers Advisory et/ ou de l'une quelconque des entités membres du réseau PwC ne pourra être engagée du fait ou à la suite d'une décision prise sur la base des informations contenues dans le présent document. © PricewaterhouseCoopers Advisory 2011. Tous droits réservés.

Contacts

Litiges et Investigations

Dominique Perrier
01 56 57 80 17
dominique.perrier@fr.pwc.com

Jean-Louis Di Giovanni
01 56 57 12 57
jean-louis.di.giovanni@fr.pwc.com