DFCG.

Memo Bank

N°43
LES CAHIERS
TECHNIQUES DFCG

RISQUES CYBER ET FRAUDES FINANCIÈRES : ÉTAT DES LIEUX DES PME ET ETI

Transformation digitale

DFCG.

PRÉAMBULE

La fraude, c'est notre nouveau front

Les chiffres de cette enquête sont sans appel : 85 % des PME et ETI ont subi au moins une tentative de fraude au cours des douze derniers mois. Nous ne sommes plus dans l'ère du risque potentiel, mais dans celle de la menace permanente. L'enquête menée par Memo Bank et la DFCG révèle une réalité brutale : les fraudeurs ne ciblent plus seulement les grands groupes, ils s'attaquent désormais méthodiquement aux entreprises de taille intermédiaire. Agissons avant qu'il ne soit trop tard, car la fraude ne prévient pas : elle frappe.

Les PME / ETI : cibles privilégiées et pourtant délaissées

Notre enquête révèle un angle mort dans la cybersécurité française : les PME et ETI sont devenues des cibles privilégiées pour les fraudeurs, mais restent un segment relativement délaissé en termes de solutions adaptées. Contrairement aux grands groupes, elles n'ont souvent ni les ressources ni l'expertise pour faire face à des attaques de plus en plus sophistiquées. Notre étude met en lumière une réalité troublante : malgré une conscience aiguë des risques en matière de cyberfraude, les dispositifs de protection demeurent insuffisants dans la majorité des entreprises sondées. À travers ce rapport, la DFCG, et en particulier son groupe d'échange Transformation digitale, met en lumière cette vulnérabilité spécifique afin d'être en mesure d'accompagner les directions financières dans le renforcement de leur résilience face à cette menace croissante.

AUTEURS

Jean-Daniel Guyot,
Cofondateur et président
du directoire de Memo Bank

Christian Laveau,
Président du groupe Transformation
digitale de la DFCG

INTRODUCTION

Une menace en pleine expansion

L'évolution alarmante des tentatives de fraude et de cyberfraude

Le constat est clair : les menaces de fraude et de cyberfraude contre les PME et ETI ont connu une accélération sans précédent ces dernières années. Si en 2020 environ 60 % des entreprises déclaraient avoir subi des tentatives de fraude,[1] ce chiffre a grimpé à 85 % selon notre enquête : une augmentation de 25 points en l'espace d'à peine cinq ans.

Cette progression spectaculaire témoigne d'un changement de stratégie des cybercriminels. Autrefois concentrés sur les grandes entreprises, ils déploient désormais leurs efforts vers des cibles perçues comme plus vulnérables et moins préparées. Cette réorientation s'explique notamment par le renforcement des dispositifs de sécurité chez les grands groupes, poussant les fraudeurs à rechercher des proies plus accessibles.

Une sophistication croissante des attaques

Au-delà de l'intensification quantitative, nous observons une évolution qualitative des méthodes employées. Les attaques de phishing simples cèdent progressivement la place à des approches combinant ingénierie sociale avancée et technologies de pointe. L'émergence de l'intelligence artificielle et des deepfakes, identifiée par 83 % des répondants comme principale menace émergente, marque un tournant inquiétant dans cette course technologique.

Pourquoi cette étude aujourd'hui ?

Face à ce phénomène en pleine mutation, Memo Bank et la DFCG ont souhaité offrir une vision précise et actualisée de la situation spécifique aux PME et ETI françaises. Contrairement aux grandes entreprises qui bénéficient d'études sectorielles régulières et de recommandations sur mesure, les organisations de taille intermédiaire ont longtemps navigué sans véritable cartographie des risques de cyberfraude adaptée à leur réalité.

Nous espérons que cette étude aidera les PME et ETI à identifier les menaces les plus préoccupantes et à mettre en place des actions concrètes et adaptées. En cartographiant le paysage actuel des risques et en partageant les bonnes pratiques observées sur le terrain, nous souhaitons contribuer à renforcer la résilience collective des PME et ETI face à cette menace grandissante.

[1] Baromètre Euler Hermes — DFCG 2021

SOMMAIRE

1. UNE PRISE DE CONSCIENCE SANS PRÉCÉDENT 5

1.1 Des attaques de plus en plus sophistiquées 5

1.2 Origine principale des tentatives de fraudes 6

1.3 Moyen de paiement impliqué en cas de fraude 7

1.4 L'impact invisible des fraudes 8

1.5 Des fonds rarement récupérés 9

1.6 Responsabilité en cas d'attaque 9

2. DES PROTECTIONS INSUFFISANTES 10

2.1 Nouvelles menaces 10

2.2 Un niveau de préparation insuffisant 11

2.3 Les principaux freins à la protection 12

3. LES DISPOSITIFS PRIVILÉGIÉS PAR LES PME ET ETI 13

3.1 La formation : le premier bouclier anti-fraude 13

3.2 Paiements sous haute surveillance 14

3.3 Audits de sécurité : une pratique encore trop rare 16

3.4 Assurances : un succès mitigé 17

CONCLUSION 18

PROFIL DES RÉPONDANTS 20

LEXIQUE 21

1. UNE PRISE DE CONSCIENCE SANS PRÉCÉDENT

1.1. Des attaques de plus en plus sophistiquées

85%

ont subi au moins **une tentative de fraude** au cours des douze derniers mois.

23%

affirment avoir subi plus de **dix tentatives** de fraude.

25%

ont déclaré avoir été **victimes d'une fraude** au cours des douze derniers mois.

Avec 85 % des directions financières ayant subi au moins une tentative sur les douze derniers mois et un quart (25 %) ayant effectivement été victimes d'une fraude aboutie, ce risque apparaît comme incontournable dans la carrière d'un directeur financier. Près d'un quart des répondants ont relevé plus de dix tentatives de fraude au cours des douze derniers mois. Un chiffre qui monte jusqu'à 40 % pour les entreprises de plus de 250 millions d'euros de chiffre d'affaires.

Les fraudes abouties ont été plus nombreuses dans les entreprises réalisant moins de deux millions d'euros de chiffre d'affaires et celles réalisant plus de 250 millions d'euros. Pour les plus petites, les mesures de protection sont plus faibles, mais pour les plus grandes, l'exposition aux risques est nettement plus importante.

Cas pratique

En 2023, un promoteur immobilier a vu 38 millions d'euros s'envoler, répartis sur 45 virements exécutés en quelques jours. Les escrocs se sont fait passer pour les dirigeants de la société, en manipulant les cadres du service financier à l'aide d'e-mails falsifiés, d'ordres de virement urgents et même de conversations téléphoniques avec des voix synthétiques générées par l'intelligence artificielle.

Cette technique de fraude, appelée fraude au président, repose sur une double mécanique : l'usurpation d'identité crédible et la pression hiérarchique ou d'urgence invoquée pour contourner les procédures internes.

Ce type d'escroquerie illustre parfaitement les dynamiques décrites dans l'enquête Memo Bank et DFCG 2025 : 85 % des PME et ETI ont subi au moins une tentative de fraude au cours des douze derniers mois, et les méthodes de plus en plus professionnelles (incluant désormais deepfakes, spoofing vocal et piratage de messageries) rendent les mécanismes traditionnels de contrôle obsolètes s'ils ne sont pas renforcés.

Dans ce cas précis, ni la double validation ni le contrôle des bénéficiaires n'étaient suffisamment stricts, et aucune alerte bancaire n'a été déclenchée. Ce cas rappelle que sans cartographie du risque ni formation ciblée, une entreprise, même très structurée, reste vulnérable face à une attaque bien préparée.

À retenir

La fraude au président est un classique toujours efficace. Elle combine ingénierie sociale et faiblesse organisationnelle, deux vulnérabilités clés identifiées dans l'enquête 2025. La généralisation de **l'IA ne fait qu'en accroître la dangerosité.**

1.2 Origine principale des tentatives de fraudes

Ne sait pas : 11 %

Si la fraude externe d'origine cyber domine largement (82 %), les 7 % de fraudes d'origine interne ou mixte ne doivent pas être sous-estimées. Ces fraudes internes ou par collusion exploitent une connaissance approfondie des processus et des failles de sécurité de l'entreprise, rendant leur détection plus complexe et leur préjudice potentiellement plus important.

Cette réalité souligne l'importance d'une approche globale de la sécurité qui ne se concentre pas uniquement sur les menaces externes mais intègre également des contrôles robustes pour prévenir et détecter les actions malveillantes provenant de l'intérieur même de l'organisation.

Canaux utilisés par les fraudeurs : top 3

TOP 1	TOP 2	TOP 3
75%	**27%**	**20%**
Faux e-mails cherchant à voler des informations (Phishing)	**Faux ordres de virement** (BEC attacks)	**Attaques des fournisseurs et partenaires** (Third party risks)

Usurpation de comptes bancaires (Account takeover)	16 %
Blocage des systèmes informatiques contre rançon (Ransomware)	14 %
Fraudes par carte bancaire (Carding)	9 %
Vol de données confidentielles (Data Breach)	5 %

La domination écrasante du phishing (75 %) et, dans une moindre mesure, des faux ordres de virement (27 %) démontre la nécessité d'une approche de défense à deux niveaux.

Comment s'en prémunir ?

D'une part, le déploiement de solutions technologiques avancées (méthodes d'authentification du courrier électronique comme le filtrage DMARC/SPF/DKIM, authentification multifacteur, analyse comportementale des e-mails) pour bloquer ces tentatives avant qu'elles n'atteignent les boîtes de réception.

D'autre part, une formation continue des collaborateurs, car même les meilleurs filtres laissent passer des menaces sophistiquées.

1.3 Moyen de paiement impliqué en cas de fraude

Virement	57 %
Carte bancaire	28 %
Prélèvement	11 %
Chèque	2 %

« Le virement est particulièrement vulnérable car il combine trois facteurs de risque : des montants potentiellement élevés, une exécution rapide et souvent irréversible, et des processus de validation souvent insuffisamment sécurisés. C'est pourquoi il représente la cible privilégiée des fraudeurs ».

— Jean-Daniel Guyot, cofondateur et président du directoire de Memo Bank

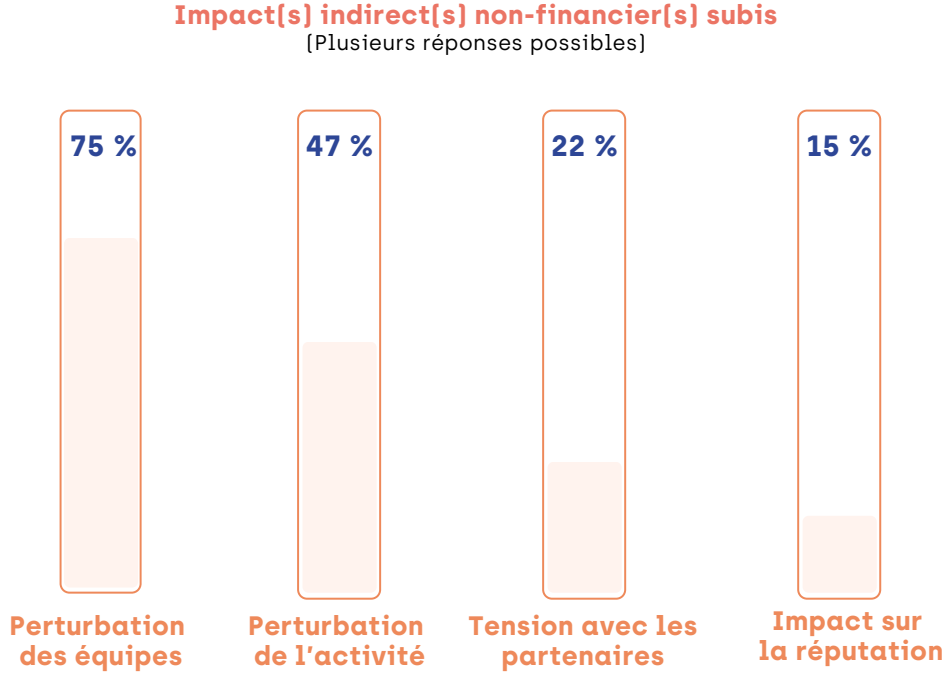
À retenir

Les entreprises doivent prioritairement sécuriser la chaîne de validation des paiements pour réduire leur exposition :

- contrôle des quatre yeux ;
- vérification des RIB ;
- contre appels.

1.4 L'impact invisible des fraudes

Même si, dans 78 % des cas, les pertes financières liées sont inférieures à 50 000 euros, leur impact indirect est important :



Au-delà des pertes financières directes, l'impact invisible de la fraude se révèle plus durable et coûteux. La perturbation des équipes met en lumière un coût psychologique et organisationnel rarement budgétisé, tandis que la tension avec les partenaires peut éroder un capital confiance bâti sur des années.

1.5 Des fonds rarement récupérés

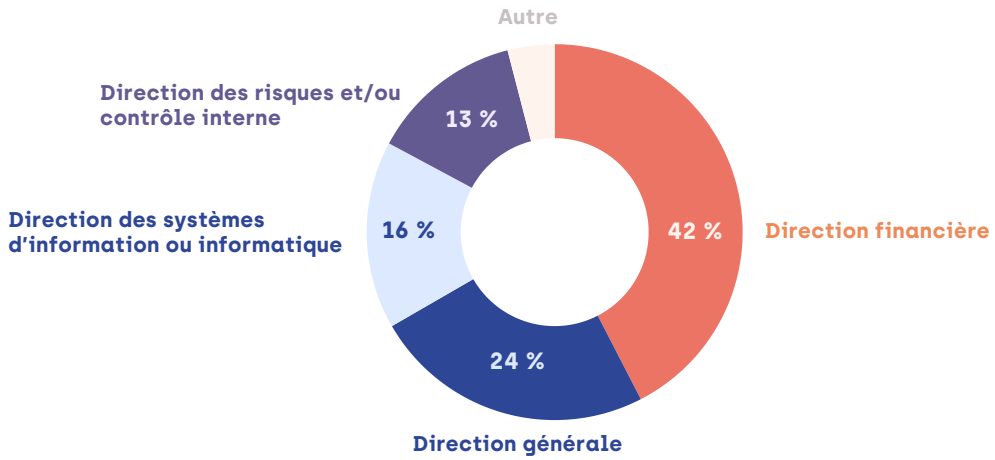
Avez-vous pu obtenir réparation du préjudice de la part de votre assureur ?

64% ont répondu ne **pas avoir obtenu** réparation du préjudice après une fraude.

Le fait que près de deux tiers des entreprises victimes (64 %) ne parviennent pas à récupérer leurs fonds souligne la nature quasiment irréversible de la fraude financière moderne. Les procédures juridiques sont longues, coûteuses et fastidieuses.

« La récupération des fonds est souvent compromise par la localisation des fraudeurs dans des juridictions étrangères, souvent peu coopératives. »
— Christian Laveau, Président du groupe Transformation digitale de la DFCG

1.6 Responsabilité en cas d'attaque



La Direction financière est la principale responsable (42 %), suivie par La Direction générale (24 %), ce qui démontre une forte attente de gouvernance au plus haut niveau. La part de responsabilité attribuée à la DSI reste étonnamment faible (16 %), tout comme celle de la Direction des risques (13 %). Certaines réponses sont préoccupantes car plusieurs entreprises ont affirmé qu'aucune responsabilité n'a été déterminée.

« Ces chiffres suggèrent une vision où la sécurité financière et cyber est considérée avant tout comme une problématique de gouvernance financière plus que technique ».
— Jean-Daniel Guyot, cofondateur et président du directoire de Memo Bank

2. DES PROTECTIONS INSUFFISANTES

2.1 Nouvelles menaces

Quelles sont, selon vous, les plus grandes menaces en matière de fraude pour les prochaines années ?

83% estiment que **l'IA et les deepfakes** représentent la plus **grande menace** en matière de cybersécurité.

Les failles humaines et les erreurs internes	**71 %**
Le crime organisé et les attaques sophistiquées	**43 %**
Les nouvelles technologies de paiement (cryptomonnaies, paiements instantanés…)	**23 %**
Le recours à des prestataires externes (le fait qu'un prestataire soit piraté, ou qu'il soit malveillant)	**22 %**
Le risque de collusion (combinaison de fraude interne et externe)	**18 %**
Le télétravail (moins de contrôle sur l'accès aux outils)	**15 %**

La plupart des entreprises perçoivent bien l'intensification des menaces puisque **62 % d'entre elles déclarent observer une augmentation du nombre de menaces sur l'année en cours**. L'IA et les deepfakes dominent largement les préoccupations (83 %), suivis de près par le facteur humain (71 %), démontrant une conscience aiguë des vulnérabilités liées aux technologies émergentes et au comportement humain.

Le crime organisé arrive en troisième position (43 %), loin devant les risques liés aux nouvelles technologies de paiement (23 %) ou aux prestataires externes (22 %), révélant un écart significatif entre les menaces perçues comme immédiates et celles considérées comme secondaires.

2.2 Un niveau de préparation insuffisant

Les résultats révèlent un décalage frappant entre la perception du risque et la préparation réelle des entreprises :

Seules 5 % des entreprises considèrent être « très bien préparées » face aux risques de fraude.

Comment évaluez-vous le niveau de préparation de votre entreprise face aux risques de fraude ?

4%
Très bien préparée

50%
Bien préparée

43%
Insuffisamment préparée

2%
Pas du tout préparée

Seules **44 % des entreprises ont des procédures formalisées** permettant d'identifier et de réagir en cas de fraude. Il existe un fossé entre la conscience du danger et la mise en place de réponses adaptées : les entreprises reconnaissent la menace mais peinent à traduire cette conscience en actions concrètes.

À noter que plus l'entreprise a un chiffre d'affaires élevé, plus elle dispose de procédures formalisées, même si le chiffre demeure faible : 67 % des entreprises de plus de 250 millions de chiffre d'affaires ont des procédures formalisées.

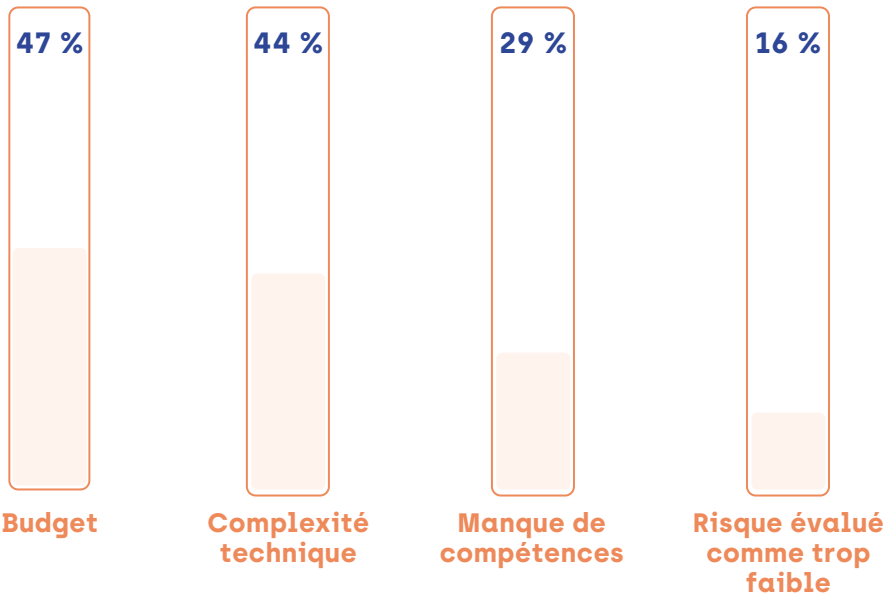
25% des entreprises ont **une assurance contre la fraude**.

2.3 Les principaux freins à la protection

60 % des entreprises interrogées déclarent ne pas augmenter le budget alloué à la prévention de la fraude pour l'année à venir. Plusieurs répondants ont mis en avant un manque de temps et de ressources humaines. D'autres répondants estiment être très bien protégés et ne comptent pas investir plus.

Face aux contraintes budgétaires (47 %), il convient de privilégier une approche progressive de la sécurité : identifier d'abord les processus financiers les plus critiques, implémenter des mesures à fort impact et faible coût comme la double validation, puis investir progressivement dans des solutions techniques plus avancées en fonction de son exposition aux risques.

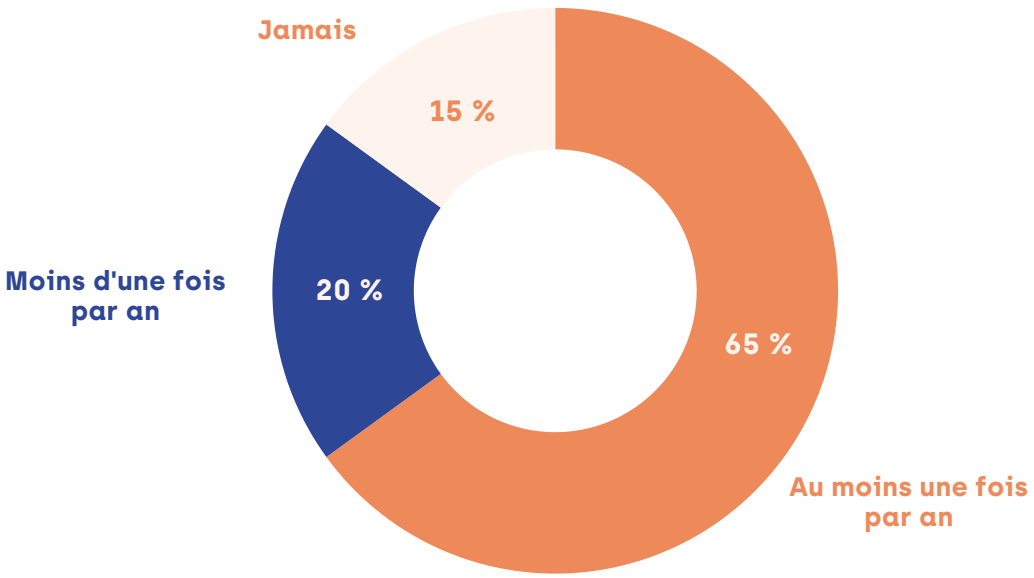
Quels sont les principaux freins à la mise en place de solutions anti-fraude ?



3. LES DISPOSITIFS PRIVILÉGIÉS PAR LES PME ET ETI

3.1 La formation : le premier bouclier anti-fraude

À quelle fréquence formez-vous vos collaborateurs aux risques liés à la cybersécurité et de fraude financière et comptable ?



La formation est un investissement efficace puisque la vigilance des employés (71 %) est une des premières clés pour déjouer les fraudes, suivie par la détection automatique des outils mis en place (26 %). Pour maximiser l'impact, privilégiez des formations courtes mais régulières, incluant des simulations réalistes et personnalisées par fonction, plutôt qu'une formation annuelle unique et générique.

3.2 Paiements sous haute surveillance

Dispositifs de préventions mis en place par les entreprises

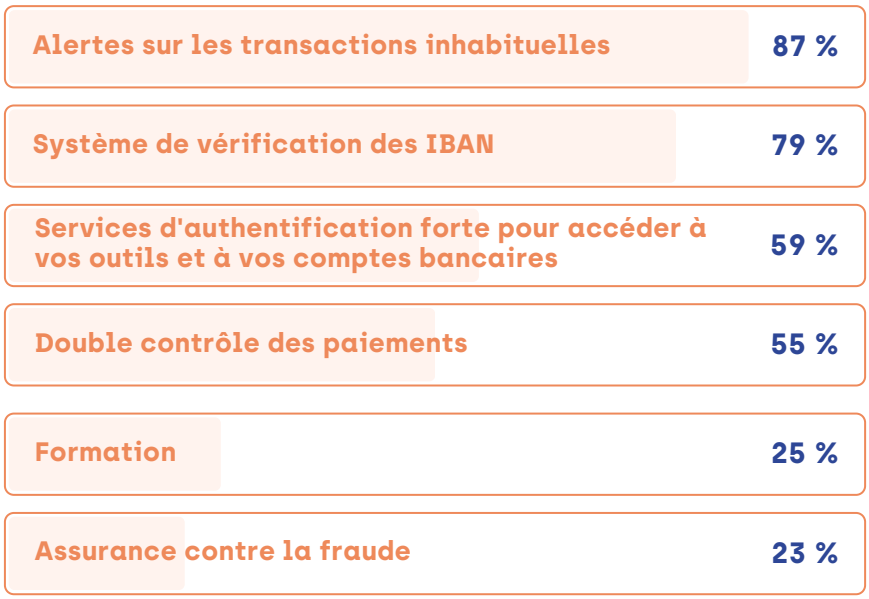
1. **81%** **Double validation des paiements**
2. **65%** Filtrage des **emails suspects et de l'accès à certains sites**
3. **57%** **Sensibilisation au quotidien** (politique interne et procédures)

- **53 %** **Double validation** des bénéficiaires ou fournisseurs
- **41 %** **Système de surveillance** des accès aux applications
- **31 %** **Contrôle interne ou externalisé**
- **19 %** **Contrôle automatisé des transactions inhabituelles** (montants, pays...)

Le taux élevé d'adoption de la double validation des paiements (81 %) montre une prise de conscience des risques, mais l'écart avec la double validation des bénéficiaires (53 %) révèle une vulnérabilité critique. En effet, c'est souvent lors du changement de coordonnées bancaires que la fraude intervient, rendant cette seconde mesure tout aussi cruciale que la première. Plus l'entreprise est de grande taille, plus la mise en place parallèle de plusieurs actions est constatée.

« Le contrôle interne est rarement privilégié dans les petites entreprises, car celles-ci n'ont pas toujours les moyens, les ressources dédiées et le temps nécessaire en interne pour le développer. Par ailleurs, la mise en place de Security Operations Centers (SOC), dont la fonction est de surveiller, prévenir, détecter et répondre aux cybermenaces, est le plus souvent réservée aux grands groupes, là encore faute de moyens suffisants pour les entreprises de taille petite ou moyenne. »
— Christian Laveau, Président du groupe Transformation digitale de la DFCG

Les attentes vis-à-vis de la banque



La forte préférence pour les alertes sur les transactions inhabituelles (87 %) et la vérification des IBAN (79 %) révèle que les entreprises attendent prioritairement de leur banque un rôle de vigilance dans la détection précoce des fraudes. Cela s'explique par la position stratégique des établissements bancaires au cœur des flux financiers, leur permettant de repérer les anomalies avant même que l'entreprise puisse les identifier.

La confiance accordée aux banques pour prévenir les fraudes varie selon la taille de l'entreprise : plus l'entreprise est petite, plus la note de confiance est élevée (note de 7/10 pour les entreprises de moins de dix millions d'euros de chiffre d'affaires, contre un score de 4,7/10 pour les entreprises de plus de 250 millions). Pour les directions financières, la banque apparaît comme un partenaire essentiel mais non suffisant, rappelant que la responsabilité ultime de la sécurité financière reste interne à l'entreprise.

3.3 Audits de sécurité : une pratique encore trop rare

À quelle fréquence réalisez-vous des audits de sécurité (logique ou cybersécurité) ?

42%
Au moins une fois par an ou plus

39%
Moins d'une fois par an

18%
Jamais

Si près de 42 % d'entre elles respectent la fréquence recommandée d'au moins un audit annuel, une proportion presque équivalente (39 %) ne procède à ces vérifications que de manière sporadique. Plus préoccupant encore, près d'une entreprise sur cinq n'effectue jamais d'audit de sécurité, s'exposant ainsi considérablement au risque de fraude

3.4 Assurances : un succès mitigé

Avez-vous souscrit une assurance contre la fraude ?

25 %	28 %	45 %
Oui	Non, mais en projet	Non

Seulement un quart des entreprises (25 %) sont assurées contre la fraude, tandis que près de la moitié (45 %) n'ont aucune couverture. Près de 28 % des entreprises envisagent de souscrire une assurance, ce qui indiquerait une prise de conscience progressive mais encore insuffisante face aux risques croissants. Cette réticence générale pourrait s'expliquer par une méconnaissance des solutions disponibles, un coût perçu comme disproportionné par rapport au risque, et particulièrement pour les 45 % restants, un scepticisme prononcé quant à l'efficacité réelle de ces assurances en cas de sinistre.

CONCLUSION

Cette enquête révèle un paradoxe inquiétant : malgré une conscience aiguë des risques, les PME et ETI françaises demeurent insuffisamment protégées face à la fraude et aux risques cyber. L'asymétrie est frappante : d'un côté, des attaquants qui professionnalisent leurs méthodes et investissent dans des technologies avancées ; de l'autre, des entreprises qui hésitent encore à allouer les ressources nécessaires à leur protection.

La bonne nouvelle, c'est que les solutions les plus efficaces ne sont pas nécessairement les plus coûteuses. La formation des équipes, la formalisation des procédures et la mise en place de contrôles systématiques lors des paiements constituent un socle de sécurité accessible à toutes les organisations, quelle que soit leur taille.

La cyberfraude, et en particulier la cyberfraude financière, n'est plus un risque exceptionnel, mais une menace permanente du paysage économique. Face à cette réalité, la résilience des entreprises reposera sur leur capacité à intégrer la sécurité non comme un centre de coût, mais comme une composante essentielle de leur gouvernance et de leur culture d'entreprise. Le chemin vers cette maturité passe par une approche progressive, pragmatique et collaborative entre les différentes fonctions de l'entreprise.

En tant que partenaire financier de confiance, Memo Bank s'engage à accompagner les PME et ETI dans cette démarche, en proposant non seulement des solutions bancaires sécurisées, mais aussi un accompagnement adapté pour naviguer dans ce nouvel environnement de risques.

PROFIL DES RÉPONDANTS

Enquête menée entre le 13 février 2025 et le 2 avril 2025 auprès de 145 PME et ETI.

Chiffre d'affaires

Moins de 2 m€	11 %
2-10 m€	18 %
10-50 m€	32 %
50-100 m€	13 %
100-250 m€	9 %
Plus de 250 m€	14 %

Principales fonctions

TOP 1	TOP 2	TOP 3
64%	23%	12%
DAF, RAF	Président, DG	Autres fonctions financières

+ de **15** secteurs d'activités différents.

À propos de Memo Bank

Memo Bank est une banque française indépendante agréée en tant qu'établissement de crédit par la Banque centrale européenne et supervisée par l'ACPR. Grâce à sa plateforme bancaire de pointe, Memo Bank transforme le quotidien des PME en leur permettant de gérer leur liquidité et leurs transactions de manière centralisée et hautement sécurisée, tout en leur offrant un accès rapide au crédit.

Ne soyez pas la prochaine victime : sécurisez vos transactions dès aujourd'hui.

Nos experts Memo Bank sont disponibles pour mettre en place rapidement des mesures de protection adaptées à votre entreprise.

https://memo.bank/

À propos de la DFCG

L'Association nationale des Directeurs Financiers et de Contrôle de Gestion (DFCG), créée en 1964, constitue la communauté de référence des professionnels des directions financières d'entreprises privées ou des services publics. La DFCG rassemble, dans 17 régions, 3500 dirigeants financiers d'entreprises de toute taille, représentatives du tissu économique français. La DFCG regroupe 2000 sociétés (dont Grands groupes 13 %, ETI et PME 70 %, TPE 17 %).

Depuis le 1er janvier 2024, l'association est présidée par Marie-Hélène Pebayle. Lieu de recherche opérationnelle en finance et contrôle de gestion, ses analyses donnent matière à une dizaine de publications annuelles. Ses prises de positions contribuent au débat économique et financier. La DFCG publie la revue bimestrielle Finance&Gestion, le blog Vox-Fi, ainsi que des études, Cahiers techniques, Essentiels et Livres blancs, en s'appuyant sur ses 18 groupes d'échange.

Sphère pédagogique pour développer les compétences de ses membres, le Centre de Formation de la DFCG propose 60 formations allant de la sensibilisation pour dirigeant aux responsabilités nouvelles, à l'expertise plus pointue en financement ou en contrôle de gestion.

Au sein de la DFCG, le Groupe d'échange Transformation Digitale a pour vocation d'aider ses adhérents dans l'initiation et la conduite de projets de transformation digitale, en favorisant la prise de conscience, la réflexion stratégique, le retour d'expérience et l'échange.

https://www.dfcg.fr/

LEXIQUE

Account takeover : prise de contrôle d'un compte en ligne légitime après avoir obtenu ses identifiants, généralement pour effectuer des transactions frauduleuses.

Authentification multifacteur (MFA) : méthode exigeant plusieurs moyens d'identification distincts pour accéder à un compte ou un système. Par exemple, après avoir saisi votre mot de passe (premier facteur : ce que vous savez), vous devez valider une notification sur votre application d'authentification (deuxième facteur : ce que vous possédez).

BEC (Business Email Compromise) : technique de fraude où les cybercriminels usurpent l'identité d'un dirigeant ou d'un partenaire commercial par email pour initier des virements frauduleux.

Carding : fraude impliquant l'utilisation frauduleuse de données de cartes bancaires volées.

Contrôle 4 yeux : principe de sécurité exigeant que deux personnes distinctes approuvent une action avant son exécution.

Data Breach : violation de données, désignant le vol ou l'accès non autorisé à des informations confidentielles d'une entreprise.

Deepfake : technologie utilisant l'intelligence artificielle pour créer des contenus audio ou vidéo falsifiés mais ultra-réalistes, notamment utilisée pour usurper l'identité vocale ou visuelle de personnes.

DMARC/SPF/DKIM : standards de protection email permettant d'authentifier l'expéditeur et de prévenir l'usurpation d'adresses email.

Fraude interne : actes malveillants commis par des collaborateurs de l'entreprise exploitant leur accès privilégié aux systèmes.

Fraude par collusion : collaboration entre un acteur interne (employé) et un acteur externe pour commettre une fraude.

Ingénierie sociale : manipulation psychologique visant à obtenir des informations confidentielles ou à faire exécuter des actions par la victime.

Comité Scientifique DFCG.

Phishing : technique consistant à envoyer des emails frauduleux imitant une entité légitime pour inciter les destinataires à révéler des informations sensibles ou à effectuer des actions non sécurisées.

Ransomware : logiciel malveillant qui bloque l'accès aux systèmes ou aux données d'une entreprise, exigeant le paiement d'une rançon pour leur déblocage.

SOC (Security Operations Center) : centre opérationnel de sécurité composé d'experts analysant en continu les menaces et incidents de sécurité.

Third party risks : risques liés à la compromission des systèmes d'un fournisseur ou partenaire commercial pour atteindre l'entreprise cible.

Prix : 20 €
Date de parution : juin 2025
ISSN : 1950-0033
ISBN : 979-10-92310-39-9