Grant Thornton

L'instinct de la croissance™

2ème ÉDITION / MARS 2017

Baromètre sur les pratiques des entreprises en matière de

LUTTE CONTRE LA FRAUDE ET LA CORRUPTION

SOMMAIRE

EXECUTIVE **SUMMARY**

Nous l'avions déjà constaté lors de la première édition de notre baromètre en 2015, mais les résultats de la version 2017 de notre étude confirment les tendances : **plus des trois quarts des entreprises interrogées déclarent avoir subi une tentative de fraude au cours des deux dernières années !**

Le constat est édifiant : ce phénomène touche toutes les entreprises, de toutes tailles et dans tous les secteurs d'activité. Pourtant la prise de conscience s'est accentuée au cours des deux dernières années, favorisée par le renforcement permanent de l'arsenal législatif, la judiciarisation croissante-pouvant conduire à la mise en cause personnelle de dirigeants- et les conséquences croissantes en termes d'image et de réputation.

Si la fraude peut revêtir des formes très diverses, **le détournement d'actifs constitue le scénario de fraude le plus couramment subi par les entreprises**, loin devant la désormais célèbre " fraude au Président " qui arrive au second rang de notre classement.

Alors que la première édition de notre baromètre visait à faire le point sur les organisations et pratiques des entreprises en matière de lutte contre la fraude, nous avons souhaité pour cette édition **réaliser un panorama des 10 scénarios de fraude les plus courants**. Il s'agit ainsi d'évaluer le niveau d'exposition des entreprises, les cas avérés mais également leur niveau de maîtrise du risque. Chacun de ces risques fait l'objet d'une fiche de synthèse, assortie de points clés en matière de vigilance.

Un premier constat, assez alarmant, s'impose : **dans presque 40 % des cas, les entreprises déclarent ne pas se sentir prêtes à faire face à des scénarios de fraudes auxquels elles considèrent pourtant être fortement exposées.**

Les enjeux financiers pour les entreprises sont significatifs : **13 % des cas de fraudes avérées ont des conséquences financières d'un montant supérieur à 1 million d'euros !**

Dans le cadre de notre panorama, plusieurs situations se dégagent.

Certains scénarios potentiels, bien que considérés comme de véritables menaces, sont déclarés comme maîtrisés.

D'autres *scénarios* correspondent à des risques comportant une forte dimension réglementaire qui a déjà amené les entreprises à travailler pour se mettre en conformité avec les exigences légales, *a minima*. Ces risques restent pour autant une véritable préoccupation pour les entreprises : toute défaillance les exposerait non seulement aux sanctions prévues par la loi, mais aurait également des conséquences lourdes en matière d'image et de réputation.

Quatre risques restent pour autant des chantiers ouverts pour les entreprises, qui considèrent ne pas les maîtriser suffisamment : **les détournements d'actifs**, **la corruption, la *cyber*criminalité** et peut-être moins envisagé, **la fraude au technicien**. Les dirigeants doivent donc poursuivre leurs efforts pour structurer et renforcer leur dispositif de lutte et prévention contre la fraude : ces efforts se feront sans doute sans ressources supplémentaires, le renforcement des équipes affectées à la lutte contre la fraude ne faisant définitivement pas partie des priorités identifiées.

Sur le plan international, nous constatons que la fraude est également un sujet de préoccupation pour les entreprises et que les scénarios de fraude que nous pouvions imaginer dépendre de la culture des pays (comme la fraude au Président) sont pourtant évalués comme représentant un niveau de risque important.

Cette injonction paradoxale peut constituer une clé de lecture pour les **actions envisagées** de manière prioritaire ; les entreprises visent désormais **à rationaliser et optimiser le dispositif plus qu'à le construire et le développer.**

La poursuite de la transformation de la culture d'entreprise

Le renforcement de la prévention et la réalisation d'actions de sensibilisation constituent les deux principales actions envisagées par les entreprises à court terme. Elles sont indispensables à la montée en puissance des équipes opérationnelles, pour devenir une première ligne de défense efficace contre le risque de fraude.

Le renforcement des mesures de surveillance

Ce renforcement passe tant par la mise en place de contrôles, que par le renforcement de *reporting* efficaces et de solutions de *data analytics*. De manière plus modérée qu'il y a deux ans en tout état de cause, ce qui peut traduire les investissements déjà réalisés et la montée en puissance des entreprises dans ce domaine, en termes d'automatisation et d'industrialisation des contrôles.

La revue de l'approche par les risques

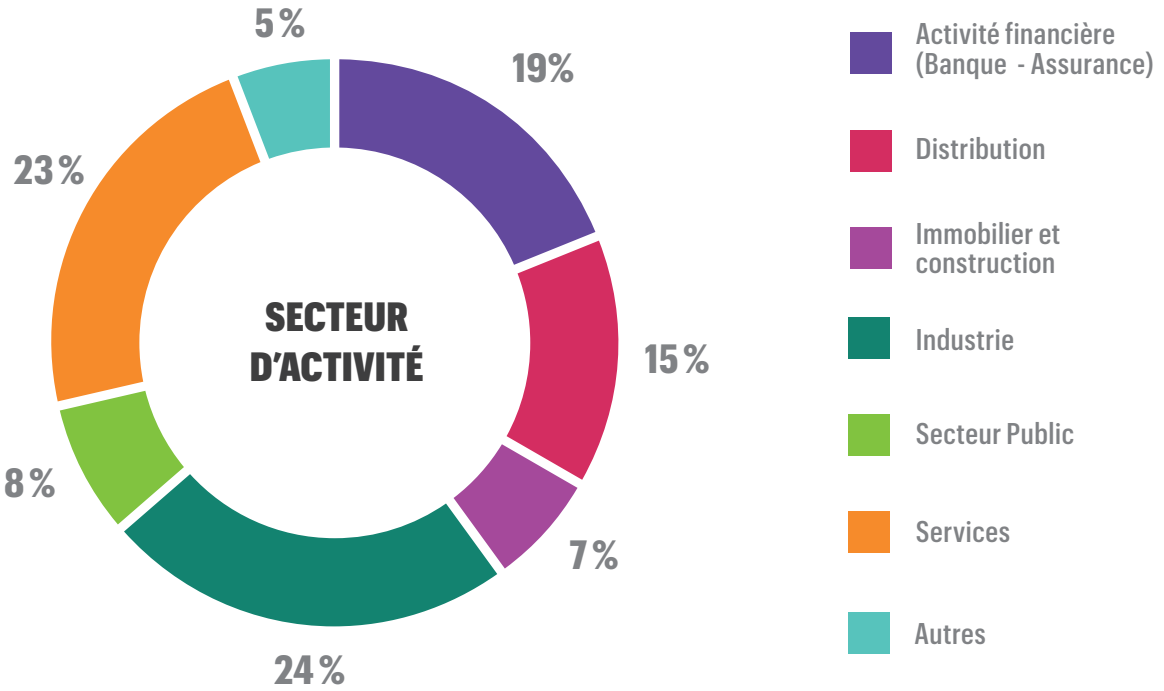
Ce dernier thème ne constituait pas une priorité majeure pour les entreprises en 2015 alors qu'il représente indéniablement le fondement de toute démarche structurée de lutte contre la fraude, en permettant de se focaliser sur les scénarios véritablement prioritaires. En 2017, ce thème prend une importance considérable et se positionne désormais en 4ème position.

MÉTHODOLOGIE **ET STRUCTURE DE L'ÉCHANTILLON**

Cette étude a été réalisée par Grant Thornton auprès d'un échantillon de 1 900 personnes, selon la méthode d'un questionnaire à choix multiples.

L'échantillon dans le présent sondage est diversifié tant en termes de secteur d'activité des entreprises que de taille. Toutefois, la répartition entre les secteurs est plus homogène que lors de la 1ère édition, au sein de laquelle le secteur financier était fortement représenté (36 % en 2015 contre 19 % en 2017).

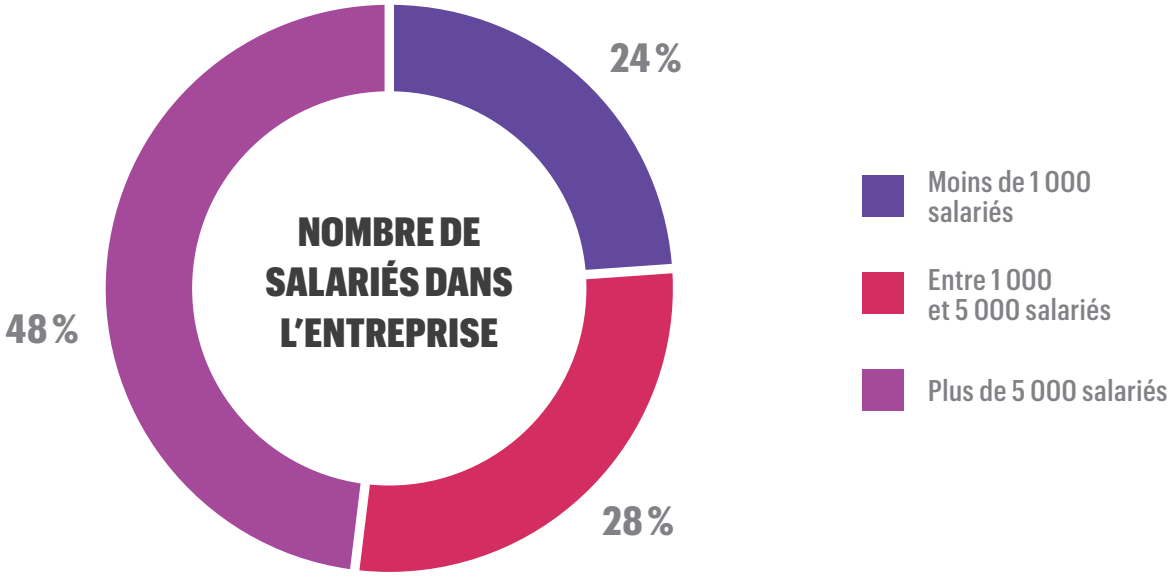
Enfin, le secteur " Immobilier et Construction " ainsi que le secteur " Public " restent les deux secteurs d'activité les moins représentés comme cela était déjà le cas il y a deux ans.



Grant Thornton
L'instinct de la croissance™

MÉTHODOLOGIE **ET STRUCTURE DE L'ÉCHANTILLON**

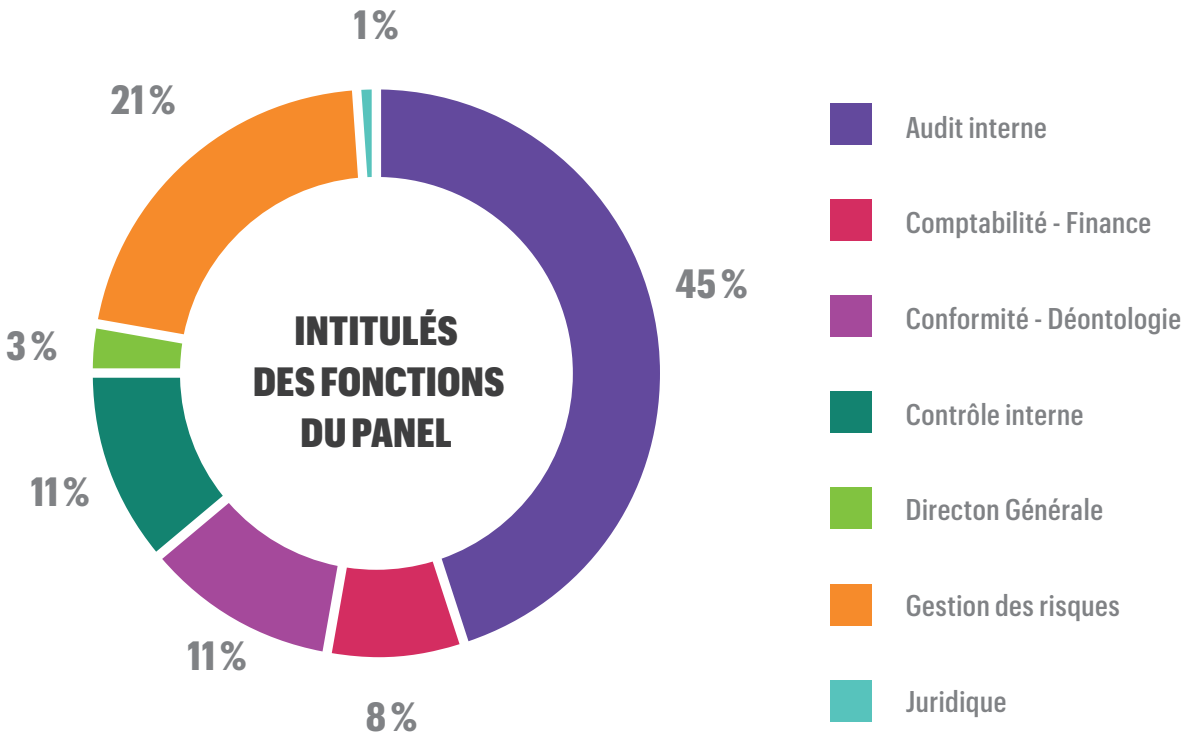
Toutes les tailles d'entreprises sont représentées dans notre panel, avec une prépondérance des entreprises de plus de 5 000 salariés.



MÉTHODOLOGIE **ET STRUCTURE DE L'ÉCHANTILLON**

Tout comme en 2015, le panel des sondés est constitué majoritairement de professionnels des fonctions audit interne et gestion des risques. Toutefois, l'on voit émerger les fonctions Conformité-Déontologie et Juridique comme " acteur " en charge du sujet de la fraude.

Paradoxalement, la fonction " Secrétaire général " ne ressort pas, alors que ce profil est un interlocuteur de plus en plus prépondérant lors de nos missions en matière de prévention et lutte contre la fraude, notamment en matière de corruption.



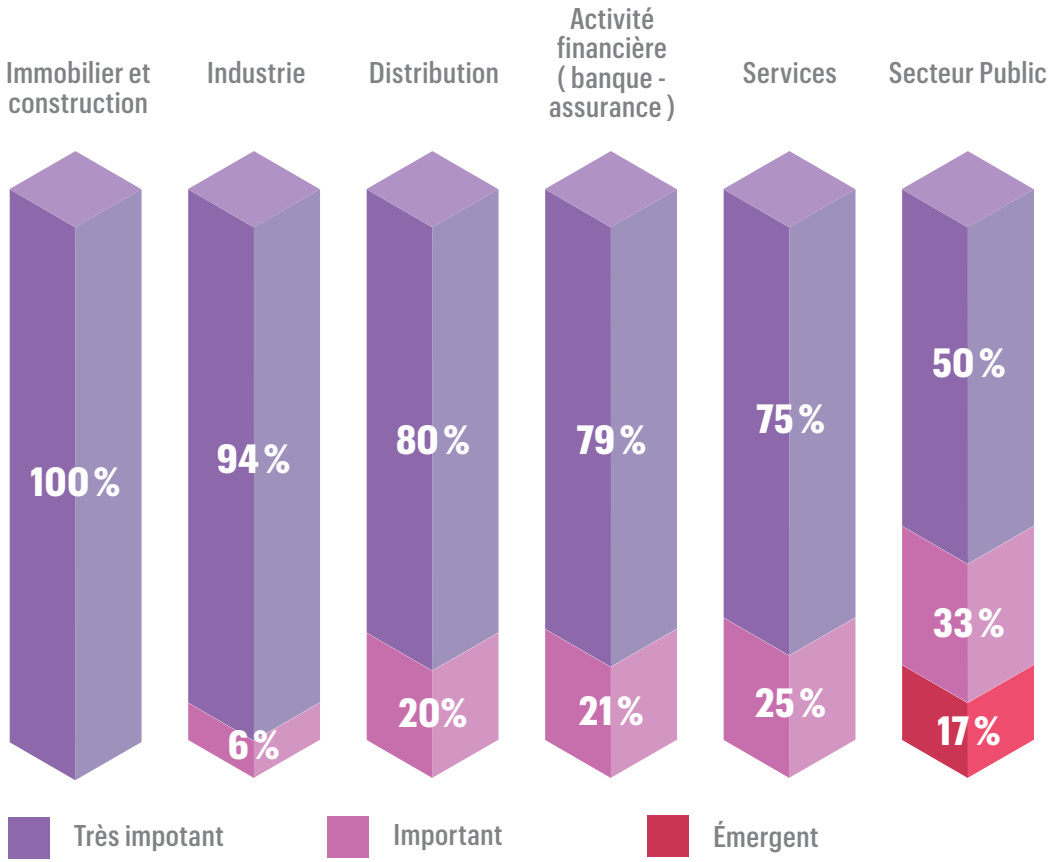
LA GESTION **DU RISQUE DE FRAUDE**

L'importance de la lutte contre la fraude

Le sujet de la lutte contre la fraude constitue **un enjeu jugé important ou très important pour 99 % des répondants**, contre un peu plus de 85 % lors de la 1ère édition de notre baromètre. Ce chiffre est en nette progression et traduit bien la prise de conscience des entreprises de l'importance de déployer un dispositif de prévention et de lutte. La disparition de la réponse " importance secondaire ", mentionnée lors du premier volet, illustre également cette tendance.

Cette **prise de conscience** repose sur **un tryptique** combinant **conformité réglementaire, responsabilité des dirigeants et protection de la réputation et de l'image de l'entreprise,** et s'explique en effet nécessairement par le renforcement régulier de l'arsenal législatif en matière de lutte contre la fraude. Au cours des derniers mois, la France a adopté la loi Sapin 2 qui comporte un volet anti-corruption particulièrement important et plus récemment la loi portant sur le devoir de vigilance des donneurs d'ordres vis-à-vis de leurs sous-traitants en matière d'éthique. La multiplication de ces textes renforce logiquement la sensibilité des entreprises en la matière.

Elle s'explique également par **la mise en cause de la responsabilité des dirigeants dans plusieurs dossiers suite à des cas de fraudes avérées** qui auraient pu, selon les plaignants, être évitées avec la mise en place d'un dispositif adapté.
Enfin, les scandales générés par des cas de fraude de grande envergure révélés dans les médias, incitent également fortement les entreprises à protéger leur image et leur réputation.
Pour autant, il reste toujours des cas isolés d'entreprises considérant encore la gestion du risque de fraude comme émergent. Cela peut s'expliquer par une culture d'entreprise globalement peu sensible aux sujets d'éthique, de conformité et de lutte contre la fraude.



L'IMPORTANCE DE LA LUTTE CONTRE LA FRAUDE

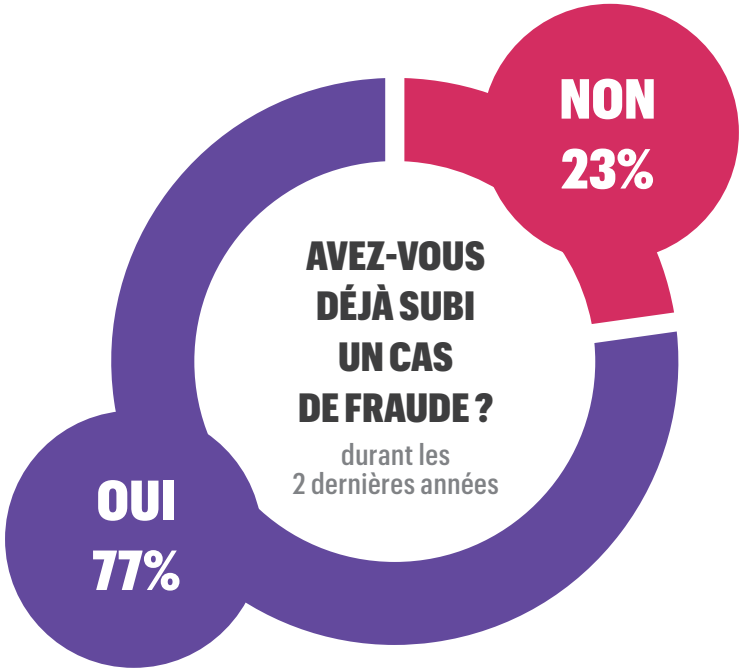
Tout comme lors de notre premier baromètre en 2015, le secteur public reste " décroché " des autres en termes d'importance accordée. Pour les autres secteurs, il est intéressant de noter une convergence progressive vers le " très important ".

LA GESTION **DU RISQUE DE FRAUDE**

Les cas de fraude avérées

Plus des trois quarts des entreprises déclarent **avoir subi un cas de fraude, tout comme à l'époque dans notre précédente analyse**. Toutefois si cette proportion est stable, il convient de noter qu'elle **porte sur les 2 dernières années** au lieu des cinq dernières années, comme indiqué dans l'enquête de 2015.

La fraude est donc plus que jamais une réalité. Le rythme des tentatives (y compris malheureusement celles couronnées de succès) ne semble pas faiblir, bien au contraire.

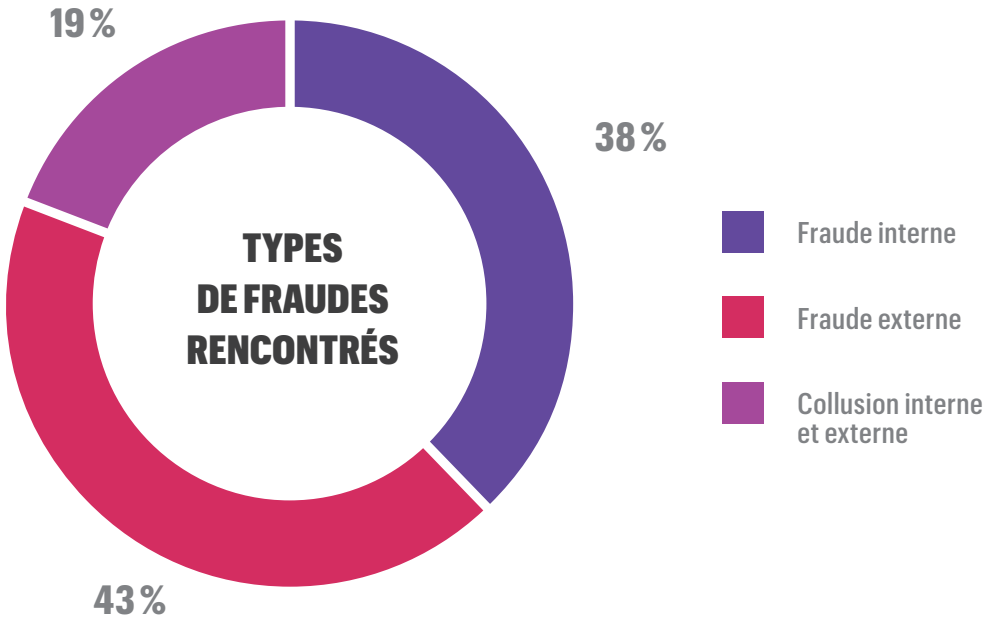


LA GESTION **DU RISQUE DE FRAUDE**

De même, et en ligne par rapport au résultat de la 1ère édition, plus **de la moitié de ces cas de fraudes subies ont impliqué,** de manière exclusive ou partielle, les collaborateurs de l'entreprise. Il est également possible de constater **une légère hausse des cas de détection de fraude interne.**

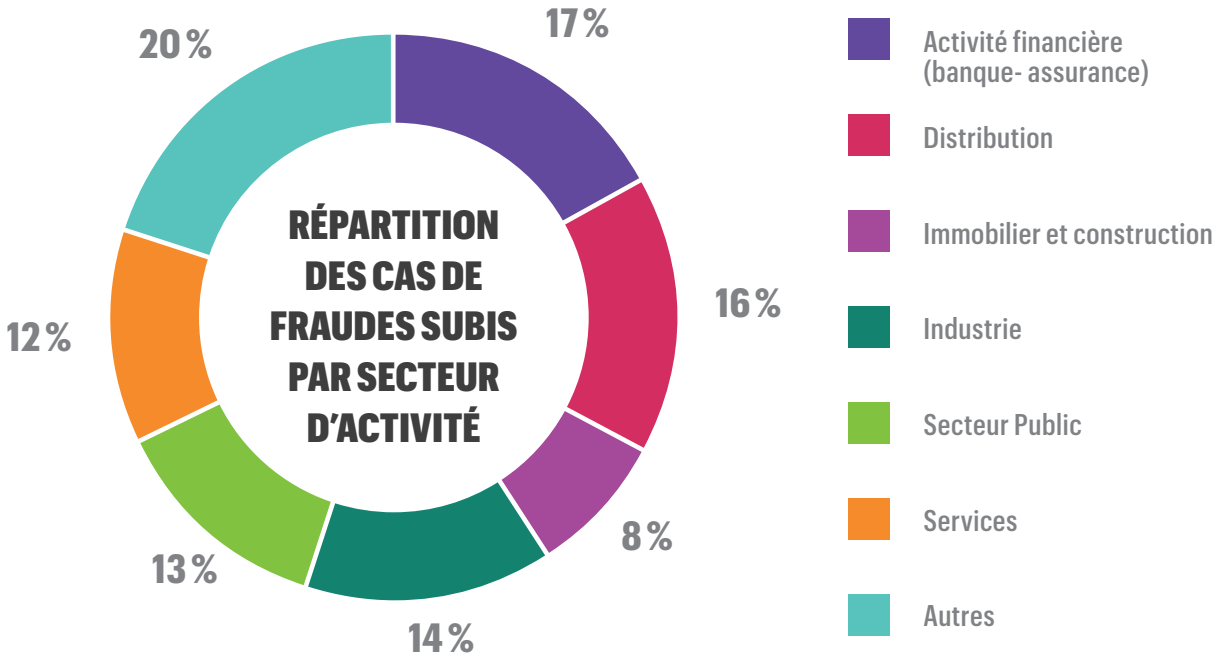
Cette dernière ne traduit pas nécessairement une augmentation des pratiques frauduleuses par les collaborateurs des entreprises mais peut être simplement, en lien direct avec le niveau de sensibilisation qui se renforce, le fait que la fraude interne ne soit plus autant un sujet tabou au cœur des entreprises que par le passé.

Cela peut également traduire le fait que la fraude soit mieux recherchée et contrôlée par les entreprises.



LA GESTION **DU RISQUE DE FRAUDE**

En termes de secteur d'activité, et au regard de la composition de notre panel, nous constatons que les secteurs de l'industrie et des services concentrent proportionnellement moins de cas de fraudes que leur poids proportionnel dans le panel (à titre d'exemple, 12% des cas de fraude pour les services alors qu'ils représentent 23% du panel, 14% et 24% pour l'industrie).
A l'inverse, le Secteur Public est sur-représenté pour ce qui concerne les cas de fraudes avérées, tout comme le secteur libellé en tant que " autres " (dont notamment les associations). Ce résultat est sans nul doute à rapprocher du niveau d'importance accordé à la fraude par ce secteur.

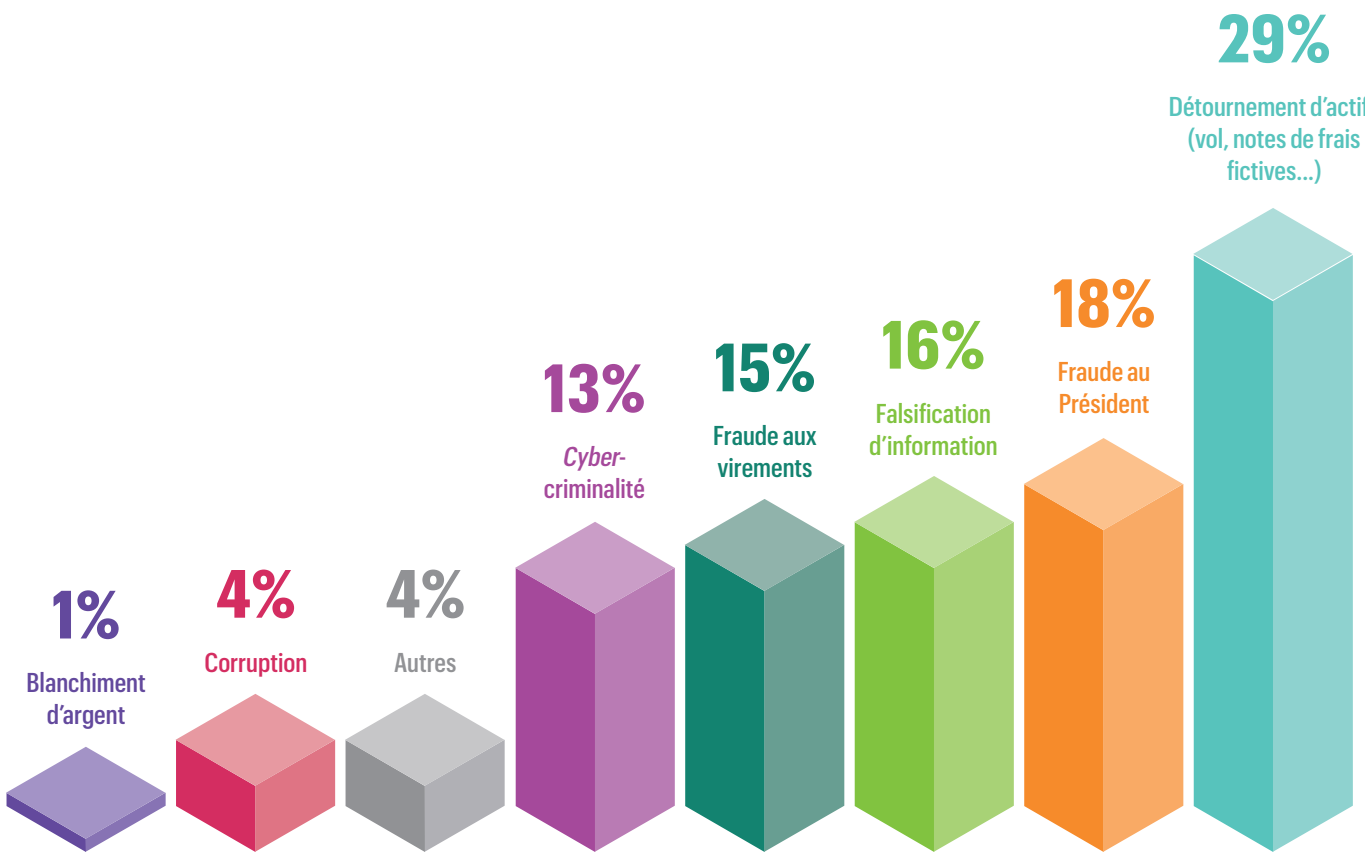


LA GESTION **DU RISQUE DE FRAUDE**

Les typologies de fraude subies sont variées. Toutefois le détournement d'actifs demeure le scénario majoritairement avéré au sein des entreprises. **En effet, 29 % des cas de fraude concernent un tel détournement** et il semble que les entreprises aient mis en œuvre des contrôles permettant de mieux les détecter (*data analytics* ou contrôles humains).
À *contrario*, la corruption et le blanchiment restent les cas de fraude avérées les plus faibles. Cela se justifie notamment par la difficulté qu'ont les entreprises à les détecter, les contrôles industrialisés n'étant pas les vecteurs les plus adaptés pour ces deux typologies.

" Décrochés ", **de plus de 10 points,** nous retrouvons les scénarios " à la mode " : - La fraude au Président,
- La fraude aux virements,
- La falsification d'informations,
- La *cyber*criminalité.

L'on pourrait penser que le caractère populaire et médiatique de ces scénarios aurait pu conduire les entreprises à s'en protéger. Il ressort de nos résultats qu'il n'en est rien et que lorsqu'ils sont mis en œuvre par des équipes expérimentées, ces types de tentatives arrivent encore aisément à passer entre les mailles du filet.
Dans la catégorie " autres " nous retrouvons des cas avérés autour **du favoritisme, de la collusion et de la fraude à l'assurance ou encore la fraude aux " cartes cadeaux "**.



LA GESTION **DU RISQUE DE FRAUDE**

À travers cette étude, nous avons également cherché à obtenir des éléments de **quantification du risque de fraude**, qui constituaient un domaine peu exploré par les entreprises lors de notre premier baromètre.

Ainsi, nous constatons que le préjudice financier associé aux cas de fraudes avérées reste significatif puisque **13 % des entreprises ayant subi une attaque déclarent un préjudice financier supérieur à 1 million d'euros.**

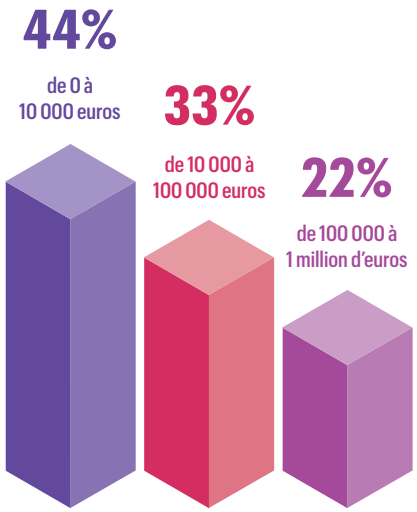
Si l'on se souvient que 75 % des entreprises de notre panel ont subi un cas de fraude au cours des deux dernières années, la tentation est forte de conclure que **9 % d'entre elles pourraient subir une fraude de plus de 1 million d'euros au cours des deux prochaines années.**

Sous un autre angle, nous avons cherché à approcher la valeur économique du risque de fraude sur la base des éléments transmis par les répondants.

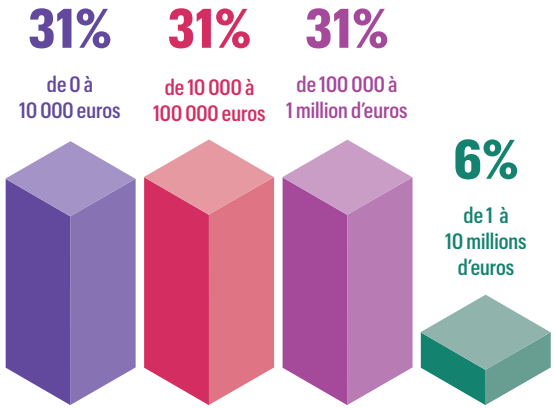
La *value at risk* à 99,5 % fait ressortir un montant de plus de 16 millions d'euros, tous *scénarios* confondus : cela positionne clairement le niveau d'enjeu pour les entreprises.

Nous pouvons constater que le préjudice financier maximum déclaré par les plus petites entreprises ne dépasse pas le million d'euros. Seules les entreprises de plus 5 000 salariés sont concernées par des préjudices financiers de plus de 10 millions .

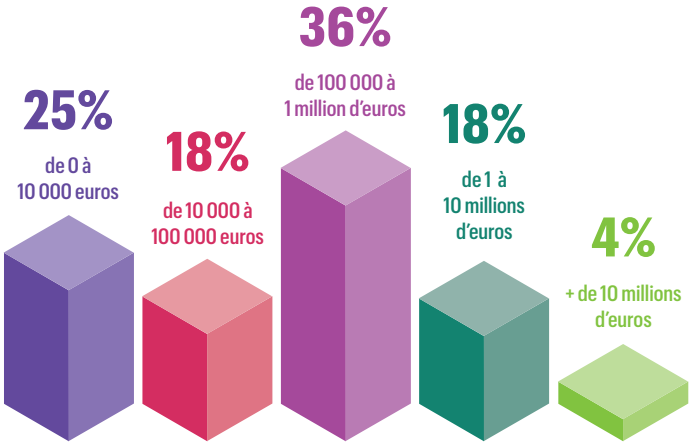
Il est intéressant de noter que **22 % des cas de fraudes subies par ces grandes entreprises équivalent à un montant supérieur à 1 million d'euros.**



MOINS DE 1 000 SALARIÉS



DE 1 000 À 5 000 SALARIÉS



PLUS DE 5 000 SALARIÉS

Grant Thornton
L'instinct de la croissance™

LA GESTION **DU RISQUE DE FRAUDE**

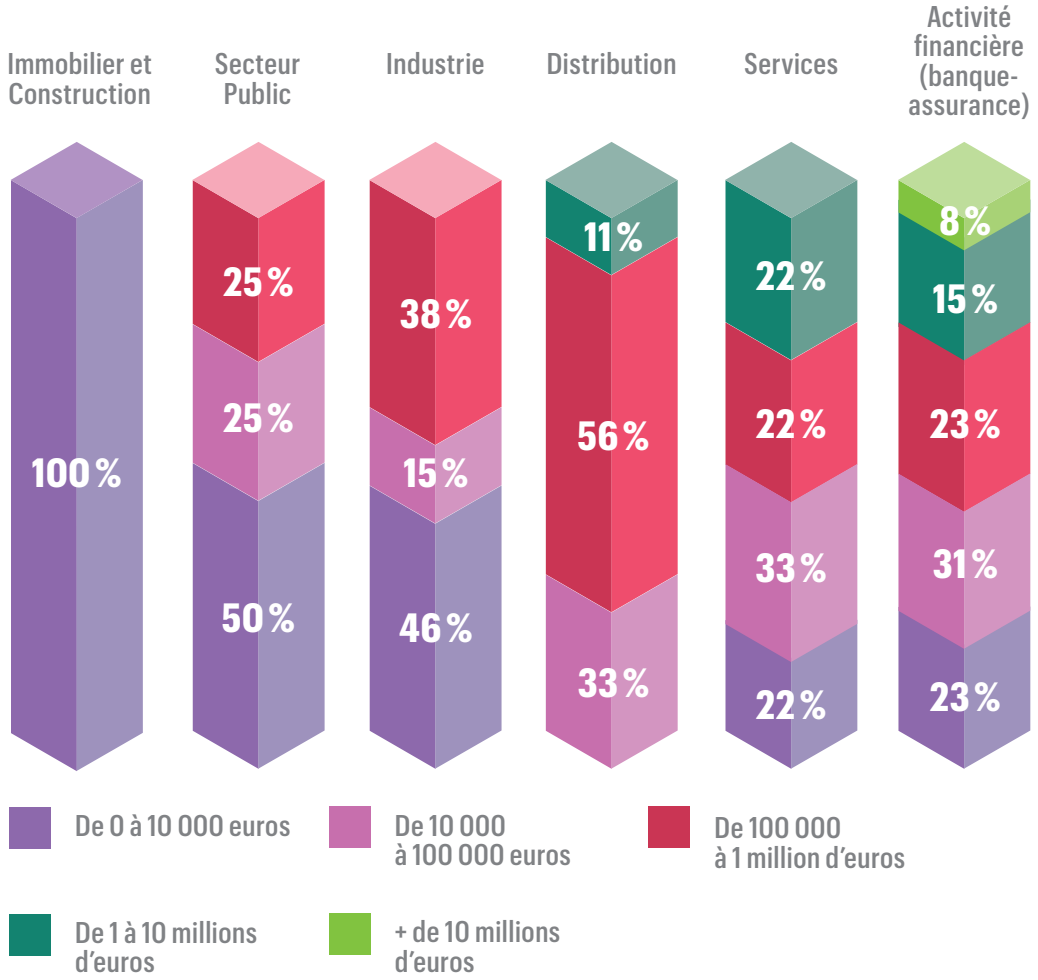
L'analyse du montant des préjudices avérés par secteurs amène plusieurs commentaires de notre part :

- Le secteur financier semble exposé à toute l'ampleur possible des conséquences des scénarios de fraude, ce qui s'explique certainement tant par la nature même de leur activité que par la maturité de leurs dispositifs de lutte, très encadrés réglementairement parlant.

- Le secteur de la distribution ne déclare aucun cas de fraude avérée d'un montant de moins de 10 000 euros, ce qui montre clairement que la démarque n'est plus considérée comme de la fraude mais assimilée pleinement au modèle économique de ces acteurs.

- Le secteur de l'industrie, tout comme le secteur Public, n'ont pas déclaré de cas supérieur à 1 million d'euros, ce qui peut s'expliquer notamment par les systèmes de contrôle et de règles d'engagement et paiement ; cela peut paraître plus surprenant dans le secteur de l'Industrie, notamment au regard de certains cas récemment rendus publics.

- Le nombre de cas signalés pour le secteur de l'Immobilier et de la Construction ne nous permet pas d'apporter de commentaires.



PANORAMA **DE LA FRAUDE**

Méthodologie

Pour ce panorama, nous avons souhaité réaliser un focus **sur 10 risques prioritaires en raison de leur notoriété dans les médias** mais également au regard **des cas avérés que nous instruisons pour le compte de nos clients :**

1 : Fraude au Président,
2 : Fraude aux faux virements,
3 : Fraude au technicien,
4 : *Cyber*criminalité,
5 : Corruption,
6 : Financement du terrorisme,
7 : Comportement non éthique,
8 : Contournement d'embargo,
9 : Falsification d'informations,
10 : Détournement d'actifs.

Pour chacun de ces risques, les entreprises ayant accepté de participer à notre étude ont été invitées à se prononcer sur leur **niveau d'exposition au scénario, le fait d'en avoir été victime ou pas, les conséquences concrètes pour elles et enfin leur niveau de confiance sur leur capacité à y faire face.**

Chacun de ces cas est présenté de manière individuelle au travers d'une fiche de synthèse dans la suite de l'étude.

PANORAMA **DE LA FRAUDE**

Vision globale

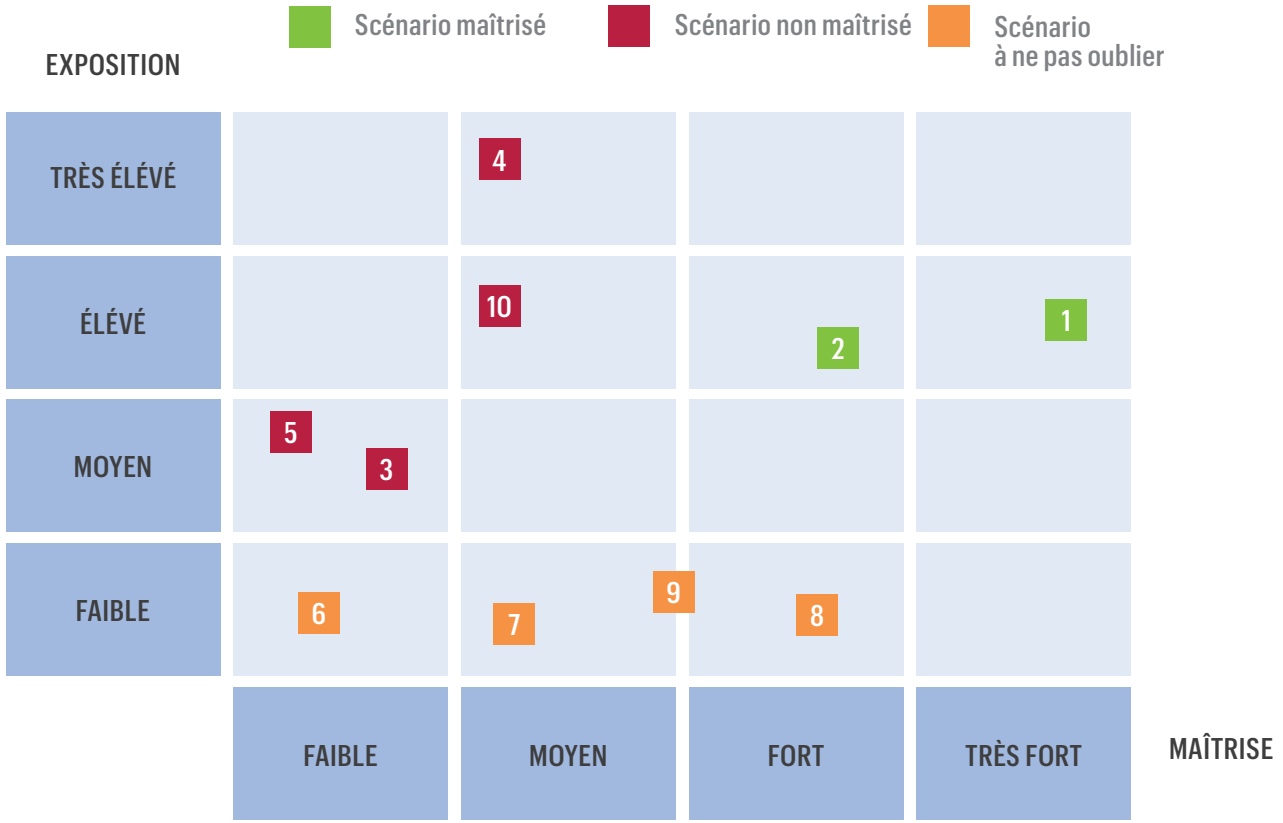
L'analyse des informations collectées lors de l'étude nous a permis de réaliser une cartographie globale des 10 risques de fraude couverts par les scénarios.

Cette cartographie recoupe le niveau d'exposition au risque par les entreprises face au niveau de maîtrise ressenti.

Avant de rentrer dans une analyse par scénario, un chiffre spécifique attire considérablement l'attention : pour **28 % des scénarios évalués** (tous niveaux d'exposition confondus), **les répondants** déclarent que leur entreprise n'est pas réellement prête à faire face. Lorsque l'on s'attache **aux scénarios de fraude auxquels les entreprises sont fortement exposées, ce chiffre monte jusqu'à 39 % des cas !**

Très classiquement, cette cartographie permet de faire émerger 3 types de situations, appelant chacune des stratégies différentes de gestion du risque.

PANORAMA GLOBAL



1 : Fraude au Président,
2 : Fraude aux faux virements,
3 : Fraude au technicien,
4 : *Cyber*criminalité,
5 : Corruption,
6 : Financement du terrorisme,
7 : Comportement non éthique,
8 : Contournement d'embargo,
9 : Falsification d'informations,
10 : Détournement d'actifs.

PANORAMA **DE LA FRAUDE**

Situation 1 – Scénario maîtrisé

Parmi les 10 scénarios soumis à l'analyse des répondants, **la fraude au Président et la fraude aux faux virements** ressortent comme parmi **les plus dangereuses pour les entreprises, mais également comme les mieux appréhendées par ces dernières.**

L'attention portée par les médias à ces situations combinée pour le second scénario aux efforts de sensibilisation des établissements financiers, expliquent pour une partie ces résultats.
Les entreprises ont aujourd'hui une compréhension très claire des mécanismes déployés par les fraudeurs et ont identifié les situations adaptées à mettre en œuvre, même si pour le deuxième cas des solutions plus industrielles sont en cours de mise au point.

Pour autant, **25 % des tentatives dans le cadre de ces deux scénarios restent couronnées de succès selon les déclarations de notre panel**. Il convient donc de maintenir une vigilance sans failles sur ces risques en réalisant régulièrement des actions de sensibilisation et en évaluant périodiquement la réalité et l'efficacité des actions de maîtrise en place.

Situation 2 – Scénario non maîtrisé

Ces **4 *scénarios*** devraient faire **l'objet d'analyses détaillées pour comprendre les modalités de survenance du risque et bâtir le plan d'actions** associé pour travailler sur l'ensemble des dimensions (tant en prévention qu'en moyens de détection).

Il existe un très fort décalage entre le positionnement du risque de corruption sur cette cartographie et les déclarations de fraudes avérées, réalisées par les entreprises. Il y a vraisemblablement un biais de perception lié à la promulgation de la loi Sapin 2 en décembre dernier, qui met inévitablement un accent sur cette typologie de risque jusque-là peu appréhendée par les entreprises. Pour mémoire, lors de notre précédent baromètre, seules 36 % des entreprises déclaraient être préoccupées par ce type de risque de fraude.

De manière plus préoccupante encore, alors que la ***cyber*criminalité et les détournements d'actifs** étaient déjà identifiés il y a deux ans comme faisant partie des **3 premières préoccupations des entreprises,** nous constatons, deux ans plus tard que **celles-ci ne se sentent toujours pas suffisamment armées pour y faire face**.

Situation 3 – Scénarios à ne pas oublier

Les scénarios tels que le financement du terrorisme, les comportements non éthiques et la falsification d'informations ressortent avec un niveau d'exposition " faible " et une maîtrise déclarée comme " faible " ou " moyenne " .

Cela pourrait laisser penser que ces situations ne font globalement pas partie des préoccupations premières des entreprises. Néanmoins, il n'est pas possible de conclure aussi rapidement.

En effet, à la différence des autres scénarios qui aboutissent principalement à des conséquences financières, les cas évoqués entrainent des conséquences pouvant avoir des effets beaucoup plus dévastateurs sur l'opinion publique et sur l'image de l'entreprise.

Le niveau d'aversion au risque de la société dans son ensemble, sur les deux premiers sujets, est aujourd'hui total. Les conséquences d'une falsification d'information, notamment pour les sociétés cotées peuvent également être dévastatrices.

De plus, ces sujets sont tous encadrés réglementairement et emportent des possibilités de sanctions importantes. Par voie de conséquence, la survenance de ces risques est très difficilement acceptable pour toute entreprise.

Le niveau d'exposition déclaré par les entreprises nous semble ainsi prendre davantage en compte la probabilité de survenance que les conséquences du risque lui-même, et semble, de ce fait, peut être sous-estimé.

En matière de maîtrise du risque, la prise en compte et la gestion de ces scénarios exigent que l'entreprise mette en place une véritable culture éthique allant bien au-delà de la simple gestion du risque de fraude et de conformité.

Il s'agit ainsi de risques " extrêmes " qui appellent un fort volet de prévention mais également une réelle capacité de réaction, notamment en termes de gestion de crise, en cas de réelle survenance.

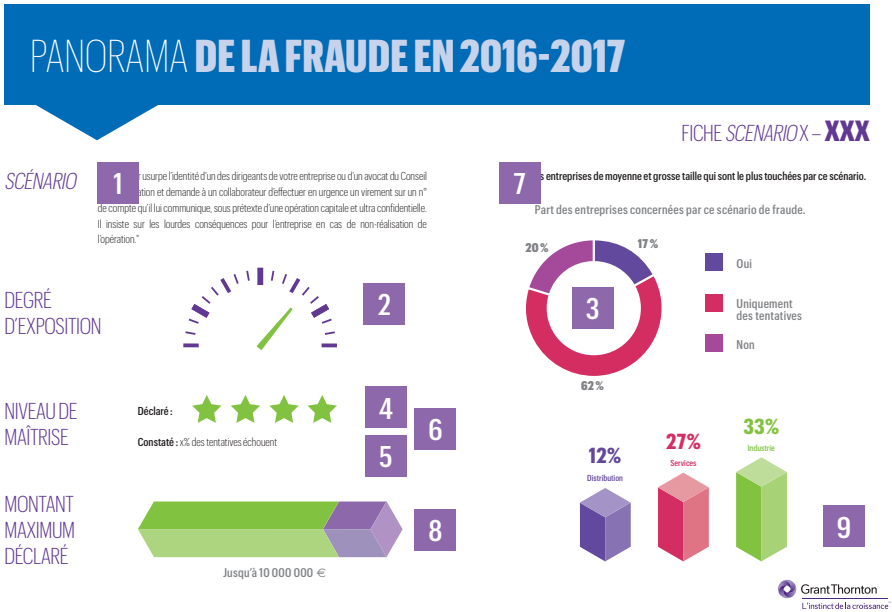
Concernant le risque d'embargo, le niveau d'exposition faible peut s'expliquer par le fait que la survenance du risque soit directement liée à la politique de l'entreprise mais aussi par le fait que le niveau d'aversion de la société civile semble plus faible que pour les trois autres. Il est important de rappeler que les conséquences financières et légales sont également extrêmement fortes, comme un certain nombre d'exemples récents ont pu le montrer.

PANORAMA **DE LA FRAUDE**

Fiche de synthèse par scénario

Nous avons établi une fiche de synthèse récapitulant l'ensemble des informations collectées lors de l'étude pour chaque scénario de fraude.

Grille de lecture



1. Description type du scénario.
2. Baromètre indiquant le niveau d'exposition global à ce scénario estimé par les répondants.
3. Répartition des entreprises concernées par ce scénario (cas avérés, tentatives ou non concernées).
4. Niveau de confiance général sur la capacité à faire face au scénario évalué, de 1 à 4 étoiles.
5. Taux d'échec de ce scénario de fraude (nombre de tentatives ratées / nombre de tentatives totales).
6. Contradiction notable entre le taux d'échec de ce scénario, de fraude et le niveau de maîtrise .
7. Taille des entreprises les plus concernées par ce scénario de fraude.
8. Montant maximum de préjudice subi déclaré.
9. Podium des secteurs les plus concernés par ce scénario de fraude.

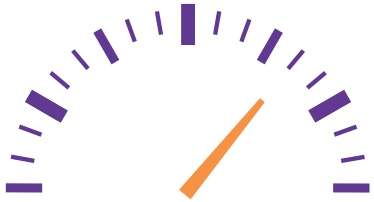
PANORAMA **DE LA FRAUDE**

FICHE SCENARIO 1 – **Fraude au Président**

SCÉNARIO

"Le fraudeur usurpe l'identité de l'un des dirigeants de votre entreprise ou d'un avocat du Conseil d'Administration et demande à un collaborateur d'effectuer en urgence un virement sur un numéro de compte qu'il lui communique, sous prétexte d'une opération capitale et ultra confidentielle.
Il insiste sur les lourdes conséquences pour l'entreprise en cas de non-réalisation de l'opération."

DEGRÉ D'EXPOSITION



NIVEAU DE MAÎTRISE

Déclaré : ★ ★ ★ ★

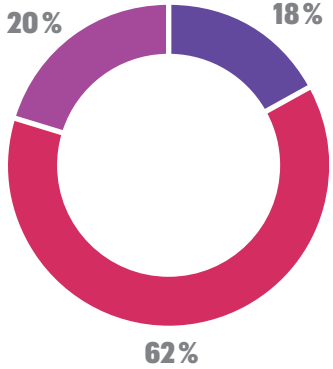
Constaté : 78 % des tentatives échouent

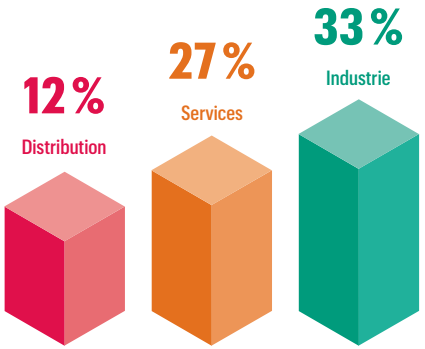
MONTANT MAXIMUM DÉCLARÉ

Jusqu'à 10 000 000 €

Ce sont les entreprises de moyenne et grande taille qui sont le plus touchées par ce scénario.

Part des entreprises concernées par ce scénario de fraude.





Oui — Uniquement des tentatives — Non

Points de vigilance :

- Sécuriser les processus de virement en ne laissant pas la possibilité à une seule personne de réaliser un virement et ce, même lors d'opérations confidentielles,
- S'assurer de l'authenticité de la personne qui est au bout du fil (ne pas déroger aux procédures même sous pression, faciliter le dialogue avec la hiérarchie...),
- Ne jamais communiquer d'informations confidentielles sur le fonctionnement de l'entreprise (exemple : information sur les noms des personnes habilitées à faire un virement, déroulé du processus...),
- Sensibiliser les équipes aux mécanismes d'ingénierie sociale.

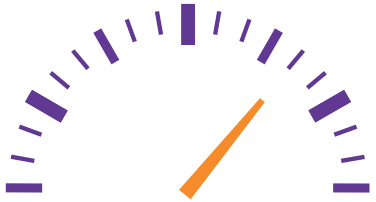
PANORAMA **DE LA FRAUDE**

FICHE SCENARIO 2 – **Fraude aux faux virements**

SCÉNARIO

"Le fraudeur usurpe l'identité d'un fournisseur de votre entreprise et contacte le service comptabilité pour lui indiquer la modification de ses coordonnées bancaires. Le comptable met à jour les coordonnées bancaires dans la fiche fournisseur. Les règlements fournisseurs seront dès lors dirigés vers ce compte."

DEGRÉ D'EXPOSITION



NIVEAU DE MAÎTRISE

Déclaré : ★ ★ ★

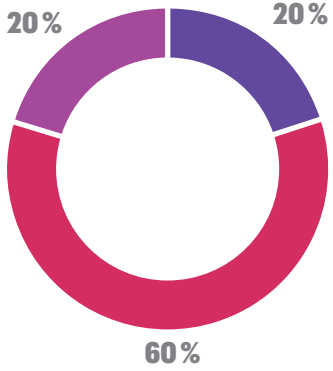
Constaté : 75 % des tentatives échouent

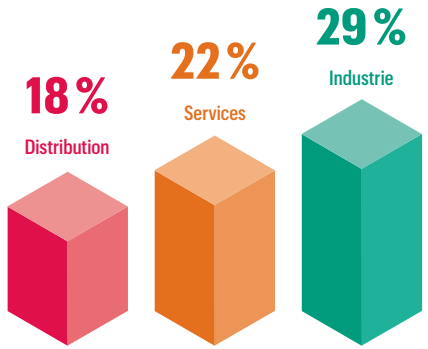
MONTANT MAXIMUM DÉCLARÉ

Jusqu'à 10 000 000 €

Ce sont les entreprises de plus grosse taille qui sont le plus touchées par ce scénario.

Part des entreprises concernées par ce scénario de fraude.





Oui | Uniquement des tentatives | Non

Points de vigilance :

- Disposer d'une base fournisseurs complète, avec des données de qualité :
  - Complétude des champs,
  - Traçabilité des demandes de changements (numéro de téléphone, fax, mail ou contact interlocuteur habituel),
- Circulariser systématiquement la demande de changement de coordonnées bancaires auprès de l'interlocuteur habituel du fournisseur,
- S'assurer de la véracité de la prestation réalisée,
- Ne jamais communiquer d'informations confidentielles sur le fonctionnement de l'entreprise (exemple : déroulé du processus).

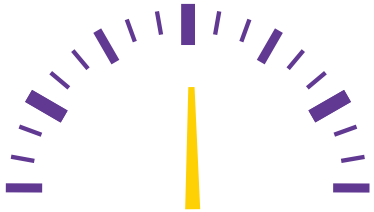
PANORAMA **DE LA FRAUDE**

FICHE SCENARIO 3 – **Fraude au technicien**

SCÉNARIO

"Le fraudeur usurpe l'identité d'un technicien informatique pour effectuer de faux tests sur les postes de services ayant des accès à des données sensibles, dans le but de récupérer des informations confidentielles, installer des logiciels malveillants, provoquer des virements frauduleux..."

DEGRÉ D'EXPOSITION



NIVEAU DE MAÎTRISE

Déclaré :

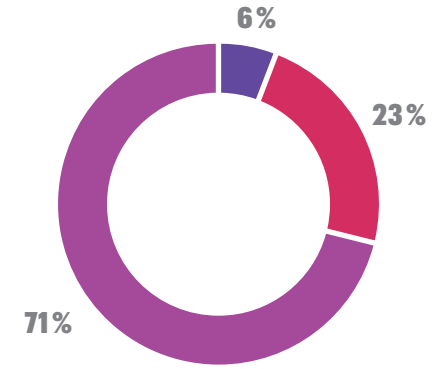
Constaté : 80 % des tentatives échouent

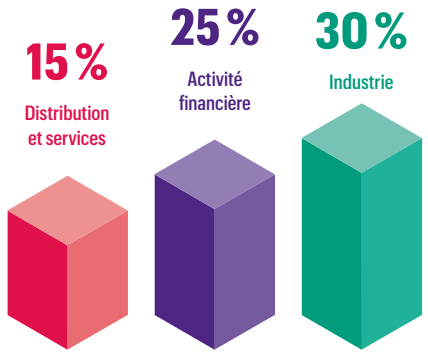
MONTANT MAXIMUM DÉCLARÉ

Jusqu'à 100 000 €

Ce sont les entreprises de plus grosse taille qui sont le plus touchées par ce scénario.

Part des entreprises concernées par ce scénario de fraude.





Oui | Uniquement des tentatives | Non

Points de vigilance :

- S'assurer de la réalité de l'intervention (notamment en interne, mais également auprès de l'établissement du prestataire),
- Ne jamais communiquer d'informations confidentielles sur le fonctionnement de l'entreprise (exemple : mots de passe et identifiants).

PANORAMA **DE LA FRAUDE**

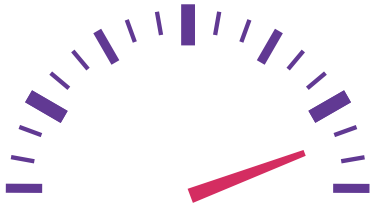
FICHE SCENARIO 4 – *Cybercriminalité*

SCÉNARIO

Malware – Spyware : Un collaborateur reçoit un *email* avec un lien ou une pièce jointe contenant un virus. Ce virus permet au fraudeur d'avoir accès ou connaissance de ce qui se passe sur l'ordinateur contaminé.

Mail-phishing : Un collaborateur reçoit un *email* provenant soit-disant de la banque de l'entreprise, lui demandant de mettre à jour certaines coordonnées sur l'entreprise, bancaires notamment. En cliquant sur le lien, le collaborateur est redirigé vers un formulaire de saisie conforme à la charte graphique habituelle de la banque.

DEGRÉ D'EXPOSITION



NIVEAU DE MAÎTRISE

Déclaré : 

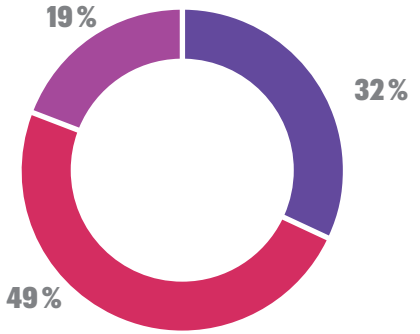
Constaté : 61 % des tentatives échouent

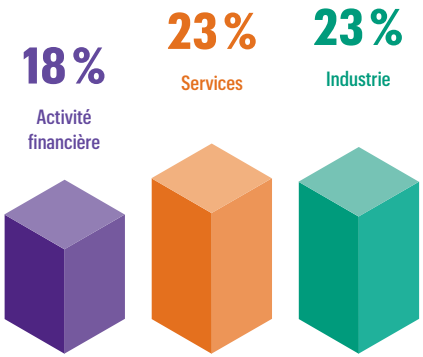
MONTANT MAXIMUM DÉCLARÉ

Supérieur à 10 000 000 €

Ce sont les entreprises de taille moyenne qui sont le plus touchées par ce scénario.

Part des entreprises concernées par ce scénario de fraude.





Oui — Uniquement des tentatives — Non

Points de vigilance :

- Mettre en place une politique de sécurité informatique et contrôler la bonne application de cette dernière,
- Rappeler régulièrement les règles à l'ensemble des collaborateurs,
- Faire tester la sécurité des systèmes d'information (tests d'intrusion).

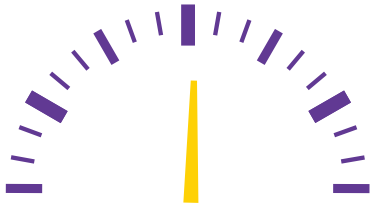
PANORAMA **DE LA FRAUDE**

FICHE SCENARIO 5 – **Corruption**

SCÉNARIO

"Un acheteur ou gestionnaire travaux de votre entreprise reçoit une compensation, (sous quelque forme que ce soit), de la part d'un fournisseur, pour être préféré par rapport à ses concurrents. Le collaborateur peut également se trouver en situation de conflit d'intérêt qu'il ne déclare pas s'il est proche de l'un des responsables d'une entreprise fournisseur. "

DEGRÉ D'EXPOSITION



NIVEAU DE MAÎTRISE

Déclaré : 

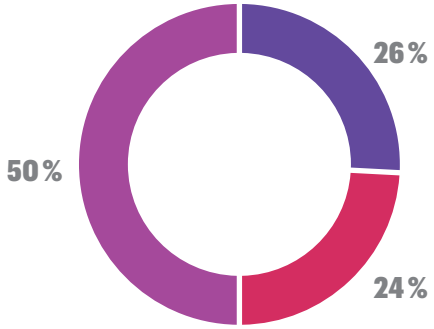
Constaté : Seulement la moitié des tentatives échouent

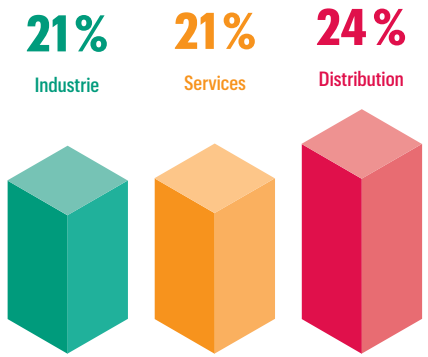
MONTANT MAXIMUM DÉCLARÉ

jusqu'à 10 000 000 €

Ce sont les entreprises de plus grosse taille qui sont le plus touchées par ce scénario.

Part des entreprises concernées par ce scénario de fraude.





Oui — Uniquement des tentatives — Non

Points de vigilance :

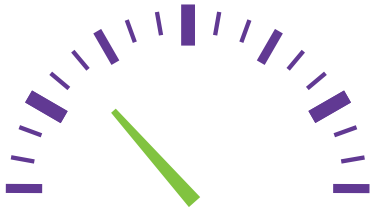
- Avoir un code éthique " pratico-pratique ". Ne pas rester sur de grands principes laissant place à l'interprétation de chacun mais bien décrire ce qui est ou non autorisé avec des exemples concrets et évocateurs pour les collaborateurs,
- Réaliser des actions de formation et sensibilisation auprès des collaborateurs les plus exposés,
- Mettre en place des indicateurs pour surveiller la bonne application du code.

FICHE SCENARIO 6 – **Financement du terrorisme**

SCÉNARIO

"Votre entreprise exploite des sites ou fait appel à des fournisseurs dans des zones contrôlées par des organisations terroristes. Des négociations ont alors lieu entre votre entreprise et l'organisation pour des laissez-passer, achats de matière premières...".

DEGRÉ D'EXPOSITION



NIVEAU DE MAÎTRISE

Déclaré :

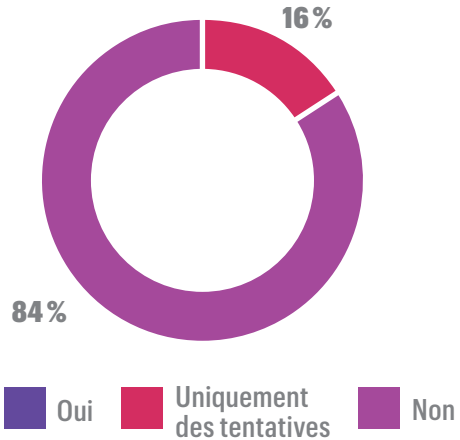
Constaté : Toutes les tentatives échouent

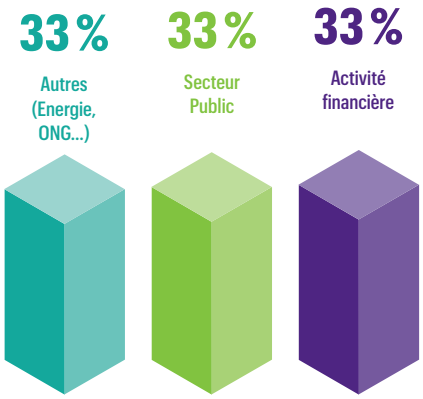
MONTANT MAXIMUM DÉCLARÉ

Non applicable car pas de cas avéré

Ce sont les entreprises de moyenne et grande taille qui sont le plus touchées par ce scénario.

Part des entreprises concernées par ce scénario de fraude.





Points de vigilance :

- Mettre en place un processus de *Know your Customer* et l'appliquer auprès de ses clients, partenaires, sous-traitants.

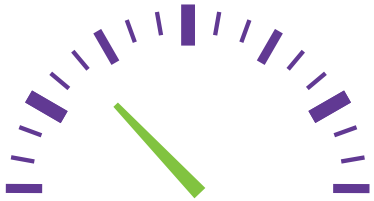
PANORAMA **DE LA FRAUDE**

FICHE SCENARIO 7 – **Comportement non éthique**

SCÉNARIO

"Votre entreprise détient des sites ou fait appel à des fournisseurs dans des pays étrangers dans lesquels les conditions de travail et les normes de sécurité ne sont pas respectées, voire sont dénoncées depuis plusieurs années par des ONG (vétusté des immeubles, incendies fréquents...)."

DEGRÉ D'EXPOSITION

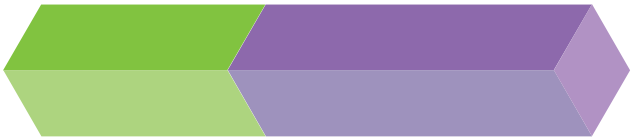


NIVEAU DE MAÎTRISE

Déclaré : ★ ★

Constaté : Les ¾ des tentatives échouent

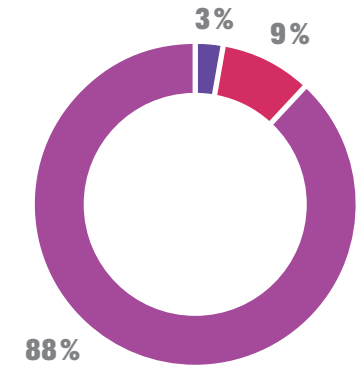
MONTANT MAXIMUM DÉCLARÉ

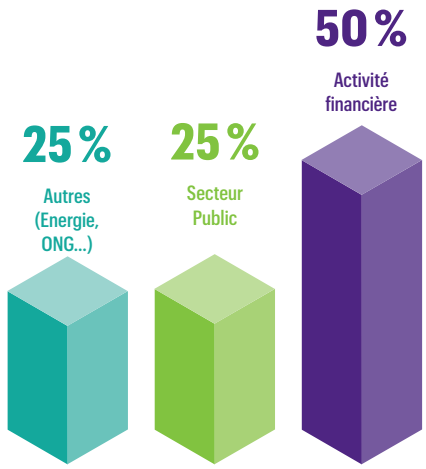


jusqu'à 100 000 €

Ce sont les entreprises de plus grande taille qui sont le plus touchées par ce scénario.

Part des entreprises concernées par ce scénario de fraude.





Oui | Uniquement des tentatives | Non

Points de vigilance :

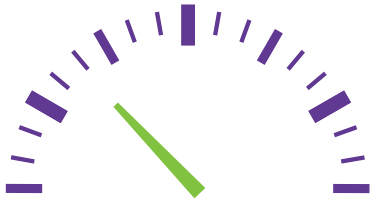
- Penser à inclure dans les contrats des clauses autour du risque de fraude,
- Systématiquement apprécier le critère " fraude et éthique " dans le choix de ses partenaires et sous-traitants,
- Réaliser des audits chez ses sous-traitants.

FICHE SCENARIO 8 – **Contournement d'embargo**

SCÉNARIO

"Un collaborateur ayant assez de pouvoir dans votre entreprise décide de ne pas respecter des décisions d'embargo et d'effectuer des transactions avec des pays ou entités sous sanction".

DEGRÉ D'EXPOSITION



NIVEAU DE MAÎTRISE

Déclaré : ★ ★ ★

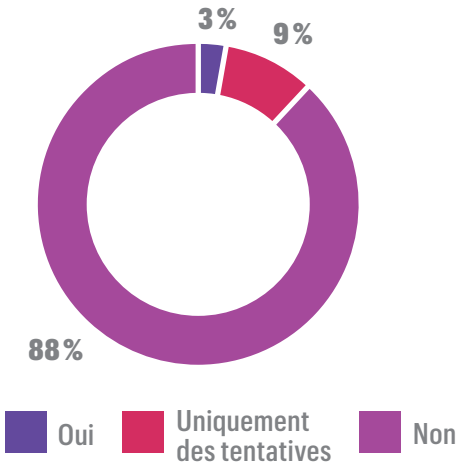
Constaté : 83 % des tentatives échouent

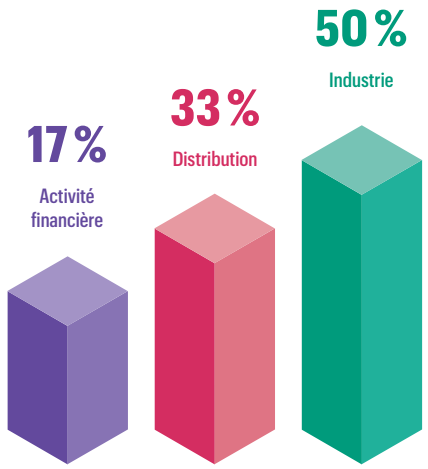
MONTANT MAXIMUM DÉCLARÉ

Non communiqué

Ce sont les entreprises de moyenne et grosse taille qui sont le plus touchées par ce scénario.

Part des entreprises concernées par ce scénario de fraude.





Points de vigilance :

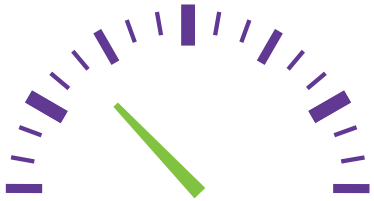
- Avoir un processus de veille sur le sujet,
- Rappeler les risques et sanctions aux dirigeants.

FICHE SCENARIO 9 – **Falsification d'informations**

SCÉNARIO

"Des collaborateurs hauts placés dans votre entreprise décident de monter des stratagèmes dans le but de maquiller la réalité. La falsification d'informations peut avoir lieu à différents niveaux comme par exemple sur la qualité des produits vendus (exemple : système de détection automatique de passage d'un test de mesure d'émission de CO2) ou sur la fiabilité des informations comptables et financières (exemple : reflet d'une situation financière plus avantageuse). "

DEGRÉ D'EXPOSITION



NIVEAU DE MAÎTRISE

Déclaré : ★ ★

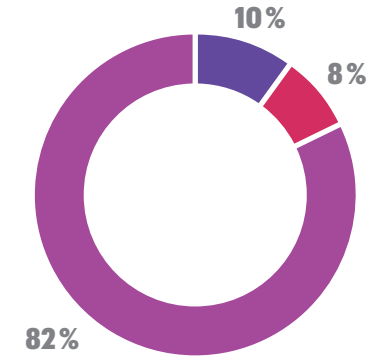
Constaté : Seulement la moitié des tentatives échouent

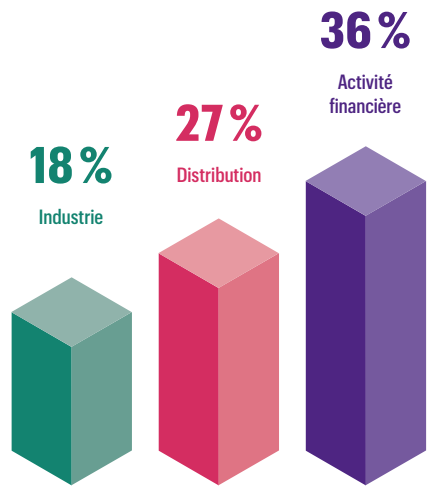
MONTANT MAXIMUM DÉCLARÉ

jusqu'à 10 000 000 €

Ce sont les entreprises de grosse taille qui sont le plus touchées par ce scénario.

Part des entreprises concernées par ce scénario de fraude.





Oui | Uniquement des tentatives | Non

Points de vigilance :

- Formaliser les procédures de contrôles comptables,
- Rapprochement bancaires,
- Contrôles d'inventaire (stock, actifs),
- Circularisation auprès des tiers (clients, fournisseurs, banques, avocats).

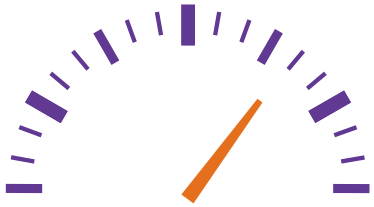
PANORAMA **DE LA FRAUDE**

FICHE SCENARIO 10 – **Détournement d'actifs**

SCÉNARIO

"Vente et achat - Détournement de chèques par un collaborateur ou par un tiers, Emission ou paiement de facture fictive... ; Paie - Salarié fantôme, double paiement de salarié, remboursement de notes de frais surévaluées... ; *Stocks* et immobilisations - Vol de matières premières, produits semi-finis ou finis par un collaborateur ou par un tiers..."

DEGRÉ D'EXPOSITION



NIVEAU DE MAÎTRISE

Déclaré : ★ ★

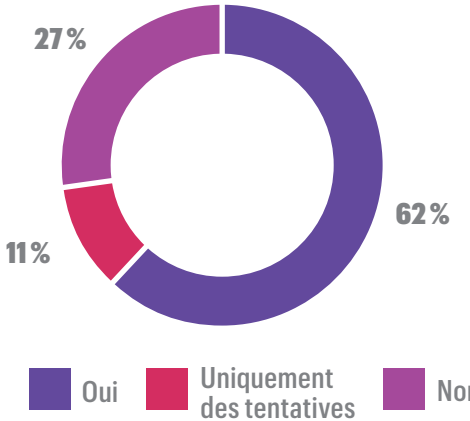
Constaté : Seulement 15 % des tentatives échouent

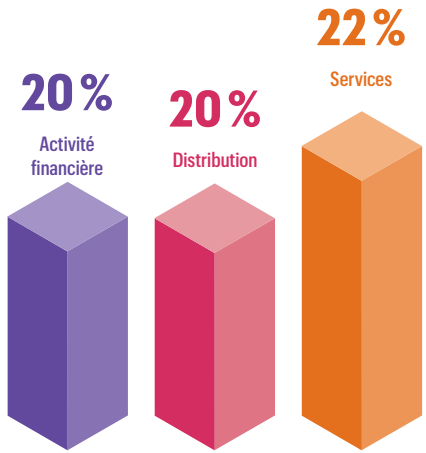
MONTANT MAXIMUM DÉCLARÉ

Supérieur à 10 000 000 €

Ce sont les entreprises de petite taille qui sont le plus touchées par ce scénario.

Part des entreprises concernées par ce scénario de fraude.





Points de vigilance :

- Industrialiser les contrôles à l'aide de solutions de type *data analytics*,
- Communiquer sur les résultats des contrôles pour montrer que le sujet est une préoccupation et qu'il est surveillé (bon outil de dissuasion pour la fraude interne).

PANORAMA **DE LA FRAUDE**

Au-delà des éléments vus pour chacun des scénarios de notre panorama, la lutte contre la fraude passe inévitablement par **un renforcement de la culture du risque au sein des entreprises.** Un rapide rappel, donc, **de trois fondamentaux en matière de culture du risque, pour mémoire :**

- **Formaliser les procédures et règles de gestion permettant de prévenir une situation de fraude.** Il est indispensable d'arrêter de partir du postulat que le " bon sens " des collaborateurs est suffisant pour prévenir un tel fléau. Le bon sens n'est pas une notion identique et universelle à l'ensemble des salariés et l'entreprise ne pourra pas s'en prévaloir en cas de fraude majeure ! C'est le dispositif de contrôle interne (que l'entreprise a l'obligation de mettre en place) qui doit représenter un facteur dissuasif pour les fraudeurs (en limitant les opportunités et en réduisant la pression du célèbre triangle de la fraude).

- **Indiquer clairement aux collaborateurs la ou les personnes qu'ils doivent solliciter pour toute question ou doute sur une opération à passer**. Il s'agit d'un point important notamment pour les entreprises de moyenne ou grande taille, au sein desquelles l'accès à la hiérarchie n'est pas toujours aussi direct que dans les petites entreprises.

- **Sensibiliser les collaborateurs aux différents scénarios de fraude auxquels l'entreprise est exposée, par la mise en œuvre de formations pratico-pratiques.**

PANORAMA **DE LA FRAUDE**

Le point de vue international

Les points de vue des différentes firmes membres de Grant Thornton interrogées à travers le monde, convergent sur un niveau " Important " ou " Extrêmement important" pour ce qui concerne les entreprises qu'elles accompagnent, à l'exception notoire de l'Afrique du Sud où le sujet est encore considéré comme secondaire.

Concernant la **pression réglementaire**, nous constatons, au travers des remontées de nos partenaires, **une situation hétérogène et paradoxale dans certains cas.**

Dans les pays anglo-saxon (US, UK), le niveau d'importance accordé au sujet s'est traduit par l'adoption de réglementations spécifiques désormais bien connues des entreprises (FCPA, UKBA).

En revanche, nous constatons qu'au sein d'autres pays il **existe un décalage entre le niveau d'importance** accordé et l'arsenal législatif, et ce dans les deux sens :

- A titre d'exemple, en Afrique du Sud, il existe une réglementation spécifique sur la corruption, le *Prevention and combating corrupt activities act,* alors que le niveau d'importance accordé par les entreprises à ce sujet est déclaré comme secondaire,
- A *contrario*, au Mexique, il n'existe aucune réglementation spécifique en la matière alors que le niveau d'importance déclaré est maximal.

Au-delà du niveau d'importance et des contraintes réglementaires, nous avons également interrogé nos homologues sur leur analyse du niveau de préparation des entreprises pour lutter contre la fraude.

Il en ressort qu'aucun pays ne considère les dispositifs en place au sein des entreprises comme " forts ", même en Grande-Bretagne, pourtant bien positionnée dans le classement de *Transparency International* (10ème). Les résultats oscillent entre un niveau " moyen " et " faible " pour certaines économies comme le Mexique déjà évoqué.

Pour dépasser les déclarations d'intention, **nous avons tenté de savoir si les entreprises étaient réellement prêtes à investir sur ce sujet et donc se prémunir.** De manière globale, **la réponse est positive** et nous constatons au travers de notre réseau international, que la demande d'assistance sur le sujet est plutôt croissante.

Ce qui est plus surprenant, c'est que cette demande semble en grande partie décorrelée des contraintes réglementaires et du niveau d'importance accordée. Il s'agit là d'une tendance globale qui concerne tous les pays ayant répondu à notre sollicitation. Elle s'explique certainement, comme c'est également le cas pour la France, par la multiplication des tentatives et des cas avérés qui sont finalement, et malheureusement, le meilleur vecteur de sensibilisation des entreprises.

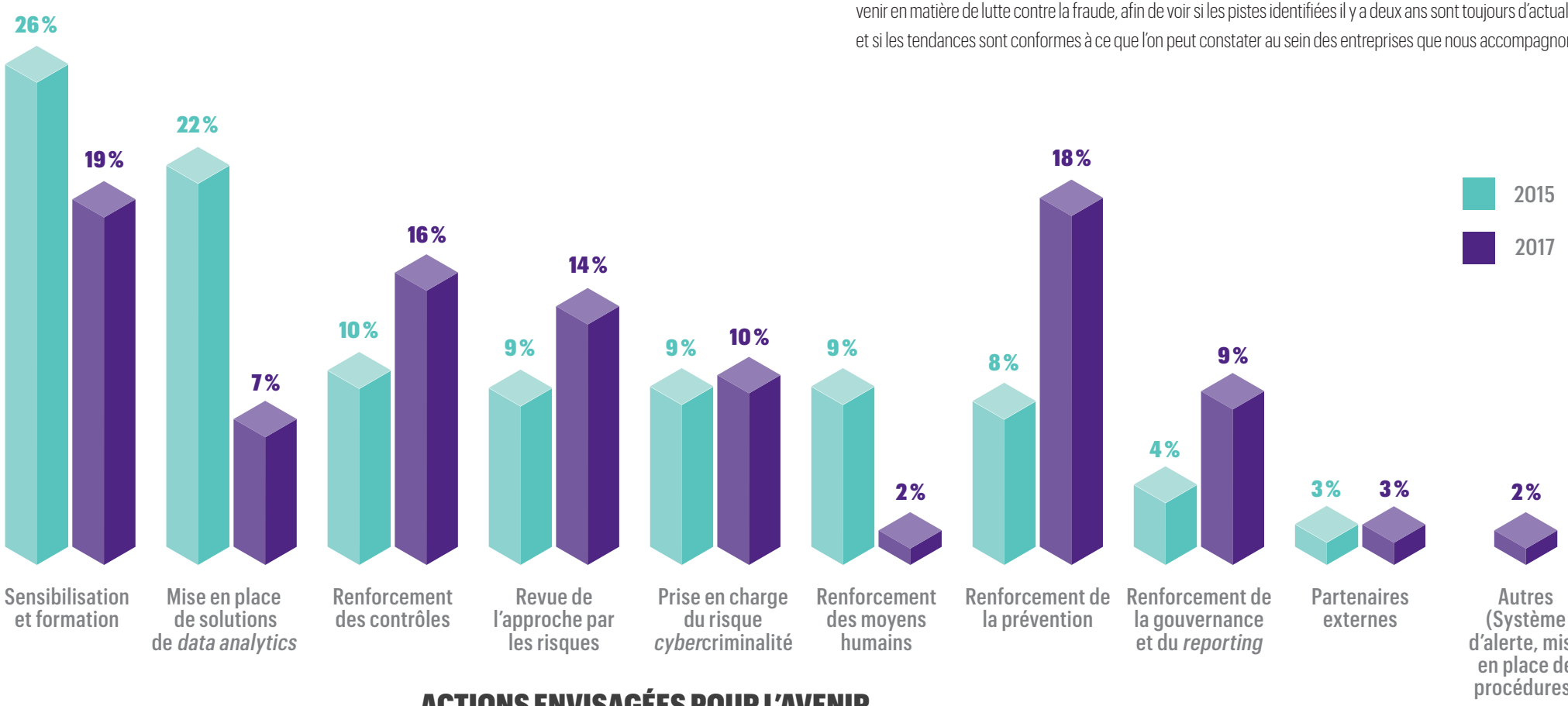
Nous avons également interrogé nos correspondants sur le niveau d'exposition dans les différents pays au regard des 10 scénarios analysés dans notre étude. Les réponses font clairement apparaître, s'il en était encore besoin, **le caractère international et universel de la fraude.** Sur les 10 scénarios envisagés, 8 sont appréciés de manière homogène par les différents pays avec un niveau d'exposition compris entre 4 et 5 sur une échelle de 5 niveaux.

Certains scénarios que l'on aurait pourtant pu imaginer dépendre de la culture des pays, par exemple la fraude au Président, sont évalués dans toutes les zones du monde comme représentant un niveau de risque très important.

Deux scénarios par contre font l'objet d'évaluations plus contrastées entre les pays : le financement du terrorisme, qui ressort comme étant une préoccupation d'abord dans les pays occidentaux et développés et le scénario relatif au respect des embargos pour lequel certains pays ne se considèrent pas comme réellement exposés.

LES ACTIONS ENVISAGÉES **POUR L'AVENIR**

Comme lors de la précédente édition de notre baromètre, nous avons interrogé les entreprises sur leurs projets à venir en matière de lutte contre la fraude, afin de voir si les pistes identifiées il y a deux ans sont toujours d'actualité et si les tendances sont conformes à ce que l'on peut constater au sein des entreprises que nous accompagnons.



ACTIONS ENVISAGÉES POUR L'AVENIR

LES ACTIONS ENVISAGÉES **POUR L'AVENIR**

Par rapport à la première édition du baromètre, il est intéressant de noter certains points majeurs.

- Une progression significative des actions suivantes :

- Renforcement de la prévention,
- Renforcement des contrôles,
- Revue de l'approche par les risques,
- Renforcement de la Gouvernance et du *reporting*.

- Un recul significatif des actions suivantes :

- Renforcement des moyens humains,
- Sensibilisation et formation,
- Mise en place de solution de *data analytics*.

Les actions envisagées démontrent clairement que les entreprises ont désormais pleinement pris conscience de la nécessité d'appréhender le risque de fraude au sens large.

En effet, un dispositif efficient de lutte passe tout d'abord par la mise en place du volet prévention lui-même, dont l'approche par les risques est fondamentale. Il constitue la colonne vertébrale du dispositif en donnant la capacité aux entreprises de prioriser leurs efforts.

De même, le fait que les entreprises souhaitent renforcer la gouvernance et le *reporting* démontre un vœu de transparence sur le sujet car, comme évoqué au début de l'enquête, **le risque de fraude n'est plus un sujet aussi confidentiel que par le passé.**

Toutefois, ces résultats ont certainement aussi été influencés par les contraintes réglementaires actuelles et notamment l'entrée en vigueur de la loi Sapin 2 qui contraint les entreprises à mettre en place un dispositif de lutte contre la corruption et les oblige donc à structurer un dispositif global de lutte contre la fraude.

Il est également intéressant de constater que l'action " formation et sensibilisation " qui était plébiscitée comme une action à venir pour 26 % des entreprises il y a deux ans, le soit aujourd'hui pour seulement 19 % d'entre elles.
Nous constatons régulièrement que les entreprises ont tendance à vouloir former leurs collaborateurs aux sujets liés à la fraude (pour pouvoir démontrer que le sujet fraude est une préoccupation) sans avoir structuré et formalisé au préalable leur dispositif.
Pourtant, former les collaborateurs sur des aspects théoriques ne permet pas une bonne appropriation du sujet, n'incite pas à prendre le sujet totalement au sérieux et ne permet pas d'acquérir les réflexes nécessaires en cas de tentative avérée. Les actions de formation et sensibilisation sont indispensables et leur caractère opérationnel constituent un facteur clé d'efficacité des dispositifs anti-fraude.

Sur un autre plan, et de manière un peu paradoxale, les entreprises déclarent vouloir renforcer les contrôles mais la mise en place de solutions de *data analytics* est en baisse au regard de notre première édition (22 % en 2015 et 7 % en 2017).

Deux pistes de réflexion pour éclairer ce paradoxe :

1. L'on peut penser que cette action ait en fait déjà été engagée, (au moins partiellement), par les entreprises afin d'industrialiser la détection de la fraude comme en témoigne, depuis plusieurs années, le nombre de sollicitations de nos équipes conduisant ce type de projets.

2. Le renforcement des contrôles ne passe pas nécessairement par la création de nouveaux indicateurs. En effet, il existe souvent des éléments dans le dispositif de contrôle interne sur lesquels il est possible de capitaliser car ceux-ci contribuent à la prévention (exemple : rotation des portefeuilles des acheteurs – taux de dépendances des fournisseurs – principe des quatre yeux ...).

Les travaux d'optimisation et de renforcement des dispositifs anti-fraude sont donc appelés à se poursuivre en privilégiant à la fois le renforcement de la culture risque et l'efficacité des dispositifs de contrôle et surveillance.

À PROPOS **DE**

Grant Thornton

Grant Thornton, groupe *leader* d'Audit et de Conseil, rassemble en France 1 700 collaborateurs dont 117 associés dans 23 bureaux, en se positionnant sur 5 métiers : **Audit, Expertise Conseil, Conseil Financier, Conseil Opérationnel et *Outsourcing* et Conseil Juridique et Fiscal.**
Grant Thornton accompagne les entreprises dynamiques (sociétés cotées, entreprises publiques et privées) pour leur permettre de libérer leur potentiel de croissance, grâce à l'intervention d'associés disponibles et impliqués, épaulés par des équipes délivrant une expertise à très haute valeur ajoutée.

Les membres de Grant Thornton International Ltd, constituent l'une des principales organisations d'Audit et de Conseil à travers le monde. Chaque membre du réseau est indépendant aux plans financier, juridique et managérial.

Grant Thornton, l'instinct de la croissance.
www.grant-thornton.fr

Grant Thornton International Ltd.

Grant Thornton International Ltd, groupe *leader* d'Audit et de Conseil, est un réseau intégré et indépendant, rassemblant plus de 47 000 collaborateurs dont 3 235 associés implantés dans 140 pays. La puissance de notre organisation internationale nous permet de mobiliser des équipes multiculturelles et de répondre aux problématiques de nos clients de manière globale, garantissant ainsi les mêmes standards de qualité, de *risk management,* de *process* et d'excellence, partout dans le monde.

Grant Thornton, *an instinct for growth.*
www.gti.org

CONTACTS :

Nicolas GUILLAUME
Associé, Directeur de la ligne de services
Risk Management
E nicolas.guillaume@fr.gt.com

Patricia POMBO
Senior manager en charge de l'offre fraude
et corruption au sein de la ligne de services *Risk Management*
E patricia.pombo@fr.gt.com

Agnès de RIBET
Directrice du *Marketing*
et de la Communication
E agnes.deribet@fr.gt.com

Grant Thornton
L'instinct de la croissance™

Grant Thornton
Membre français de Grant Thornton International Ltd.
29 rue du Pont 92200 Neuilly-sur-Seine