BEC : anatomie de la fraude email professionnelle et réponse

> BEC (Business Email Compromise) : comprendre les 5 types d'attaque, techniques d'usurpation, détection DMARC et réponse à incident en France.

Le Business Email Compromise (BEC) est aujourd'hui la cybermenace la plus lucrative au monde pour les attaquants. Selon le rapport IC3 2025 du FBI, les pertes mondiales liées au BEC ont dépassé 3 milliards de dollars en une seule année, surpassant largement les dommages causés par les ransomwares. Contrairement aux attaques techniques pures, le BEC exploite avant tout la confiance humaine, les processus organisationnels défaillants et la difficulté à distinguer un email légitime d'un email frauduleux. En France, le phénomène de fraude au président — l'une des formes les plus connues du BEC — a causé des centaines de millions d'euros de préjudices depuis 2015, touchant des TPE, des collectivités territoriales et des groupes du CAC 40. Ce guide propose une analyse technique et organisationnelle complète : anatomie des attaques, signaux d'alerte, outils de détection, procédures de réponse à incident et cadre légal français. Comprendre le BEC en profondeur, c'est se donner les moyens de l'arrêter avant que le virement soit exécuté.

À RETENIR

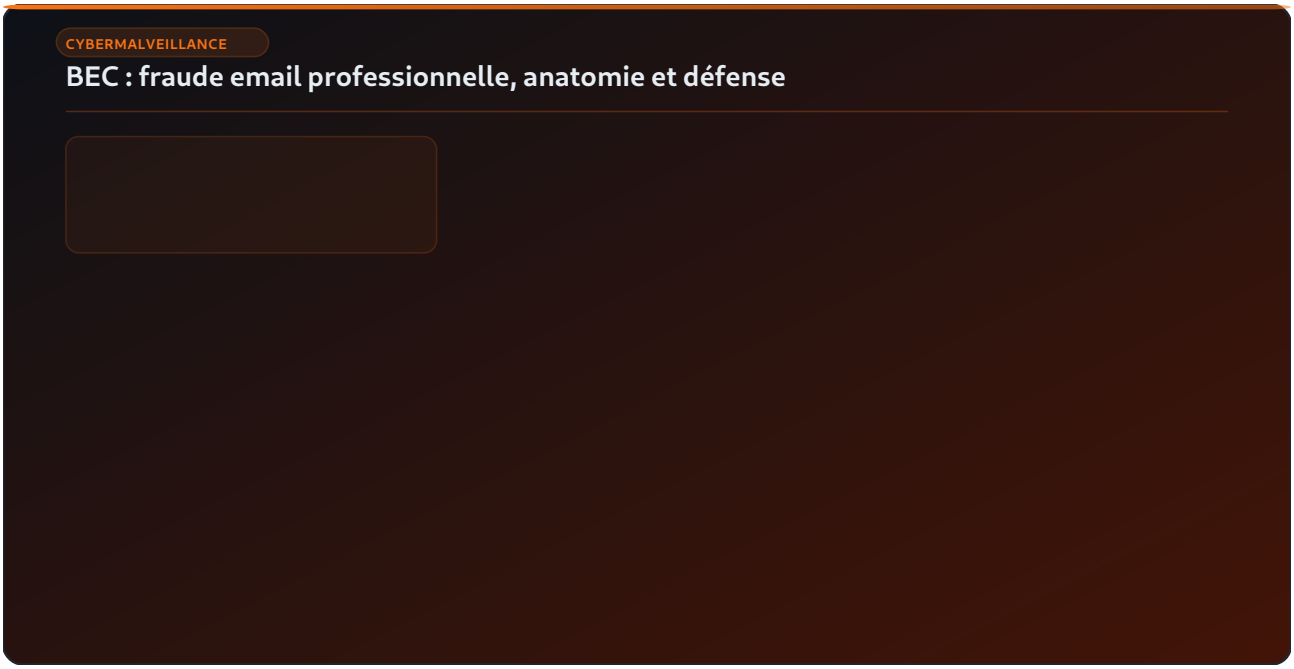
À retenir :

Le BEC génère plus de 3 milliards de dollars de pertes annuelles selon le FBI IC3 2025, soit plus que tous les ransomwares réunis.

Les 5 types principaux (CEO fraud, fausse facture fournisseur, usurpation d'avocat, vol de données RH, détournement de paie) ciblent tous les processus financiers de l'entreprise.

DMARC en mode p=reject, la double validation téléphonique des virements et la MFA sur les boîtes mail sont les trois défenses les plus efficaces.

> En France, une victime dispose de 72 heures pour contacter sa banque et demander le rappel du virement ; passé ce délai, la récupération des fonds devient très difficile.



Le Business Email Compromise désigne une famille d'escroqueries dans lesquelles un attaquant usurpe l'identité d'un dirigeant, d'un fournisseur ou d'un prestataire de confiance pour convaincre un employé d'effectuer un virement bancaire frauduleux, de divulguer des données sensibles ou de modifier des coordonnées de paiement. La définition officielle du FBI inclut cinq variantes distinctes, mais toutes partagent la même caractéristique : l'exploitation du facteur humain plutôt que d'une vulnérabilité logicielle.

Ce qui rend le BEC particulièrement dévastateur tient à plusieurs facteurs convergents. D'abord, les emails de BEC sont soigneusement contextualisés : l'attaquant a préalablement étudié l'organigramme de l'entreprise, le style d'écriture du dirigeant impersonné, les relations avec les fournisseurs, et parfois même le calendrier des opérations financières. Ensuite, les sommes en jeu sont considérables : le montant moyen d'un virement BEC réussi dépasse 120 000 dollars selon

l'IC3. Enfin, une fois le virement effectué vers un compte mule, les fonds transitent en quelques heures vers des juridictions où leur récupération est quasi impossible.

En France, la fraude au président est la forme la plus médiatisée, mais elle n'est plus la plus fréquente. Les attaques de type fausse facture fournisseur — où l'attaquant intercepte une communication légitime pour substituer ses propres coordonnées bancaires — représentent désormais la majorité des cas traités par la BEFTI (Brigade d'enquêtes sur les fraudes aux technologies de l'information).

Les 5 types de BEC : anatomie détaillée

CEO Fraud (fraude au président)

L'attaquant se fait passer pour le PDG, le DG ou un membre du comité de direction. Il contacte généralement la DAF ou un comptable avec une demande urgente et confidentielle de virement, souvent associée à un contexte créant une pression temporelle : acquisition secrète, audit fiscal, opération sensible à ne pas divulguer. Le message enjoint la cible de court-circuiter les procédures habituelles. La spécificité française de ce vecteur est l'exploitation des périodes de vacances où les validations hiérarchiques habituelles sont absentes.

> ⚡ **Retour terrain**
>
> Dans mes interventions post-incident pour des PME victimes de cyberattaques, la constante est l'absence de plan de réponse : les équipes découvrent ce qu'elles doivent faire en même temps qu'elles le font. J'ai développé un modèle de plan de réponse à incident en 2 pages — actions immédiates (0-2h), actions à court terme (2-24h), communication (interne, clients, CNIL), et reprise d'activité — que les dirigeants peuvent

tenir dans leur tiroir. Ce n'est pas un PRIS ISO 27035, c'est un filet de sauvetage minimal pour les 10 premières heures.

Supplier Invoice Fraud (fausse facture fournisseur)

C'est la variante en forte croissance. L'attaquant compromet soit la boîte mail d'un fournisseur réel, soit crée un domaine sosie (invoice@acme-solutions.fr au lieu d'invoice@acme-solution.fr). Il envoie une facture modifiée avec de nouvelles coordonnées bancaires, souvent dans le prolongement d'une conversation en cours pour maximiser la crédibilité. Le montant est identique à celui de la facture légitime attendue. La victime paye de bonne foi.

Attorney Impersonation (usurpation d'avocat)

Cette variante cible les dirigeants plutôt que les comptables. L'attaquant se fait passer pour un cabinet d'avocats ou un notaire impliqué dans une transaction confidentielle (fusion-acquisition, règlement d'un litige). La nature juridiquement sensible de l'opération justifie le secret et la rapidité. Les victimes sont souvent des chefs d'entreprise habitués à traiter directement des dossiers sensibles avec des conseils juridiques.

Data Theft (vol de données RH)

Moins immédiatement financier, ce vecteur vise l'obtention de données sensibles sur les employés : fiches de paie, numéros de sécurité sociale, contrats. L'attaquant se fait passer pour un RH, un cabinet de recrutement ou l'URSSAF. Ces données servent ensuite à d'autres escroqueries (faux remboursements, usurpation d'identité) ou sont revendues sur le darkweb.

Payroll Redirect (détournement de paie)

L'attaquant compromet la boîte mail d'un employé ou usurpe son identité pour contacter les RH et demander la modification du RIB sur lequel son salaire est versé. Simple, discret, et souvent

non détecté avant la fin du mois. La médiane des pertes est plus faible que pour les autres variantes, mais le volume est en forte hausse selon l'ANSSI.

Anatomie d'une attaque BEC : de l'OSINT à la compromission

Phase 1 : Reconnaissance et OSINT

Avant d'envoyer le moindre email, l'attaquant consacre plusieurs jours à la collecte d'informations en sources ouvertes. LinkedIn fournit l'organigramme complet, les noms des DAF, comptables et assistantes de direction, ainsi que leurs adresses email professionnelles déduites du format standard (prenom.nom@entreprise.fr). Les réseaux sociaux de l'entreprise révèlent les déplacements du PDG, les conférences auxquelles il participe, et parfois des informations sur des opérations en cours. Les appels d'offres publics, les rapports annuels et les mentions légales complètent le tableau. En 2026, des outils d'IA sont utilisés pour analyser le style d'écriture du dirigeant impersonné à partir de posts publics et générer des emails quasi indiscernables des communications authentiques.

Phase 2 : Préparation de l'infrastructure d'attaque

L'attaquant enregistre un ou plusieurs domaines sosies. Les techniques de typosquatting sont variées : substitution de caractère (acme-group.fr vs acme-group.fr avec un 'l' majuscule ressemblant à un 'i'), ajout de tiret (acme-solutions.fr vs acmesolutions.fr), changement de TLD (acme.fr vs acme.com), ou homoglyphes Unicode (acme.fr avec un 'a' cyrillique). Ces domaines sont configurés avec des enregistrements MX valides pour pouvoir envoyer et recevoir des emails. L'absence de politique DMARC sur ces domaines est exploitée dans les cas de spoofing direct du domaine légitime.

Phase 3 : Compromission de boîte mail (BEC avancé)

Dans les attaques les plus sophistiquées, l'attaquant ne se contente pas d'usurper une adresse : il compromet réellement la boîte mail du dirigeant ou du fournisseur via du spear phishing ou en exploitant des identifiants volés. Une fois l'accès obtenu, il installe silencieusement des règles de transfert automatique vers sa propre boîte, ce qui lui permet de surveiller les échanges en temps réel pendant des semaines avant d'intervenir au moment opportun. Cette technique de thread hijacking est particulièrement efficace car l'attaquant répond dans une conversation existante, avec l'historique complet, rendant la détection humaine quasi impossible.

Phase 4 : Exécution et collecte des fonds

Le message frauduleux est envoyé au moment précis où il maximise les chances de succès : début de journée pour profiter du rush matinal, vendredi après-midi pour la pression temporelle du week-end, pendant les vacances du responsable légitime. Les fonds virés transitent rapidement par des comptes mules dans plusieurs pays, puis sont convertis en cryptomonnaies ou en mandats Western Union, rendant toute récupération extrêmement difficile.

Techniques techniques : le détail que les filtres ne voient pas

Spoofing et contournement SPF/DKIM/DMARC

L'email spoofing exploite les configurations DNS incomplètes. Sans politique DMARC en mode `p=reject`, un attaquant peut envoyer un email avec l'adresse d'affichage (From header) d'un dirigeant tout en utilisant une infrastructure d'envoi différente. SPF ne protège que le domaine d'envoi technique (Return-Path / MAIL FROM), pas l'adresse visible par l'utilisateur. DKIM signe cryptographiquement le message mais ne protège pas contre l'usurpation d'adresse d'affichage. DMARC est la seule politique qui aligne ces mécanismes et peut rejeter les emails frauduleux, mais seulement si la politique est configurée en `p=reject` et non `p=none`. En 2025,

selon Valimail, plus de 60% des domaines d'entreprises françaises n'ont toujours pas de politique DMARC active.

Thread Hijacking et règles de transfert silencieuses

Une fois la boîte compromise, l'attaquant crée des règles Exchange ou M365 qui transfèrent silencieusement les emails entrants vers une adresse externe tout en les marquant comme lus. La victime ne voit rien d'anormal. L'attaquant monitore les échanges et attend le bon moment pour injecter un message frauduleux dans une conversation existante légitime. Depuis Exchange Online PowerShell, ces règles se créent avec la commande `New-InboxRule` et sont difficilement visibles depuis l'interface web standard d'Outlook.

```
 # Détecter les règles de forwarding suspectes dans M365
Get-Mailbox -ResultSize Unlimited | Get-InboxRule | Where-Object {
    $_.ForwardTo -ne $null -or $_.ForwardAsAttachmentTo -ne $null -or $_.RedirectTo -ne $null
} | Select-Object Name, MailboxOwnerID, ForwardTo, RedirectTo | Export-Csv /tmp/forwarding_rules.
```

Détection : signaux faibles et outils

Analyse DMARC et anomalies DNS

La mise en place d'un reporting DMARC (balise `rua` dans l'enregistrement DNS) permet de recevoir des rapports agrégés sur tous les emails envoyés avec votre domaine. Des outils comme DMARC Analyzer, Dmarcian ou PowerDMARC permettent de visualiser ces rapports et de détecter des tentatives de spoofing de votre propre domaine. Côté destinataire, les headers d'authentification (Authentication-Results) dans chaque email reçu indiquent si SPF, DKIM et DMARC ont passé.

Règles Exchange / Microsoft 365

La défense en profondeur dans M365 passe par plusieurs couches. Les règles de flux de messagerie (transport rules) permettent d'injecter des bannières d'avertissement sur les emails externes usurpant des domaines internes, de rejeter les emails dont le From header ne correspond pas au domaine d'envoi, et de bloquer les domaines sosies connus. Microsoft Defender for Office 365 Plan 2 intègre des fonctionnalités anti-impersonation spécifiquement conçues pour le BEC.

```
 # Règle Exchange pour bannière externe usurpant le domaine interne
New-TransportRule -Name "BEC-ExternalSpoofWarning" `
  -SenderDomainIs "votredomaine.fr" `
  -FromScope NotInOrganization `
  -PrependSubject "[ATTENTION - Expéditeur externe] " `
  -SetHeaderName "X-BEC-Warning" `
  -SetHeaderValue "External sender impersonating internal domain"
```

UEBA : détection comportementale des boîtes compromises

Les solutions UEBA (User and Entity Behavior Analytics) comme Microsoft Sentinel, Varonis ou Exabeam analysent les comportements habituels de chaque boîte mail. Des anomalies comme la création soudaine de règles de transfert, des connexions depuis des localisations inhabituelles, une activité à des heures atypiques, ou l'accès massif à des emails constituent des signaux d'alerte automatiquement remontés. L'intégration de ces alertes dans un SIEM permet une corrélation avec d'autres indicateurs.

Cas réel analysé : fraude fournisseur dans une ETI industrielle

En 2024, une ETI française du secteur industriel (200 salariés, CA 45 M€) a subi une perte de 380 000 euros via une attaque BEC de type supplier invoice. L'attaquant avait préalablement compromis la boîte mail du directeur commercial d'un fournisseur italien avec lequel l'ETI travaillait depuis 8 ans. Pendant 3 semaines, il avait lu tous les échanges. Il attendait la réception d'une facture en cours d'approbation pour 380 000 euros. Au moment exact où le service

comptable attendait le rappel téléphonique de validation habituel, l'attaquant avait envoyé — depuis la vraie boîte mail du fournisseur — un email modifiant le RIB avec un prétexte légitime (changement de banque suite à une fusion). L'email était parfaitement rédigé, dans le style habituel du contact, et référençait les échanges précédents. La comptable avait bien appelé, mais le numéro de téléphone indiqué dans l'email était celui d'un complice. Signaux d'alerte manqués : aucun appel entrant du fournisseur habituel pour confirmer la facture, légère différence dans l'adresse de retour (reply-to différent du From), et IBAN d'un pays inhabituel pour ce fournisseur.

Réponse à incident BEC : les 72 heures critiques

Actions immédiates (0-2 heures)

Dès la détection d'une tentative ou d'un virement suspect, les premières actions sont critiques. Contactez immédiatement votre banque pour demander le SWIFT recall (rappel du virement) ou le *freeze* des fonds si le bénéficiaire est dans la zone SEPA. La fenêtre d'action effective est de 24 à 72 heures maximum. Simultanément, isolez la boîte mail compromise ou suspectée : réinitialisez le mot de passe, révoquez toutes les sessions actives (dans M365 : `Revoke-AzureADUserAllRefreshToken`), supprimez les règles de transfert suspectes. Préservez l'intégralité des headers des emails suspects avant toute suppression.

Préservation des preuves

La préservation des preuves numériques est indispensable pour la plainte pénale et la relation avec l'assurance cyber. Exportez les emails complets avec leurs headers (format .eml ou .msg), capturez les journaux de connexion de la boîte mail (M365 Unified Audit Log sur 90 jours minimum), documentez la chronologie précise, et conservez les coordonnées bancaires frauduleuses. En France, l'article 323-1 du Code pénal criminalise l'accès frauduleux à un système informatique ; les preuves numériques préservées dans les règles de l'art sont recevables devant les tribunaux.

Notifications obligatoires

En cas de virement supérieur à 10 000 euros vers un compte frauduleux, l'entreprise peut être tenue de signaler l'incident à TRACFIN (Traitement du renseignement et action contre les circuits financiers clandestins). Le dépôt de plainte auprès de la BEFTI (Brigade d'enquêtes sur les fraudes aux technologies de l'information) est fortement recommandé — c'est la condition nécessaire pour la prise en charge par l'assurance cyber. Si des données personnelles ont été compromises (emails de clients, données RH), une notification à la CNIL sous 72 heures est obligatoire au titre du RGPD.

Mesures préventives : la checklist anti-BEC en 15 points

La prévention du BEC repose sur trois piliers : technique, procédural et humain. Voici les 15 mesures fondamentales.

Pilier technique :

DMARC p=reject — Configurez votre DNS avec `v=DMARC1; p=reject; rua=mailto:dmarc@votredomaine.fr`. C'est la mesure technique la plus impactante.

SPF strict — Utilisez `~all` au minimum, idéalement `-all` pour rejeter les emails non autorisés.

DKIM sur tous les flux — Signez cryptographiquement tous les emails sortants, y compris les emails de services SaaS (Salesforce, Hubspot, etc.) via CNAME.

MFA sur toutes les boîtes mail — Prioritairement sur les comptes de direction, finance et RH. Préférez FIDO2/passkeys aux SMS.

Bannières email externe — Injection automatique d'un avertissement visible sur tous les emails provenant de l'extérieur.

Blocage des règles de transfert externe — Dans M365, désactivez la possibilité pour les utilisateurs de créer des règles redirigeant vers des adresses externes.

Monitoring des connexions anormales — Alertes automatiques sur connexions depuis de nouveaux pays ou à des heures inhabituelles.

Pilier procédural :

Double validation téléphonique des virements — Tout virement au-delà d'un seuil défini (ex : 5 000 €) requiert une confirmation vocale sur un numéro préenregistré, jamais sur un numéro fourni dans l'email.

Blocage des modifications de RIB par email seul — Toute demande de changement de coordonnées bancaires doit passer par un formulaire signé + vérification via canal indépendant.

Liste blanche des IBAN fournisseurs — Base de données des IBAN valides par fournisseur avec processus de modification contrôlé.

Procédure d'urgence connue — Chaque employé en contact avec des finances doit connaître le contact direct de sa banque pour un rappel de virement d'urgence.

Pilier humain :

Formation anti-BEC spécifique — Simulations de CEO fraud et fausse facture, pas seulement du phishing générique.

Culture "ça m'arrive aussi" — Déstigmatiser le signalement des tentatives et des erreurs pour favoriser la remontée d'incidents.

Vérification des signaux d'alerte — Former à reconnaître : urgence anormale, demande de confidentialité, changement de RIB par email, numéro de téléphone fourni dans l'email de demande.

Test régulier des procédures — Réaliser trimestriellement un test de résistance sur le processus de validation des virements.

Configuration DMARC complète : exemple pratique

La configuration DMARC est souvent mal implémentée. Voici un exemple complet d'enregistrement DNS pour un déploiement production.

```
 ; SPF - autoriser seulement les serveurs légitimes
votredomaine.fr. IN TXT "v=spf1 include:_spf.google.com include:mailjet.net ip4:203.0.113.10 -all

; DKIM - publier la clé publique (générée depuis votre MTA)
mail._domainkey.votredomaine.fr. IN TXT "v=DKIM1; k=rsa; p=MIGfMA0GCSqGS..."

; DMARC - politique de rejet avec rapports
_dmarc.votredomaine.fr. IN TXT "v=DMARC1; p=reject; sp=reject; pct=100; rua=mailto:dmarc-rua@votr
```

La transition vers `p=reject` doit être progressive : commencez par `p=none` pour collecter les rapports, passez à `p=quarantine; pct=10`, puis augmentez progressivement jusqu'à `p=reject; pct=100`. Cette transition prend généralement 4 à 8 semaines pour ne pas bloquer des flux email légitimes non encore couverts par SPF/DKIM.

Pour une analyse approfondie des techniques d'attaque AiTM qui contournent la MFA et vont au-delà du BEC classique, consultez notre article sur Evilginx et le phishing AiTM qui bypasse la MFA. Le durcissement de votre infrastructure email Microsoft est couvert en détail dans notre guide sur le durcissement Exchange Online et anti-phishing. Si votre organisation utilise M365, notre livre blanc sécurité Microsoft 365 détaille l'ensemble de la posture de sécurité. Enfin, la vulnérabilité récente Microsoft 365 Copilot de 2025 illustre comment les surfaces d'attaque évoluent dans les suites collaboratives.

Cadre légal français : déclaration et recours

En France, la réponse judiciaire au BEC repose sur plusieurs dispositifs complémentaires. La BEFTI, rattachée à la Direction de la Police Judiciaire de la Préfecture de Police de Paris, est spécialisée dans les fraudes aux technologies de l'information. Le dépôt de plainte (ou la pré-plainte en ligne sur masecurite.interieur.gouv.fr) déclenche l'enquête judiciaire. Parallèlement, l'OCRGDF (Office Central pour la Répression de la Grande Délinquance Financière) peut être saisi pour les montants importants.

TRACFIN, le service de renseignement financier de Bercy, doit être notifié pour les transactions suspectes dépassant les seuils légaux. Les établissements financiers sont soumis à cette obligation de déclaration, mais les entreprises victimes peuvent également transmettre des

informations directement. Cybermalveillance.gouv.fr (ACYMA) propose une assistance aux victimes et une mise en relation avec des prestataires certifiés PRIS (Prestataires de Réponse aux Incidents de Sécurité).

Sur le plan de la récupération des fonds, la procédure de recall SWIFT permet dans certains cas de bloquer le virement si la contrepartie bancaire coopère. Dans la zone SEPA, la procédure d'urgence auprès de la banque dans les 24 à 72 heures peut aboutir à un gel des fonds. Au-delà, la récupération passe par une procédure judiciaire internationale (commission rogatoire) dont le taux de succès est faible.

Les ressources officielles de référence incluent le rapport annuel de l'Internet Crime Complaint Center (IC3) qui documente les tendances BEC mondiales, et le portail cybermalveillance.gouv.fr pour l'assistance aux victimes et les ressources de prévention françaises.

FAQ — Questions fréquentes sur le BEC

Comment savoir si notre boîte mail de direction a été compromise et surveille nos échanges ?

Plusieurs indicateurs permettent de détecter une compromission silencieuse. Vérifiez les règles de messagerie depuis Exchange Admin Center ou via PowerShell (`Get-InboxRule -Mailbox CEO@entreprise.fr`) à la recherche de règles de transfert vers des adresses inconnues. Analysez les journaux de connexion (M365 Unified Audit Log, onglet Connexions dans Azure AD) pour repérer des connexions depuis des IP ou des pays inhabituels. Vérifiez les appareils enregistrés dans le compte : un appareil inconnu est un signal fort. Enfin, Microsoft Secure Score et les alertes Identity Protection peuvent signaler des comportements anormaux de connexion en temps réel.

Notre assurance cyber couvre-t-elle le BEC, et quelles sont les conditions ?

La plupart des polices cyber modernes couvrent les pertes financières liées au BEC, mais les conditions varient significativement. Les assureurs exigent généralement : un dépôt de plainte dans les délais impartis, la preuve que des mesures de sécurité minimales étaient en place (DMARC, MFA), et souvent une procédure documentée de validation des virements. Certaines polices excluent les pertes dues au "social engineering" si elles ne sont pas explicitement couvertes. Lisez attentivement les exclusions et demandez à votre courtier une clarification sur la couverture BEC avant de souscrire.

Un fournisseur dont la boîte a été compromise peut-il être tenu responsable des pertes subies ?

La question de la responsabilité du fournisseur est complexe sur le plan juridique français. Si la compromission de la boîte mail du fournisseur est établie et qu'il n'avait pas mis en place de mesures de sécurité minimales (MFA, détection d'intrusion), une action en responsabilité civile délictuelle peut être envisageable. Cependant, la jurisprudence en la matière est encore limitée. La plupart des dossiers aboutissent à un partage de responsabilité, voire à l'absence de condamnation du fournisseur si les mesures de sécurité étaient dans la norme du secteur. La prévention reste préférable au contentieux.

