Baromètre des fuites de données personnelles

ÉDITION 2026

Ce baromètre est élaboré par le Forum INCYBER en partenariat avec Hexatrust et avec la participation de la CNIL pour les données en *open data*.

IN CYBER FORUM EUROPE

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

édito

Fuites de données personnelles : 2025, le changement d'échelle

En 2025, les brèches se sont multipliées, touchant successivement le secteur de la santé via des prestataires de tiers payant, des opérateurs télécom, des administrations publiques déjà fragilisées et même des dispositifs d'aide sportive gérés par l'État.

La question n'était plus de savoir « si » une fuite allait survenir, mais « où » et « par qui ». Sur la période septembre 2024 — septembre 2025, 8 613 violations de données personnelles ont été notifiées à la CNIL, contre 5 919 un an plus tôt — une hausse de 45 % en un an. Rapporté au quotidien, cela représente près de 24 fuites par jour, contre 16 l'an dernier. Une fuite toutes les heures.

Cette banalisation se lit aussi du côté des victimes. En 2025, Cybermalveillance.gouv.fr a enregistré environ un demi-million de demandes d'assistance via le dispositif 17Cyber, contre un peu plus de 420 000 en 2024 et 280 000 en 2023. Une progression continue, qui traduit moins une montée soudaine de la vigilance qu'une exposition devenue structurelle des particuliers comme des organisations.

Cette cascade d'incidents, frappant des organisations très diverses, a un point commun : elle consacre l'industrialisation de la cybercriminalité. La France a ainsi vécu une véritable « année noire » en matière de données personnelles.

Les attaquants ont délaissé les attaques opportunistes au profit de cibles à fort effet de levier. Ils ciblent désormais les hubs : plateformes ultra-centralisées, prestataires mutualisés et briques techniques partagées. Une seule faille suffit à ouvrir la porte à des volumes colossaux de profils. Administrations publiques, télécoms, santé… tous exposés pour les mêmes failles récurrentes : accès mal contrôlés, dépendances tiers ingérables, systèmes informatiques trop complexes, maturité sécurité à la traîne face à la digitalisation effrénée.

Autre mutation : l'usage des données volées. Elles alimentent une économie structurée — revente, enrichissement, fraudes à la carte — mais servent aussi à déstabiliser. Montrer qu'un État ou un grand service ne protège plus ses citoyens, c'est déjà gagner la bataille de l'opinion. Et certaines informations – numéro de Sécurité sociale, identifiants administratifs – sont irrémédiables : impossible de les « réinitialiser » comme un mot de passe.

La leçon de 2025 n'est pas « soyons plus vigilants ». C'est réduire l'impact à la source. NIS2 et DORA imposent des règles, mais c'est l'exécution qui change la donne : MFA généralisée sans exception, gestion stricte des accès et supervision renforcée des tiers, segmentation des réseaux ou encore détection et réponse ultra-rapides.

Et le vrai point aveugle, souvent politique : la minimisation. Collecter moins. Conserver moins longtemps. Centraliser moins. En 2025, le luxe ultime en cybersécurité ? Ne pas avoir autant de données à perdre. 2026 sera-t-elle l'année du sursaut, ou celle de la résignation ?

Mélissa PÉRIÉ BETTON
Rédactrice en chef
INCYBER News

8 613 violations de données personnelles ont été notifiées à la CNIL

Sur la période septembre 2024 – septembre 2025, contre 5 919 un an plus tôt, soit une hausse de 45 % en un an.

Typologie et nature des incidents en 2025

Les données 2025 confirment une évolution nette du paysage des incidents de sécurité, marquée par la montée en puissance des fuites malveillantes et des actes externes.

Fuites accidentelles

2024 2025

1 284
1 655
+28,9 %

...dont fuites accidentelles avec données sensibles

259
346
+33,6 %

Fuites malveillantes

3 649
5 841
+60,1 %

Nature des incidents

ACTES EXTERNES

3 730
5 905
+58,3 %

ACTES INTERNES

1 736
+22,2 %

385
actes malveillants

Les fuites d'origine malveillante enregistrent la plus forte hausse. Leur nombre passe de 3 649 en 2024 à 5 841 en 2025, soit une augmentation de 60,1 %. Elles constituent désormais la majorité des fuites observées, traduisant une montée en puissance des actions intentionnelles. Cette progression est notamment alimentée par la généralisation du *phishing*, des *infostealers* et du vol d'identifiants, désormais au cœur des scénarios d'attaque.

Les fuites accidentelles progressent également, mais à un rythme plus modéré. Elles passent de 1 284 à 1 655 incidents sur un an, soit +28,9 %. Cette hausse s'accompagne d'un impact accru : 346 fuites accidentelles impliquent des données sensibles, contre 259 en 2024, soit une augmentation de 33,6 %. Au-delà des volumes, ces fuites exposent de plus en plus des données sensibles et des accès critiques, augmentant fortement les impacts opérationnels et réglementaires pour les organisations.

Par ailleurs, une part significative des incidents trouve son origine au niveau du poste de travail. Celui-ci est devenu un point d'entrée privilégié pour les attaques, en raison de l'usage simultané de la navigation web, de la messagerie et des accès aux applications métier sur un même environnement.

Cette évolution se reflète dans la nature des incidents. En 2025, les actes d'origine externe atteignent 5 905 incidents, contre 3 730 l'année précédente (+58,3 %). Ils constituent désormais la principale source d'incidents. Les actes internes restent plus limités, avec 1 736 incidents recensés, dont 385 de nature malveillante, soit 22,2 % des actes internes.

Chaque jour en France, 24 fuites de données sont déclarées à la CNIL

En 2025, leur nombre connaît un essor sans précédent, atteignant 8 613 notifications, soit une augmentation de 45 % par rapport à 2024

focus assurance

Assurance cyber : un marché sous tension, un rôle de courtier en mutation

Le risque cyber s'est imposé comme l'un des risques majeurs pour les entreprises. En France, la hausse continue des incidents traités par l'ANSSI et le fait que près de deux entreprises sur trois déclarent avoir subi au moins une cyberattaque, traduisent un changement d'échelle durable. Les fuites de données et les rançongiciels demeurent la principale source de sinistres, avec des impacts majeurs, liés notamment à l'interruption d'activité et à la gestion de crise. Le cyber n'est plus un sujet uniquement technique : il affecte directement la continuité d'activité, la responsabilité juridique et la gouvernance.

Face à cette sinistralité croissante, le marché de l'assurance cyber a gagné en maturité. Les primes mondiales dépassent 14 milliards de dollars et devraient doubler d'ici 2027. Cette dynamique s'accompagne parfois d'un durcissement des conditions : exclusions élargies, franchises renforcées et exigences accrues en matière de cybersécurité. L'assurance cyber est devenue conditionnelle : les assureurs évaluent désormais la capacité réelle des entreprises à prévenir, détecter et gérer une attaque, au-delà de leur seul secteur ou chiffre d'affaires.

Dans ce contexte, le rôle du courtier en assurance évolue profondément. Il ne s'agit plus seulement de placer une police, mais de structurer l'assurabilité du risque. L'expérience de terrain de Verspieren montre que l'accès à une couverture efficace repose sur une compréhension fine de l'exposition réelle, l'identification de scénarios de pertes crédibles et la maîtrise de la rédaction contractuelle. La police d'assurance cyber est un objet complexe, dont la portée effective dépend étroitement des clauses négociées en amont.

La valeur de l'assurance se révèle pleinement au moment du sinistre. La gestion d'une attaque cyber impose une coordination rapide entre experts techniques, juridiques et assureurs, sous forte pression opérationnelle. Chaque sinistre constitue un accélérateur de maturité, permettant de réaligner prévention et couverture assurantielle.

À l'heure des nouvelles réglementations européennes (NIS2, DORA) et de la judiciarisation croissante des incidents, l'assurance cyber s'inscrit durablement dans la gouvernance globale des risques. Le courtier spécialisé en cyber occupe donc une position stratégique : celle d'un tiers de confiance capable de traduire un risque technique complexe en un dispositif de protection cohérent.

Diego SAINZ
Référent Technique Cyber
Groupe Verspieren

VERSPIEREN
COURTIER EN ASSURANCES

Secteurs les plus touchés

	2024	2025	
ACTIVITÉS FINANCIÈRES & ASSURANCE	885	2 153	+143 %
ACTIVITÉS SPÉCIALISÉES, SCIENTIFIQUES & TECHNIQUES	631	1 535	+143 %
SANTÉ HUMAINE & ACTION SOCIALE	591	858	+45,2 %
ADMINISTRATION PUBLIQUE	937	979	+4,3 %
COMMERCE & RÉPARATION AUTO-MOTO	615	915	+25,6 %

Ampleur et impact des fuites

ESTIMATION DU TOTAL DE PERSONNES IMPACTÉES	8 millions	12,2 millions	+53 %

Typologie et nature des incidents en 2025

Les données 2025 confirment une évolution nette du paysage des incidents de sécurité, marquée par la montée en puissance des fuites malveillantes et des actes externes.

JANVIER

Kiabi

Vecteur : **Faille dans l'application**
Données concernées : **IBAN**
Impact potentiel : **20 000 clients**

Chronopost
(Groupe La Poste)

Vecteur : **Faille dans l'application**
Données concernées : **signatures, coordonnées, numéros de téléphone**
Impact potentiel : **210 000 clients**

FÉVRIER

Conforama

Vecteur : ***Credential stuffing*** **(non officiel)**
Données concernées : **Données personnelles**
Impact potentiel : **9,4 millions de clients**

Harvest (éditeur logiciel)

Vecteur : **Compromission d'identifiants avec contournement de l'authentification multi-facteurs**
Données concernées : **informations clients (nom, identifiants et mots de passe)**
Impact indirect potentiel : **55 000 clients de la MAIF mais aussi de BPCE, d'Axa France ou de Swiss Life**

Caisse des dépôts

Vecteur : **Compromission d'identifiants d'employeurs publics (accès frauduleux via comptes légitimes)**
Données concernées : **Noms, prénoms, dates et lieux de naissance, et numéro de sécurité sociale**
Impact potentiel : **70 000 personnes**

MARS

La Poste

Vecteur : **Intrusion via le site Élection du timbre**
Données concernées : **Données personnelles**
Impact potentiel : **50 000 utilisateurs**

Autosur

Vecteur : **Exposition de bases de données mal sécurisées**
Données concernées : **Jusqu'à 10 millions de plaques d'immatriculation et coordonnées clients**
Impact potentiel : **Environ 4 millions de personnes**

Intersport

Vecteur : **Accès frauduleux au système d'information via un accès compromis (revente d'accès)**
Données concernées : **Données identitaires : adresses postales, numéros de téléphone, mail, noms, prénoms**
Impact potentiel : **3,3 millions de personnes**

Alain Afflelou

Vecteur : **Faille de sécurité chez un prestataire externe**
Données concernées : **Identité, coordonnées, historique d'achat, mutuelles**
Impact potentiel : **1,5 millions de personnes**

Easy Cash

Vecteur : **Incident de cybersécurité localisé sur l'ordinateur d'un magasin**
Données concernées : **Identité, dates de naissance**
Impact potentiel : **92 000 clients**

MAI

Dior

Vecteur : **Accès non autorisé à une base de données clients (modalités techniques non précisées)**
Données concernées : **Données personnelles des clients asiatiques**
Impact potentiel : **20 000 clients**

JUIN

Sorbonne Université

Vecteur : **Intrusion informatique ayant entraîné une compromission de systèmes (non précisé publiquement)**
Données concernées : **Données sensibles compromises incluent des adresses e-mail professionnelles, des coordonnées bancaires et des numéros de sécurité sociale**
Impact potentiel : **32 000 utilisateurs**

Les données personnelles immuables

Certaines données personnelles sont immuables ou non réinitialisables, ce qui les rend particulièrement sensibles en cas de fuite :

- → **Numéro de Sécurité sociale (NIR) : attribué à la naissance, unique et permanent pour chaque personne**
- → **Données biométriques : empreintes digitales, reconnaissance faciale… uniques et impossibles à modifier**
- → **Données génétiques : ADN, profil génétique… immuables et identifiables de manière unique**

Pourquoi c'est important : contrairement à un mot de passe, ces informations ne peuvent pas être « réinitialisées ».
Une fois exposées, le risque lié à ces données persiste toute la vie.

Cadre légal : le RGPD les considère comme des données sensibles, nécessitant une protection renforcée et des traitements stricts. (cnil.fr)

OCTOBRE

France Travail

Vecteur : **Compromission d'identifiants professionnels**
Données concernées : **1,6 millions de personnes concernées (attestations de Sécurité sociale, contrats de travail, données sensibles)**
Impact potentiel : **1,6 million de personnes**

URSSAF (Pajemploi)

Vecteur : **Accès non autorisé à un système de traitement de données (vol de données)**
Impact potentiel : **Environ 1,2 million de comptes**

NOVEMBRE

Fédération française de Tir (FFTir)

Vecteur : **Accès non autorisé à un système de traitement de données**
Données concernées : **Identité, adresses de contact**
Impact potentiel : **1 million de données de licenciés et anciens licenciés**

Weda

Vecteur : **Accès non autorisés via comptes compromis**
Données concernées : **Dossiers médicaux complets, identité des patients, numéro de Sécurité sociale, coordonnées, données de facturation**
Impact potentiel : **23 000 professionnels impactés (sur 85 000 utilisateurs revendiqués)**

AOÛT

Bouygues Telecom

Vecteur : **Accès non autorisé à des systèmes de traitement de données (origine non communiquée)**
Données concernées : **Données personnelles (contacts, civilité, données contractuelles, IBAN pour certains profils)**
Impact potentiel : **Environ 6,4 millions de comptes**

JUILLET

Air France

Vecteur : **Compromission d'un prestataire tiers (accès frauduleux à un système externe de relation client)**
Données concernées : **Données clients (périmètre en cours d'évaluation)**
Impact potentiel : **Données non publiques**

SEPTEMBRE

Hôpitaux publics des Hauts-de-France

Vecteur : **Compromission d'identifiants professionnels**
Données concernées : **Données d'identité des patients**
Impact potentiel : **Données non publiques**

DÉCEMBRE

Caisse des allocations familiales (CAF)

Vecteur : **Exfiltration via un tiers**
Données concernées : **Données d'identité et de contact**
Impact potentiel : **22 millions de lignes (équivalent ~3,5–8 millions foyers allocataires, données Pass'Sport)**

Ministère de l'Intérieur

Vecteur : **Compromission de l'infrastructure de messagerie interne**

Données concernées : **Documents internes confidentiels issus des serveurs de messagerie et fichiers de police sensibles, dont : des éléments issus du Traitement des antécédents judiciaires (TAJ) ; des informations liées au Fichier des personnes recherchées (FPR)**

Ces fichiers peuvent contenir, selon les cas : identités, données administratives, informations judiciaires (personnes mises en cause, victimes, personnes recherchées).

SCÉNARIO 1

Le prestataire comme point d'entrée

POINT D'ENTRÉE

Compromission d'un compte ou d'une infrastructure chez un prestataire (tiers payant, infogérant, éditeur SaaS, centre d'appels, etc.).

MÉCANISME

Un accès légitime est utilisé pour se connecter à une plateforme mutualisée. Les contrôles de segmentation sont insuffisants, permettant un accès transversal aux données de plusieurs clients.

TYPE DE DONNÉES EXPOSÉES

Données personnelles à grande échelle, souvent sensibles (santé, identifiants administratifs).

FACTEURS AGGRAVANTS

- → Accès persistants non révoqués
- → Absence de supervision des activités du prestataire
- → Concentration massive de données chez un acteur unique, etc.

CONSTAT CLÉ

Une seule compromission, des millions de personnes exposées. Le risque n'est plus local, il est systémique.

SCÉNARIO 2

Phishing + MFA absent ou contourné

Quand l'attaquant se connecte « normalement »

POINT D'ENTRÉE

Courriel de *phishing* ciblé (employé, prestataire, support IT).

MÉCANISME

Vol d'identifiants, puis connexion aux systèmes internes. Dans de nombreux cas, l'absence de MFA (authentification multifacteur) ou son contournement (fatigue MFA, validation automatique) permet une intrusion sans exploitation technique avancée.

TYPE DE DONNÉES EXPOSÉES

Bases clients, données RH, documents internes, parfois données sensibles.

FACTEURS AGGRAVANTS

- → MFA partiel ou mal configuré
- → Droits d'accès trop larges
- → Journalisation insuffisante, etc.

CONSTAT CLÉ

L'attaque ne ressemble plus à une attaque.
Elle emprunte les chemins de l'utilisateur légitime.

Analyse des *modus operandi* et leviers de prévention clés

SCÉNARIO 3

Mauvaise configuration *Cloud*

La fuite sans attaquant visible

POINT D'ENTRÉE

Configuration erronée d'un service *Cloud* (stockage, base de données, API).

MÉCANISME

Données accessibles sans authentification forte, parfois indexées ou explorables via des requêtes automatisées.

TYPE DE DONNÉES EXPOSÉES

Données personnelles brutes, parfois issues d'environnements de test ou de sauvegarde.

FACTEURS AGGRAVANTS

- → Reprise de données réelles en préproduction
- → Absence d'audit de configuration
- → Responsabilités floues entre équipes IT et métiers, etc.

CONSTAT CLÉ

La fuite peut durer des mois sans déclencher d'alerte. Elle est souvent découverte par un tiers.

SCÉNARIO 4

Ransomware avec exfiltration préalable

La fuite comme arme de pression

POINT D'ENTRÉE

Accès initial via *phishing*, vulnérabilité non corrigée ou prestataire compromis.

MÉCANISME

Exfiltration discrète des données avant chiffrement. La fuite devient un levier autonome : menace de publication, revente ou exploitation frauduleuse.

TYPE DE DONNÉES EXPOSÉES

Données clients, données internes stratégiques, parfois données immuables.

FACTEURS AGGRAVANTS

- → Détection tardive
- → Sauvegardes non isolées
- → Plans de réponse incomplets, etc.

CONSTAT CLÉ

Même sans paiement, la fuite est irréversible. Le chiffrement n'est plus l'enjeu principal.

Prévenir les fuites : où casser la chaîne d'attaque ?

La fuite comme arme de pression

SCÉNARIO OBSERVÉ EN 2025	POINT DE RUPTURE CRITIQUE	LEVIER RÉELLEMENT EFFICACE
Prestataire compromis	Accès tiers trop larges et persistants	IAM strict + segmentation
Phishing / vol d'identifiants	Connexion légitime non détectée	MFA généralisée + supervision
Mauvaise configuration *Cloud*	Exposition publique prolongée	Gouvernance *Cloud* + audits
Ransomware avec exfiltration	Extraction silencieuse des données	Détection + chiffrement

Prévenir les fuites de données
LEVIERS CLÉS

Réduction de la surface d'exposition

La plupart des fuites massives de 2025 ont un point commun : trop de données accessibles depuis trop peu de points. Réduire la surface d'exposition consiste à limiter la centralisation, restreindre les périmètres d'accès et raccourcir les durées de conservation. Ce levier n'empêche pas l'intrusion, mais il en limite immédiatement l'ampleur.

Gestion des accès et des identités (IAM)

En 2025, l'attaque commence le plus souvent par une connexion réussie. Une gestion stricte des identités — MFA généralisée, droits minimaux, accès temporaires — permet de contenir la propagation après compromission. L'IAM *(Identity Access Management)* ne supprime pas le risque, mais il empêche un accès légitime de devenir un accès illimité.

Sécurisation des environnements *Cloud*

Le *Cloud* n'est pas intrinsèquement plus vulnérable, mais il rend les erreurs plus rapides et plus massives. La sécurisation repose moins sur la technologie que sur la gouvernance : configurations contrôlées, audits réguliers et responsabilités clairement définies entre équipes internes et prestataires. Sans cela, une simple erreur devient une fuite silencieuse.

Chiffrement des données

Le chiffrement ne prévient pas la fuite, mais il en réduit drastiquement les conséquences. Données chiffrées au repos et en transit, clés protégées et isolées : en cas d'exfiltration, les données volées deviennent inexploitables. C'est un levier de résilience, pas une protection absolue.

Gérer un incident de fuite de données

De la détection à la maîtrise de l'impact

En 2025, la gravité d'une fuite tient moins à son existence qu'à la manière dont elle est détectée, qualifiée et gérée dans les premières heures. Les retours d'incidents montrent que les organisations échouent rarement sur la technique seule, mais sur la coordination et le tempo.

Détection et qualification

La détection tardive reste le principal facteur d'aggravation. Dans de nombreux cas, la fuite est identifiée après une alerte externe. La priorité n'est pas de comprendre tout de suite l'origine exacte, mais de qualifier rapidement trois éléments clés : nature des données exposées, volume potentiel, et statut de l'attaque (en cours ou terminée). Sans cette qualification initiale, toute décision ultérieure est fragilisée.

Rôles et coordination des équipes

La gestion de crise efficace repose sur une répartition claire des responsabilités, dès les premières heures.

- → RSSI / IT : contenir l'incident, sécuriser les accès, préserver les preuves techniques.
- → DPO : évaluer l'impact sur les données personnelles, qualifier les risques pour les personnes concernées, piloter la conformité réglementaire.
- → Juridique : sécuriser les décisions, anticiper les risques contentieux, encadrer la communication.
- → Direction / communication : arbitrer, assumer la prise de parole et éviter les messages contradictoires.

L'absence de coordination formalisée entre ces fonctions est l'un des angles morts les plus fréquents observés en 2025.

Notification à la CNIL et communication

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

La notification à la CNIL n'est pas un simple exercice déclaratif. Elle engage la crédibilité de l'organisation. Une notification tardive, incomplète ou incohérente avec la communication publique fragilise durablement la gestion de crise.

La communication externe doit répondre à un objectif unique : informer sans aggraver. Minimiser expose à un effet boomerang, sur-communiquer crée de la confusion. La cohérence entre les messages adressés à la CNIL, aux personnes concernées et aux partenaires est un facteur clé de résilience.

Les erreurs classiques qui transforment un incident en crise

ATTENDRE D'AVOIR « TOUTES LES RÉPONSES » AVANT D'AGIR

En 2025, les organisations qui retardent la qualification ou la notification dans l'espoir de clarifier la situation perdent du temps critique. L'incertitude n'excuse pas l'inaction.

SOUS-ESTIMER L'IMPACT HUMAIN

Raisonner uniquement en termes techniques ou juridiques conduit à minimiser le risque pour les personnes concernées. Cette approche est régulièrement sanctionnée a posteriori, sur le plan réglementaire comme réputationnel.

GÉRER L'INCIDENT EN SILOS

RSSI, DPO, IT, juridique et communication agissent encore trop souvent de manière séquentielle. Or une décision technique peut avoir des conséquences juridiques ou médiatiques immédiates.

DÉCOUVRIR LA CNIL AU MOMENT DE LA CRISE

L'absence de relation préalable avec la CNIL complique la notification et alourdit le dialogue en situation d'urgence.

MINIMISER PUBLIQUEMENT, CORRIGER EN PRIVÉ

Les messages incohérents entre communication externe, notification réglementaire et informations transmises aux partenaires constituent l'un des principaux facteurs de perte de confiance observés en 2025.

Assurance, résilience et reprise

Après la fuite, ce qui tient… et ce qui ne tient pas

En 2025, l'après-incident est devenu une phase aussi critique que l'attaque elle-même. Assurance cyber, équipes internes, prestataires de réponse à incident et capacités de reprise sont désormais mobilisés presque systématiquement. Mais leur efficacité dépend moins de leur existence que de leur préparation en amont.

Le rôle des assureurs cyber

L'assurance cyber n'est ni une protection, ni une solution de rattrapage. Elle intervient après la fuite, pour financer, coordonner et parfois accélérer la gestion de crise. En pratique, les assureurs jouent un rôle de chef d'orchestre : mise à disposition de prestataires (forensic, juridique, communication), aide à la prise de décision, cadrage des coûts.

Mais en 2025, les conditions se durcissent. Les assureurs exigent des preuves de maturité (MFA, sauvegardes, procédures) et limitent de plus en plus les garanties en cas de défaillances connues. L'assurance ne compense plus l'absence de prévention.

Coordination avec les équipes internes

Une assurance cyber efficace suppose une organisation interne déjà structurée. Sans articulation claire entre RSSI, DPO, IT, juridique et direction, l'intervention de l'assureur ralentit au lieu d'accélérer la gestion de crise.

Les incidents les mieux maîtrisés sont ceux où :

- → Les rôles sont définis avant l'incident
- → Les canaux de décision sont identifiés
- → L'assureur est intégré au dispositif de crise, et non sollicité en urgence sans contexte, etc.

Sauvegardes et *data recovery*

Les sauvegardes restent un pilier de la résilience, mais leur simple existence ne suffit plus. En 2025, de nombreux incidents montrent des sauvegardes :

- → incomplètes
- → trop anciennes
- → ou compromises en même temps que les systèmes de production

La capacité de reprise repose sur des sauvegardes isolées, régulièrement mises à jour et protégées contre les accès non autorisés. Sans cela, la restauration devient théorique.

Tests de restauration

Le test est le grand impensé de la résilience. Beaucoup d'organisations découvrent en situation de crise que leurs procédures de restauration ne fonctionnent pas comme prévu.

Tester régulièrement la restauration, c'est :

- → Vérifier les délais réels de reprise
- → Identifier les dépendances critiques
- → Réduire l'incertitude au moment où le temps devient un facteur clé, etc.

En 2025, les organisations résilientes ne sont pas celles qui n'ont pas d'incident, mais celles qui savent revenir à un état maîtrisé.

Ce que 2025 a réellement changé

CE QUI NE CHANGE PAS

Les mécanismes de fuite restent largement identiques. *Phishing,* erreurs de configuration, accès trop larges, dépendances tierces mal maîtrisées : rien de fondamentalement nouveau sur le plan technique.

La sophistication des attaques progresse moins vite que la répétition des mêmes failles organisationnelles. En 2025, la majorité des incidents auraient pu être évités ou fortement limités par des mesures déjà connues et documentées.

CE QUI S'AGGRAVE

L'ampleur et la portée des fuites augmentent nettement. Une compromission n'expose plus un système, mais des écosystèmes entiers. La centralisation des données, la mutualisation des services et l'interconnexion croissante des acteurs transforment chaque incident en risque systémique.

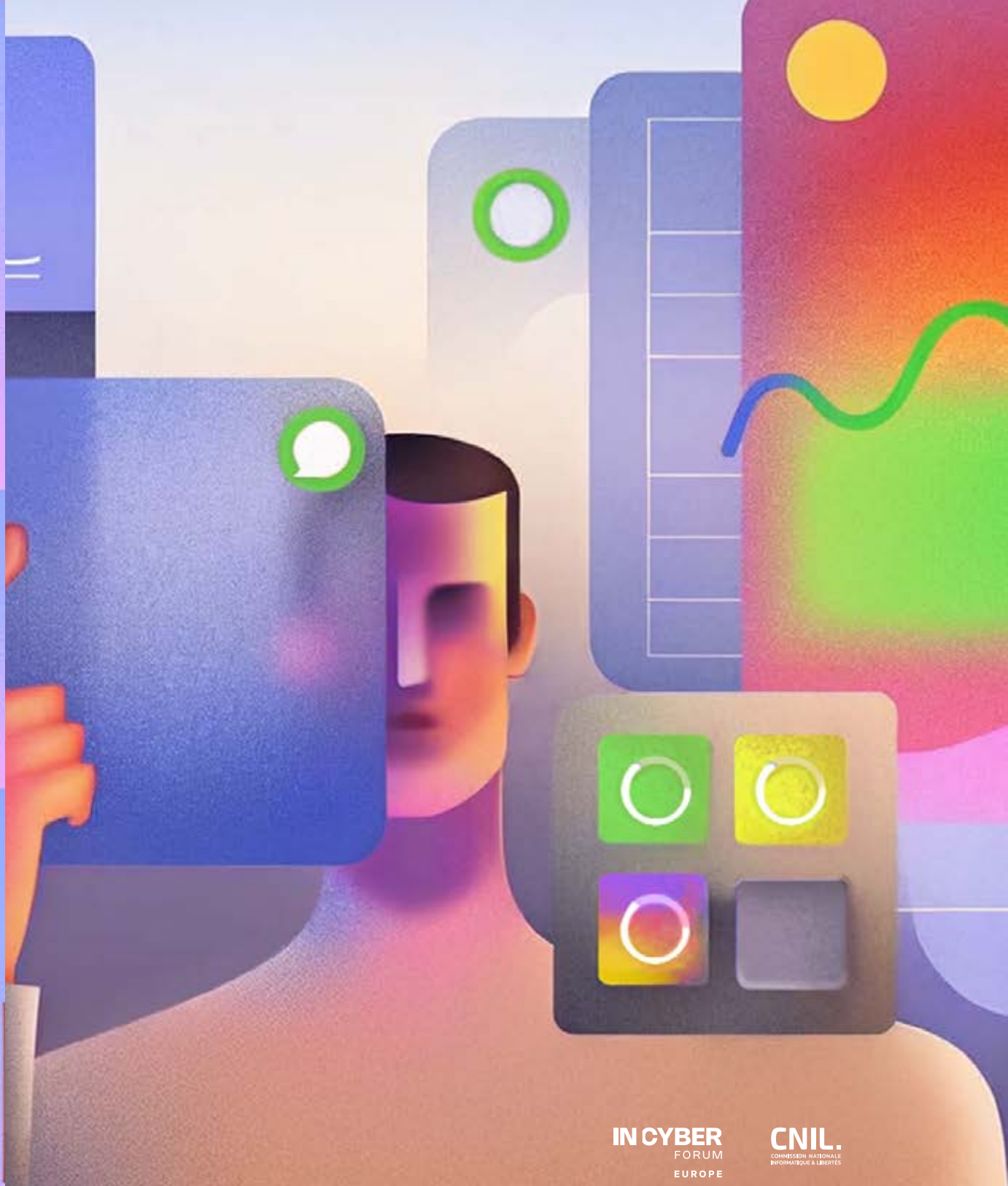
Parallèlement, l'impact humain s'alourdit. Le nombre de personnes concernées progresse plus vite que le nombre d'incidents, signe que chaque fuite touche désormais des volumes beaucoup plus importants, souvent avec des données difficilement ou impossibles à renouveler.

LES ANGLES MORTS PERSISTANTS

Malgré les alertes répétées, plusieurs angles morts demeurent largement sous-traités :

- → La minimisation des données, encore perçue comme une contrainte réglementaire plutôt qu'un levier de réduction du risque.
- → Les accès tiers, toujours traités comme un risque secondaire alors qu'ils constituent un vecteur central.
- → La détection, trop souvent passive, avec des incidents découverts par des acteurs externes.
- → La préparation à la crise, souvent pensée après coup, alors qu'elle conditionne l'impact réel d'une fuite.

Ces angles morts ne relèvent pas d'un déficit technologique, mais de choix organisationnels et de priorités.



IN CYBER FORUM EUROPE

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

Sources

CNIL
ANSSI
CERT
Cybermalveillance.gouv
Libération
Global Security Mag

Baromètre des fuites de données personnelles

ÉDITION 2026