Breizh Cyber x ANOZR WAY

1ère étude sur le risque cyber humain

Décryptage du risque cyber humain à partir des empreintes numériques de 17 988 dirigeants, cadres stratégiques, salariés et agents

- Juin 2025 -

Sommaire

Résumé

Cette étude inédite sur le risque humain en cybersécurité apporte un éclairage précieux sous l'angle des métiers. **Elle confirme nos observations de terrain, notamment sur les dirigeants, où près de 70 % des membres de Comité exécutif (Comex) et Comité directeur (Codir) présentent un niveau de risque élevé à très élevé**. Cette étude révèle qu'1 dirigeant sur 5 a au moins une adresse email professionnelle fuitée.

Mais elle va plus loin en révélant que d'autres fonctions, souvent moins visibles mais fortement exposées, sont également vulnérables : les métiers de la communication et du marketing en première position. **1 personne sur 4 travaillant dans les services marketing et communication est à très haut et haut risque.** Ce constat est d'autant plus préoccupant que les attaques par ingénierie sociale — usurpation d'identité, phishing ciblé, fraude — sont désormais largement automatisées et alimentées par les fuites massives de données.

Ces données sensibles — credentials, informations bancaires, données de santé, etc. — proviennent à la fois de la sphère professionnelle et personnelle. Or, plus une donnée est critique, plus elle est convoitée et exploitable par les attaquants.
L'exposition numérique d'un collaborateur ne s'arrête pas à son périmètre professionnel : elle est intimement liée à son usage personnel du numérique.

L'étude illustre parfaitement la tendance identifiée par Forrester [1] en 2024 : **la nécessité de passer d'une sensibilisation générique à une véritable gestion du risque humain. Cela implique de personnaliser les actions de prévention selon le profil de risque individuel.**

[1] The Future Is Now: Introducing Human Risk Management, Forrester

1

Introduction

ANOZR WAY et Breizh Cyber, le centre de réponse aux incidents cyber (CSIRT) de Bretagne, ont noué un partenariat pour **mener la 1ère étude d'analyse du risque cyber humain sur un échantillon d'entreprises bretonnes, de tailles diverses allant de la très petite entreprise (TPE) aux grands groupes industriels** et appartenant à des secteurs variés en Bretagne. L'ambition de cette étude est **d'évaluer la surface d'attaque humaine pour chaque organisation étudiée et d'identifier des tendances par secteur et/ou par catégorie de métiers.**

1.1. Qu'entend-on par risque cyber humain ?

Le risque cyber humain regroupe l'ensemble des comportements, actions ou omissions — volontaires ou involontaires — **susceptibles de compromettre la sécurité informatique d'une organisation ou d'une personne.**
Aujourd'hui, **les vulnérabilités humaines sont la principale porte d'entrée pour les cybercriminels**. Ces derniers exploitent la masse d'informations accessibles en sources ouvertes (OSINT) et issues de fuites de données sur le dark web pour affiner leurs scénarii d'attaque : ingénierie sociale, hameçonnage (phishing), usurpation d'identité, compromission de comptes, fraude, etc. Pour eux, les données personnelles exposées sont une véritable mine d'or.
Les profils publics, les empreintes numériques non maîtrisées ou les corrélations entre identifiants professionnels et usages personnels forment ainsi une surface d'attaque élargie, souvent peu couverte par les approches de cybersécurité techniques classiques.

1.2. Etat des lieux du risque cyber humain

1,93 milliards de données url/login/mot de passe en clair sont échangées sur les réseaux cybercriminels chaque semaine en moyenne

(Source : ANOZR WAY, 2025)

De manière générale, le risque cyber humain tend à augmenter sous l'effet de plusieurs facteurs :

- **Augmentation de la masse de données personnelles** susceptible d'être utilisée par les pirates liée à l'usage massif et de plus en plus répandu des réseaux sociaux ;
- **Attaques massives d'organismes publics ou privés** dans le but de récolter les données personnelles critiques des utilisateurs ;
- **Essor du télétravail et de la porosité entre la vie professionnelle et personnelle** ;
- **Perfectionnement des techniques d'OSINT** (Open Source intelligence) utilisées par les attaquants ;
- **Automatisation et industrialisation des attaques par ingénierie sociale** (ex : phishing/smishing personnalisés, usurpation d'identité et de comptes) ;
- **Montée en puissance des technologies Deepfake**.

Exemple de la fuite massive ayant touché Free [2]

Fin 2024, l'opérateur téléphonique Free a été touché par une cyberattaque de grande ampleur divulguant ainsi les données personnelles de plus de 19 millions de clients. De nombreuses données ont été exfiltrées : nom, prénom, adresses email et postale, date et lieu de naissance, numéro(s) de téléphone, identifiant abonné et données contractuelles, et, pour certaines personnes, références du compte bancaire ou IBAN (International Bank Account Number). Les conséquences sont nombreuses, et notamment le risque d'attaques par ingénierie sociale (usurpation d'identité, phishing, smishing, arnaque au faux coursier, prélèvement frauduleux sur leur compte bancaire, etc.).

[2] Cybersécurité : Free victime d'une fuite de données, 100 000 IBAN déjà exposés
Violation de données personnelles de l'opérateur Free : situation, risques et recommandations

2

L’analyse du risque cyber humain

ANOZR WAY est un éditeur de logiciels spécialisé dans la **gestion du risque cyber humain** proposant dans ses produits, différentes méthodologies pour évaluer le risque cyber humain **des entreprises et des personnes.** En fonction des besoins, ces méthodologies vont de **l'exposition professionnelle à l'exposition personnelle** complète, en passant par la quantification des usages et risques hybrides.

Pour cette étude, nous avons retenu une méthodologie d'évaluation simplifiée et décomposée comme suit, basée sur des indicateurs issus de nos référentiels internes.

L'**exposition professionnelle** prend en compte la compromission de l'adresse électronique professionnelle actuelle, de la présence d'au moins un mot de passe lié à l'environnement professionnel dans les fuites de données détectées par ANOZR WAY ainsi que de la détection d'au moins une inscription à un site tiers avec l'adresse professionnelle actuelle.

L'**exposition personnelle** englobe quant à elle la détection d'une autre adresse électronique (professionnelle ou personnelle), d'au moins un autre mot de passe, d'un numéro de téléphone (professionnel ou personnel) ainsi que de l'exposition d'une adresse postale. Nous avons effectué un premier niveau d'évaluation uniquement pour les personnes ayant une porosité vie professionnelle / vie personnelle détectée.

Les personnes ayant un haut risque signifie que leur niveau de risque se situe entre 6 et 8 sur 10, et un très haut risque signifie que le niveau de risque est supérieur à 8 sur 10.

2.1. L'analyse par secteur

L'étude se base sur un échantillon composé de **81 entités tant publiques que privées, allant de la TPE aux grands groupes industriels, représentant les 14 secteurs d'activité** suivants : les activités juridiques et comptables, l'agroalimentaire, les assurances, les banques, le commerce, la construction, l'énergie, l'enseignement, l'industrie, l'information et la communication, les transports logistiques, les travaux publics, la santé et le secteur public.

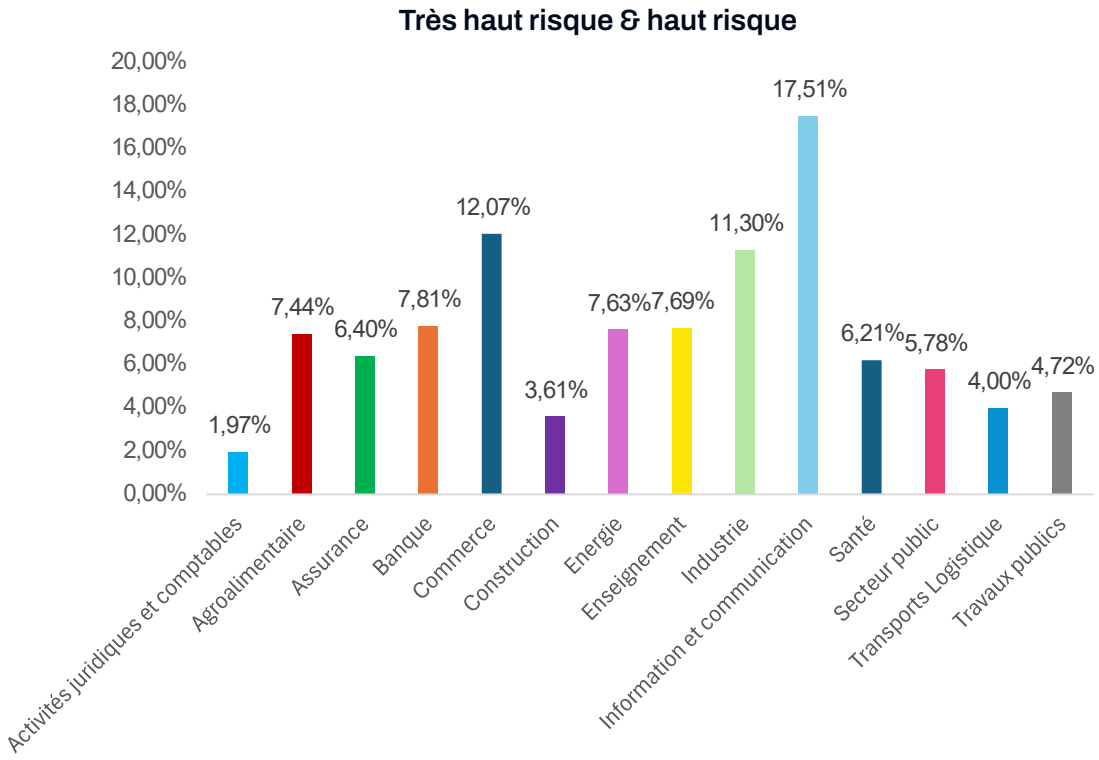

Figure 1 – La répartition du risque humain classé comme haut et très haut par secteur d'activité (en %)

Les secteurs les plus exposés au risque cyber d'origine humaine semblent être l'information et la communication (17,51 %), le commerce (12,07 %) et l'industrie (11,30 %).

Bien que le secteur de l'information et de la communication semble ressortir comme le secteur le plus à risque, ces résultats doivent être interprétés avec précaution. En effet, **la surface d'exposition au risque cyber d'origine humaine d'une entreprise dépend étroitement du nombre de collaborateurs.** La répartition d'entreprises hétérogènes en termes de taille et de maturité numérique au sein des 14 secteurs d'activité considérés, constitue une limite méthodologique qui restreint la portée explicative de l'approche sectorielle et nuit à une représentation fidèle des spécificités propres à chaque secteur.

Il apparaît ainsi que les résultats relatifs au risque cyber d'origine humaine, lorsqu'ils sont analysés par secteur d'activité, reflètent en réalité davantage la distribution quantitative de certaines catégories de métiers que les caractéristiques intrinsèques des secteurs eux-mêmes.

Dans cette perspective, et afin de dégager des tendances significatives à l'échelle de la Bretagne, une analyse croisée par type de métiers semble offrir une lecture plus pertinente et plus représentative des vulnérabilités humaines en cybersécurité que l'approche strictement sectorielle.

2.2. *Les métiers les plus à risque*

17 988 personnes analysées

L'approche la plus pertinente pour tirer des tendances globales nous a mené à définir des catégories de métiers/fonctions. **Les résultats des 17 988 dirigeants, salariés, agents de la fonction publique, indépendants analysés ont donc été répartis en 14 catégories de métiers/fonctions** (détails dans la partie Méthodologie, page 33).

Au regard de l'exposition numérique globale, comprenant les résultats de l'exposition professionnelle et de l'exposition personnelle, 3 catégories de métiers/fonctions ressortent comme étant les plus à risque. Il s'agit de **la communication et du marketing, des dirigeants et des métiers de la sécurité informatique.** Les métiers de l'informatique et du développement informatique, des ressources humaines et de la logistique (ex æquo) viennent également compléter ce classement des professions les plus exposées.

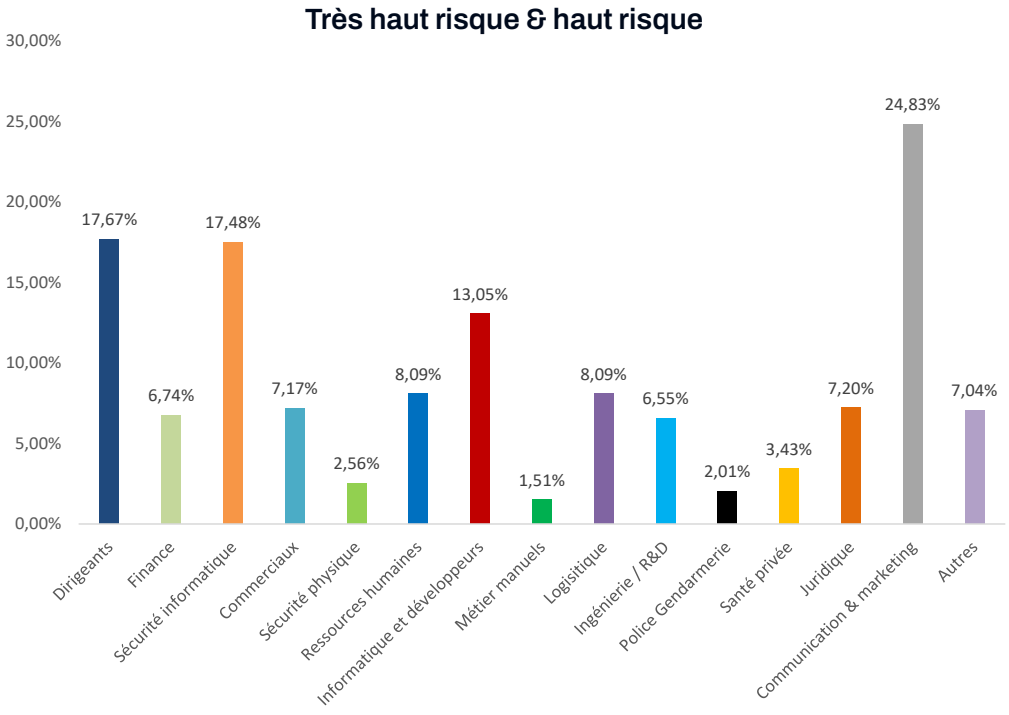

Figure 2 – L'analyse du risque humain des catégories de métiers/fonctions étudiés (en %)

2.2.1. Les métiers du marketing et de la communication : experts en diffusion… victimes de leur exposition

1 personne sur 4 travaillant dans les services marketing & communication est à très haut et haut risque

Les professionnels de la communication et du marketing sont les plus exposés aux risques numériques, tant sur **le plan personnel que professionnel.** Ils présentent le plus grand nombre d'emails professionnels compromis, d'adresses email alternatives exposées, et de mots de passe non liés à leur adresse professionnelle actuelle ayant fuité. Tous ont utilisé leur email professionnel pour s'inscrire à des sites tiers. Nous appelons site tiers, tous sites internet liés au métier, ou à un usage personnel sur lequel l'inscription a été faite avec l'adresse email professionnelle.

Ils sont également **les plus nombreux à exposer une adresse postale**, bien que celle-ci puisse parfois être celle de leur entreprise. Ils sont également fortement concernés par la fuite de mots de passe associés à leur adresse email professionnelle, ce qui est notable compte tenu de leur forte utilisation de cette adresse pour des inscriptions externes. Enfin, ils occupent la deuxième position en termes d'exposition du numéro de téléphone (personnel ou professionnel).

Quels sont les risques ?

Adresse email et/ou Numéro de téléphone fuités = risque d'attaques par ingénierie sociale, de type phishing (hameçonnage) ou smishing

Inscription à des sites tiers = plus l'adresse email professionnelle est utilisée sur des sites tiers, plus elle est exposée à de potentielles fuites de données

Du fait de leur présence sur les réseaux sociaux, la multiplicité d'outils en ligne utilisés quotidiennement, et leur accès aux listes de diffusion comprenant des milliers de contacts, les experts du marketing et de la communication sont des cibles de choix pour les attaquants.

2.2.2. Les dirigeants : pilotes de la stratégie, mais pas de leur empreinte numérique

Les dirigeants occupent la deuxième position parmi les catégories les plus exposées. **Cette nouvelle analyse vient confirmer les tendances déjà observées lors de notre précédente étude consacrée à l'exposition numérique des dirigeants et des cadres stratégiques** [3].

Les dirigeants sont particulièrement exposés à la divulgation de leur numéro de téléphone, qui constitue la principale fuite les concernant. Ils arrivent ensuite en deuxième position pour ce qui est des fuites d'adresses email professionnelles, de mots de passe (professionnels ou autres) et d'adresses postales.
Ils suivent de près les métiers de la communication et du marketing pour l'exposition de l'adresse physique et le taux global de fuite d'emails.

Etat des lieux de l'exposition cyber des dirigeants en France, ANOZR WAY

Enfin, ils se classent au troisième rang en ce qui concerne la présence d'une autre adresse email dans les fuites de données, ainsi que l'inscription à des sites tiers à l'aide de leur adresse email professionnelle. **Cette forte exposition s'explique par leur visibilité médiatique, leur usage mixte des outils professionnels et personnels, ainsi que leurs pratiques numériques souvent peu cloisonnées.**
Toutes ces informations aident les malfaiteurs à construire des scénarii crédibles.

Quels sont les risques ?

Usage mixte des outils professionnels et personnels = croisement des données fuitées pour compromettre un compte professionnel

Adresse postale fuitée = risques qui dépassent la sphère numérique, ouverture vers les risques physiques (intimidation, chantage, cambriolage, home-jacking, enlèvement…)

[3] Étude sur l'exposition cyber des dirigeants et hauts cadres français, ANOZR WAY

2.2.3. Les métiers de la sécurité informatique : les cordonniers les plus mal chaussés

Les professionnels de la sécurité informatique occupent la troisième position dans l'analyse du risque humain. Ils se distinguent par une deuxième place concernant la détection d'une autre adresse email compromise, une troisième place pour la fuite d'un autre mot de passe, et une quatrième place en ce qui concerne l'inscription à des sites tiers avec leur adresse email professionnelle ainsi que l'exposition de leur adresse postale

À noter : aucun mot de passe associé à leur adresse professionnelle n'a été retrouvé. **Une confiance élevée dans la maîtrise technique du digital — qu'elle vienne des équipes sécurité ou des développeurs — peut parfois créer un angle mort dans l'évaluation globale du risque. Or même les professionnels de la sécurité peuvent être victimes de manipulation, surtout dans un contexte de stress ou de routine.**

Quels sont les risques ?

Identifiants et mots de passe fuités = compromission de comptes possibles pour accéder au système d'information

Usurpation d'identité = voir son identité usurpée pour duper certains collaborateurs afin d'accéder à leur compte, prendre le contrôle de leur PC, accéder au système d'information

2.2.4. Les informaticiens et développeurs informatiques : ils patchent les failles… sauf les leurs

Les développeurs informatiques se classent quatrièmes pour la divulgation de leur adresse email professionnelle, ainsi que pour la fuite de mots de passe liés à cette dernière et sixièmes concernant l'exposition de leur adresse physique. Ils figurent en sixième position pour l'inscription à des sites tiers avec leur adresse professionnelle, et quatrièmes pour la détection d'autres adresses email (pro ou perso). Ils occupent également la quatrième place avec les métiers juridiques en matière d'exposition des numéros de téléphone, qu'ils soient personnels ou professionnels.

Quels sont les risques ?

Usurpation / Fraude au faux service technique = se faire passer pour un technicien pour obtenir un accès à distance à un ordinateur d'un collaborateur afin d'accéder à leur compte, prendre le contrôle de leur PC, accéder au système d'information

2.2.5. Les métiers des ressources humaines et de la logistique : ils assurent la continuité… sauf quand le numérique s'enraye

Métiers des ressources humaines

Les métiers des ressources humaines demeurent des métiers exposés au risque cyber humain. Ils se positionnent respectivement cinquième et sixième en matière de mots de passe professionnels fuités et d'adresses email professionnelles fuitées. 22 % d'entre eux ont utilisé leur email professionnel pour s'inscrire à des sites tiers. Cette exposition peut s'expliquer par la nature même des missions RH qui impliquent **l'utilisation de services tiers pour la gestion des paies, la gestion des données personnelles des collaborateurs ou la gestion des recrutements**.
Ce sont donc **des cibles privilégiées par les cyberattaquants car ils gèrent quotidiennement des données hautement sensibles**, telles que les coordonnées bancaires des salariés, les bulletins de paie, les contrats de travail ou encore des informations médicales confidentielles.

Quels sont les risques ?

Compromission de compte = extraction de bulletins de paie, coordonnées bancaires des salariés ou données personnelles via des accès RH

Escroquerie au faux candidat = une personne malveillante se fait passer pour un candidat afin d'infiltrer la société ou envoie des CV/pièces jointes contenant des logiciels malveillants pour compromettre les systèmes RH

Métiers de la logistique

Au même titre que les métiers des ressources humaines, les métiers de la logistique ressortent comme cinquième métier à risque. Ces fonctions sont en interaction avec des acteurs externes (fournisseurs, transporteurs, clients) et utilisent des outils numériques (ERP, gestion des stocks, systèmes de suivi des livraisons) qui élargissent leur surface d'attaque. **Par ailleurs, elles font face à une évolution de la menace visant la supply chain. Un tiers victime d'une cyberattaque peut être la source d'une cyberattaque par rebond. C'est l'un des enjeux que l'Union européenne souhaite adresser à travers la directive NIS 2.**

2.3. *Les métiers avec un risque plus faible*

Le risque zéro n'existe pas. Toutefois, selon notre étude, certaines catégories de métiers présentent un niveau de risque humain plus faible. Dans l'ordre décroissant : les métiers manuels, les forces de l'ordre (Police/Gendarmerie), la sécurité physique et la santé privée.

Il est difficile de faire un rebond vers les éléments personnels de ces métiers à partir de leurs emails professionnels. Cela ne veut pas dire qu'ils n'ont pas une forte exposition personnelle mais cela reflète surtout une utilisation de leurs emails et une exposition professionnelle limitées, ce qui rend plus difficile les rebonds vers leur vie personnelle selon la méthode d'analyse de ces statistiques.

N'ayant pas la vue sur leur exposition personnelle, il est difficile de quantifier le risque réel de ces personnes. Pour avoir une vue complète, il faudrait ajouter des informations personnelles avec leur accord (email personnel, numéro de téléphone personnel) pour élargir la recherche de leurs données fuitées ou exposées. **Les usages personnels présentent un réel risque et sortent du champ de vision et d'action des équipes techniques.**

Les métiers de la comptabilité et finance, métiers principalement de « back-office », sont peu exposés car nécessitent moins d'interactions avec l'extérieur de l'organisation ou d'accès à de nombreux outils en ligne en comparaison d'autres métiers. Ce sont, pour autant, **des cibles très convoitées par les cybercriminels, notamment pour orchestrer des fraudes au faux ordre de virement international (FOVI) ou des fraudes au changement de RIB.**

3

3. Le détail des tendances

3.1. Le risque émanant de l'exposition professionnelle

L'analyse de l'exposition professionnelle des individus étudiés se base sur la détection de l'adresse professionnelle actuelle dans des bases de données fuitées, sur l'identification d'au moins un mot de passe lié à ladite adresse email professionnelle mais également sur l'utilisation de l'adresse professionnelle sur des sites tiers ayant fait l'objet d'une fuite de données.

Les pourcentages de chaque graphique sont pondérés par le nombre d'individus par catégorie de métiers.

3.1.1. La fuite des credentials professionnels

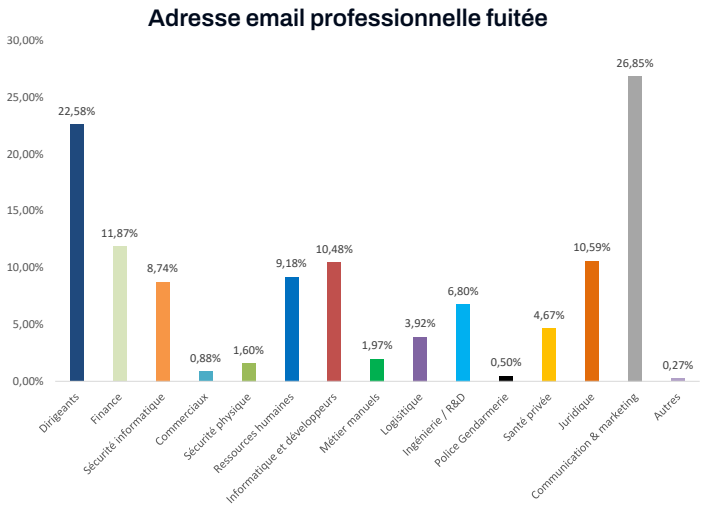

Figure 3 – Détection des emails professionnels ayant fuité, par catégorie de métiers (en %)

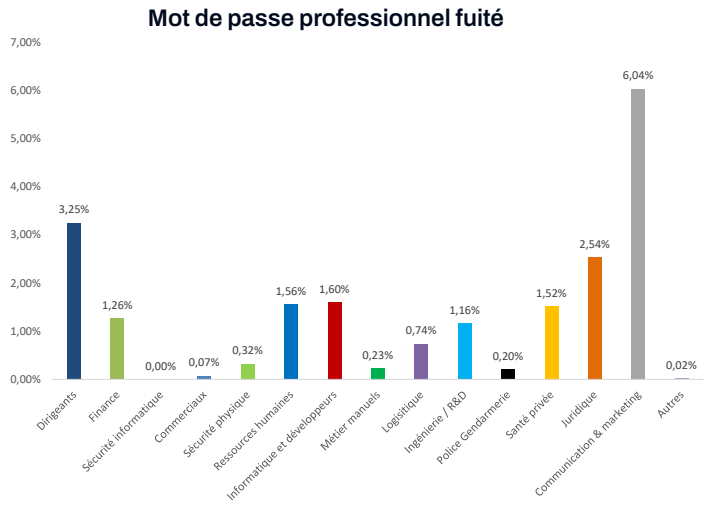

Figure 4 – Détection des mots de passe fuités, liés à une adresse email professionnelle, par catégorie de métiers (en %)

Plus d'1 dirigeant sur 5 a au moins un email professionnel fuité

Le top 3 des métiers qui ont un email professionnel fuité est pratiquement identique à ce que l'on a pu constater précédemment, à l'exception des métiers de la finance qui sont particulièrement exposés :

1. **Les métiers de la communication et du marketing (26,85 %)**
2. **Les dirigeants (22,58 %)**
3. **Les métiers de la finance (11,87 %)**

Concernant les fuites de mots de passe professionnels, **les métiers de la communication et du marketing arrivent en tête des catégories professionnelles les plus exposées à la fuite de mots de passe associés à une adresse email professionnelle** (6,04 %). **Cette forte exposition s'explique par l'emploi fréquent de leur adresse professionnelle dans des contextes variés.**

La deuxième catégorie la plus concernée est celle des dirigeants, avec 3,25 %, suivie par les professionnels du secteur juridique (2,54 %). Les informaticiens et les développeurs occupent la quatrième position (1,60 %), juste devant les ressources humaines (1,56 %).

Lorsqu'un attaquant trouve un mot de passe professionnel en clair, **il peut facilement tenter de l'utiliser sur plusieurs sites différents, dans l'hypothèse où la personne utiliserait ce même mot de passe ailleurs.** Ce phénomène est très répandu : 94 % des mots de passe sont réutilisés ou dupliqués [4].
Un seul mot de passe compromis peut donc être une porte d'entrée pour compromettre de multiples autres comptes. La bonne pratique est de générer un mot de passe robuste et unique pour chaque inscription et d'utiliser un gestionnaire de mots de passe pour les stocker.

[4] 19 billion leaked passwords reveal deepening crisis: lazy, reused, and stolen, Cybernews

3.1.2. L'inscription à des services tiers avec une adresse email professionnelle

100 % des professionnels de la communication et du marketing ont utilisé leur adresse email professionnelle pour s'inscrire sur un site tiers

Les professionnels de la communication et du marketing se distinguent très nettement des autres catégories socio-professionnelles analysées. **En raison de la nature même de leur activité, ils sont plus enclins à utiliser des plateformes externes dans un cadre professionnel, ce qui explique que 100 % des individus étudiés dans ce secteur sont inscrits sur au moins un site tiers avec leur adresse email professionnelle.**
Les ressources humaines occupent la deuxième place avec un taux de 22,24 %, suivies de près par les dirigeants (21,17 %), la sécurité informatique (18,45 %), l'ingénierie et la R&D (17,33 %) et les informaticiens et développeurs (17,22 %). À l'inverse, les membres des forces de l'ordre (police et gendarmerie) apparaissent très peu exposés, avec un taux d'inscription négligeable de 0,70 %.

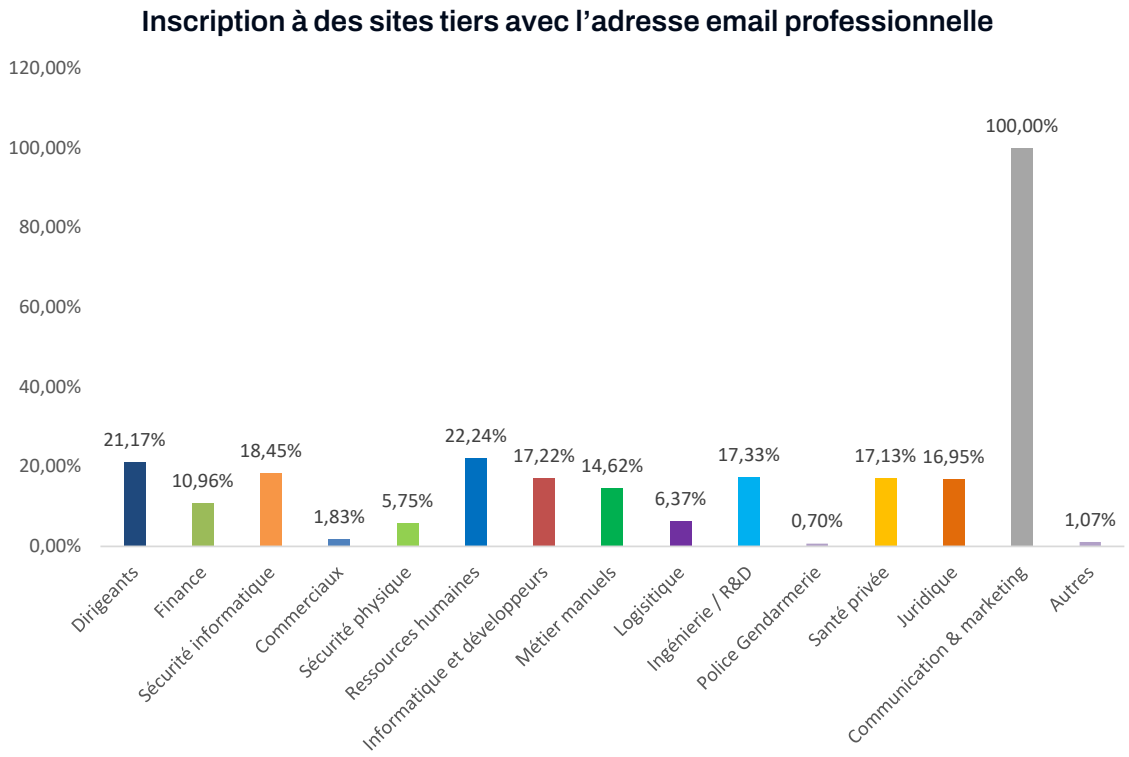

Figure 5 - Répartition des inscriptions détectées sur des sites tiers utilisant l'adresse email professionnelle par catégorie de métiers (en %)

Plus une adresse email est utilisée, plus elle est exposée au risque de fuite ou de compromission. La bonne pratique est de segmenter ses usages en utilisant plusieurs adresses email pour réduire le risque de compromission totale. Par exemple, une pour les usages professionnels, une personnelle pour les achats sur des sites e-commerce, une personnelle pour les formalités administratives, etc.

3.2. Le risque émanant de l'exposition personnelle

Dans le cadre d'une évaluation du risque humain, les outils d'ANOZR WAY analysent les fuites de données détectées afin d'y rechercher toute information liée à l'individu concerné. **Grâce aux pivots automatiques, il est souvent possible d'identifier des données personnelles supplémentaires, telles que d'autres adresses email (professionnelles ou personnelles), un ou plusieurs mots de passe, ainsi qu'un numéro de téléphone ou une adresse physique.**

3.2.1. L'exposition d'autres credentials

Plus d'1 communiquant sur 5 a au moins 2 autres mots de passe fuités sur le dark web

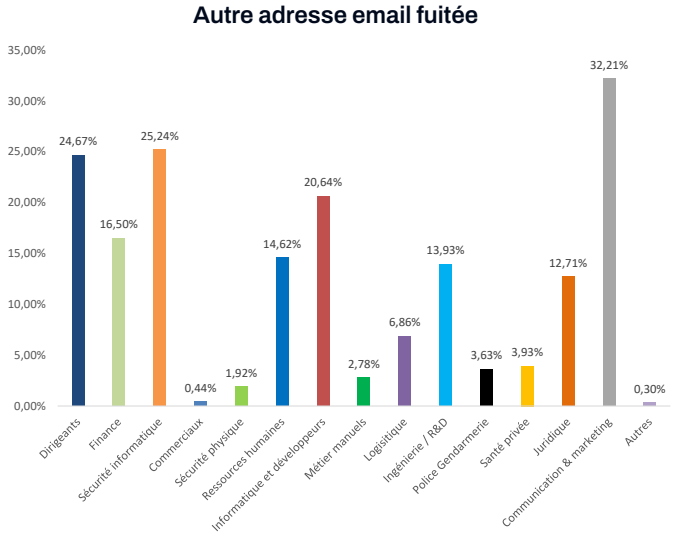

Figure 6 - Détection d'une autre adresse électronique dans les fuites de données détectées par ANOZR WAY, par catégorie de métiers (en %)

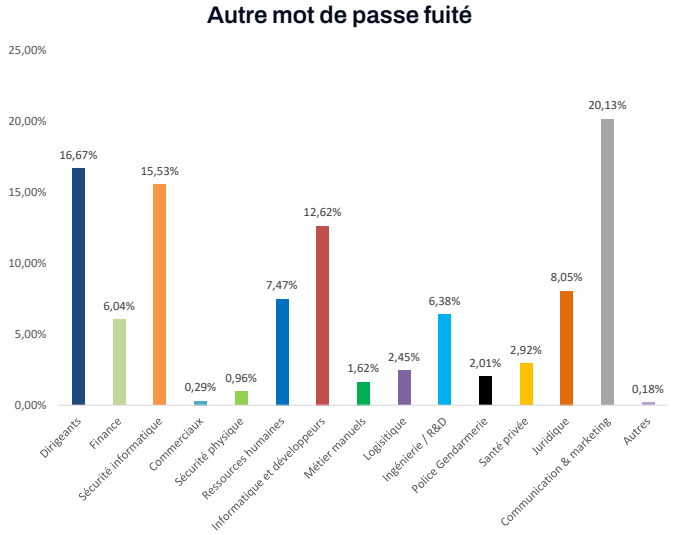

Figure 7 - Détection d'autres mots de passe (dont potentiellement des mots de passe personnels), par catégorie de métiers (en %)

L'analyse de l'exposition d'autres mots de passe englobe à la fois des mots de passe professionnels et personnels. Les catégories les plus concernées sont la communication et le marketing (20,13 %), les dirigeants (16,67 %) et la sécurité informatique (15,53 %).

En revanche, il est difficile d'établir des liens vers les données personnelles des commerciaux, des professionnels de la sécurité physique, des métiers manuels, des forces de l'ordre (police/gendarmerie) et de la santé privée à partir de leur adresse email professionnelle. Cela ne signifie pas nécessairement qu'ils ne sont pas exposés sur le plan personnel, mais cela reflète surtout une utilisation professionnelle restreinte de leur adresse email, ce qui limite les possibilités de rebond vers leur sphère privée selon la méthodologie d'analyse utilisée.

3.2.2. L'exposition d'un numéro mobile

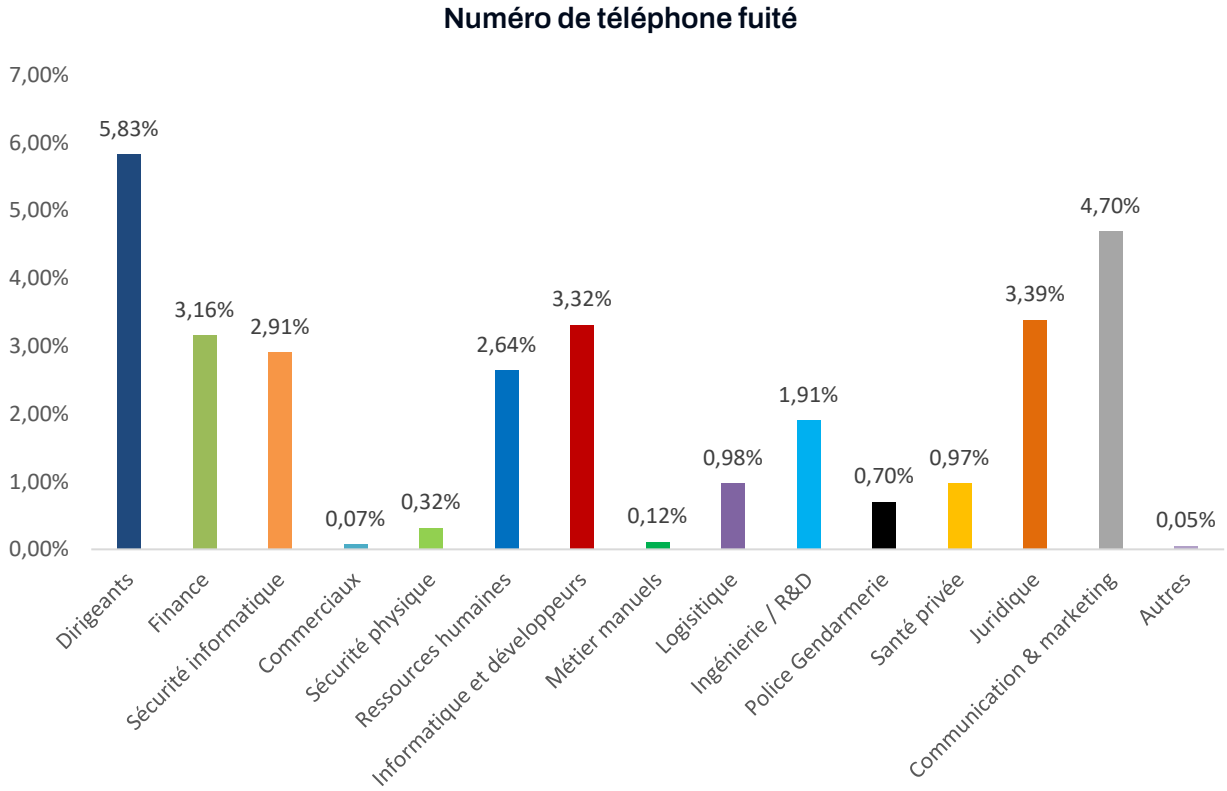

Figure 6 – Répartition des numéros de téléphone ayant fuité par catégorie de métiers (en %)

En ce qui concerne les numéros de téléphone mobile figurant dans les fuites de données, les tendances observées se rapprochent de celles déjà mentionnées, bien que de légères variations soient à noter : les dirigeants sont les plus exposés, avec un taux de 5,83 %. Ils sont suivis par les professionnels de la communication et du marketing (4,70 %) et des métiers du juridique (3,39 %).

3.2.3. L’exposition de l’adresse physique

Les professionnels de la communication et du marketing ainsi que les dirigeants sont ceux dont l’adresse physique apparaît le plus fréquemment dans les fuites de données détectées par les outils d’ANOZR WAY, même si cette adresse peut parfois correspondre à celle de leur entreprise. À l’opposé, les métiers manuels, les commerciaux, la sécurité physique et la santé privée figurent parmi les catégories les moins exposées.

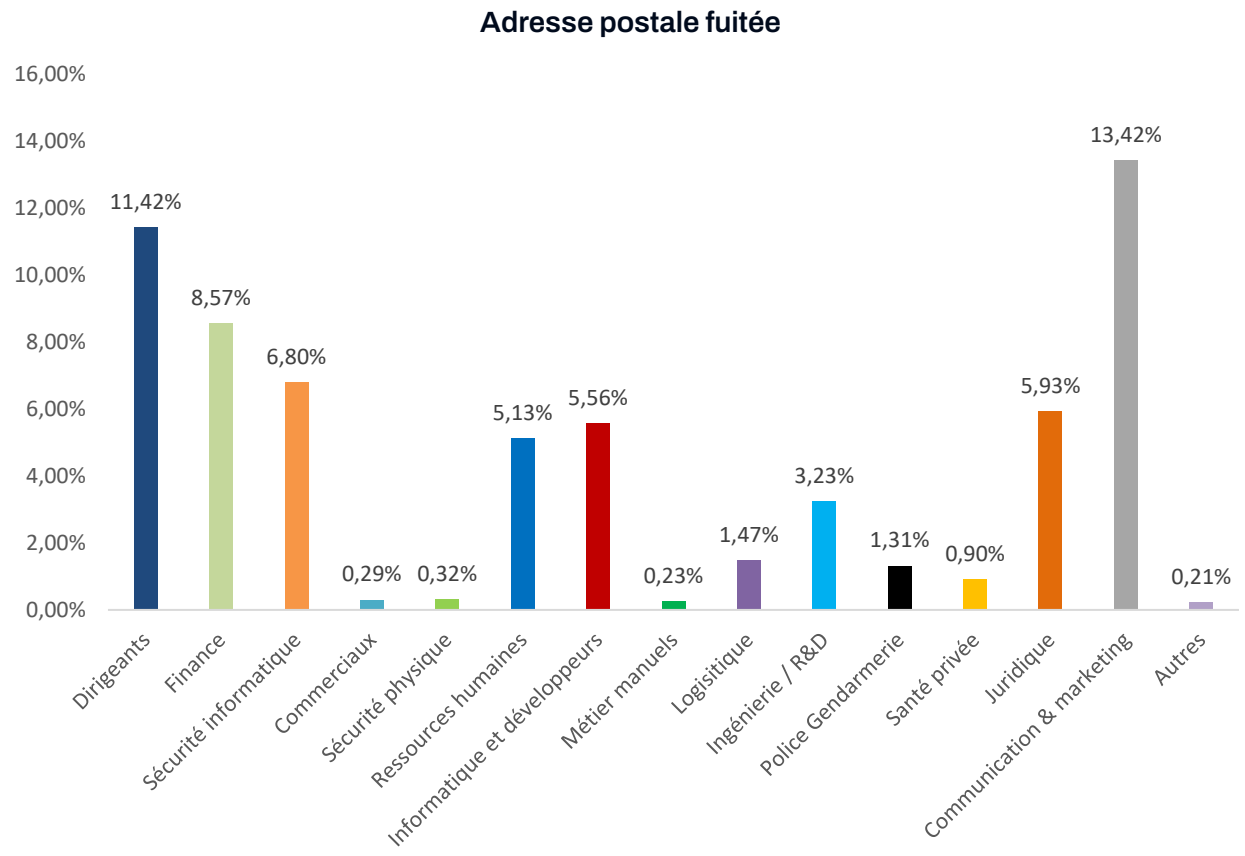

Figure 8 - Détection des adresses de résidences personnelles, par catégorie de métiers (en %)

Quels sont les risques ?

Si une adresse postale est exposée sur Internet, sur les réseaux sociaux ou se trouve dans une fuite de données, le risque ne se limite plus à la sphère numérique. Les menaces physiques existent bel et bien, et notamment lorsqu'il s'agit de dirigeants, de cadres stratégiques ou de personnes à forte visibilité. Il peut s'agir, entre autres, de :

- **Chantage ciblé pour faire pression et avoir accès à des informations confidentielles**
- **Enlèvement ou intimidation de proches pour réclamer une rançon**
- **Tentative d'intrusion ou home-jacking**

Ce type de menace, longtemps sous-estimé, fait désormais partie des scénarii d'attaque pris en compte dans les stratégies de sécurité intégrant le facteur humain. C'est pourquoi la maîtrise de l'exposition personnelle (y compris des adresses physiques) est un enjeu central, en particulier pour les profils sensibles.

Exemple des crypto kidnappings [5]

Depuis le début de l'année 2025, une vague d'enlèvements vise les figures influentes du secteur des cryptomonnaies. Dirigeants, fondateurs… mais aussi leurs proches : conjoints, enfants, parents. Les attaques sont désormais physiques, parfois en pleine rue, sous les yeux de témoins.

Ces actes ne sont pas le fruit du hasard. Ils peuvent commencer par une phase de reconnaissance numérique : email, adresse du domicile, numéro de téléphone, relations familiales, habitudes…

Des informations trop souvent accessibles en ligne publiquement ou via des fuites de données massives. Ce ne sont plus des attaquants isolés, mais des groupes organisés et sans scrupules, qui exploitent chaque donnée exposée.

Ce risque est proche de celui s'exerçant sur les dirigeants et familles fortunées, tous secteurs confondus.

[5] Fear and anger in France's crypto community after spate of kidnappings, Reuters
Crypto-kidnapping : comment la France veut protéger les magnats du Bitcoin des criminels, 01.net

4

Recommandations

4.1. Repenser les priorités de protection à partir des données réelles

Les profils les plus à risque ne sont pas forcément ceux que l'on imagine. Preuve en est avec cette étude, qui tout en confirmant certains scénarii classiques, met en lumière **des métiers souvent sous-estimés en matière de cybersécurité, mais qui peuvent constituer des portes d'entrée critiques pour les attaquants.** Les fonctions support, les profils très exposés médiatiquement ou ceux en interaction fréquente avec l'extérieur peuvent présenter un niveau de vulnérabilité élevé, sans pour autant figurer dans la liste habituelle des collaborateurs « sensibles ».

4.2. Quantifier le risque avant de mettre en place un plan d'action cyber

Avant de mettre en place des mesures de protection, il est nécessaire de **quantifier le risque réel.** Cela implique de cartographier l'exposition numérique individuelle à partir **de données factuelles accessibles publiquement sur le web, les réseaux sociaux et le dark web** (approche OSINT).

4.3. Adapter les actions de sensibilisation aux profils de risque

Une sensibilisation globale ne peut répondre à tous les enjeux. Il est essentiel de **personnaliser la sensibilisation en fonction du profil de risque** de chaque collaborateur. Pour susciter l'adhésion, les messages doivent être ciblés et illustrer par des cas d'usage concrets qui parleront au collaborateur.

4.4. Diminuer le risque en corrigeant les failles

Ces actions de sensibilisation personnalisées doivent s'accompagner d'une démarche de correction individuelle de l'exposition. L'objectif : rendre l'utilisateur acteur de sa propre protection, afin de diminuer son exposition numérique, et par ricochet le risque de l'organisation.

Le point de vue de Breizh Cyber

« Les bonnes pratiques concernant la protection des identités sont :

• La sensibilisation de vos utilisateurs au risque d'exposition de données, aux pratiques dangereuses (tel le téléchargement d'outils de « cracking » embarquant des infostealers) et à la compréhension des modes opératoires des acteurs malveillants (réutilisation d'informations d'anciennes attaques pour en mener de nouvelles) reste évidemment une nécessité

• Pour les RSSI, il ressort que l'exposition aux risques n'est pas homogène suivant les fonctions et les groupes de travail dans l'entreprise. Il est donc certainement possible de moduler les efforts en fonction des groupes de travail. Il apparaît ainsi prioritaire de sensibiliser les fonctions les plus exposées comme les dirigeants, les équipes informatiques (dont les professionnels de la sécurité) et les fonctions marketing et communication tout en continuant à sensibiliser des fonctions prioritaires comme la comptabilité et les ressources humaines au regard des risques spécifiques de ces métiers

• Le différentiel de compromission de mots de passe des sphères personnelle et professionnelle confirme le besoin d'interdire les pratiques de BYOD pour limiter la contamination de la sphère professionnelle par la sphère personnelle

• La généralisation de l'utilisation de coffre-fort de mots de passe à tous les utilisateurs permettant de générer des mots de passe robustes et uniques pour chaque service

• L'authentification multi-facteur pour tous les services sensibles et/ou exposés sur Internet permettant d'éviter tout risque de compromission d'identité même en cas de compromission d'identifiants

• La surveillance et la détection d'identifiants compromis de manière proactive par la souscription à des services tels qu'ANOZR WAY et l'accompagnement des utilisateurs à diminuer leur niveau d'exposition »

Guillaume CHÉREAU, Directeur

Breizh Cyber

5

Ce qu’il faut retenir et suites de l’étude

5.1. Ce qu'il faut retenir

Les statistiques remontées par cette étude confirment que le risque humain est un facteur de vulnérabilité de cybersécurité pour les organisations, qu'elles soient publiques ou privées et quelle que soit leur taille. La généralisation de la compromission d'identifiants professionnels par des acteurs malveillants est une nouvelle donne à prendre en compte et à gérer, sachant qu'**il en suffit d'un pour potentiellement compromettre l'organisation.**

Ce constat est corroboré par les travaux en Cyber Threat Intelligence (CTI) qui ont pu documenter la structuration de l'écosystème cybercriminel avec l'émergence depuis quelques années des Initial Access brokers (ou IAB)[6]. Ces derniers sont des acteurs de la cybercriminalité spécialisés dans l'obtention d'accès non autorisés à des réseaux ou systèmes informatiques, qu'ils revendent ensuite à d'autres cybercriminels.

Breizh Cyber dans le cadre de son activité a pu documenter des incidents impliquant la compromission de comptes d'une organisation comme vecteur initial de compromission d'une attaque. Il s'agit là d'un risque bien réel.

[6] 2025 Initial Access Brokers Report Cyberint
Publication du rapport annuel relatif à la cybercriminalité, Commandement du ministère de l'Intérieur dans le cyberespace (COMCYBER-MI)

Le point de vue d'ANOZR WAY

« Cette étude unique sur le risque humain apporte un éclairage sous l'angle métier. Elle a plutôt confirmé ce que nous voyons sur le terrain autour du risque sur les dirigeants où nous observons généralement que 70 % des membres de Comex/Codir sont exposés à un niveau de risque élevé à très élevé.

En revanche cette étude introduit le fait que d'autres types de métiers et fonctions dans l'entreprise sont particulièrement vulnérables. Ce phénomène est spécifiquement préoccupant compte-tenu de l'automatisation grandissante des attaques par ingénierie sociale (usurpation de compte, phishing personnalisé, fraude, etc.) exploitant les fuites de données massives des dernières années.

Cette étude illustre enfin la tendance de fond décrite en 2024 par Forrester [7] sur le besoin d'évoluer vers une véritable gestion du risque humain. Cette approche, qui dépasse la simple sensibilisation générique, plaide pour une personnalisation des actions de prévention en fonction du profil de risque des personnes. Cette approche ciblée marque un tournant vers une cybersécurité plus humaine, plus stratégique, et surtout plus efficace.

Chez ANOZR WAY, nous avons fait de cette personnalisation un pilier de notre accompagnement, en analysant l'empreinte numérique individuelle et le profil de risque pour adapter les mesures de protection. »

Nicolas Laurenchet, Directeur Commercial

[7] The Future Is Now: Introducing Human Risk Management, Forrester

5.2. Les suites de l'étude

Cette étude, menée conjointement entre Breizh Cyber et ANOZR WAY a pour vocation d'être reconduite. Si cette première édition a permis de confirmer certaines hypothèses sur un échantillon limité, tout en révélant des éléments spécifiques, l'élargissement du périmètre, avec un plus grand nombre de secteurs représentés, d'entités scannées et d'individus analysés, permettra de pondérer les résultats et d'affiner la cartographie du risque humain à l'échelle de la Bretagne.

Par ailleurs cette étude met en évidence une magnifique opportunité de décloisonnement de la cybersécurité. En effet, les grandes fonctions d'une entreprise ont désormais leur référentiel et savent que leurs métiers peuvent parfois les exposer à des risques supérieurs à ceux de leurs collègues.

Enfin, cette étude ouvre une perspective sur les risques cyber des particuliers. Dans ce contexte d'automatisation des attaques par ingénierie sociale, les cibles principales de demain seront les particuliers. **Equiper ses dirigeants et salariés de solutions de protection des risques cyber humains deviendra ainsi un avantage salarial dans les entreprises !**

6

La méthodologie

6.1. La méthodologie

L'échantillon considéré est composé de 81 entités publiques et privées, qui se sont portées volontaires pour représenter 14 secteurs différents : les activités juridiques et comptables, l'agroalimentaire, les assurances, les banques, le commerce, la construction, l'énergie, l'enseignement, l'industrie, l'information et de la communication, les transports logistiques, les travaux publics, la santé, et le secteur public.
La méthodologie d'évaluation du risque humain complète, telle qu'elle a été développée par ANOZR WAY, comprend le croisement d'informations disponibles en sources ouvertes à celles issues des bases de données ayant fuité. Ce sont les empreintes numériques de près de 18 000 individus qui ont été quantifiées et analysées.

Pour cette étude, nous avons retenu une méthodologie d'évaluation simplifiée se basant sur les éléments individuels suivants :

- La détection d'un compte LinkedIn sur lequel l'individu déclare faire partie de l'entité étudiée ;
- La détection de l'adresse email professionnelle actuelle dans des fuites de données ;
- La détection d'un mot de passe lié à l'adresse email professionnelle dans des fuites de données ;
- La détection d'une autre adresse email (professionnelle ou personnelle) dans des fuites de données ;
- La détection d'une adresse postale dans les fuites de données ;
- La détection d'un numéro de téléphone dans les fuites de données ;
- La détection d'inscription à des sites tiers avec l'adresse email professionnelle

Les catégories de métiers/fonctions retenues pour l'étude sont :

- Les dirigeants (direction, management, fondateurs)
- La finance (finance, comptabilité, audit)
- Les métiers juridiques (juristes, assistants juridiques, etc.).
- La sécurité informatique (sécurité informatique, cybersécurité)
- Les commerciaux (commercial, vente)
- La communication et le marketing
- La sécurité physique (sécurité physique, maintenance, exploitation)
- Les ressources humaines (ressources humaines, recrutement)
- L'informatique et les développeurs (informatique, développement logiciel)
- Les métiers manuels (métiers manuels, opérationnels, terrain)

- La logistique (logistique, chaine d'approvisionnement, achats)
- L'ingénierie / R&D (ingénierie, R&D, qualité, production)
- Les services de l'ordre (Police, Gendarmerie, Pompiers)
- La santé privée
- Autres (les métiers ne pouvant pas être classés dans les catégories précédentes)

Les pourcentages de chaque graphique sont pondérés par le nombre d'individus par catégorie de métier. Les personnes ayant un haut risque signifie que leur niveau de risque se situe entre 6 et 8 sur 10, et très haut risque signifie que le niveau de risque est supérieur à 8 sur 10.

L'évaluation du risque humain est intrinsèquement liée aux éléments individuels détectés puisqu'il admet la possibilité pour un cyberattaquant d'utiliser ses informations personnelles à des fins malveillantes pour cibler l'individu et/ou l'entreprise ou l'organisation à laquelle il appartient.
Les résultats présentés dans cette étude ont été entièrement anonymisés afin de garantir la confidentialité des entités et des individus concernés.

6.2. Les experts :

Fabrice LITAIZE

Fabrice LITAIZE, expert en cybercriminalité, a passé 31 ans au sein de la Gendarmerie parmi les services d'Enquête Financière et Cybercriminalité. Il accompagne au quotidien des dirigeants et VIP dans la protection de leurs données personnelles et de leur entreprise.

Esther PICCINALI

Esther PICCINALI est diplômée d'un master 2 en Géopolitique et Sécurité Internationale obtenu à l'Institut Catholique de Paris. Elle a débuté sa carrière dans l'analyse géopolitique au sein d'entreprises françaises de services de sécurité et de défense (ESSD). Elle se spécialise ensuite en cybersécurité. Après une première expérience chez CybelAngel, elle rejoint les équipes d'ANOZR WAY en 2024.

Alban ONDREJECK

Alban ONDREJECK est Directeur Général et Co-fondateur d'ANOZR WAY.
Diplômé d'un master en ingénierie des télécommunications, il rejoint l'Ecole de l'air et de l'espace et commence sa carrière en tant qu'Agent de renseignement pour le ministère des armées pendant 8 ans. Il rejoint ensuite l'entreprise Orange Business Services pendant 11 ans où il occupe dans un premier temps le poste de Consultant en sécurité de l'information puis de Directeur cybersécurité client. C'est en 2017 qu'il décide de cocréer avec Philippe LUC la société ANOZR WAY.

Guillaume CHÉREAU

Guillaume CHÉREAU est un expert en cybersécurité avec plus de 10 ans d'expérience dans le domaine avec des compétences dans la gouvernance de la sécurité, la gestion de crise et la réponse aux incidents. Actuellement directeur de Breizh Cyber, il a précédemment occupé un poste de consultant et responsable d'une équipe de consultants chez Orange Cyberdefense et à l'ANSSI, où il a dirigé le Bureau Management des Crises Cyber, contribuant à l'élaboration de la politique publique de gestion de crise cyber au niveau national et européen et participant au dispositif de gestion de crise de l'ANSSI à un niveau stratégique.

Valentin CHUZEL

Valentin CHUZEL est un expert en cybersécurité notamment dans le domaine de la détection et réponse à incident. Après une carrière de sous-officier spécialiste cyber au sein du ministère des armées, durant laquelle il a occupé les postes d'administrateur système et réseau, formateur en cybersécurité pour les spécialités réponse à incident et sécurité des systèmes, et manager à la section détection du SOC de la DIRISI, il a pris les fonctions de directeur adjoint de Breizh Cyber.

A propos d'ANOZR WAY

ANOZR WAY est un éditeur de logiciels breton dont la mission est de protéger les organisations, les dirigeants et les collaborateurs des attaques par ingénierie sociale : phishing, compromission de compte, usurpation d'identité...
Fondé par un expert en Open Source Intelligence et un spécialiste de la gestion des risques, ANOZR WAY propose une suite logicielle de gestion des risques cyber humains et de protection des personnes, conçue pour contrer les menaces cyber ciblant les collaborateurs.
ANOZR WAY a réalisé une première levée de fonds de 2 M€ en 2021 (BPI, Breizh Up et BNP Développement), puis une seconde de 6 M€ début 2024 (Dentressangle).

anozrway.com/fr | @anozrway | /company/anozrway

A propos de Breizh Cyber

Pour faire face à l'accroissement de la cybermenace, la Région Bretagne a créé, avec le soutien de l'Etat et de l'agence nationale de la sécurité des systèmes d'information (ANSSI), un centre de réponse aux incidents de sécurité informatique (CSIRT – Computer Security Incident Response Team). A l'échelle régionale, Breizh Cyber accompagne les entreprises, associations et collectivités bretonnes dans la réponse aux attaques ou l'anticipation des menaces cyber.

breizhcyber.bzh | /company/breizh-cyber