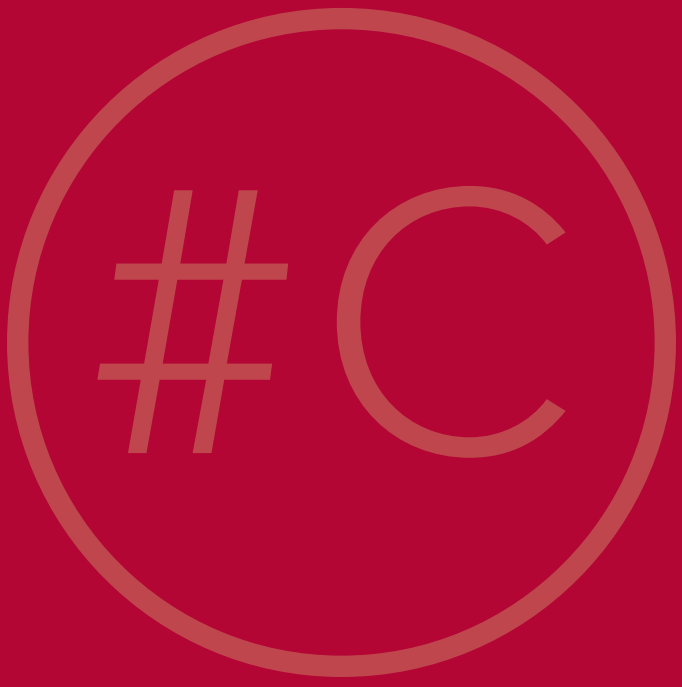


Le management des informations sensibles

*Étude Wellcom - Opinion Way, réalisée du 30 septembre au 20 octobre 2015, sur un échantillon de 402 cadres-dirigeants d'entreprise, constitué selon la méthode des quotas au regard du nombre de salariés et du secteur d'activité. Les résultats de ce sondage doivent être lus en tenant compte des marges d'incertitude : 2 à 5 points au plus pour un échantillon de 400 répondants.

LE MANAGEMENT
DES INFORMATIONS SENSIBLES

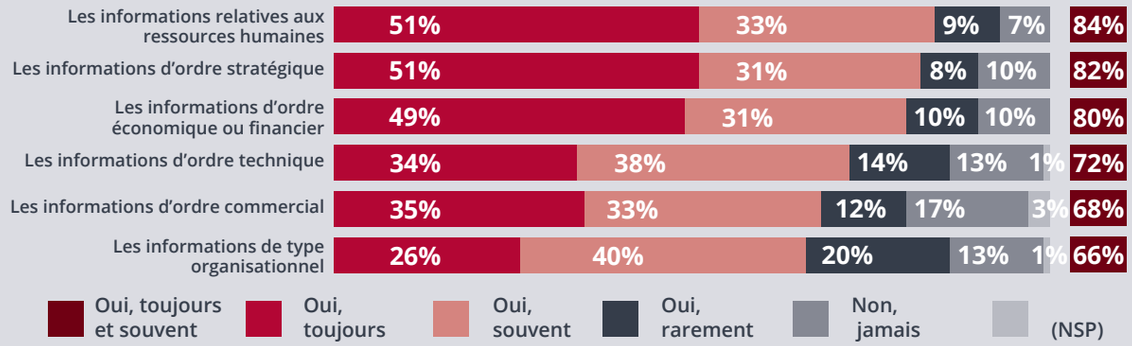
L'étude sur « Le management des informations sensibles » est destinée à comprendre et analyser la perception des cadres-dirigeants quant à la sécurité et la nature de leurs données sensibles ou secrètes relatives à leur entreprise. Comment les dirigeants des entreprises perçoivent-ils leurs informations sensibles ? Comment les protègent-ils ? Comment les entreprises communiquent avec leurs collaborateurs et leurs parties prenantes pour assurer leur sécurité ? Pour répondre à ces questions, WELLCOM* a interrogé en 2015, 400 dirigeants d'entreprises Françaises, représentatives de l'ensemble des secteurs d'activité, des tailles d'entreprises et des bassins de vie.

Rappelons que cette démarche fait suite à une étude qualitative initiée par Wellcom auprès de quinze Dirigeants ou Directeur de la sécurité de grands groupes industriels et qui a donné naissance à la méthode Miss® (Management des Informations Sensibles et Secrètes), démarche exclusive de gestion des informations destinée aux organisations et aux entreprises de tous secteurs d'activité.

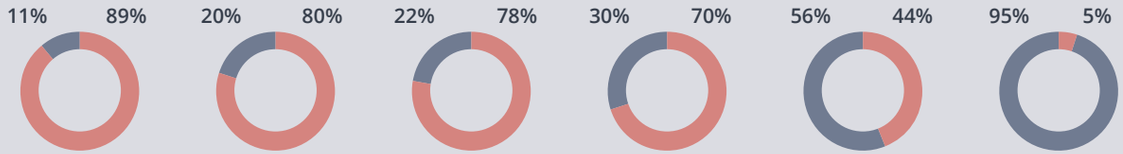
Les Informations sensibles, ce sont :

- Des informations ou **seulement une partie des publics** d'une organisation, qui peut parfois être très restreinte, **a le « droit d'en connaître ».**
- Des informations qui, quelle qu'en soit la ou les raisons, l'organisation considère **qu'il vaut mieux qu'elles ne soient pas divulguées** à tout ou partie soit de ses parties prenantes, soit de sa concurrence soit du grand public soit de la totalité de ses publics.
- Des informations **qu'il convient** d'**identifier**, de **classer**, de donner des **droits d'accès** et une **durée de péremption**.
- Des informations que l'organisation se doit de **protéger contre toute violation du secret.**

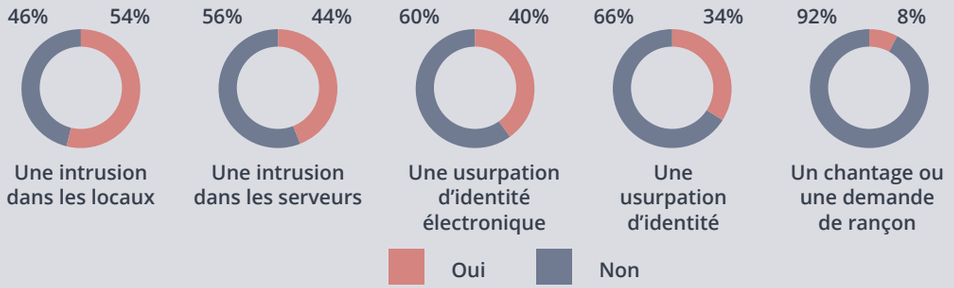
DANS VOTRE ENTREPRISE, CHACUNE DES CATÉGORIES D'INFORMATIONS SUIVANTES A-T-ELLE UN CARACTÈRE SENSIBLE QUI NÉCESSITE **UNE PROTECTION PARTICULIÈRE** ?



UTILISEZ-VOUS CHACUN DES SUPPORTS SUIVANTS **POUR CONSERVER LES INFORMATIONS SENSIBLES** ?

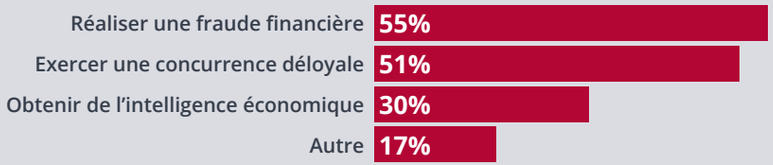


INTRUSION PHYSIQUE OU NUMÉRIQUE ET USURPATION D'IDENTITÉ SONT LES PRINCIPALES MENACES PERÇUES.



FRAUDE ET INTELLIGENCE ÉCONOMIQUE SERAIENT LES PRINCIPALES FINALITÉS DE CES ATTAQUES.

Question posée uniquement à ceux estimant être exposés à au moins une attaque soit 67% de l'échantillon (Plusieurs réponses possibles. Total supérieur à 100%)



La nature **des informations sensibles ou secrètes** en question…

Les cadres-dirigeants d'entreprise ont conscience qu'il existe au sein de leur entreprise des informations sensibles nécessitant une protection particulière.

- Il s'agit notamment des informations relatives aux ressources humaines (84%), les informations d'ordre stratégique (82%) et les informations d'ordre économique ou financier (80%). Dans une moindre mesure, les informations d'ordre technique (72%), les informations d'ordre commercial (68%) ou les informations de type organisationnel (66%) sont également perçues comme sensibles par les dirigeants, sans qu'elles constituent une source de risque récurrente.
- De manière significative, les dirigeants d'entreprises les plus importantes, (en termes de ressources humaines ou de chiffre d'affaires), sont marqués par le sentiment que toutes ces informations ont un caractère sensible.

Un **sentiment de sécurité** entoure (à tort) la gestion des informations sensibles…

Pour mettre à l'abri ces informations, les cadres-dirigeants d'entreprise ont recours à des espaces et des outils de protection dédiés qu'ils estiment sécurisés, qu'ils soient physiques ou numériques.

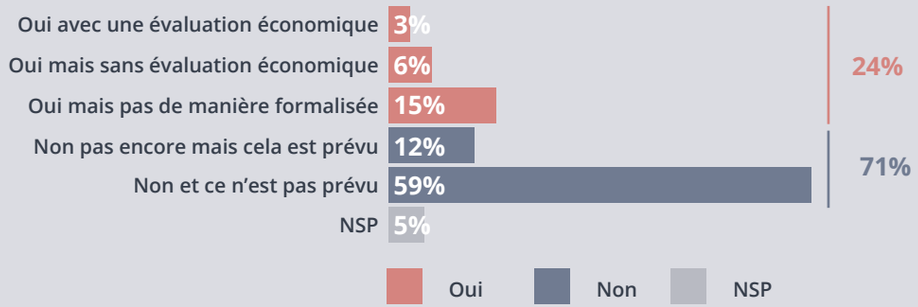
- L'armoire fermée à clé est ainsi le premier moyen envisagé par les dirigeants pour conserver leurs informations (81%), devant le coffre-fort (66%) et la pièce sécurisée (58%). Cette dernière, solution la plus sécurisée, s'avère plus largement utilisée dans les grandes entreprises, de 250 salariés et plus (71%) et de 50 millions d'euros et plus (72%).
- Les moyens numériques utilisés sont plus divers, les cadres-dirigeants d'entreprise privilégiant un serveur à accès sécurisé (89% d'utilisation), devant un serveur internet ou intranet (80%), un sur un poste de travail (78%), ou un disque dur dédié (70%). Le stockage sur serveur externe (Cloud, 44%) ne semble pour le moment pas faire partie des outils utilisés.

Afin de garantir la sûreté des informations présentes sur ces différents outils et système de stockage, les cadres-dirigeants d'entreprise affirment avoir entamé des démarches de sécurisation, de leurs systèmes d'information (88%).

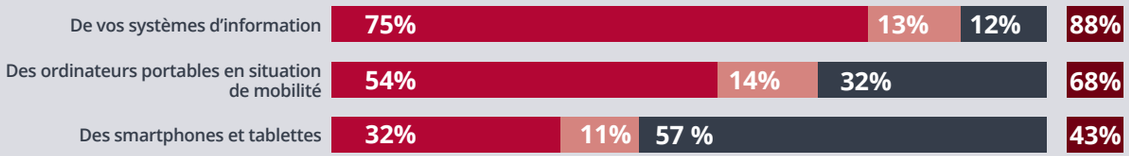
- Si les systèmes d'information sont à l'origine d'une surveillance particulière, les ordinateurs portables en situation de mobilité (68%), et surtout les smartphones et tablettes (43%) font nettement moins l'objet d'une protection, indice que les cadres-dirigeants sont moins alertes sur la question de la protection de leurs données qu'il n'y parait de premier abord.
- De plus, on remarque que la plupart des dirigeants font confiance aux systèmes de sécurisation qu'ils ont mis en place, et, suivant l'outil, seuls 11 à 14% des dirigeants reconnaissent que le procédé de sécurisation n'est peut-être pas suffisant.

La disparité entre la sensibilité des informations et les moyens mis en œuvre pour les protéger révèle ainsi véritablement un manque de prise de conscience de la part des dirigeants et la vulnérabilité des espaces de stockage, qu'ils soient physiques ou numériques.

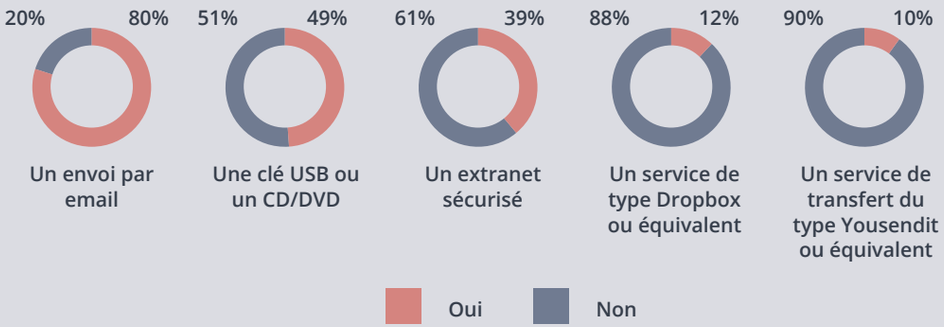
AVEZ-VOUS ÉVALUÉ LE PRÉJUDICE POTENTIELLEMENT LIÉ **À UNE RUPTURE DE CONFIDENTIALITÉ DE VOS INFORMATIONS SENSIBLES** ?



AVEZ-VOUS MIS EN PLACE **UNE DÉMARCHE DE SÉCURISATION**... ?



POUR COMMUNIQUER AVEC DES PERSONNES SITUÉES À L'EXTÉRIEUR DE VOTRE ENTREPRISE (comme par exemple vos clients, vos partenaires techniques, vos commerciaux), UTILISEZ-VOUS LES OUTILS SUIVANTS **POUR LA DIFFUSION DE DOCUMENTS QUI PEUVENT CONTENIR DES INFORMATIONS SENSIBLES** ?



... masquant la prise en compte insuffisante des risques et entraînant **des comportements dangereux pour la sécurité**...

Les cadres-dirigeants d'entreprise se montrent ainsi particulièrement confiants dans la sécurité de leur entreprise, minimisant les menaces auxquelles ils peuvent être exposés. Seule une intrusion dans les locaux semble être envisagée par la majorité d'entre eux (54%).

- Alors même que le serveur à accès sécurisé est le premier emplacement de stockage des données sensibles, seuls 44% des dirigeants craignent une intrusion étrangère dans leurs serveurs, témoin de la confiance qu'ils éprouvent envers la sécurité de leurs systèmes informatiques. Les dernières sources de menace pour les dirigeants sont finalement les usurpations d'identité, numériques (40%) ou non (34%), loin devant le chantage ou les demandes de rançon.

- Volonté de fraude financière (55%), de concurrence déloyale (51%) ou d'intelligence économique (30%) représentent pour eux les trois principales causes de menace contre la sécurité des entreprises.

Preuve de leur méconnaissance des risques entourant les informations sensibles, 71% des dirigeants n'ont pas effectué d'évaluation des préjudices relatifs à une rupture de confidentialité, parmi lesquels la plupart (59%) n'envisagent pas d'y avoir recours.

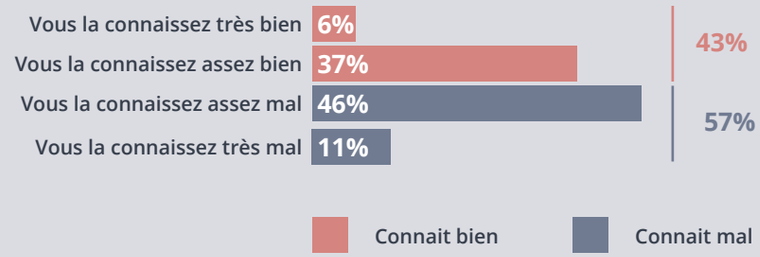
- Plus inquiétant encore, force est de constater que parmi les 24% de chefs d'entreprise ayant effectué ce type d'évaluation, il ne s'agit pour la plupart que d'une évaluation non formelle (15%).

L'absence d'un sentiment d'urgence ou de vulnérabilité de l'entreprise face aux attaques extérieures entraîne des comportements à risque de la part des entreprises.

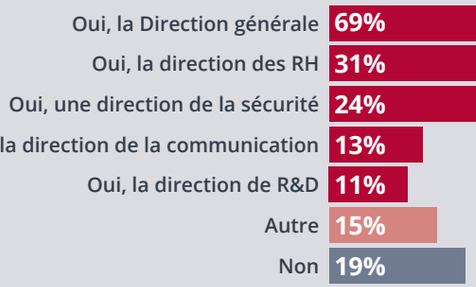
- Comme évoqué précédemment, les dirigeants n'ont pas encore pris le réflexe de protéger les ordinateurs portables en situation de mobilité (32%) ou de mettre en place une sécurisation des smartphones et tablettes (57%). Mais, en minimisant les menaces auxquelles sont exposés leurs outils de travail, ils mettent également en péril leurs informations sensibles au moment de leur transmission. 80% des dirigeants reconnaissent ainsi envoyer des informations sensibles à leurs clients par email ou par clé USD ou DVD (49%), des outils facilement exposés au vol ou au détournement.

- Les systèmes mis en place pour protéger ces informations font l'objet d'un contrôle insuffisant : 30% des cadres-dirigeants d'entreprise confirment n'avoir mis en place aucun dispositif de contrôle de la sécurité des informations sensibles et 29% effectuent un contrôle moins d'une fois par an.

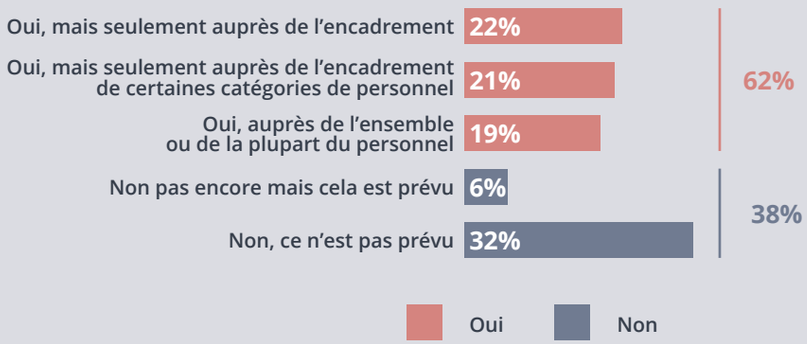
57% DES ENTREPRISES CONNAISSENT MAL LA RÉGLEMENTATION
LÉGALE EN MATIÈRE DE GESTION DES INFORMATIONS SENSIBLES.



AU SEIN DE VOTRE ENTREPRISE, DES PERSONNES SONT-ELLES SPÉCIFIQUEMENT
HABILITÉES À LA GESTION DES INFORMATIONS SENSIBLES ?



R&D ET COMMUNICATION SONT PEU INFORMÉS
SUR LA SÉCURITÉ INTERNE DES ENTREPRISES.



Une communication interne insuffisante

La sous-estimation des risques concernant le management des données sensibles se reflète dans le manque d'attention portée par les dirigeants à acquérir une connaissance ferme de leurs responsabilités juridiques en cas d'attaque.

- Quel que soit le secteur d'activité ou la taille l'entreprise, la majorité des dirigeants reconnait mal connaître la législation en matière de gestion des informations sensibles (57%), une méconnaissance qui accentue les défauts de gestion de ces informations.

- Autre reflet de ce manque d'encadrement juridique ferme, les cadres-dirigeants peinent à définir une durée fixe de conservation pour les documents sensibles. 25% des cadres-dirigeants reconnaissent qu'ils conservent les documents de façon indéterminée sans règle particulière (28% dans les entreprises au chiffre d'affaire inférieur à 15 millions d'euros) et 50% estiment que cette durée est définie en fonction de la nature des documents, autre manière d'avancer qu'il n'y a pas de directive particulière au sein de l'entreprise.

Le manque de connaissance législative des dirigeants s'accompagne d'un déficit de processus réglementés et de communication autour des informations sensibles qui mettent en péril leur sécurité.

- Dans près de la moitié des entreprises (44%), les personnes destinées à accéder aux informations sensibles n'ont pas reçu de formation ou d'habilitation particulière. Il apparait d'autant plus fondamental de mettre en place un système d'habilitation que les personnes habilitées à manipuler les informations sensibles se trouvent à des niveaux variés de la chaîne de valeur de l'entreprise. Il s'agit principalement de la direction générale (68%), de la direction des ressources humaines (31%) de la direction de la sécurité (24%), de la direction de la communication (13%) ou de la direction de la recherche et du développement (11%).

- Si les directions concernées ne sont pas nécessairement soumises à des processus d'habilitation, il apparaît que le personnel est encore plus faiblement mobilisé autour de la sécurité des données. Seuls 19% des cadres dirigeants affirment avoir mis en œuvre une communication liée à la gestion de la sécurité dans l'entreprise auprès de l'ensemble du personnel ou presque.

- Pour 43% des cadres-dirigeants, cette communication ne concerne aujourd'hui que les fonctions d'encadrement ou de catégories de personnel spécifique, quand encore 38% d'entre eux n'ont pas engagé de démarche de communication auprès de l'interne. Pour tous, qu'ils aient ou non recours à cette démarche d'information, l'outil privilégié d'une communication sur la sécurité est l'e-mail (53%), suivi de près par l'intranet (47%), le tableau d'affichage (47%), le livret d'accueil (44%), les procédures internes (37%) ou les brochures ou autres documents imprimés (26%).

En synthèse, cette étude révèle **4 grands enseignements** :

1. On s'aperçoit que la notion d'informations sensibles fait appel à **une compréhension mosaïque mettant à des niveaux équivalents des enjeux vitaux[1] des entreprises et des enjeux plus conjoncturels[2].**

2. **On constate un sentiment de sécurité qui induit un déficit de prise en compte de la part des dirigeants, de la complexité et de l'omniprésence des menaces concernant les outils et canaux de communication** utilisés par l'entreprise pour ses données sensibles, ainsi que de l'impact néfaste d'une fuite de ces données, que ce soit en termes économiques ou judiciaires.

3. Les grandes entreprises, en nombre de salariés ou de chiffre d'affaires, ainsi que les entreprises du secteur de l'industrie et de la construction, même si leur prise en compte des risques se révèle limitée, ont pris, pour une partie d'entre elles, de moins mauvais réflexes concernant la sécurisation et le management de leurs données sensibles et l'information de l'interne concernant la sécurité.

4. **Il apparait urgent pour les entreprises de travailler à la mise en place de démarches de communication envers l'interne**, incluant également des processus d'habilitation au management des données sensibles, afin de renforcer la mobilisation autour de la sécurité et de réduire les comportements à risque.

[1] Enjeux vitaux: information d'ordre stratégique, information d'ordre commercial, information d'ordre économique ou financier.

[2] Enjeux plus conjoncturels : information de type organisationnel, information relative aux ressources humaines.

Retrouvez ici
toutes les publications Wellcom