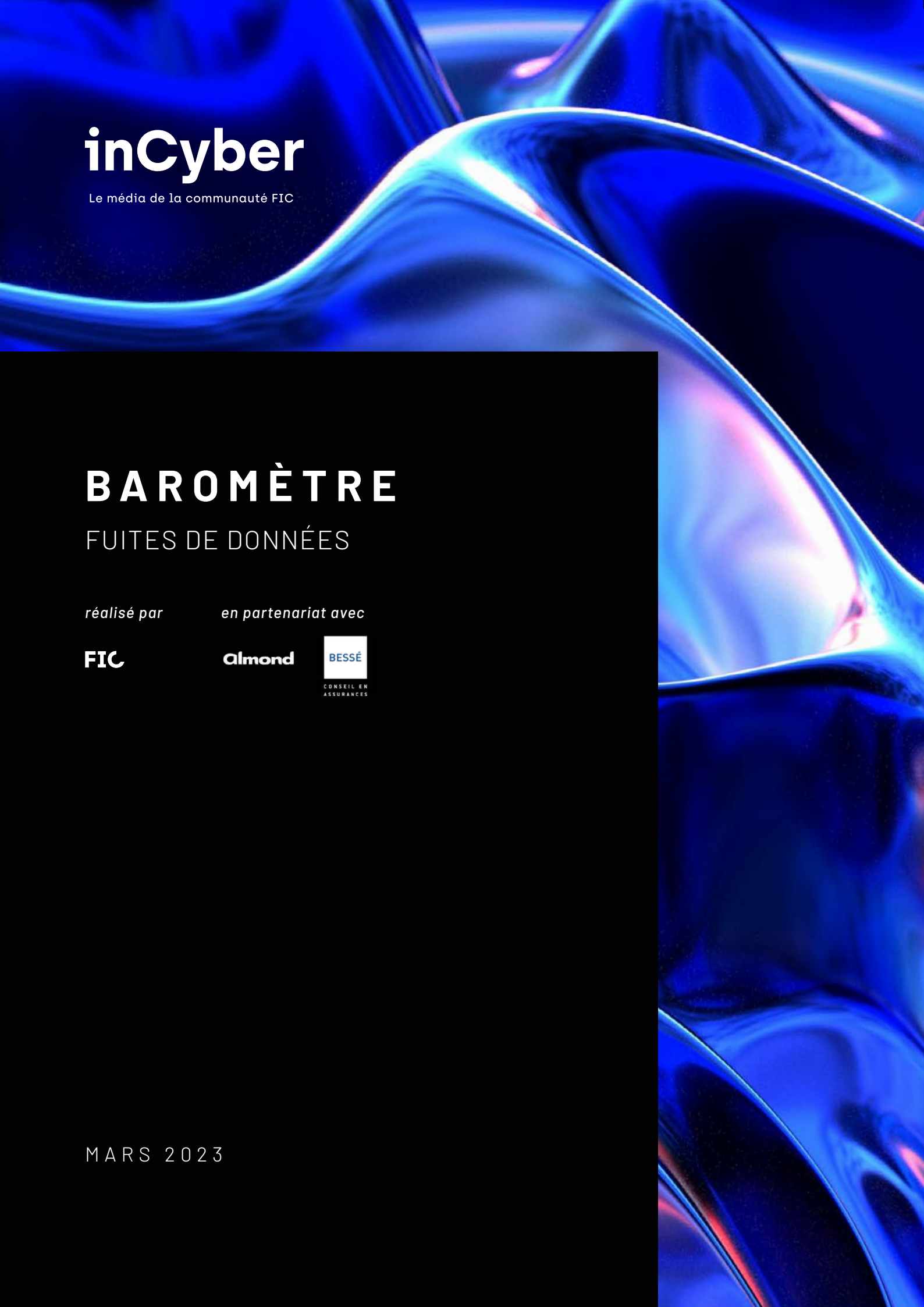


inCyber

Le média de la communauté FIC

BAROMÈTRE

FUITES DE DONNÉES

réalisé par FIC

en partenariat avec Almond, BESSÉ CONSEIL EN ASSURANCES

MARS 2023

BAROMÈTRE
DATA BREACH

Ce baromètre est animé par le FIC en partenariat avec Bessé et Almond et avec la participation de la CNIL.

L'année 2021 n'avait rien d'une exception. Si le nombre de violations de données à caractère personnel notifiées à la CNIL a connu un léger fléchissement (- 3,11 %) l'an dernier, il reste à un niveau particulièrement élevé. Après avoir profité de la désorganisation des entreprises et des acteurs publics durant la crise sanitaire, les cybercriminels continuent à exercer une menace constante, multipliant des campagnes toujours plus sophistiquées.

Pour les organisations victimes, une fuite de données n'a jamais rien d'anodin. Elle entraîne des conséquences plus ou moins lourdes sur les plans financier, opérationnel, réputationnel, judiciaire ou réglementaire. Se fondant sur les données publiées par la CNIL, ce baromètre entend évaluer le phénomène et ses conséquences.

2022, UNE NOUVELLE ANNÉE RECORD

Avec près de 13 fuites de données par jour et 4 731 notifications d'incidents reçues par la CNIL l'an dernier, 2022 fait figure de nouvelle année record. En cumul, ces fuites de données à caractère personnel concernent un très grand nombre d'individus en France. En retenant, par hypothèse, le nombre moyen de personnes concernées par violation, on peut estimer qu'environ cinq millions de Français ont été impactés en 2022.
Si la méthode n'a rien de scientifique, elle permet de mettre en évidence l'importance du phénomène.

Rappelons qu'une violation de données à caractère personnel est, selon l'article 4.12 du RGPD, constituée « une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises (…) ou l'accès non autorisé à de telles données ».

Le RGDP introduit, par ailleurs, une obligation de notification par les responsables de traitement en cas de *data breach*. Ils doivent alerter la CNIL dans les meilleurs délais, si possible dans les 72 heures après en avoir pris connaissance.
Le manquement à cette obligation peut entraîner une amende s'élevant jusqu'à 10 millions d'euros, ou 2 % du chiffre d'affaires annuel mondial de l'entreprise.

4 731
notifications à la CNIL de violations de données à caractère personnel

5 millions
de personnes concernées

La menace vient avant tout des cybercriminels.
Sur les 4 731 notifications enregistrées par la CNIL entre septembre 2021 et septembre 2022, les deux tiers (3 160) relèvent de causes externes. L'origine de ces actes est bien davantage malveillante (3 011) qu'accidentelle (169).
En revanche, la proportion est inverse concernant les 1 049 fuites dont l'origine est à trouver au sein d'une organisation. Les causes de ces actes internes sont majoritairement d'origine accidentelle (842) et non malveillante (207).

Ces données confirment, en chiffres absolus, que la cybercriminalité est principalement le fait d'individus extérieurs à une organisation. Un phénomène en hausse puisque, en un an, le nombre d'actes malveillants d'origine externe a progressé de 10,6 %. Les actes malveillants d'origine interne augmentent dans une proportion équivalente (+ 11,89 %). Ce qui doit interroger les organisations sur les processus à mettre en œuvre pour contrer ces « ennemis de l'intérieur ».

En ce qui concerne les actes internes d'origine accidentelle, on peut légitimement penser que la généralisation du télétravail, introduit depuis la pandémie de Covid-19, accentue les facteurs de risques.

À leur domicile, les appareils des collaborateurs ne disposent pas du même niveau de protection que celui de leur entreprise. Le télétravail a aussi pour effet d'abaisser le niveau de vigilance. Seuls devant leur écran et sans les conseils avisés de collègues présents sur le même plateau, les employés deviennent une proie plus facile des campagnes de *phishing*.

En revanche, le nombre de fuites « d'origine inconnue » a baissé de 49 % en un an. Alors qu'on fêtera, en mai prochain, les cinq ans de la mise en œuvre du RGPD, les entreprises et administrations ont visiblement gagné en maturité. Au fil des années, elles ont progressivement mis en place les outils permettant de tracer l'origine des incidents.

4 731
notifications

3 160
actes externes

1 049
actes internes

3 011
de nature malveillante

842
de nature accidentelle

LE NOMBRE DE VIOLATIONS SE MAINTIENT À UN NIVEAU ÉLEVÉ

Chiffres-clés

+35 % de DPO

(délégués à la protection des données)

soit

17 432

personnes nommées

à cette fonction clé

-3,11 %

repli des notifications enregistrées

Cette stabilisation peut être mise au crédit des organisations qui ont gagné en maturité en matière de cybersécurité.

x2

nombre de violations

entre 2019 et 2021

Après une très forte hausse du nombre de violations entre 2019 et 2021, on note un léger repli des notifications enregistrées sur la dernière année.

Focus

Après une très forte hausse du nombre de violations entre 2019 et 2021, on note un léger repli des notifications enregistrées (- 3,11 %) sur la dernière année. Cette stabilisation peut être mise au crédit des organisations qui ont gagné en maturité en matière de cybersécurité.

La médiatisation d'un nombre croissant de cyberattaques au rançongiciel affectant aussi bien des entreprises privées de toute taille que des hôpitaux ou des collectivités locales a accéléré la prise de conscience des dirigeants. Les organisations ont augmenté le budget dédié à la cybersécurité et relevé leurs niveaux de défense.

L'effort de protection ne porte pas seulement sur les investissements en logiciels et matériels. La politique de confidentialité des données personnelles est de plus en plus incarnée. Le nombre de délégués à la protection des données (DPO) a crû de **35 % en une année pour atteindre 17 432 personnes nommées à cette fonction-clé.** Pour rappel, le RGPD rend obligatoire la désignation d'un DPO pour les organismes publics et les entreprises privées menant des traitements de données sensibles à grande échelle (Article 37).

En dépit de ces signes encourageants, le nombre de violations reste sur un palier particulièrement élevé. Avec la crise sanitaire, le niveau de menace est monté d'un cran, les cybercriminels profitant des vulnérabilités engendrées par la désorganisation des entreprises et la généralisation du télétravail. **Le nombre de violations a plus que doublé entre 2019 et 2021.** Cette pression ne semble pas avoir baissé depuis.

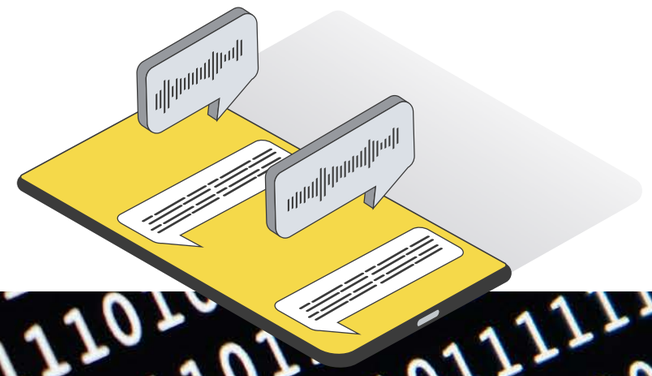
Les conséquences potentielles d'une fuite de données sont de nature diverse. Le premier risque porte sur l'utilisation illégitime des informations exfiltrées. Une telle usurpation peut prendre des formes variées et incontrôlées.

Une violation de données peut déstabiliser l'organisation d'une entreprise et entraîner une paralysie partielle ou totale de son activité. Ce qui génère une baisse de productivité et, *de facto*, une perte financière. Une organisation victime d'un rançongiciel n'est pas assurée, par ailleurs, de recouvrer l'intégralité de son système d'information.

Par ailleurs, la révélation d'une fuite de données nuit à la réputation d'une entreprise et peut affecter durablement la confiance placée en elle.

Enfin, une organisation s'expose à des poursuites juridiques de la part des personnes morales et physiques concernées par la violation de données et à une sanction, en cas de manquement grave et avéré, par l'autorité de contrôle. En l'occurrence la CNIL pour la France.

La CNIL rappelle, en effet, qu'en cas de fuite de données « susceptible d'engendrer un risque élevé pour les droits et les libertés », l'organisme responsable a « l'obligation d'informer individuellement les personnes concernées du fait que leurs données ont été compromises et publiées en ligne. »



LE SECTEUR DES SERVICES PARTICULIÈREMENT TOUCHÉ

Chiffres-clés

Le secteur des services administratifs et de soutien
concentrent près de

30 %
des violations de données

Viennent ensuite les
activités extraterritoriales
(ambasssades, consulats, institutions internationales)
qui représentent

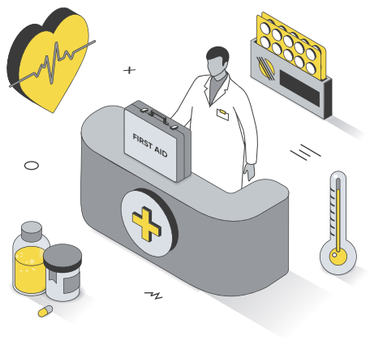
10 %
des violations de données

Les rançongiciels touchent particulièrement les
collectivités territoriales

23 %

et les
établissements publics de santé

10 %



Focus

Un secteur d'activité concentre à lui, seul, près de 30 % du total des violations de données à caractère personnel. Il s'agit de celui des **services administratifs et de soutien.** Derrière ce code NAF de l'INSEE, on retrouve les activités liées à la location, aux voyages, à l'emploi, à la sécurité et plus généralement les sociétés de services aux entreprises.

Viennent ensuite, autour et sous la barre des 10 %, **les activités extraterritoriales – à savoir les ambassades, les consulats ou les institutions internationales –,** puis les établissements financiers et les compagnies d'assurance, les professionnels de l'immobilier, les cabinets juridiques, comptables ou d'architecture, les activités scientifiques et techniques.

Répartis entre différents secteurs d'activité, les acteurs publics sont particulièrement exposés. Dans son *Panorama de la cybermenace 2022*, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) rappelle que **les rançongiciels touchent particulièrement les collectivités territoriales (23 %) et les établissements publics de santé (10 %).**

La liste est longue des acteurs publics victimes de cybercriminels. Parmi les cas médiatisés les plus récents, on peut citer les centres hospitaliers de Versailles et de Corbeil-Essonnes, l'Ehpad de Beuzeville, les mairies de Brunoy et de Chaville, les conseils départementaux de Seine-et-Marne et des Alpes-Maritimes.

Ces entreprises privées ou ces organismes publics ont pour point commun d'être en avance de phase dans leur transformation numérique. Revers de la médaille, la dématérialisation généralisée de leurs processus augmente mécaniquement leur exposition aux risques de fuite de données.

***A contrario,* les activités faiblement digitalisées comme la construction, l'hôtellerie-restauration ou l'industrie manufacturière n'ont à déplorer qu'un faible nombre de violations.** Il est à noter qu'entre 2021 et 2022, l'ordre du classement reste inchangé. Le secteur des activités de services administratifs et de soutien conforte même sa première place avec une progression de 34 % en un an.

TÉMOIGNAGES
ORGANISATIONS VICTIMES

“ IL A FALLU ÉTEINDRE LA LUMIÈRE

C’est durant une nuit d’été de 2020 que cette société d’assurances a été victime d’une cyberattaque. Opérationnel 24 heures sur 24 et 7 jours sur 7, le service de détection et de réponse aux menaces cyber relève une tentative d’intrusion par *ransomware*.

Des investigations plus poussées montrent que l’attaque a abouti, corrompant desserveurs de l’entreprise.
En revanche, le cœur de son système d’information (SI), où sont stockées les applications métiers et les données sensibles, est – pour l’heure - épargné.

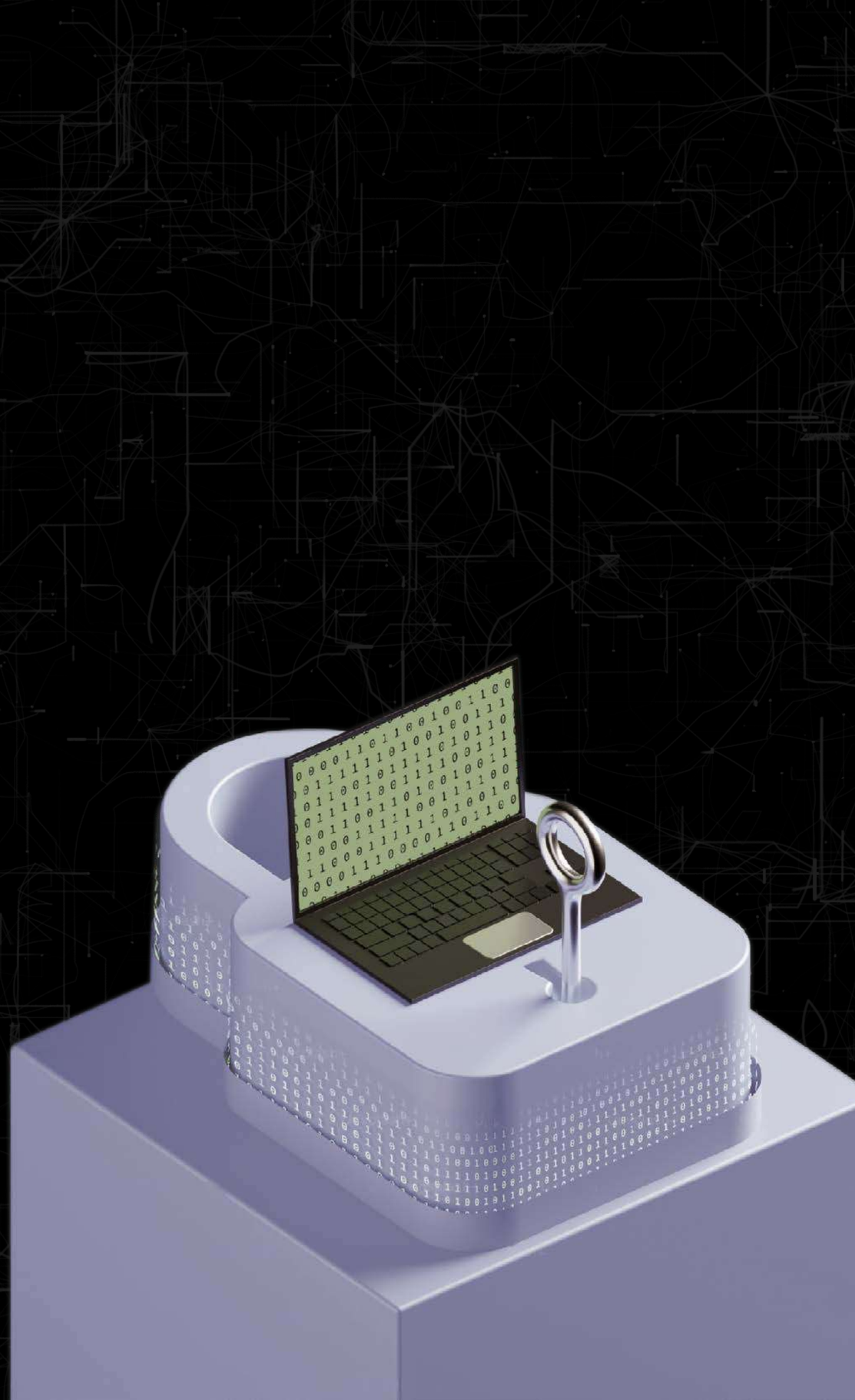
Aussitôt activée, la cellule de crise décide de couper toute communication entre les serveurs et les *legacies*. « Il ne s’agissait pas d’une décision facile à prendre.
C’était toutefois la seule possible pour que le logiciel malveillant ne se propage pas à l’ensemble du SI », se souvient le directeur général. « Éteindre la lumière», c’est-à-dire mettre à l’arrêt les serveurs a des conséquences immédiates.

L’entreprise n’a plus de site internet ni même de messagerie interne. Les agences se retrouvent devant un écran noir. L’ensemble de l’activité étant digitalisée, ils ne peuvent plus traiter les déclarations de sinistres et les demandes d’indemnisation de leurs clients.

Il faudra dix jours et dix nuits à l’équipe technique pour passer au peigne fin les 1 200 serveurs du groupe et mettre au rebut les matériels corrompus.
Aucune fuite de données ne sera à déplorer.
Entretemps, l’assureur a prévenu l’ANSSI.
Une rançon est réclamée mais il ne procédera à aucun paiement. L’assureur met aussi en place des procédures d’urgence.
Exceptionnellement, les agents sont habilités à indemniser sur le compte de l’agence les clients qui se retrouvent dans des situations délicates à la suite d’un sinistre. Un centre d’appel informe, par ailleurs, les clients de la situation et traite manuellement certains dossiers quand c’est possible.

Après coup, l’assureur a procédé à un audit approfondi pour tirer toutes les conséquences de cette cyberattaque et renforcer ses procédures de sécurité. Cet audit montrera que le plan de continuité d’activité (PCA) n’avait pas envisagé ce cas hautement improbable où la société devait couper toute son informatique, interrompant ainsi le principe même de continuité de service.

Depuis, le PCA a été complété et renforcé.
Opérateur de service essentiel (OSE), la société avait déjà redondé sa salle blanche, ses accès réseaux ou son alimentation électrique. Elle dispose désormais d’un plan de secours informatique (PSI) plus sophistiqué qui peut être lancé à tout moment.



LA CYBERCRIMINALITÉ, À L'ORIGINE DU MAL

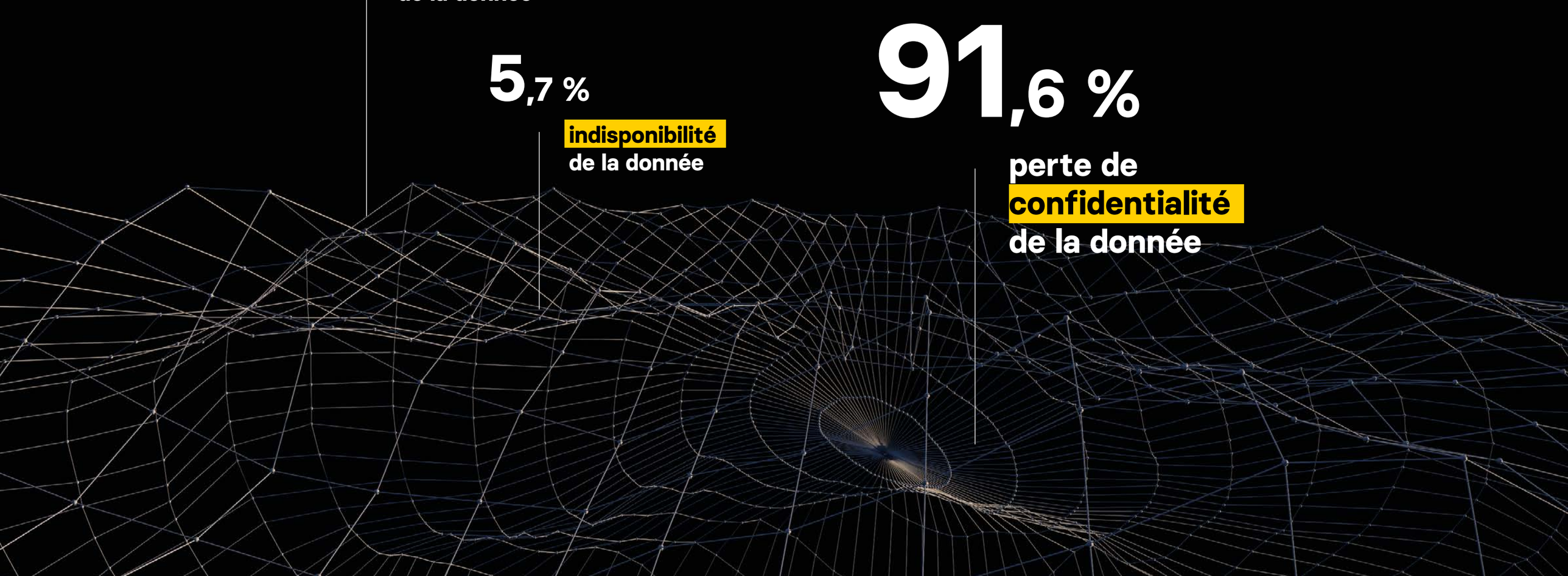
Piratage, *phishing*, logiciel malveillant de type rançongiciel…
Sans surprise, la cybercriminalité est à l'origine des deux tiers des violations de données.
Un chiffre encore en augmentation de 3 % en un an.

CONSÉQUENCE DES VIOLATIONS :

2,6 %
remise en cause de l'intégrité de la donnée

5,7 %
indisponibilité de la donnée

91,6 %
perte de confidentialité de la donnée



Focus

Piratage, *phishing*, logiciel malveillant de genre rançongiciel… Sans surprise, la cybercriminalité est à l'origine des deux tiers des violations de données. Un chiffre encore en augmentation de 3 % en un an.

Puis rarement, le vol ou la perte de matériel informatique ou de documents papier et la publication non volontaire d'informations (erreur d'envoi, transmission accidentelle à un tiers) entraînent une fuite de données.

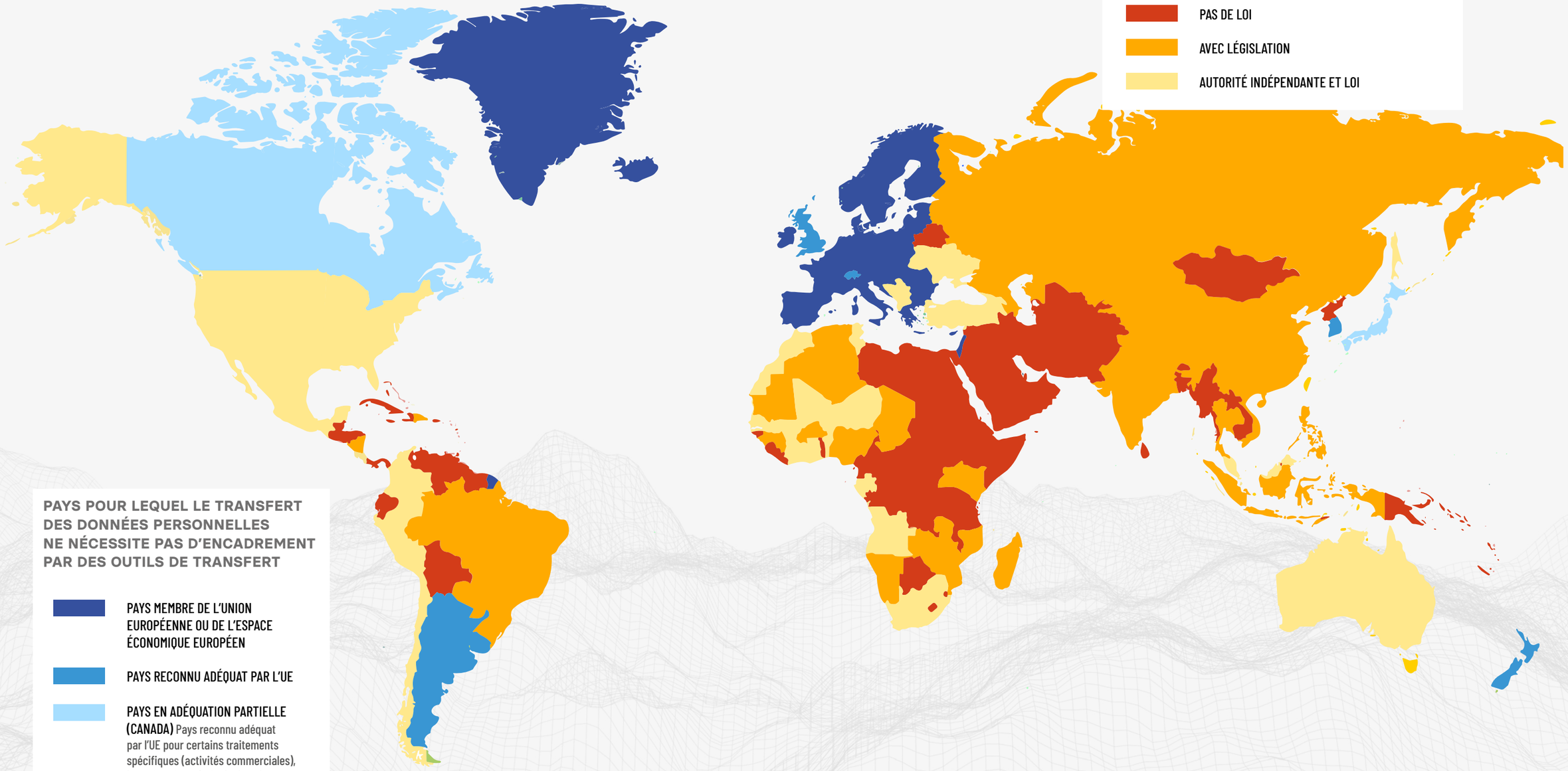
Quelle que soit l'origine des incidents, la mise en circulation d'informations sensibles vient souvent, in fine, alimenter la cybercriminalité. Ces données non seulement se monnaient sur le *darkweb*, mais servent à préparer des campagnes d'attaques toujours plus sophistiquées.

Ces violations conduisent très majoritairement à une perte de confidentialité de la donnée (91,6 %), loin devant son indisponibilité (5,7 %) ou la remise en cause de son intégrité (2,6 %). Cette progression de l'impact sur la confidentialité peut s'expliquer par la forte poussée d'attaques par rançongiciel. Ce genre d'attaque ne se limite plus au chiffrement des données et à la demande de rançon, elle se double le plus souvent d'une publication des données.

Dans son *Panorama de la cybermenace 2022*, l'Anssi note que les attaques par ransomware ont connu un regain d'activité fin 2022. Cette menace cybercriminelle touche particulièrement les TPE, PME et ETI avec 40 % des rançongiciels traités ou rapportés à l'Anssi en 2022.

En termes de criticité des données divulguées, les fuites de données sensibles concernent un quart du nombre total de notifications reçues. Une proportion équivalente à celle observée en 2021.

LÉGISLATIONS
DES ÉTATS EN MATIÈRE DE PROTECTION DES DONNÉES PERSONNELLES



PAYS POUR LEQUEL LE TRANSFERT DES DONNÉES PERSONNELLES NE NÉCESSITE PAS D'ENCADREMENT PAR DES OUTILS DE TRANSFERT

- PAYS MEMBRE DE L'UNION EUROPÉENNE OU DE L'ESPACE ÉCONOMIQUE EUROPÉEN
- PAYS RECONNU ADÉQUAT PAR L'UE
- **PAYS EN ADÉQUATION PARTIELLE (CANADA)** Pays reconnu adéquat par l'UE pour certains traitements spécifiques (activités commerciales), les autres transferts de données personnelles nécessitant d'être encadrés par des outils de transfert

PAYS NON RECONNU COMME ADÉQUAT PAR L'UE ET DONT LE TRANSFERTDES DONNÉES PERSONNELLES NÉCESSITE D'ÊTRE ENCADRÉ PAR DES OUTILS DE TRANSFERT

- PAS DE LOI
- AVEC LÉGISLATION
- AUTORITÉ INDÉPENDANTE ET LOI

AVIS D'EXPERT

CHRISTOPHE MADEC

Directeur de clientèle grandes entreprises, expert cyber et fraude au sein de Bessé, cabinet de conseil en assurances

En 2022, le nombre de violations de données notifiées à la CNIL reste à un niveau équivalent à celui de l'année précédente. Les prochains baromètres permettront de voir s'il faut désormais s'accoutumer à ce nombre important de fuites de données qui a littéralement explosé en 2020.
À ce niveau particulièrement élevé, ce ne sont pas moins de 5 millions de personnes *a minima* qui sont concernées.

Cette tendance résulte de l'accroissement de la menace cyber depuis trois ans, les actes externes d'origine malveillante étant très majoritairement à l'origine de ces violations. Cette menace a été toutefois moins active sur le premier semestre 2022, un grand nombre de *hackers* étant *a priori* mobilisés sur d'autres enjeux avec la guerre en Ukraine.

Les organisations gagnent, par ailleurs, en maturité. Depuis deux ans, elles ont fortement augmenté le budget dédié à la sécurité et renforcé leur politique cyber. De même, le RGPD est entré dans une nouvelle phase d'adoption. Près de cinq ans après sa mise en place, plus aucun responsable de traitement ne peut ignorer le sujet de la confidentialité des données personnelles. Clémente et faisant œuvre de pédagogie dans les premiers temps, la CNIL a, depuis, prononcé des sanctions importantes.

Tous les secteurs d'activité sont concernés. Les cybercriminels cherchent une sorte de compromis en attaquant les organisations détenant des données sensibles mais dont le système d'information présente des vulnérabilités. Les établissements publics de santé s'apparentent ainsi a des proies plus faciles que des acteurs de la finance et de la bancassurance, particulièrement protégés.

Le « modèle économique » des attaques par *ransomware* a évolué avec le temps. Initialement, les cybercriminels se contentaient de crypter les données et d'exiger une rançon pour les déchiffrer. Cette extorsion se double aujourd'hui de la menace de divulguer les données.

La France n'est pas dans une culture du paiement de la rançon. Non seulement, il s'agit de ne pas encourager les demandes de rançons, mais il est également inexact de de penser qu'en payant la rançon une organisation récupère du jour en lendemain son système d'information.

Si la fuite est massive et concerne des informations à forte criticité, la CNIL peut contraindre l'organisation victime à communiquer auprès de ses clients sur le volume et la nature des données corrompues.

Cette communication exige un certain formalisme, et il est préférable qu'elle soit conseillée dans sa rédaction par des experts et des avocats spécialisés.

En dépit de l'importance des fuites de données, il y a en proportion très peu de réclamations et de contentieux de la part de clients qui s'estiment lésés.
À la différence des États-Unis où le cadre juridique est aussi différent, notre pays n'a pas une culture de la procédure et des demandes de dommages et intérêts.

La menace ne vient pas uniquement de groupes de *hackers* agissant depuis de lointains pays. Elle peut aussi venir de l'intérieur. Ce baromètre 2022 relève, tout comme en 2021, que 10% des fuites sont d'origines internes, ce qui interroge sur la motivation et la volonté de nuire des collaborateurs à l'origine de ces fuites. Ceci implique pour les organisations une vigilance interne au niveau des contrôles et une gestion stricte des droits d'accès aux données sensibles.

Les fuites d'origine interne peuvent être aussi accidentelles. Un effort particulier de sensibilisation doit être entrepris auprès des collaborateurs en situation de mobilité, de plus en plus nombreux avec la généralisation du télétravail. La perte ou le vol d'un ordinateur portable contenant un volume certain de données personnelles doit faire l'objet d'une déclaration à la CNIL.

L'assurance cyber est un marché encore jeune qui ne s'est vraiment développé en France que depuis 2017, catalysé par les évènements NotPetya et WannaCry. Avec la vague des sinistres consécutive à la multiplication des attaques *ransomwares*, les portefeuilles cyber des assureurs ont été très impactés.

Confrontés à des pertes, ils ont dû à la fois augmenter les primes, les franchises et durcir leur politique de souscription.

Si les grands comptes et bon nombre d'ETI sont assurés, le taux d'équipement des entreprises reste faible. Encore beaucoup d'entreprises estiment ne pas être des cibles potentielles. D'autres sous-estiment les impacts d'une attaque cyber ou n'en ont simplement aucune idée. Certaines s'estiment suffisamment protégées.

Le marché de l'assurance cyber s'oriente plus favorablement en 2023 que les deux dernières années. Souhaitons que cela participe à renforcer la mutualisation de ce risque, condition indispensable à la pérennisation de la branche d'assurance cyber.

AVIS D'EXPERT

FRANCESCA SERIO

Responsable des offres Gestion de Crise
et *Data Privacy* au sein du cabinet Almond

Entre 2022 et 2021, les notifications de violation à la CNIL restent stables. Cette stabilité est notamment due à une augmentation de 35% du nombre de DPO, ce qui a permis de renforcer la maîtrise des données à caractère personnel traitées par les organisations.

Cette stabilité peut également correspondre à une sous-signalisation des violations. La notification est un exercice encore redouté par certaines organisations. Elles craignent que cette notification déclenche un contrôle de la CNIL, ce qui constituerait une double peine dans le contexte d'une crise qu'elles connaissent déjà à la suite d'une cyberattaque.

Un travail de pédagogie, auquel Almond participe, doit permettre de sensibiliser les dirigeants à l'obligation de notification. Il convient de leur rappeler qu'il s'agit de protéger les personnes concernées. Les consignes qui leur sont communiquées, comme changer leur mot de passe ou bloquer leur carte bancaire, visent à réduire les impacts de la menace qui pèse sur elles.

Parmi les violations notifiées, il apparaît que 70 % sont d'origine malveillante externe, en hausse de 10 % par rapport à 2021. On observe qu'une organisation notifie plus facilement une fuite d'origine criminelle.

En subissant une cyberattaque, elle est perçue comme une victime. Par ailleurs, ces chiffres ne signifient pas forcément que les organisations soient plus vulnérables. Les *hackers* sont aussi plus « performants ». Leurs techniques évoluent et s'améliorent grâce notamment à l'apport de l'IA qui facilite la rédaction de campagne de phishing et, sur le long terme, l'élaboration d'outils de *ransomware*.

Confrontés à des pertes, ils ont dû à la fois augmenter les primes, les franchises et durcir leur politique de souscription.

Si les grands comptes et bon nombres d'ETI sont assurés, le taux d'équipement des entreprises reste faible. Encore beaucoup d'entreprises estiment ne pas être des cibles potentielles. D'autres sous estiment les impacts d'une attaque cyber ou n'en ont simplement aucune idée. Certaines s'estiment suffisamment protégées.

Le marché de l'assurance cyber s'oriente plus favorablement en 2023 que les deux dernières années. Souhaitons que cela participe à renforcer la mutualisation de ce risque, condition indispensable à la pérennisation de la branche d'assurance cyber.

En ce qui concerne les secteurs d'activité, la répartition établie par la CNIL en reprenant la nomenclature NAF de l'Insee n'est pas forcément représentative de la réalité du terrain. Par ailleurs, on parle bien de notifications et non de cyberattaques. En cela, les acteurs publics, collectivités ou établissements de santé, semblent sous-minorés. Les services de santé humaine et action sociale se classent ainsi en 19e et avant dernière place du classement, avec deux notifications recensées entre les mois de septembre 2021 et septembre 2022.

Quel que soit le secteur d'activité, de plus en plus d'organisations sont conscientes des risques encourus avec la médiatisation des cyberattaques. Selon la formule consacrée, la question n'est plus de savoir si une structure va ou non subir une cyberattaque mais quand. Toute crise s'anticipe et, malheureusement, on observe un déficit de préparation en amont.

Une organisation doit se préparer et s'entraîner à des situations de stress intense. Cela suppose de concevoir un plan de gestion de crise, de s'assurer de son maintien à jour et de le tester à intervalles réguliers. Nous conseillons, par ailleurs, de généraliser les analyses d'impacts (PIA). Ce travail de cartographie permet d'avoir une vision claire de l'impact d'une violation de données et la nécessité ou non de la notifier à la CNIL puis de communiquer auprès des personnes concernées.

Toujours en amont, il s'agit de définir une stratégie de communication unique et harmonisée. Maîtriser cette communication permet de ne pas se faire dépasser le moment venu. Sur le plan pratique, les modes de communication traditionnels, comme la messagerie, peuvent être compromis et il convient de prévoir un canal alternatif.

La communication n'est pas seulement externe. Il est important d'informer les collaborateurs de la situation. Ils peuvent être concernés à plusieurs titres. Victimes éventuellement de la fuite de données, ils verront peut-être leur activité ralentie voire stoppée par une cyberattaque. Enfin, ils devront communiquer auprès des clients, des partenaires, de la presse.

La principale conséquence des violations pour les organisations est dans 90 % des cas de notifications, une perte de confidentialité, contre 78 % en 2021. À l'inverse, la perte d'intégrité et de disponibilité est en baisse. On peut supposer que la disponibilité des données est désormais bien maîtrisée par les sauvegardes. En revanche, les attaques par ransomware se doublent, au-delà du chiffrement des données, d'une menace d'une divulgation.

Pour les organisations, cette divulgation des données exfiltrées est appréhendée comme un risque plus important que le paiement d'une rançon. Contrairement à la disponibilité ou à l'intégrité, la perte de confidentialité est très difficilement réparable et ses effets peuvent perdurer très longtemps.

inCyber

Le média de la communauté FIC

incyber.org