ÉTUDE CLUSIF

Menaces informatiques et pratiques de sécurité en France

Édition 2020

- Les entreprises de plus de 100 salariés

CLUSIF

Remerciements

Le Clusif remercie les personnes qui ont constitué le Comité d'experts ayant participé à cette étude et tout particulièrement :

Les responsables du groupe de travail

M. MOURER Lionel	MANIKA	Responsable de l'étude et de la partie Entreprises
M. BRAS Cyril	GRENOBLE-ALPES MÉTROPOLE	Responsable de la partie Collectivités territoriales
M. NOTIN Jérôme	GIP ACYMA	Responsable de la partie Internautes

Les membres du Comité d'experts

M. ARDOUIN Philippe	EAU17
M. BLUM Patrick	CLUSIF
M. BOUET Grégory	TOULOUSE MÉTROPOLE
M. BOUVET Adrien	APIXIT
M. CAILLEAUX Cédric	AXIANS
M. DAMI Saïd	CHUBB EUROPEAN GROUP LTD
M. DELUARD Raphaël	NEURONES IT
M. ÉGÉA Éric	NTT FRANCE
M. HENNIART Thierry	RÉGION HAUTS-DE-FRANCE
M. JANGWA Valentin	BITGLASS INC.
M. JOUAS Jean-Philippe	CLUSIF
M. KEFI Mehdi	HARMONIE TECHNOLOGIE
M. MILLOT Francis	SYSTANCIA
M. MINASSIAN Vazrik	ADENIUM SAS
M. PETERSEN Axel	WAVESTONE
M. POINTU Frédéric	GRAND LYON
M^{me} QANDAR Jamila	CONIX
M. STEUER Philippe	BORDEAUX MÉTROPOLE
M. TETELIN Éric	MINISTÈRE DE LA TRANSITION ÉCOLOGIQUE ET SOLIDAIRE
M. TOUVET Jean-Christophe	SIMPLOS
M. WURSTHEISER Philippe	HUAWEI TECHNOLOGIES FRANCE

Le Clusif remercie également vivement les représentants des entreprises et des collectivités territoriales ainsi que les internautes qui ont bien voulu participer à cette enquête.

Enquête statistique réalisée pour le Clusif par le cabinet GMV Conseil.

Synthèse de l'étude

Au travers de l'édition 2020 de son enquête sur les menaces informatiques et les pratiques de sécurité (MIPS), le Clusif réalise, comme tous les deux ans, un bilan approfondi des usages en matière de sécurité de l'information en France.

Cette enquête se veut une référence du fait de la taille et de la représentativité des échantillons d'entreprises (350 ont répondu) interrogées. Par ailleurs, elle se veut la plus exhaustive possible, en reprenant, cette année encore, l'ensemble des 14 thèmes de la norme ISO 27002:2013, relative à la sécurité de l'information.

L'enquête est structurée, cette année encore, sur quatre tranches d'effectifs (100-249, 250-499, 500-1 999 et plus de 2 000 salariés) permettant, depuis 2018 et dans les années à venir, d'identifier les pratiques des plus petites entreprises…

Entreprises : « sécurité de l'information, tout le monde pense que c'est important, elle avance… mais les budgets restent précaires !

Au fil des ans, les entreprises ont gagné en maturité, des organisations et des structures se sont mises en place. Ainsi, en 2020, un chiffre marque les esprits : 56 ! Cinquante-six pour cent, c'est en effet la part des budgets alloués à la sécurité de l'information « entièrement remis en cause chaque année » (seuls 8 % sont « sanctuarisés »).

Ce chiffre montre, à lui seul, à quel point la sécurité de l'information peine à prendre sa place au plus haut niveau des entreprises. Combien de responsables de la sécurité des systèmes d'information (RSSI) ou du système d'information (DSI/RSI) font aujourd'hui partie des plus hautes instances de direction ? La réponse est « trop peu » et la question reste posée ! Dans le détail et cette année encore, la mise en place de solutions reste en tête des investissements, avec 40 % (+ 17 points), prouvant une fois de plus que la sécurité est toujours perçue comme une histoire de « technologie ».

Pour autant, tout n'est pas sombre et la sécurité de l'information, soumise à des contraintes légales et réglementaires en constante évolution (règlement général sur la protection des données – RGPD –, loi de programmation militaire – LPM –, directive européenne *Network and Information System Security* – NIS – , etc.) continue d'avancer, tranquillement…

Du côté de la politique de sécurité de l'information (PSSI), le nombre d'entreprises l'ayant formalisée continue de progresser pour atteindre 75 % (+ 6 points par rapport à 2018), cette évolution étant tirée vers le haut par les entreprises de 100 à 249 salariés. La Direction générale (DG) reste prépondérante dans la formalisation de la PSI (52 %), suivi de la Direction des systèmes d'information (DSI) (58 %) et du RSSI (41 %).

La fonction de RSSI est en évolution sensible, le pourcentage d'entreprises qui en sont aujourd'hui dotées s'élevant à 72 % (*vs* 58 % en 2018), voire 93 % dans le secteur des banques et des assurances ! Les RSSI sont pour 56 % d'entre eux rattachés à la Direction générale, améliorant grandement leur « pouvoir d'arbitrage » et pour 31 % à la DSI.

Du côté des ressources humaines, si les chartes sont aujourd'hui bien déployées (85 % en ont), seuls 34 % sont orientées vers les prestataires. Pour la sensibilisation, 60 % en déploient, dont 30 % qui la mesurent (part en évolution de 15 points). La sensibilisation commence à prendre une place importante, apportant sa pierre à la mise en place d'une véritable acculturation en matière de sécurité de l'information.

L'inventaire des actifs (en tout ou partie) est réalisé à 95 % et 80 % des entreprises ont classifié leurs actifs. Par ailleurs, une large majorité (88 %) des entreprises a dressé un inventaire des risques, mais peu d'entre elles (23 %) ont réalisé une analyse formelle en s'appuyant sur une méthode ou un référentiel. Lorsque c'est le cas, elles ont utilisé les normes ISO 27005 (39 %), Ebios (16 %), Méhari (12 %), etc.

Pour le contrôle d'accès, toutes les technologies augmentent, sauf la biométrie. Les procédures de gestion de comptes sont déployées dans 80 % des entreprises et la gestion des comptes à hauts privilèges progresse (82 %, + 15 points *vs* 2018).

La cryptographie est toujours peu utilisée (28 % en font l'usage, – 2 points *vs* 2018) avec toutefois une grande disparité selon la taille de l'entreprise et, lorsqu'elle l'est, c'est la DSI qui en a largement le contrôle (92 %).

La sécurisation physique reste portée par les mêmes trois dispositifs majeurs : contrôle d'accès par badge (71 %), détecteur d'incendie (65 %) et caméra (61 %).

Du côté des technologies de protection, les outils dits « classiques » (solutions antivirus et *antimalware,* antispam, pare-feu – *firewall*) sont unanimement adoptés, de 89 % à 100 %, quand le taux d'utilisation des outils plus « spécifiques » (sondes de détection d'intrusion – *Intrusion Detection System,* IDS –, gestion d'événements de sécurité – *Security Information and Event Management,* SIEM –, contrôleur d'accès au réseau – *Network Access Control,* NAC –, protection contre la fuite de données sensibles – *Data Leak Protection,* DLP) se situe entre 33 % à 66 %. À noter : la mobilité est de plus en plus prise en compte.

Une veille permanente en vulnérabilités et en solutions de sécurité de l'information est réalisée par 86 % des entreprises et 57 % ont formalisé des procédures de déploiement des correctifs de sécurité (patch management).

L'usage des équipements personnels (*Bring Your Own Device* – BYOD) est interdit pour 62 % (– 10 points) des entreprises…

La sécurité dans le cycle de développement régresse encore et reste, de fait, toujours insuffisante : prise en compte à 25 % (+ 11 points tout de même), elle demeure une des grandes oubliées… Pourtant, un grand nombre d'attaques sont possibles du fait de failles applicatives liées au développement (injection, XSS, etc.) et les pratiques de développement (*development operations* – DevOps) apportent leur lot de vulnérabilités.

L'infogérance représente 51 % (+ 7 points) de la gestion des SI des entreprises, dont 7 % en totalité (– 6 points). Quand c'est le cas, 26 % (– 12 points) ne mettent toujours pas en place d'indicateurs de sécurité et 31 % (– 24 points) ne réalisent aucun audit sur cette infogérance.

Côté « incidents de sécurité de l'information », le trio de tête est composé des pannes d'origine interne (29 % *vs* 31 % en 2018), des pertes de services essentiels (29 % *vs* 33 % en 2018) et des vols (22 % *vs* 21 % en 2018). La cellule de collecte et de traitement des incidents de sécurité de l'information existe maintenant dans 59 % (+ 18 points) des entreprises. De plus, au regard du *Panorama de la cybercriminalité* du Clusif, 12 % ont connu des attaques par rançongiciel *(ransomware),* avec pour 38 % d'entre elles un impact fort.

Pour la continuité d'activité, c'est toujours l'indisponibilité des systèmes informatiques de gestion qui représente le scénario le plus couvert (62 %). Le bilan d'impact sur l'activité (BIA), prenant en compte les attentes des « métiers » est réalisé dans 51 % (dont 14 % en cours) des entreprises : comment les autres s'assurent-elles que leur plan de continuité d'activité (PCA) répond aux attentes de l'entreprise ? Enfin, pour celles qui en disposent, 23 % des plans « utilisateurs » et 14 % des plans « IT » ne sont jamais testés : alors, sont-ils réellement efficients ?

Le délégué à la protection des données (DPD, *Data Privacy Officer* – DPO) est présent dans 57 % des entreprises et s'occupe de la mise en conformité au RGPD. Cette conformité est totale pour 73 % des entreprises et partielle pour 24 %.

Sur une période de deux ans, 81 % des entreprises interrogées ont réalisé au moins un audit ou un contrôle de sécurité du SI (68 % des tests d'intrusion et 58 % des audits organisationnels). Ces audits sont motivés principalement par des exigences contractuelles ou réglementaires (59 %, + 26 points).

Les tableaux de bord de la sécurité de l'information (TBSSI) sont déployés dans 30 % des entreprises (22 % en 2018) : c'est encore trop peu ! Pourtant, le TBSSI reste un moyen simple et efficace, pour autant que l'on ait choisi les bons indicateurs, de « piloter » la sécurité de l'information au sein de son entreprise…

En résumé pour les entreprises de plus de 100 salariés, s'il est clair que le niveau global de maturité continue d'évoluer « tranquillement », cette évolution est plus liée aux obligations existantes (légales, réglementaires, contractuelles) qu'à la prise en compte réelle de l'importance de la sécurité de l'information. Cet état de fait est encore plus visible lorsque l'on regarde la taille des entreprises, les plus grandes ayant clairement une meilleure maturité que les plus petites. Pour autant, les menaces sur l'information ne faiblissent pas et plus que jamais, les organisations doivent être prêtent à réagir au moindre incident et, finalement, se poser la question de leur propre résilience…

Pour conclure…

La menace qui pèse sur l'information est toujours bien présente en 2020 et l'enquête montre une nouvelle fois à quel point les erreurs (personne n'est parfait…), les malveillances (certains se lèvent le matin pour cela…) et les incidents de sécurité liés à l'information ne fléchissent pas !

La maturité de tous et toutes (entreprises, collectivités territoriales et particuliers) en matière de sécurité de l'information dépend encore pour beaucoup soit des « attaques » que ces différents acteurs ont vécues au sein de leur SI, soit des lois et règlements qui leur incombent. En 2018, j'écrivais : « Le temps des politiques de sécurité "parapluie", que l'on formalise pour se donner bonne conscience, est globalement terminé ! » Comme j'aurais aimé que cela soit entendu… Mais il n'est pas trop tard : Messieurs les Dirigeants, comprenez[1] que la sécurité de l'information est aujourd'hui incontournable, il y va de la survie de vos organisations, au regard des enjeux qu'elles portent et des données dont elles ont la responsabilité…

Alors, « au travail », afin que la sécurité de l'information prenne enfin toute sa place ! Et n'oublions pas : « Quand un arbre tombe, on l'entend, quand la forêt pousse, pas un bruit…[2] »

Pour vous aider dans la mise en œuvre de vos mécanismes de sécurité de l'information (organisationnels et techniques, vous pouvez toujours prendre en compte les bonnes pratiques issues (liste non exhaustive) de l'Agence nationale de la sécurité des systèmes d'information (Anssi)[3], de la Confédération des petites et moyennes entreprises (CPME)[4], du groupement d'intérêt public « Action contre la cybermalveillance » (GIP Acyma)[5] et, bien entendu, du Clusif[6]…

Épilogue

Comme précisé au chapitre « Méthodologie », les questions posées pour formaliser l'étude MIPS 2020 portent sur l'année 2019. « Et le coronavirus ? », me direz-vous… Cette crise, encore en cours, a touché en plein cœur nombre d'organisations et, de fait, certains paradigmes sont clairement en train d'évoluer… Pour mémoire, l'étude MIPS n'a pas vocation à traiter à chaud l'actualité, mais il n'en est pas moins certain que la COVID-19 va rebattre les cartes au regard d'habitudes qui vont nécessairement devoir évoluer ! Alors, vivement l'étude 2022, qui nous permettra d'y voir plus clair…

Enfin et pour les plus courageux d'entre vous, l'étude détaillée et argumentée vous attend dans le reste de ce document…

Bonne lecture !

Lionel MOURER

Pour le Groupe de Travail « Enquête sur les menaces informatiques et les pratiques de sécurité »

[1] Pour vous aider à comprendre 😉 : https://clusif.fr/publications/livre-blanc-la-cybersecurite-a-lusage-des-dirigeants/

[2] Proverbe sud-africain.

[3] https://www.ssi.gouv.fr/

[4] http://cien.cpme.fr/2016/07/03/guide-bonnes-pratiques-informatiques/

[5] www.cybermalveillance.gouv.fr

[6] https://clusif.fr/

Sommaire

Liste des figures

Méthodologie

L'enquête du Clusif sur les menaces informatiques et les pratiques de sécurité en France en 2020 a été réalisée de début janvier à mi-mars 2020, en collaboration avec le cabinet spécialisé GMV Conseil, sur la base de questionnaires d'enquête élaborés par le Clusif. Les questions posées portaient sur l'année 2019.

Comme dans les études précédentes, trois cibles ont été retenues pour l'édition 2020 :

- les entreprises de plus de 100 salariés : 350 entreprises de cette catégorie ont répondu à l'enquête ;
- les collectivités territoriales : 202 structures ont accepté de répondre ;
- les particuliers internautes (âgés de 15 ans et plus) : 998 personnes issues d'un panel d'internautes représentatifs français ont participé à cette étude en répondant *via* Internet.

Pour les deux premières cibles, le questionnaire utilisé a été construit en reprenant les thèmes de la norme ISO 27002:2013 décrivant les différents items à couvrir dans le domaine de la sécurité de l'information. L'objectif était de mesurer de manière la plus exhaustive possible le niveau actuel d'implémentation des meilleures pratiques dans ce domaine. Ces différents thèmes sont numérotés de 5 à 18.

- Thème 5 : Politique de sécurité de l'information
- Thème 6 : Organisation de la sécurité de l'information
- Thème 7 : Sécurité des ressources humaines
- Thème 8 : Gestion des actifs
- Thème 9 : Contrôle d'accès
- Thème 10 : Cryptographie
- Thème 11 : Sécurité physique et environnementale
- Thème 12 : Sécurité liée à l'exploitation
- Thème 13 : Sécurité des communications
- Thème 14 : Acquisition, développement et maintenance des systèmes d'information
- Thème 15 : Relations avec les fournisseurs
- Thème 16 : Gestion des incidents liés à la sécurité de l'information
- Thème 17 : Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité
- Thème 18 : Conformité

Pour ce qui concerne les particuliers internautes, les thèmes suivants ont été abordés :

- caractérisation socioprofessionnelle des personnes interrogées et identification de leurs outils informatiques (ordinateurs et smartphones) ;
- usages de l'informatique et d'Internet à domicile ;
- perception de la menace informatique, sensibilité aux risques et à la sécurité, incidents rencontrés ;
- pratiques de sécurité mises en œuvre (moyens et comportement).

Les réponses aux questions ont été consolidées par le cabinet GMV Conseil en préservant un anonymat total des informations, puis les résultats statistiques ont été analysés par un groupe d'experts du Clusif, spécialistes du domaine de la sécurité de l'information.

Afin de simplifier la compréhension du document, le choix a été fait de ne citer que les années de publication des rapports, à savoir 2020, 2018, 2016, etc. Les enquêtes ont été réalisées sur le premier trimestre de l'année de publication mais les chiffres cités portent donc sur l'année précédente, soit respectivement 2019, 2017, 2015, etc.

Enfin, le groupe d'experts tient à préciser que toute enquête de ce type contient nécessairement des réponses discordantes dues à la subjectivité de l'observation sur des domaines difficilement quantifiables ou, dans le cas du spécifique de la sécurité du système d'information, de la personne répondant aux questions, de la « culture » et de la maturité de chaque entreprise, collectivité territoriale ou internaute.

Le présent document porte sur la cible « Entreprises ». Les autres cibles sont disponibles chacune dans un rapport spécifique. Un rapport complet présentant les 3 cibles est également disponible.

Entreprises

- Présentation de l'échantillon
- Moyens consacrés à la sécurité de l'information par les entreprises
- Thème 5 : Politique de sécurité de l'information (PSSI)
- Thème 6 : Organisation de la sécurité de l'information
- Thème 7 : Sécurité des ressources humaines
- Thème 8 : Gestion des actifs
- Thème 9 : Contrôle d'accès
- Thème 10 : Cryptographie
- Thème 11 : Sécurité physique et environnementale
- Thème 12 : Sécurité liée à l'exploitation
- Thème 13 : Sécurité des communications
- Thème 14 : Acquisition, développement et maintenance des systèmes d'information
- Thème 15 : Relation avec les fournisseurs
- Thème 16 : Gestion des incidents liés à la sécurité de l'information
- Thème 17 : Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité
- Thème 18 : Conformité

Les entreprises de plus de 100 salariés

Présentation de l'échantillon

Pour l'édition 2020 de son enquête, le Clusif a interrogé un échantillon d'entreprises identique à celui sur lequel s'était basée l'étude réalisée en 2018. Ainsi, la cible est constituée des entreprises de plus de 100 salariés des secteurs d'activité suivants :

- Banques – Assurances ;
- Commerce ;
- Industrie – BTP ;
- Services ;
- Transports – Télécoms.

Au total, 350 entreprises ont répondu à la sollicitation du Clusif (entretien d'une durée de 32 minutes en moyenne), avec un taux d'acceptation d'environ 9 % (*vs* 6 % en 2018) : sur 100 entreprises contactées, seulement neuf ont accepté de répondre à nos questions, ce qui a impliqué de contacter environ 3 900 entreprises !

L'échantillon est construit selon la méthode des quotas avec deux critères – l'effectif et le secteur d'activité des entreprises – pour obtenir les résultats les plus représentatifs de la population des entreprises.

Cet échantillon est ensuite redressé sur l'effectif et le secteur d'activité pour se rapprocher de la réalité des entreprises françaises, sur la base des données de l'Institut national de la statistique et des études économiques (Insee) (démographie des entreprises de plus de 100 salariés).

Taille / Secteur	100-249 salariés	250-499 salariés	500-1 999 salariés	2 000 et plus	Total	Total en %		Données Insee
Banques – Assurances	6	6	4	6	**22**	**6,4 %**	→	**5,0 %**
Commerce	45	10	6	2	**63**	**18,3 %**	→	**23,3 %**
Industrie – BTP	91	35	17	6	**149**	**43,3 %**	→	**37,2 %**
Services	44	20	15	8	**87**	**25,3 %**	→	**20,0 %**
Transports – Télécoms	11	4	7	1	**23**	**6,7 %**	→	**14,5 %**
Total	**197**	**75**	**49**	**23**	**344**	**100,0 %**		**100,0 %**
Total en %	**57,3 %**	**21,8 %**	**14,2 %**	**6,7 %**	**100,0 %**			
Redressement →	↓	↓	↓	↓				
Données Insee	**62,9 %**	**20,6 %**	**13,3 %**	**3,2 %**	**100,0 %**			

Redressement ↑

Au sein de chaque entreprise, nous avons cherché à interroger en priorité le responsable de la sécurité des systèmes d'information (RSSI). Pour 22 % (*vs* 25 % en 2018) des entreprises interrogées, celui-ci a accepté de répondre, ce taux atteignant 36 % dans les entreprises entre 500 et 1 999 salariés et 35 % dans les entreprises de plus de 2 000 salariés (40 % en 2018).

Toutes tailles et tous secteurs confondus, les personnes sondées sont à plus de 89 % des directeurs des systèmes d'information (DSI), des directeurs ou responsables informatiques ou des RSSI (73 % en 2018).Moyens consacrés à la sécurité de l'information par les entreprises

En préambule, toutes les entreprises – tous secteurs confondus et quelle que soit leur taille – confirment, cette année encore, que l'informatique est perçue comme stratégique. Ce fait est plus que jamais acté.

Une reprise sensible des budgets liés à la sécurité de l'information

Seuls 34 % des entreprises (+ 14 points *vs* 2018) identifient les coûts (ce qui ne se traduit pas forcément à un budget) liés à la sécurité de l'information : cela reste faible !

Globalement, le pourcentage des budgets « constants » est de 43 % (*vs* 35 % en 2018), mais encore 16 % des interviewés ne connaissent pas l'évolution du budget alloué à la sécurité de l'information dans leur entreprise ! Les budgets en augmentation (forte ou moyenne) représentent quant à eux 39 % (*vs* 30 % en 2018) des budgets alloués à la sécurité de l'information, cette tendance étant la plus marquée (47 %) dans le secteur des banques et des assurances, le « mauvais élève » – les services – affichant des taux cumulés de 35 %, avec une belle progression tout de même !

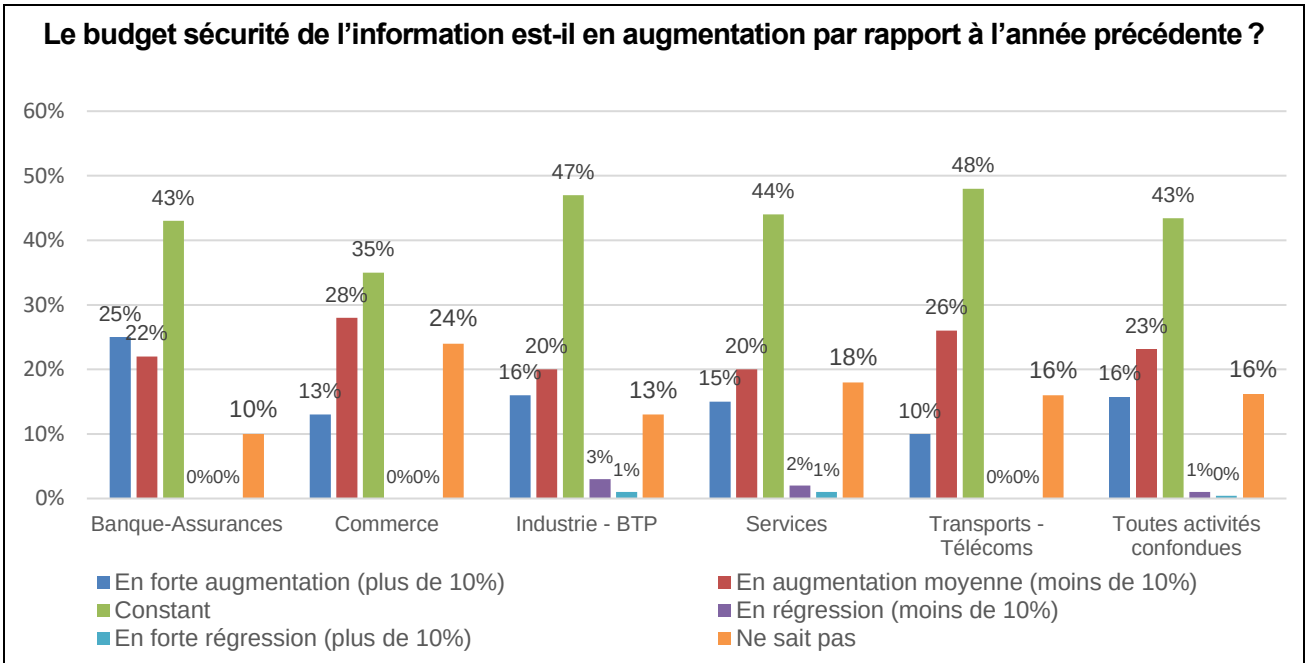


Figure 1 – Évolution du budget sécurité selon les secteurs d'activité

Par ailleurs, les budgets sont « sanctuarisés » pour seulement 8 % des entreprises, alors que pour 56 %, ils sont « entièrement remis en cause chaque année ».

Enfin, les trois postes prioritaires, qui enregistrent de très belles progressions, sont :

- la « mise en place de solutions » (40 %, + 17 points *vs* 2018), confirmant que pour beaucoup d'entreprises, la sécurité de l'information relève de solutions techniques ;
- la « formation/sensibilisation » (25 %, + 13 points), qui fait plus que doubler, assurant (enfin !) qu'un quart des entreprises (peut mieux faire) ont intégré l'importance de placer l'humain au cœur du dispositif de sécurité de l'information ;
- la « mise en place d'éléments organisationnels » (24 %, + 14 points), qui, elle aussi, fait plus que doubler, avec la même remarque que pour le poste précédent.

À noter : les « contrôles & audits » (19 %, – 2 points) en quatrième position sortent du podium.

Les contraintes organisationnelles et le budget freinent encore le RSSI

Enfin, lorsque l'on cherche à connaître les freins à la conduite des missions de sécurité dans leur entreprise, les RSSI citent les points présentés ci-dessous.

Citez les principaux freins à la conduite des missions de sécurité de l'information

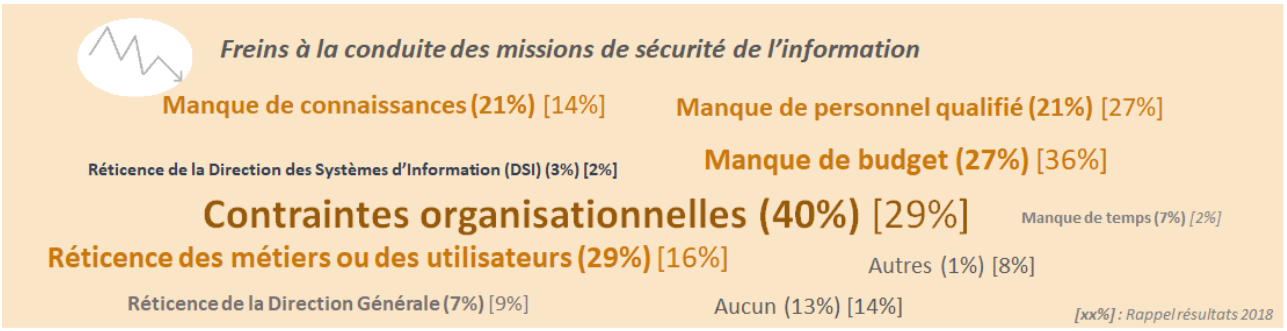


Figure 2 – Principaux freins à la conduite des missions de sécurité de l'information

Pour la deuxième enquête consécutive, la réticence de la Direction générale est très faible (7 % en 2020, 9 % en 2018 et supérieure à 15 % en 2016 et 2014), confirmant la prise en compte de la sécurité de l'information au plus haut niveau ; il en est de même de la DSI (3 % *vs* 2 % en 2018). Il semble donc que la sécurité de l'information a, dans un cadre législatif et réglementaire de plus en plus contraint, (enfin) atteint une certaine reconnaissance… qui commence à se répercuter dans les budgets. En effet, le manque de moyens budgétaires, premier frein observé dans les trois études précédentes, arrive aujourd'hui en troisième position (27 % *vs* 36 % en 2018), derrière les contraintes organisationnelles (40 % *vs* 29 % en 2018) et les réticences des métiers ou des utilisateurs (29 % *vs* 16 % en 2018) !

Arrive ensuite le manque de personnel qualifié. Bien que le chiffre diminue de 6 points en 2020, il est le signe (et ce, depuis de nombreuses années maintenant) d'une continuelle difficulté à recruter dans le secteur de la sécurité de l'information.

Thème 5 : Politique de sécurité de l'information (PSSI)

Progression de la formalisation et confirmation de son importance

Le nombre d'entreprises ayant formalisé leur PSSI continue de progresser, à près de 75 % (*vs* 69 % il y deux ans).

Votre entreprise a-t-elle formalisé sa politique de sécurité de l'information ?

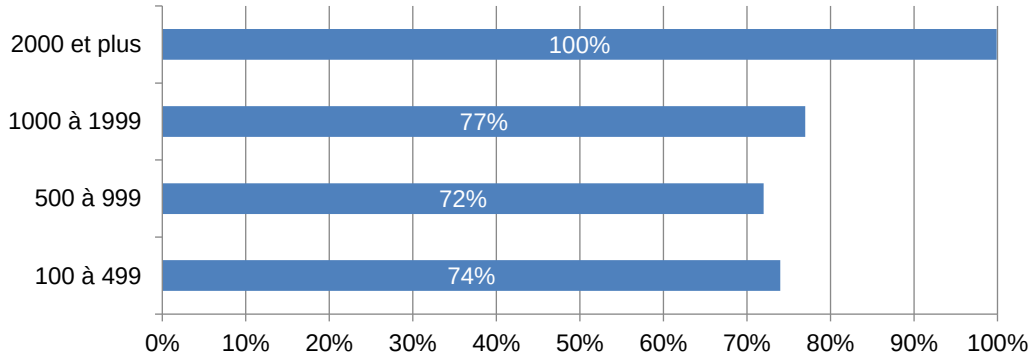


Figure 3 – Entreprises ayant formalisé leur politique de sécurité

De plus, cette politique apparaît très majoritairement à jour, et ce, désormais, quelle que soit la taille de l'entreprise.

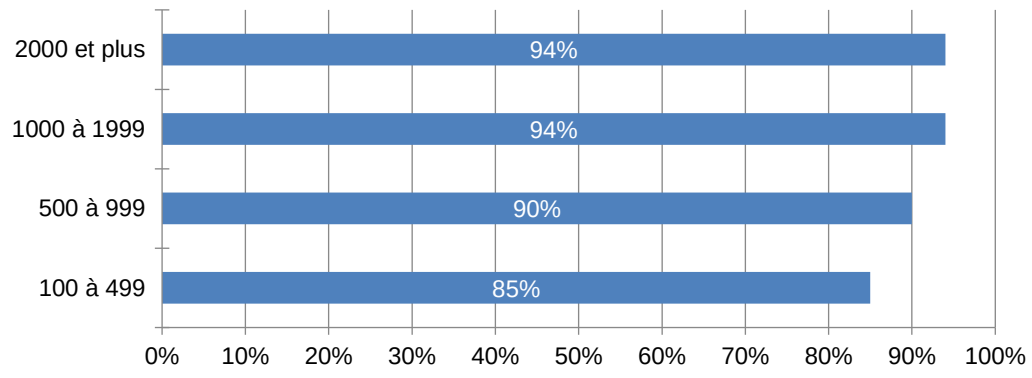


Figure 4 – Part des entreprises ayant mis à jour leur politique depuis moins de trois ans

Enfin, la PSSI des entreprises reste massivement soutenue par la Direction générale pour près de 95 % des entreprises répondantes (en très légère progression).

Communication de la politique de sécurité de l'information

La PSSI est toujours largement diffusée à l'ensemble des parties prenantes (78 %, dont 36 % de manière proactive et explicite et 42 % pour information, sans accompagnement spécifique). Le chiffre global reste stable, malgré une baisse de la communication proactive (36 % *vs* 47 % en 2018).

La Direction générale… très impliquée dans l'élaboration de la politique de sécurité !

L'implication de la Direction générale se confirme et elle est citée par un peu plus de 75 % des entreprises, ce chiffre étant en légère augmentation par rapport à 2018 (70 %).

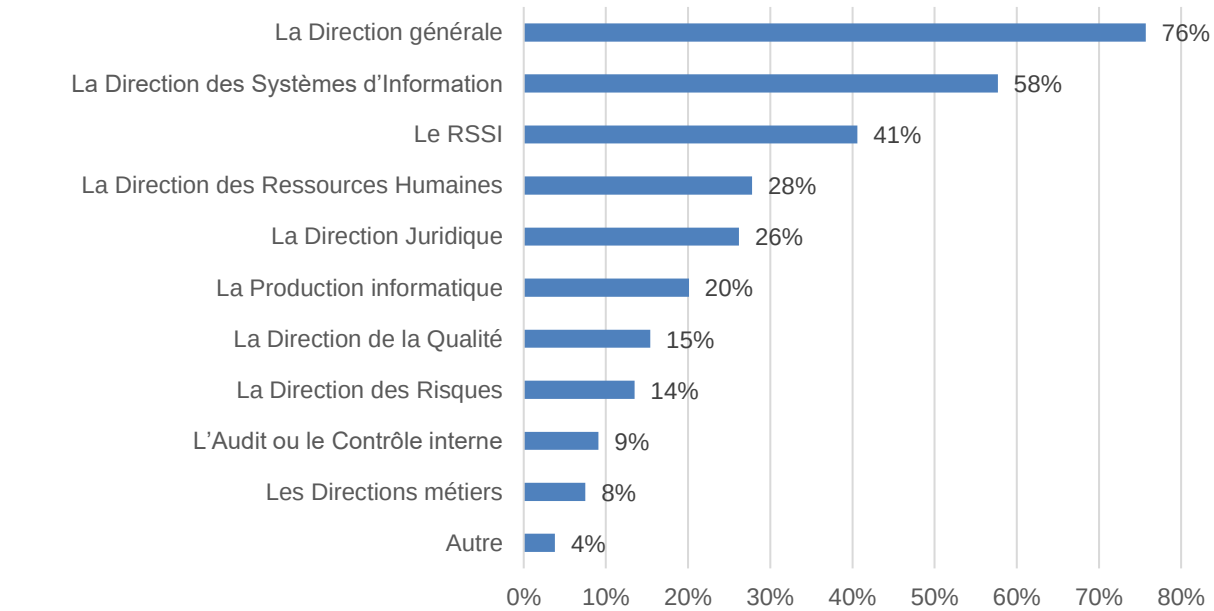


Figure 5 – Entités impliquées dans la politique de sécurité de l'information

Pilotage de la sécurité de l'information

La question posée en 2018 était relative au pilotage de la sécurité de l'information et avait obtenu des réponses variées, montrant que la notion de « pilotage » était interprétée de manière assez diverse par les entreprises. Elle a été modifiée cette année, ce qui a permis de mettre en évidence les bases sur lesquelles les mesures de sécurité ont été mises en place.

Il apparaît clairement que la mise en place des mesures de sécurité est majoritairement basée sur la PSSI, et qu'elle est globalement, presque à 50 %, sur une ou plusieurs normes, le management des risques n'étant cité que par un quart des entreprises.

Bases sur lesquelles repose la mise en place de mesures de sécurité de l'information	
■ La politique de sécurité interne	**69 %**
■ Les bonnes pratiques reconnues	**49 %**
■ Une ou plusieurs normes (ISO ou autre), et plus particulièrement :	**44 %**
ISO 27001 et 27002	23 %
RGPD	14 %
LPM/Directive NIS	4 %
PCI-DSS	3 %
Autre	5 %
■ Le management des risques, et en s'appuyant sur un référentiel :	**25 %**
ISO 27005	11 %
Ebios	6 %
Méhari	4 %
Autre	5 %
■ Le management des incidents	**22 %**

On notera cependant que ces résultats varient fortement en fonction de la taille des entreprises. Ainsi :

- le management des risques n'est utilisé majoritairement (à plus de 60 %) que par les entreprises de plus de 2 000 personnes, alors que son taux d'utilisation ne dépasse pas 30 % pour les entreprises de taille inférieure ;
- pour les entreprises les plus petites, dont l'effectif est inférieur à 500 personnes, tous les types de référentiels autres que la PSSI ont un taux d'utilisation inférieur à 50 %.

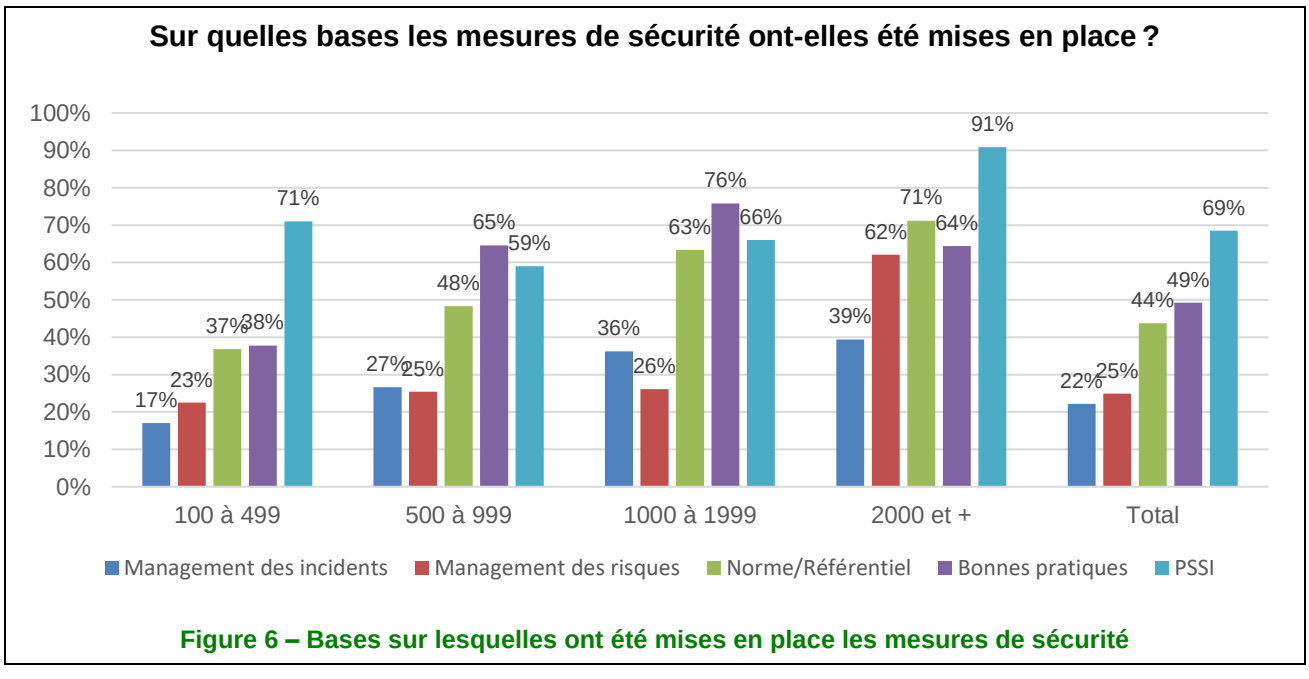


Figure 6 – Bases sur lesquelles ont été mises en place les mesures de sécurité

Thème 6 : Organisation de la sécurité de l'information

Augmentation sensible de l'identification et de l'attribution de la fonction RSSI

Le nombre d'entreprises ayant identifié et attribué la fonction de RSSI a sensiblement augmenté entre 2018 et 2020, passant de 58 % à 72 %. Ce pourcentage est de 93 % dans le secteur des banques et des assurances et varie entre 68 % et 75 % pour les autres secteurs d'activité.

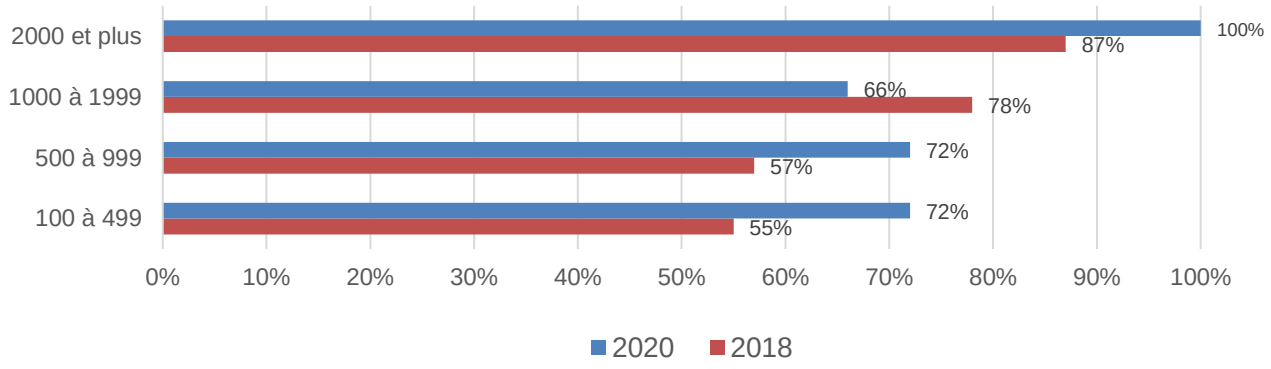


Figure 7 – Identification et attribution de la fonction de RSSI

La fonction de RSSI est attribuée de façon variable en fonction de la taille des entreprises (51 % pour celles dont l'effectif se situe entre 250 et 999 salariés à 96 % pour celles de 2 000 salariés et plus) ; le cas échéant, elle est occupée à plein temps pour 66 % (+ 13 points *vs* 2018) des entreprises. *A contrario,* quand elle n'est pas attribuée, elle est en très grande majorité (92 %) assurée par le DSI ou le RSI, au risque d'être juge et partie. À noter que dans 7 % des cas, le RSSI est un consultant externe.

Un RSSI de plus en plus rattaché au plus haut niveau

Le RSSI, quand la fonction est attribuée, est rattaché majoritairement à la Direction générale (56 %, + 7 points *vs* 2018), la DSI figurant en deuxième position (31 %, stable), nouvelle preuve que la sécurité de l'information est de plus en plus prise au sérieux.

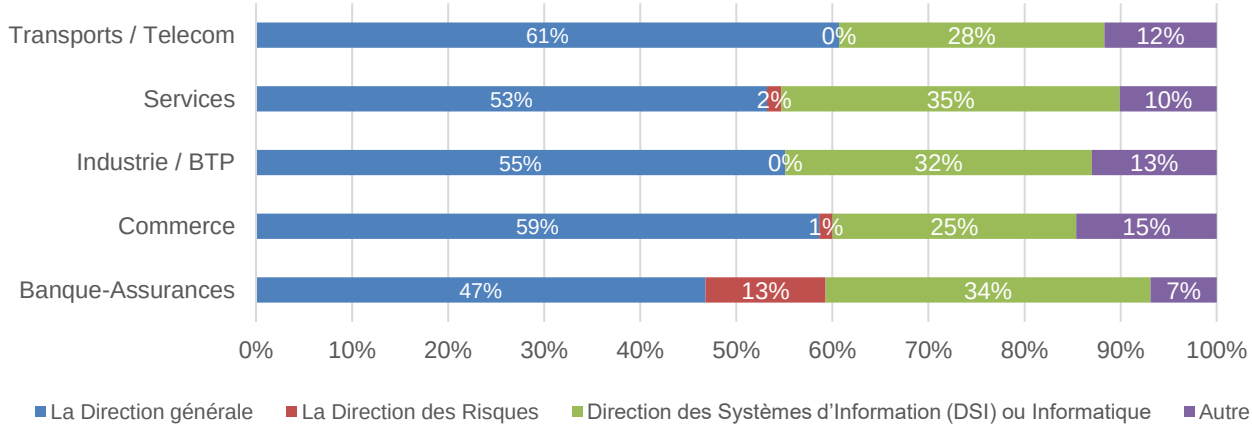
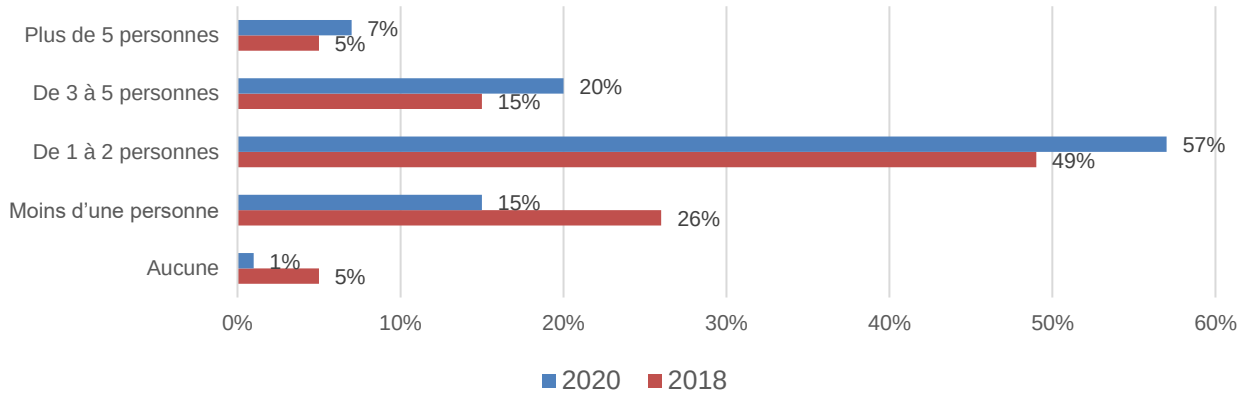


Figure 8 – Rattachement du RSSI (lorsque la fonction est attribuée)

On note par ailleurs une augmentation du nombre de personnes rattachées au RSSI par rapport à 2018. Concernant les équipes de cinq personnes et plus, c'est dans le secteur des banques et des assurances

qu'elles sont les plus nombreuses (16 %), suivi de celui des transports et des télécoms (15 %) avec, en fin de peloton, l'industrie et le BTP (4 %).

Quel est l'effectif total (en ETP*) de l'équipe sécurité de l'information au sein de votre entreprise (sous la responsabilité directe du RSSI et y compris le RSSI) ?



** ETP : Équivalent temps plein*

Figure 9 – Nombre de personnes rattachées au RSSI (en ETP)

Stabilité dans les différents aspects de la fonction du RSSI…

Globalement, le temps consacré par le RSSI aux différents aspects de sa fonction évolue peu en 2020, avec une légère diminution des aspects opérationnels (– 5 points) au profit des aspects juridiques (+ 2 points) et de la communication (+ 3 points).

Dans le cadre des missions du RSSI/RSI, quel pourcentage représente le temps consacré aux aspects… ?

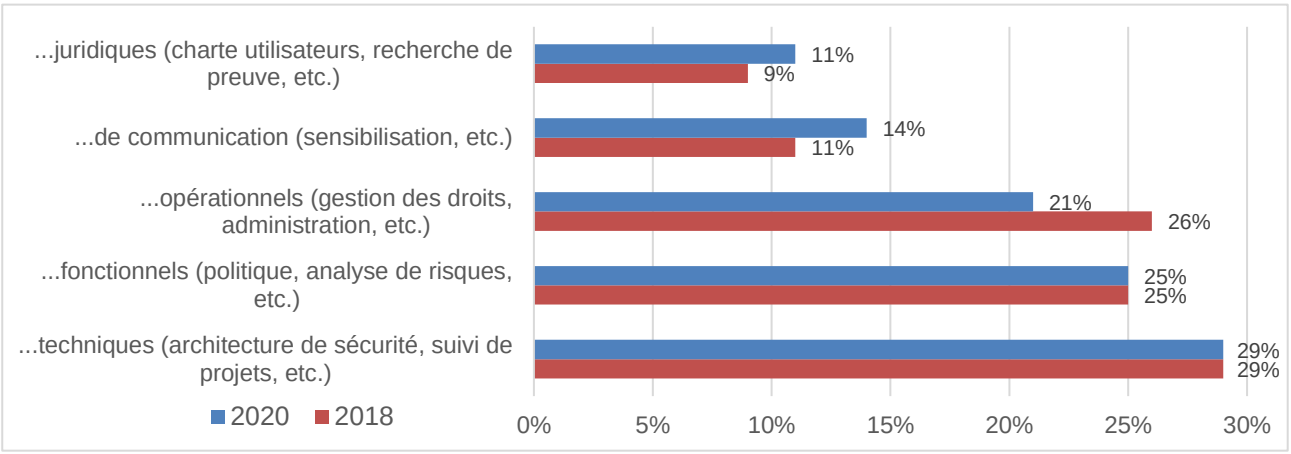


Figure 10 – Temps passé par le RSSI à ses différentes tâches/activités

Thème 7 : Sécurité des ressources humaines

Charte d'usage ou d'utilisation du SI : Une présence massive dès 250 salariés

Parmi les entreprises interrogées, 85 % affirment posséder une charte d'usage ou d'utilisation du système d'information (SI), en cours d'élaboration dans 15 % des cas, ce qui confirme la tendance observée en 2018 puisque la précédente étude affichait déjà un taux global de 84 %. Toutefois, le nombre d'entreprises possédant une de ces chartes à l'état « finalisé » accuse un net recul (8 points) par rapport à 2018, passant de 78 % à seulement 70 % cette année.

À noter, la mise en œuvre de telles chartes est adoptée massivement à partir de 250 salariés.

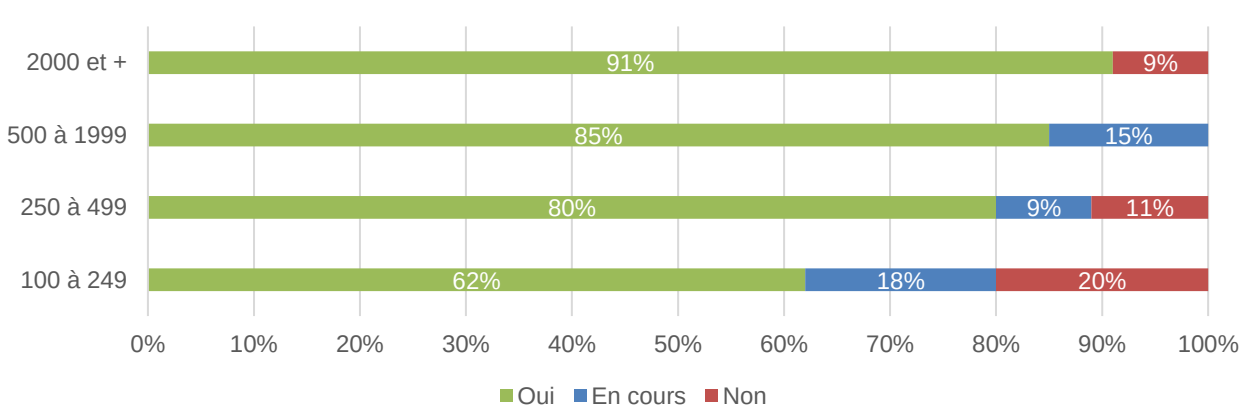


Figure 11 – Présence d'une charte informatique par taille d'entreprise

Comme dans l'étude de 2018, le plus fort taux d'adoption est observé dans le secteur des banques et des assurances qui distance celui des services de 9 points, mais ce dernier subtilise cette année la deuxième place aux transports et aux télécoms.

C'est sans surprise que ces chartes sont une nouvelle fois destinées à 99 % au personnel de l'entreprise contre seulement 34 % à leurs prestataires et fournisseurs, en baisse de 25 % par rapport aux études de 2016 et 2018. Elles sont également en grande majorité (93 %) soumises aux instances représentatives du personnel ou en cours de l'être.

Les entreprises, quelle que soit leur taille, prouvent leur implication dans le domaine de la sécurité des ressources humaines en communiquant ces chartes à tous les utilisateurs, y compris les nouveaux arrivants pour 96 % d'entre elles. À noter que les deux tiers de ces entreprises ne se contentent pas de les communiquer, mais les font également signer.

Les programmes de sensibilisation à la sécurité de l'information évoluent légèrement

En 2020, c'est désormais plus de la moitié des entreprises qui ont développé des programmes de sensibilisation à la sécurité de l'information (dont 18 % qui sont en cours d'élaboration), soit 60 % de l'échantillon étudié, contre 50 % lors de la précédente étude MIPS. Il faut noter tout de même que 80 % des entreprises dont l'effectif se situe au-delà du seuil de 500 collaborateurs ont un programme de sensibilisation (finalisé ou en cours de conception).

À la question « Mesurez-vous l'efficacité de votre programme de sensibilisation ? », 30 % des entreprises déclarent disposer d'indicateurs. Rappelons qu'il y a deux ans, elles étaient seulement 15 % à mesurer cette sensibilisation. Notons le pourcentage élevé dans le secteur des banques et des assurances (68 %) ainsi que dans les entreprises de plus de 2 000 collaborateurs, tous secteurs confondus (68 % également).

Parmi les moyens utilisés dans le cadre du programme de sensibilisation, nous retrouvons à la première place, sans surprise, les publications, sur support numérique (articles mis en ligne sur l'intranet, e-mails) ou imprimé (affiches).

À la seconde position, et avec une nette évolution par rapport aux études MIPS précédentes, la sensibilisation dédiée pour des populations spécifiques d'utilisateurs est un moyen privilégié, notamment dans le secteur des transports et des télécoms.

Par rapport à 2016, la sensibilisation de la Direction générale a fortement augmenté. Les nombreux faits d'actualité diffusés dans les médias et la vulgarisation ont contribué à cette évolution.

Notons que l'utilisation de moyens ludiques (quiz ou *serious game,* par exemple) est en forte augmentation, notamment au sein des entreprises de plus de 500 collaborateurs.

Enfin, de façon générale, toutes les utilisations de moyen de sensibilisation augmentent d'année en année.

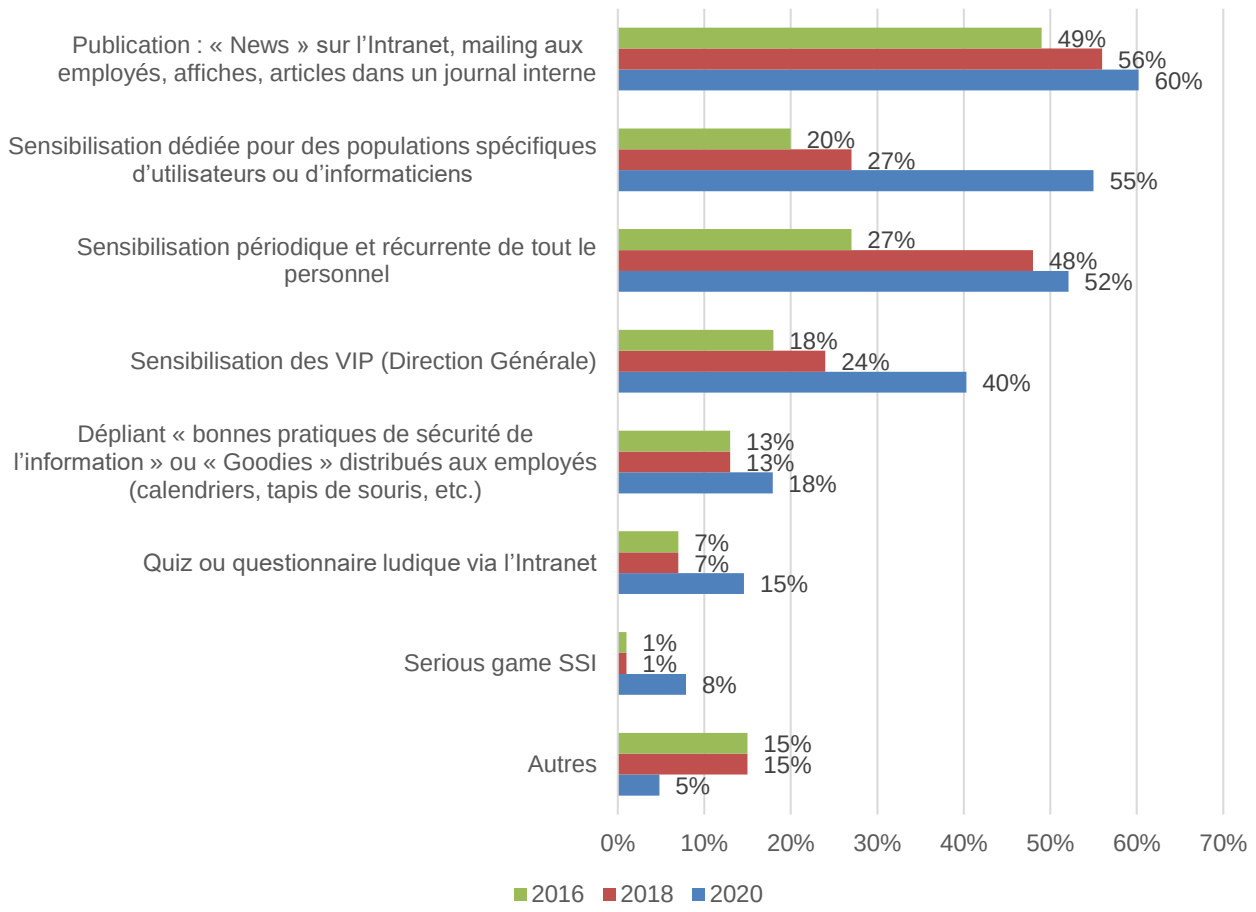


Figure 12 – Principaux moyens utilisés pour sensibiliser les collaborateurs

La gestion des départs ou des mutations

Une immense majorité d'entreprises (80 %) disposent aujourd'hui d'une procédure pour gérer, en cas de départ ou de mutation d'un collaborateur, la suppression de tous ses droits d'accès et la restitution de l'ensemble de son matériel professionnel (9 % sont en cours de réalisation de cette procédure). Ceci est valable chez toutes les entreprises, quelle que soit leur taille.

Ce taux est globalement en légère augmentation par rapport à l'étude MIPS de 2018, où il se situait à 77 % (et 8 % en cours de réalisation de la procédure), le secteur d'activité le plus en avance sur ce sujet étant celui des services.

Thème 8 : Gestion des actifs

Un inventaire des actifs (informations et supports) en progression ainsi que leur classification

Le pourcentage d'entreprises ayant réalisé un inventaire au moins partiel de leurs actifs informationnels progresse encore en 2020 pour atteindre 95 % (*vs* 87 % en 2018), marquant ainsi un progrès constant d'année en année.

À noter cependant la régression des entreprises ayant réalisé un inventaire complet.

Avez-vous inventorié tous les actifs (informations et leurs supports) de votre entreprise ?

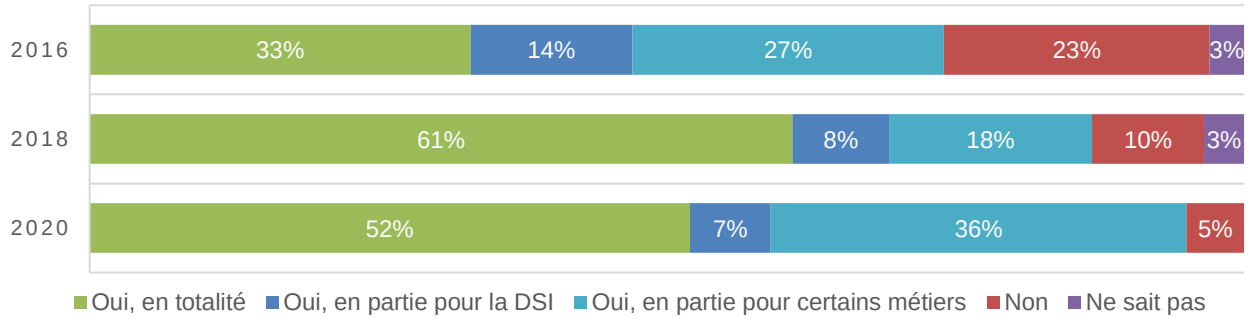


Figure 13 – Inventaire des actifs

Concernant la classification des actifs, la croissance constatée est plus importante pour les entreprises ayant classifié, au moins partiellement, leurs actifs puisqu'elle représente près de 20 % d'actifs supplémentaires sur deux ans.

Avez-vous classifié les actifs pour indiquer le besoin de protection ?

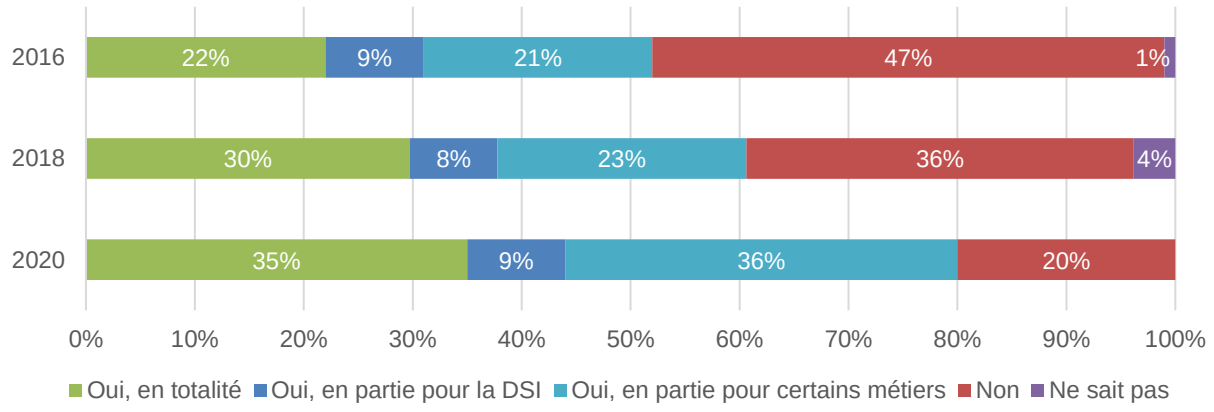


Figure 14 – Classification des actifs

Néanmoins, malgré une progression de 5 points par rapport à 2018, le pourcentage d'entreprises ayant classifié totalement leurs actifs demeure faible puisque celles-ci représentent à peine un peu plus d'un tiers de l'échantillon.

Quant au processus de classification en lui-même, très peu d'entreprises (16 %) l'ont outillé ou industrialisé.

Concernant le nombre de niveaux de sensibilité des informations, les entreprises en utilisent en grande majorité 3[7], et dans 97 % des cas, ce chiffre ne dépasse pas 4.

Combien de niveaux de sensibilité avez-vous définis pour la classification des actifs ?

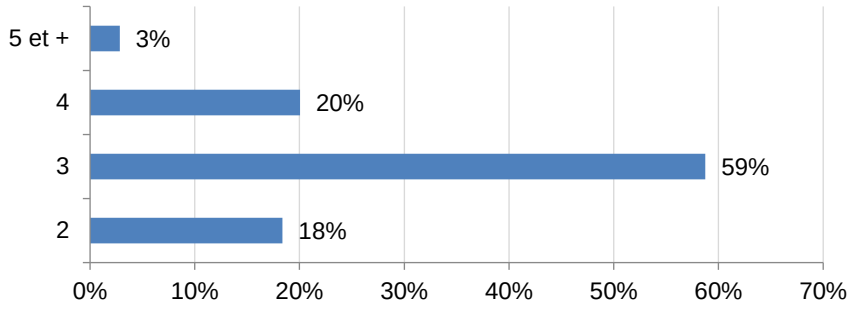


Figure 15 – Nombre de niveaux de sensibilité utilisés pour la classification des actifs

Une large majorité des entreprises a dressé un inventaire des risques, mais peu d'entre elles en ont fait une analyse formelle par la suite

La majorité (88 %) des entreprises interrogées ont procédé à un inventaire au moins partiel des risques, ce qui représente une progression de 7 points par rapport à 2018.

Cependant, la part des entreprises ayant réalisé un inventaire total de leurs risques a fortement baissé en 2020 pour atteindre 23 % contre 35 % en 2018.

Avez-vous effectué un inventaire des risques auxquels votre entreprise est exposée ?

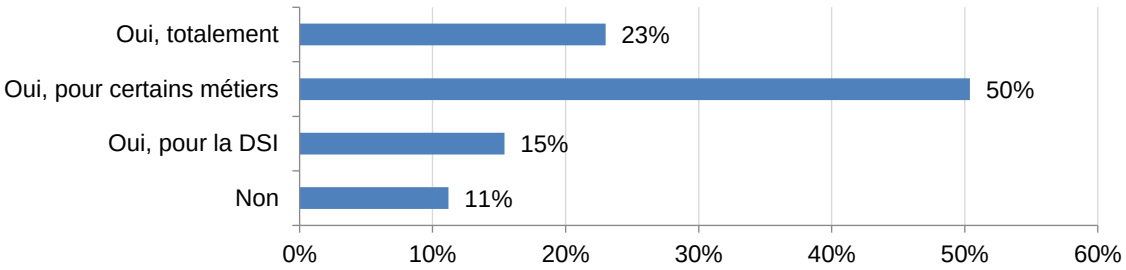


Figure 16 – Inventaire des risques

Notons que les entreprises qui réalisent un inventaire total de leurs risques sont celles qui effectuent en grande majorité une analyse formelle des risques. La part des entreprises réalisant un inventaire complet et une analyse formelle de leurs risques est de 14 % environ.

Type d'inventaire des risques effectué	Part d'entreprises ayant effectué, après leur inventaire, une analyse formelle des risques
Inventaire total	62 %
Inventaire partiel, pour la DSI	30 %
Inventaire partiel, pour certains métiers	38 %

[7] À noter que cette question a reçu, cette année encore, plusieurs réponses anormales ou dénotant une mauvaise compréhension de la question posée (réponse : « 0 », « 1 » ou « plus de 10 » par exemple) dont il n'a pas été tenu compte dans les pourcentages.

Les méthodes utilisées pour cette analyse formelle sont diverses et diffèrent notablement selon le type d'inventaire qui a été effectué.

Sur quelle méthode d'analyse des risques ou référentiel vous êtes-vous basé ? (si évaluation formelle réalisée)

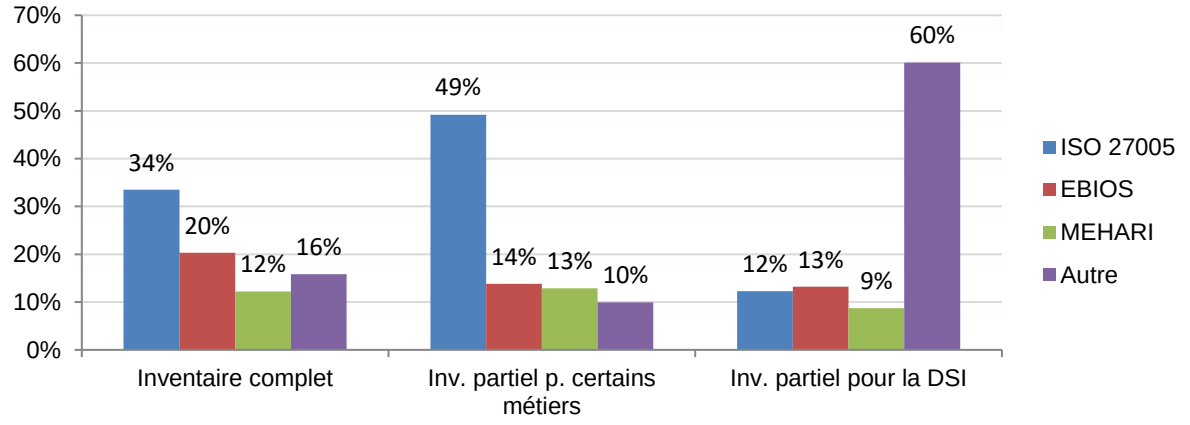


Figure 17 – Méthodes d'analyse de risques utilisées

Notons enfin que, lorsqu'elle est réalisée, l'analyse des risques l'est, dans 84 % des cas, par le RSSI ou le DSI, ce qui n'est pas surprenant puisqu'il s'agit de leur domaine de compétence et de responsabilité.

Des plans de réduction des risques déconnectés de l'analyse formelle des risques

Les plans de réduction des risques mis en œuvre à la suite de leur inventaire – qu'une analyse formelle ait eu lieu ou non – sont en très nette progression puisqu'ils sont observés, pour les plans au moins partiels, dans 88 % des entreprises interrogées, soit près du double du taux relevé en 2018.

Bien que très peu d'entreprises aient effectué un inventaire total et une analyse formelle de leurs risques (14 %), une grande majorité a néanmoins défini un plan de réduction des risques, ce qui nous amène à penser que la plupart traitent leurs risques de façon empirique.

Pour celles qui avaient réalisé un inventaire complet de leurs risques, près de 50 % ont élaboré un plan complet de réduction des risques.

Avez-vous défini et argumenté le plan d'action d'amélioration de la sécurité de l'information ?

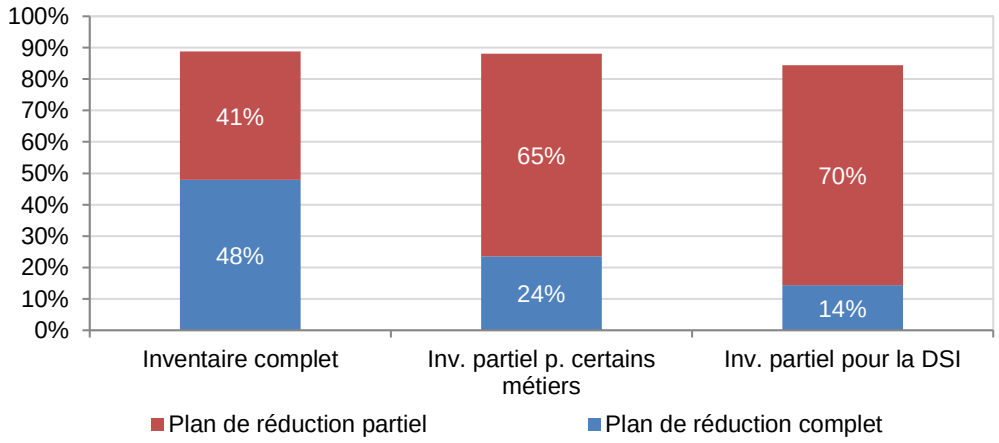


Figure 18 – Mise en place d'un plan de réduction des risques

Enfin, les directions générales ont très largement accepté les risques résiduels et validé les plans d'action, au moins partiels.

La Direction générale a-t-elle accepté les risques résiduels et validé le plan d'action ?

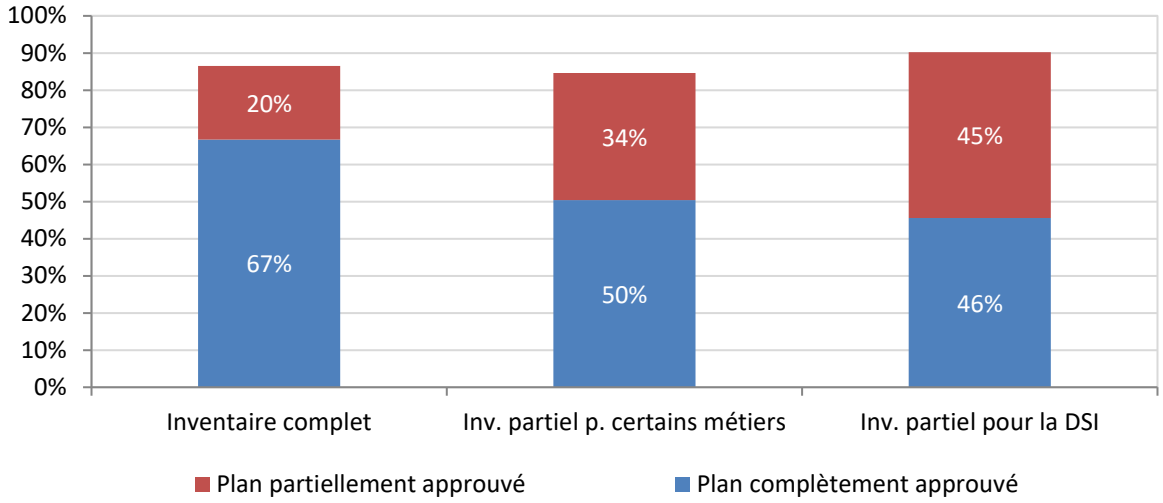


Figure 19 – Acceptation des risques résiduels et validation du plan d'action

Thème 9 : Contrôle d'accès

Les technologies de sécurisation en large progrès

La sécurisation des accès au SI reste une des préoccupations majeures pour l'ensemble des directions informatiques. Avec les menaces cybercriminelles qui ne cessent de s'intensifier ces dernières années, les organismes de sécurité recommandent de renforcer le contrôle des accès en privilégiant des solutions d'authentification multifacteur (*Multi-Factor Authentication* – MFA). Par rapport à l'enquête MIPS 2018, on peut, à une exception près, noter une progression très significative de l'ensemble des technologies d'authentification. L'authentification forte par certificat électronique sur support matériel passe à 53 % (*vs* 45 %) alors que celle par certificat électronique logiciel atteint les 62 %.

La prolifération des environnements hybrides (*On-Premise* et cloud) intensifie également l'usage des technologies de sécurisation des accès à base d'authentification unique (*Single Sign-On* – SSO). Qu'elles soient ou non renforcées par des facteurs supplémentaires (MFA), elles sont en croissance de 11 points par rapport à 2018. Les technologies d'authentification SSO/e-SSO passent de 44 % à 55 % alors que celle du Web SSO passe à 39 % (*vs* 28 % en 2018).

Seule l'authentification biométrique, très certainement pour des raisons liées aux contraintes d'exploitation et à la complexité de mise en œuvre, recule de 6 points à 9 %.

Progression des *workflows* d'approbation des habilitations par rôle métier

Du fait de l'augmentation des cyberrisques liés aux diverses attaques informatiques, les réglementations en matière de sécurité du SI sont aujourd'hui beaucoup plus contraignantes pour les organisations. Elles garantissent que celles-ci sont en mesure de protéger l'intégrité de leur SI ainsi que les données qui leur sont confiées. Le durcissement de ces obligations réglementaires leur impose d'adopter des solutions de gestion des identités et des accès (*Identity and Access Governanc*e – IAG) pour gérer l'ensemble des identités et des habilitations des utilisateurs et être en capacité de réagir en temps réel en cas d'action malveillante.

Les résultats de l'étude mettent en évidence une croissance homogène à deux chiffres pour l'ensemble des points traités sur ce registre. Les modèles d'habilitation sur base de rôles métiers passent ainsi de 50 % à 61 %, l'utilisation des *workflows* d'approbation des habilitations, de 35 % à 54 % et le provisionnement *(provisioning)* automatique de comptes atteint aujourd'hui les 54 % alors qu'il n'était que de 32 % en 2018.

Le radar ci-dessous reprend les évolutions des technologies citées et les approches de sécurisation.

Quelle(s) technologie(s) utilisez-vous pour le contrôle d'accès (plusieurs réponses possibles) ?

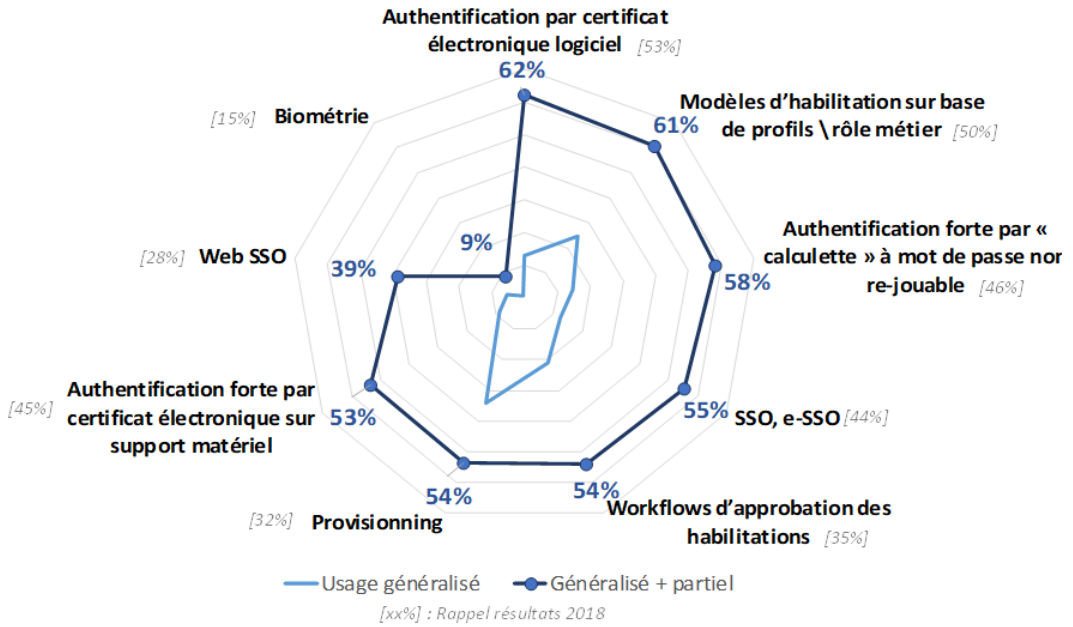


Figure 20 – Évolution de l'usage des technologies et des approches de sécurisation

Des écarts qui se minimisent entre les PME et les grandes entreprises

L'étude montre une utilisation hétérogène des différentes technologies d'authentification, qui varie selon la taille des organisations. Néanmoins, les contraintes de sécurité d'accès au SI, réglementées par les nouvelles législations, tendent à réduire les écarts entre les PME et les grandes entreprises.

Le secteur des transports et des télécoms, qui affiche des taux d'utilisation bien supérieurs à la moyenne, en est le parfait exemple. C'est le cas pour les modèles d'habilitation sur base de rôle métier (*Role Based Access Control* – RBAC) (79 %), les authentifications fortes par calculette (78 %), ainsi que pour l'utilisation de technologies de SSO (76 %) ou encore de Web SSO (70 %).

À l'inverse, l'industrie et le BTP font figure de mauvais élèves avec un petit 52 % (*vs* une moyenne de 61 %) pour les modèles RBAC et un ridicule 38 % (*vs* une moyenne de 55 %) concernant l'utilisation de technologies de SSO, alors que les entreprises de 2 000 personnes et plus l'utilisent, elles, à 100 %.

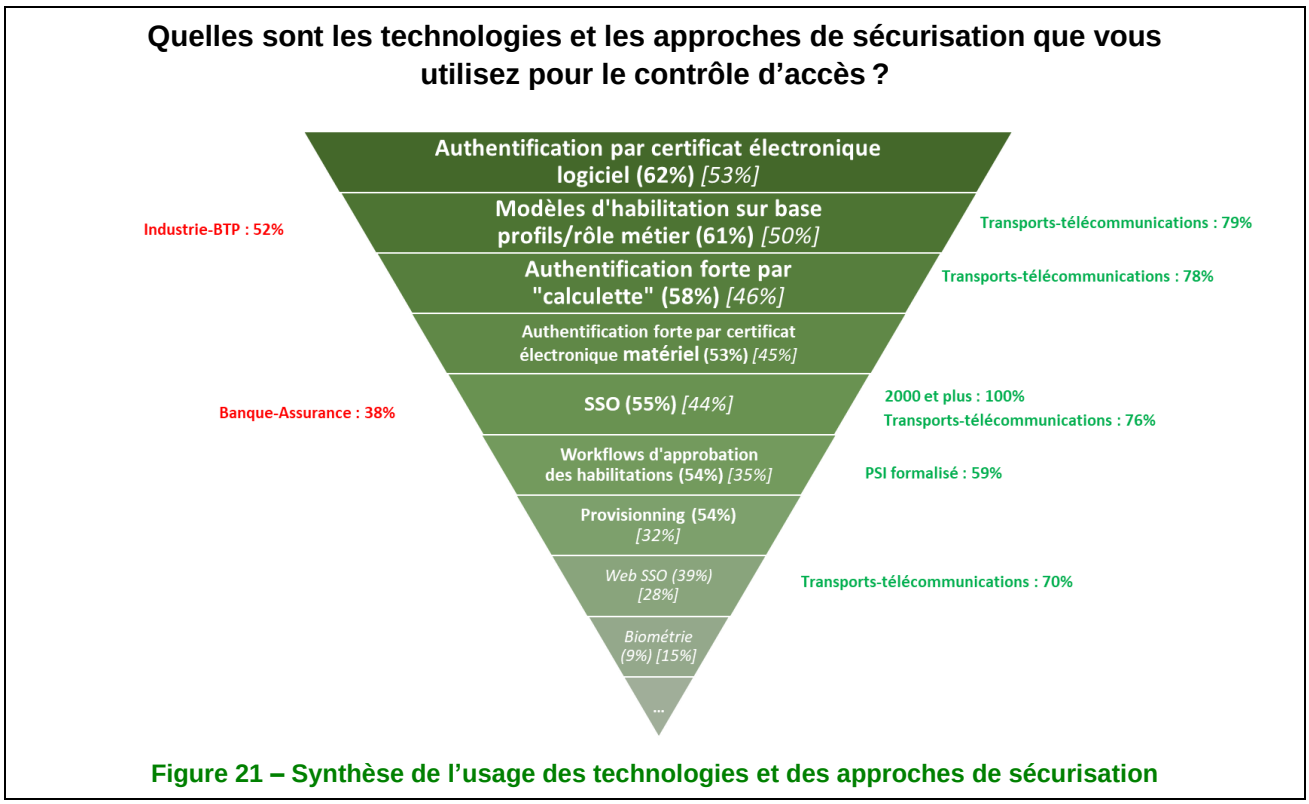


Figure 21 – Synthèse de l'usage des technologies et des approches de sécurisation

Les procédures de gestion des comptes à privilèges en hausse

Aujourd'hui, plus de 80 % des entreprises disposent de procédures de gestion de comptes.

En comparant les chiffres avec ceux de 2018, on s'aperçoit que l'adoption des procédures de gestion pour les comptes utilisateurs nominatifs est en légère augmentation. Toutefois, même si elle accuse une baisse (– 10 points), cette adoption est totale pour 51 % des organisations ; *a contrario,* elle reste partielle pour 35 % des entreprises, bien que cette proportion soit en hausse (+ 15 points) par rapport à la précédente étude MIPS.

On constate cependant une augmentation beaucoup plus significative (+ 15 points) concernant les procédures de gestion des comptes spécifiques aux administrateurs dont le taux d'adoption atteint les 82 %, même si cette hausse est moins marquée pour les entreprises de 100 à 249 salariés (75 %). L'adoption est totale pour 54 % des organisations, a contrario de 28 % d'entre elles qui n'en font qu'un usage partiel.

Cette progression est principalement liée au fait que ces deux dernières années, un grand nombre d'entreprises ont eu recours à des solutions de gestion des accès à privilèges (*Priviledged Access Management* – PAM) pour protéger les accès à leur SI. D'un point de vue réglementaire, elles ont dû appliquer les préconisations relatives à la cybersécurité décrites entre autres dans plusieurs guides, notamment le PA-022 de l'Anssi ou en rapport avec des règles édictées par la LPM.

Une légère augmentation (+ 3 points) est également à mettre au bénéfice de l'adoption de règles de constitution et de péremption de mots de passe pour les accès.

Existe-t-il une procédure formelle de création, modification et suppression de comptes utilisateurs nominatifs (non génériques) ?

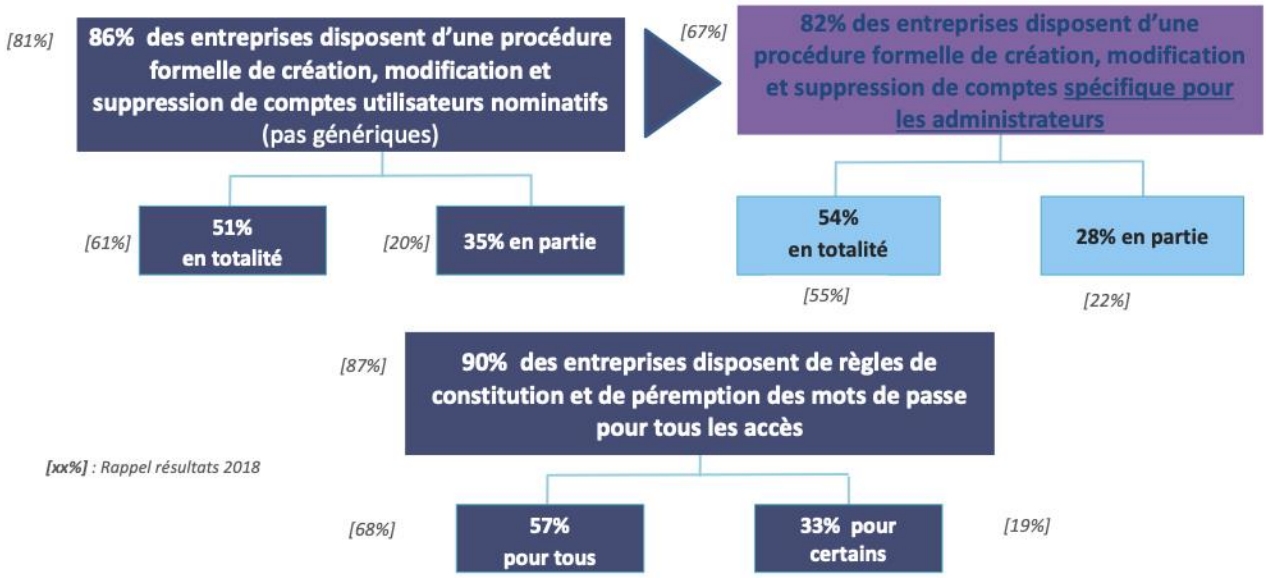


Figure 22 – Procédures de gestion des accès

Thème 10 : Cryptographie

Des moyens de cryptographie encore peu développés, mais mieux suivis

La cryptographie, moyen de sécurisation des données et de leur transport, reste relativement peu utilisée. Moins d'un tiers (28 %) des entreprises déclare en effet l'utiliser. Ce chiffre stable (– 2 points par rapport à l'étude 2018) cache toutefois une très grande disparité selon la taille des entreprises.

Utilisez-vous de la cryptographie au sein de votre entreprise ?

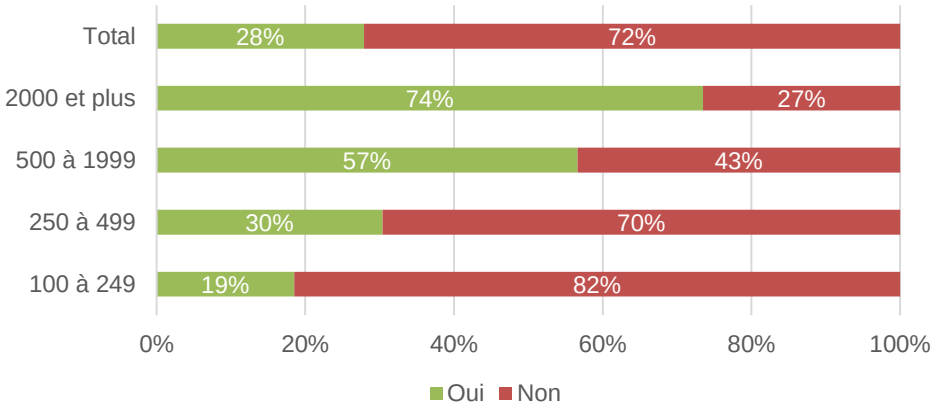


Figure 23 – Usage de la cryptographie par catégorie d'entreprise

Le secteur des banques et des assurances reste largement majoritaire et, étonnamment, est le seul qui augmente son taux d'usage sur les années passées.

Utilisez-vous de la cryptographie au sein de votre entreprise ?

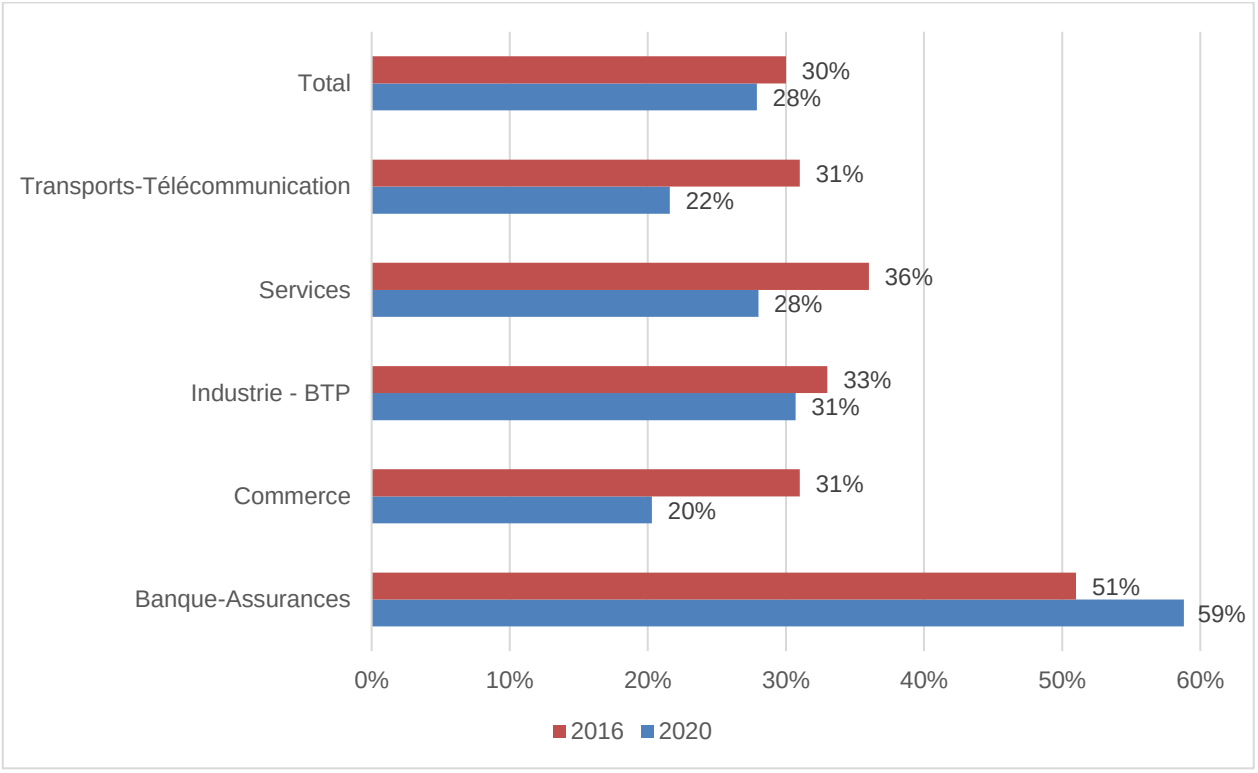


Figure 24 – Usage de la cryptographie par type d'entreprise

Lorsqu'elle est utilisée, c'est très largement la DSI (92 %, + 16 points en deux ans) qui porte la responsabilité des moyens cryptographiques (attribution, révocation, distribution, destruction des clés).

On constate depuis la dernière étude MIPS une forte augmentation (55 %, + 19 points) du nombre d'entreprises qui formalisent le suivi des moyens de cryptographie (cycle de vie des certificats, clés, etc.).

Thème 11 : Sécurité physique et environnementale

La protection des données sur support physique

La sécurité de l'information englobe la protection des données sur support physique amovible (clé USB, bande, CD, papier, etc.) pour 69 % des entreprises (dont 10 % qui sont « en cours de mise en place »), chiffre équivalent (1 point) que celui de l'étude MIPS 2018.

Cependant, et contrairement à l'étude précédente, cette approche est désormais valable de façon homogène dans tous les secteurs d'activité, ainsi que pour toutes les tailles d'entreprises. Le fait d'avoir formalisé une PSSI ou même d'être plus ou moins conforme au RGPD n'influe pas sur la prise en compte de ces supports dans le périmètre de la sécurité de l'information.

Détection d'incendie, caméra de surveillance et contrôle d'accès par badge : toujours aussi plébiscités pour la sécurisation des infrastructures physiques

On observe que les dispositifs de sécurité physiques en entreprise sont, comme dans l'étude MIPS menée en 2018, majoritairement dominés par le contrôle d'accès par badge, la détection d'incendie et la caméra de surveillance. Le contrôle d'accès par badge est devenu la priorité des entreprises pour protéger les salles machines des entreprises, avec un bond de 9 points enregistré en deux ans pour atteindre 71 %, alors que les systèmes de détection d'incendie, quant à eux, ont subi un recul de 8 points (65 %).

Des dispositifs de sécurité physique sont-ils implémentés pour sécuriser l'accès aux salles des machines dans votre entreprise ?

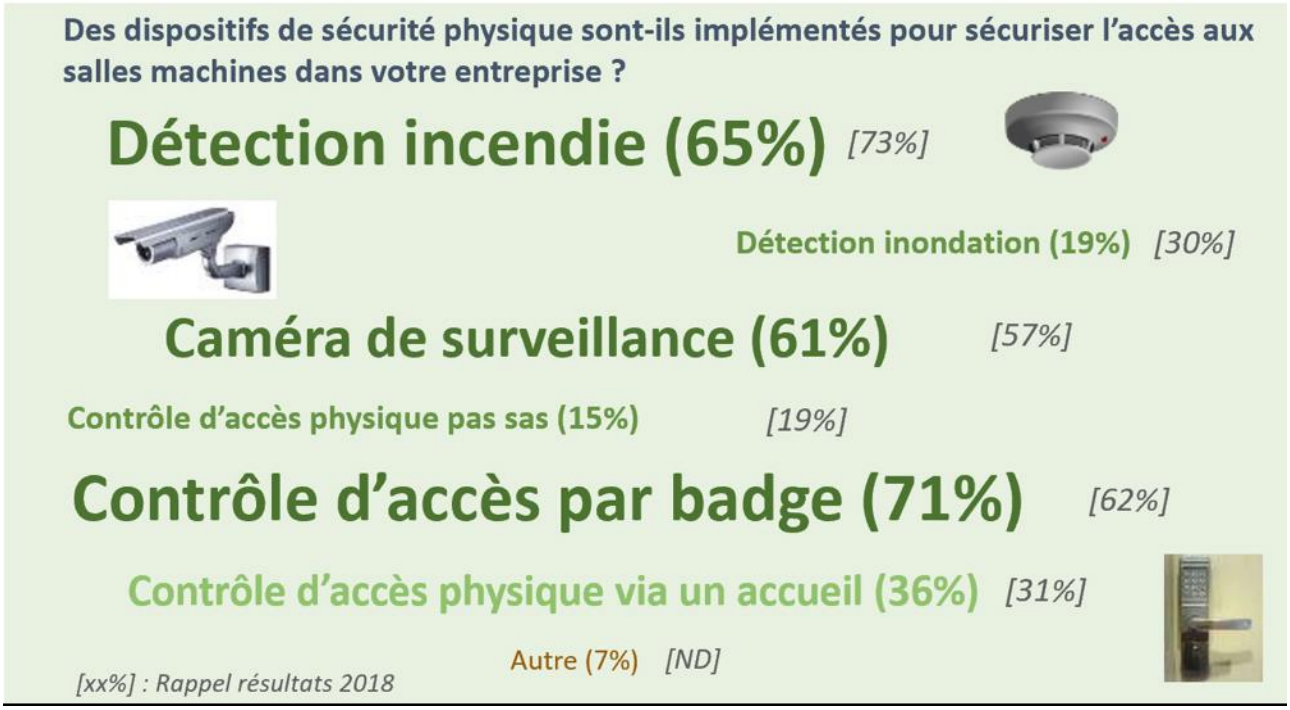


Figure 25 – Dispositifs de sécurité physiques en entreprise pour la protection des salles machines

On peut noter que l'implémentation de tels dispositifs (réalisée ou en cours) n'est pas formellement liée à une PSSI formalisée et que ces derniers sont mis en place à plus de 82 % dans les entreprises supérieures à 250 salariés.

Tout comme le secteur des banques et des assurances (93 %), les entreprises de 500 à 1 999 salariés sont les seules à considérer la détection d'incendie comme la priorité dans la sécurisation de ces salles machines, avec un taux de 92 %, alors que pour les autres tailles d'entreprises, la palme revient au contrôle d'accès physique par badge.

Thème 12 : Sécurité liée à l'exploitation

L'utilisateur au cœur de la protection et en forte croissance s'il est mobile…

La quantité et la richesse des outils et des sources d'information disponibles pour sécuriser l'exploitation sont toujours importantes. Globalement, les protections se classent dans deux catégories :

- les outils « classiques », relativement simples et unanimement adoptés : solutions antivirus et *antimalware* (100 %), antispam (98 %), *firewall* (100 % ou 89 %) ;
- des outils plus « spécifiques » et relativement complexes : sondes IDS (66 %), SIEM (56 %), *Network Access Control* (52 %), *Data Leak Protection* (33 %).

De plus, le chiffrement continue sa (trop lente ?) progression à 59 % (*vs* 40 % en 2018) sur les PC portables et 59 % (*vs* 42 % en 2018) pour le chiffrement des échanges.

Bien entendu, la protection de la mobilité a pris une large part dans les outils de sécurisation mis en œuvre, avec des progressions sensibles sur les outils suivants :

- 66 % (+ 21 points) pour les outils de contrôle des périphériques autorisés sur le poste de travail (clés USB, etc.) ;
- 42 % (+ 20 points) pour les outils de chiffrement sur smartphones et tablettes ;
- 59 % (+ 19 points) pour les outils de chiffrement sur PC portable ;
- 65 % (+ 16 points) pour les antivirus/*antimalware* sur smartphones et tablettes.

À noter, sur les 68 % des entreprises déclarant l'utilisation de tablettes et smartphones « personnels » (BYOD), seuls 25 % déploient des protections sur les équipements personnels.

Quels sont les outils déployés au sein de votre entreprise pour vous protéger contre les menaces « logiques « ?

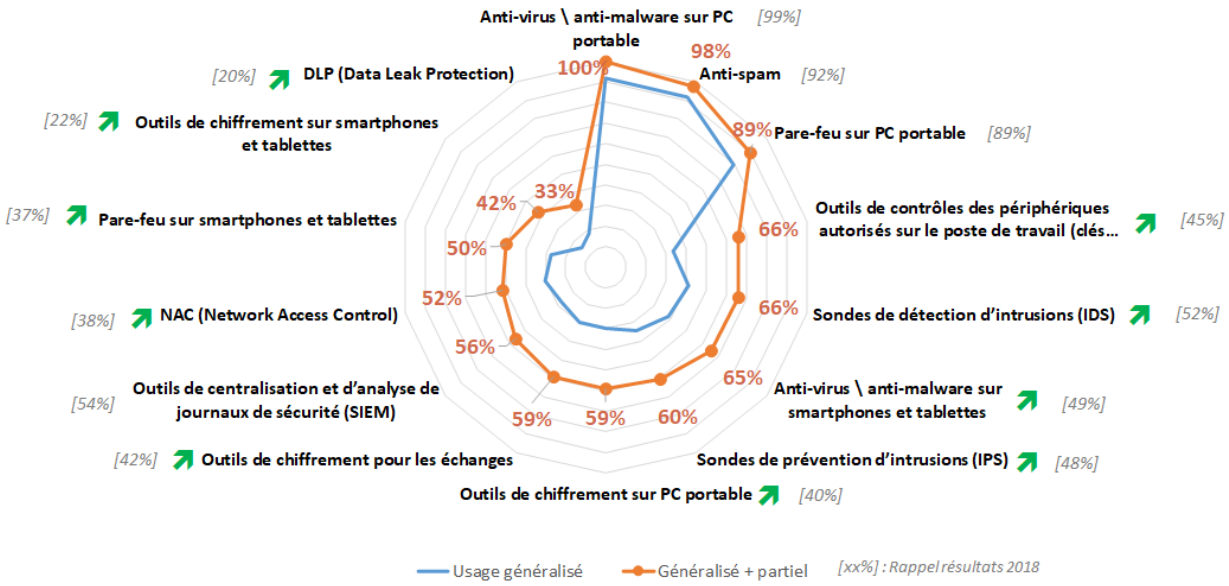


Figure 26 – Protection contre les menaces « logiques »

Le poste « utilisateur » est globalement en forte progression quant à la sécurité de son écosystème numérique. Si les raisons sont diverses, on peut retenir :

- la part croissante du nomadisme, avec pour corollaire la nécessité de sécuriser le poste de l'utilisateur en dehors de l'entreprise (95 % des entreprises interrogées l'autorisent, parfois même sans conditions) ;
- les attaques les plus significatives (cryptolocker, rançongiciel) qui sont passées par le poste de l'utilisateur avant de s'étendre à l'ensemble de l'entreprise ;
- une utilisation importante du matériel de l'entreprise pour accéder à des sites et messageries non professionnels.

Finalement, si la sécurité du SI innove peu, elle devient clairement plus globale. Il reste donc à « supprimer » les freins au déploiement des solutions plus complexes qui sont des briques nécessaires à une protection efficace des matériels et des données.

Une gestion des vulnérabilités techniques en augmentation constante

Aucune solution n'est invulnérable et le système d'information n'échappe pas à cette règle… Les logiciels, les matériels, contiennent des vulnérabilités qui sont utilisées, « exploitées » par des tiers pour voler des données, en tirer un profit financier ou tout simplement nuire…

Une réponse est alors d'identifier et de pallier ces vulnérabilités, et ce dans les meilleurs délais. Pour ce faire, les entreprises s'appuient sur une « veille technologique » : en 2020, 86 % des entreprises en réalisent (contre 75 % en 2018 et 61 % en 2016).

Comment réalisez-vous une veille permanente en vulnérabilités et en solutions de sécurité de l'information ?

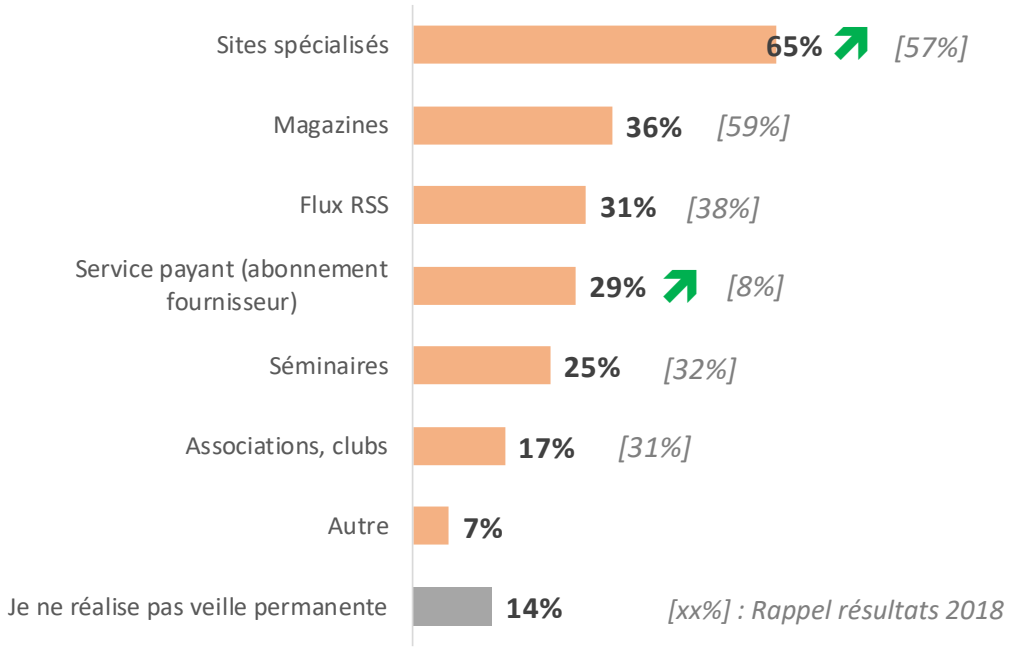


Figure 27 – Prise en compte de la veille technologique

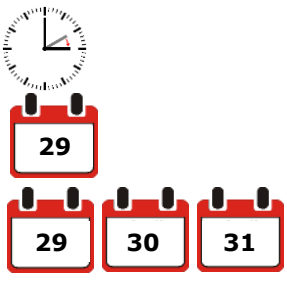
La veille est réalisée au travers de plusieurs canaux, où les « sites spécialisés » se taillent la part du lion (en hausse de 8 points). À noter, la progression de l'usage de services payants (abonnement fournisseur) passant à 29 % (+ 8 points) et la forte chute des magazines (qui demeurent malgré tout le second canal de veille) à 36 % (– 23 points).

Faire de la veille, c'est bien… Déployer les correctifs, c'est mieux !

Seuls 57 % (+ 1 point *vs* 2018) des entreprises ont formalisé les procédures de déploiement de correctifs de sécurité. Avec une répartition inégale selon les secteurs (67 % dans les banques et les assurances et 50 % dans le commerce) ou selon la taille de l'entreprise (79 % pour les organisations de 2 000 salariés et plus et 52 % pour celles de 100 à 249 salariés).

En cas de menace grave, la très grande majorité des entreprises (67 %) déploie les correctifs dans la journée.

En cas de menace grave, quel délai est nécessaire en moyenne pour déployer les correctifs ?



Dans l'heure : 17% *[21%]*

Dans la journée : 67% *[49%]*

Dans les 3 jours : 12% *[12%]*

Lors de sessions planifiées de mise à jours : 4% *[5%]*

Figure 28 – Délais de mise en œuvre des correctifs

Thème 13 : Sécurité des communications

Augmentation sensible dans l'usage des outils de communication…

Par rapport à l'enquête précédente (2018), on constate une augmentation assez sensible dans l'ouverture des SI et l'usage des outils de communication.

En 2020, 95 % des entreprises autorisent ainsi l'accès aux SI depuis l'extérieur par un poste maîtrisé (fourni par l'entreprise), contre 92 % en 2018. Cependant l'usage d'un poste non maîtrisé (BYOD) reste minoritaire avec 36 % des entreprises qui l'autorisent, même si son usage a augmenté de 5 points par rapport à 2018.

Quelle est la position de votre politique de sécurité de l'information vis-à-vis des sujets suivants ?

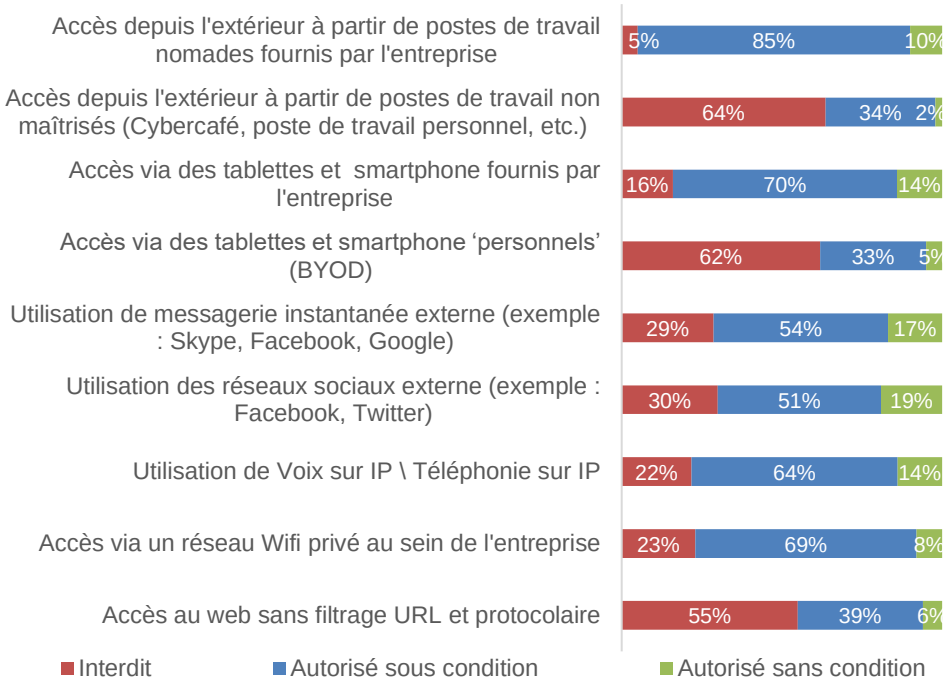


Figure 29 – Position de la PSSI concernant la sécurité des communications

L'usage des tablettes et des smartphones pour l'accès aux SI a fortement augmenté, notamment quand ils sont fournis par les entreprises. En 2020, 84 % des entreprises autorisent leur usage contre 66 % en 2018. L'usage des tablettes et smartphones non fournis par l'entreprise (BYOD) a également augmenté, passant de 28 % en 2018 à 38 % en 2020.

L'utilisation de la messagerie instantanée et des réseaux sociaux est de plus en plus tolérée. L'autorisation de l'usage de la messagerie instantanée passe de 56 % en 2018 à 71 % en 2020, et celle de l'usage des réseaux sociaux, de 59 % en 2018 à 70 % en 2020.

On note une augmentation de l'acceptation de l'usage de la voix sur IP (VoIP) et de la téléphonie sur IP de 17 % qui s'établit à 78 % en 2020, contre 61 % en 2018. Il en est de même pour l'autorisation de l'usage du Wi-Fi qui passe de 72 % en 2018 à 77 % en 2020.

Enfin, l'autorisation de l'accès au Web sans filtrage d'URL a progressé de 15 % pour atteindre 45 % en 2020 contre 30 % en 2018. Cependant, seuls 6 % des entreprises l'autorisent aujourd'hui sans condition.

Thème 14 : Acquisition, développement et maintenance des systèmes d'information

Le développement sécurisé peine à arriver…

Les lois et règlements actuels (LPM, PCI-DSS, RGPD, etc.) impliquent une augmentation de plus en plus importante de la sécurité dans le développement *(Security by Design),* qu'il soit effectué en interne ou *via* des prestataires.

Un cycle de développement sécurisé doit comporter divers éléments comme :

- sécurité du design de l'architecture du logiciel ;
- codage sécurisé *(secure coding)* ;
- tests de sécurité (revue de code, tests d'intrusions, tests unitaires sécurité) ;
- suivi en production des vulnérabilités ;
- etc.

Si l'augmentation est notable entre 2018 (11 %) et 2020 (25 %, + 14 points), il n'en demeure pas moins que seules un quart d'entreprises ont mis en place de réels cycles de développement sécurisé. Les organisations n'ont toujours pas pris pleinement conscience de l'impact des vulnérabilités applicatives au sein de leur métier, malgré des différences notables observées en fonction des secteurs d'activité.

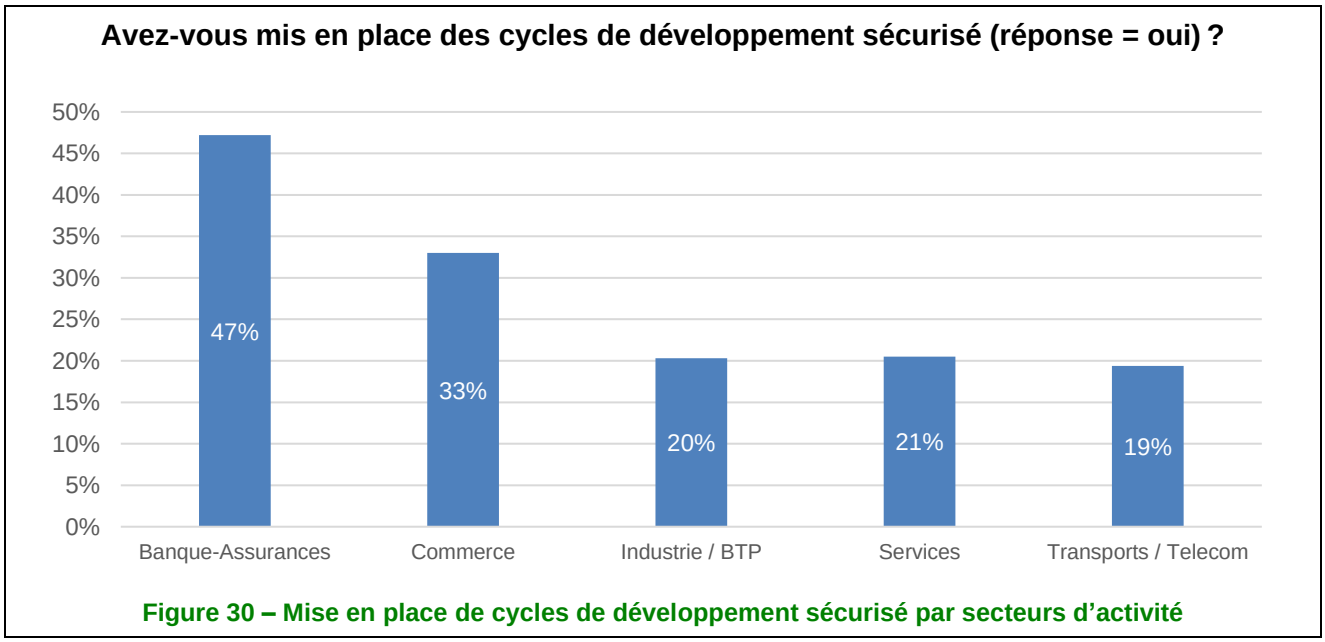


Figure 30 – Mise en place de cycles de développement sécurisé par secteurs d'activité

De plus, les entreprises ont mis en place, pour 48 % d'entre elles (29 % en interne et 19 % en externe), un référent (coach ou facilitateur) sécurité pour les problèmes relatifs aux développements (51 % dans le secteur des banques et des assurances et 19 % dans celui des services).

Quant aux méthodes utilisées par les entreprises ayant mis en place un cycle sécurisé, la norme ISO 27034 émerge fortement, suivie de peu par les bonnes pratiques pragmatiques.

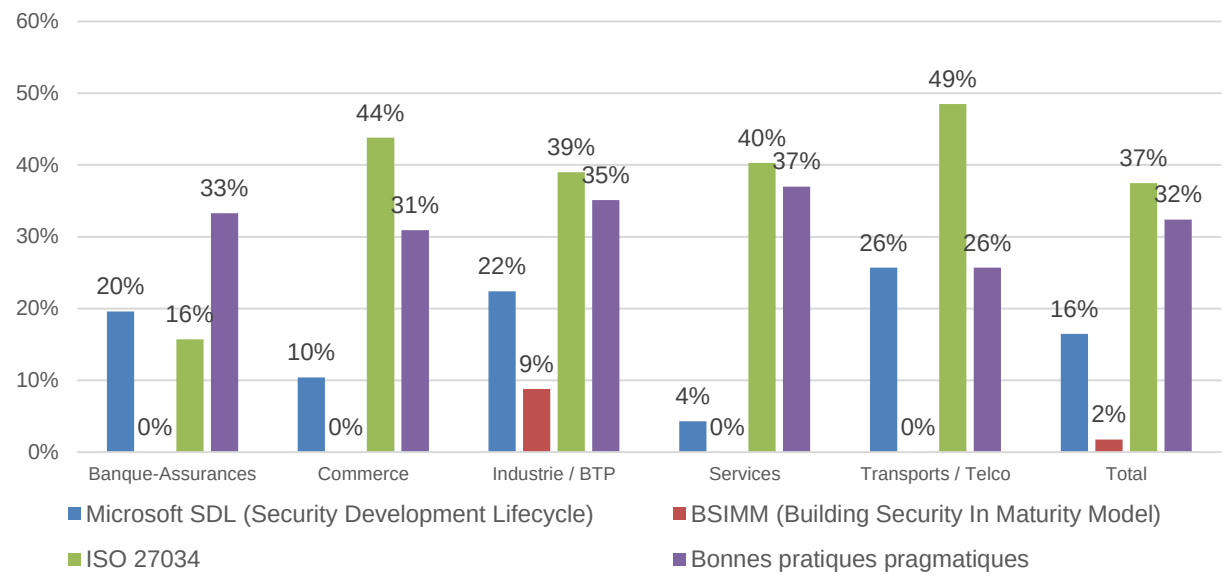


Figure 31 – Méthodes de développement sécurisé

Thème 15 : Relation avec les fournisseurs

L'infogérance gagne du terrain avec une explosion du recours aux solutions cloud

La délégation totale ou partielle de la gestion du SI à un infogéreur a augmenté de 7 points depuis 2018 avec un peu plus de la moitié des entreprises ayant recours à ce type de prestations (51 % en 2020 contre 44 % en 2018). Cependant, cet accroissement ne constitue pas un blanc-seing. On note en effet une part plus faible d'entreprises qui délèguent entièrement la gestion de leur SI puisqu'elles représentent seulement 7 % de l'échantillon étudié en 2020 contre 13 % en 2018.

Le niveau de contrôle des infogéreurs a également progressé significativement depuis 2018 :

- une majorité des prestations d'infogérance fait l'objet d'un suivi régulier (74 % en 2020 contre 62 % en 2018). Il faut préciser que la progression s'accélère, passant de 9 points entre 2016 et 2018 à 12 points entre 2018 et 2020 ;
- dans le même esprit, les audits pratiqués sont en forte augmentation : 69 % des entreprises déclarent pratiquer des audits de leurs infogéreurs en 2020. Ils n'étaient que 45 % en 2018.

Figure 32 – Mise en infogérance (totale ou partielle) du SI

La confiance portée aux infogéreurs est également en augmentation, mais elle s'accompagne d'un plus grand nombre de contrôles et d'audits. En 2020, le marché des infogéreurs est toujours tendu. Au-delà des certifications de sécurité, comme l'ISO 27001, les prestataires se démarquent par un niveau de service accru, comme la personnalisation du cloud, une haute disponibilité ou encore une proactivité pour accompagner la transformation digitale. Quant à l'ISO 22301, orientée « continuité d'activité » ou SecNumCloud de l'Anssi, elles sont encore très peu présentes.

Les directions métiers et/ou les utilisateurs ont-ils recours à des services en cloud ?

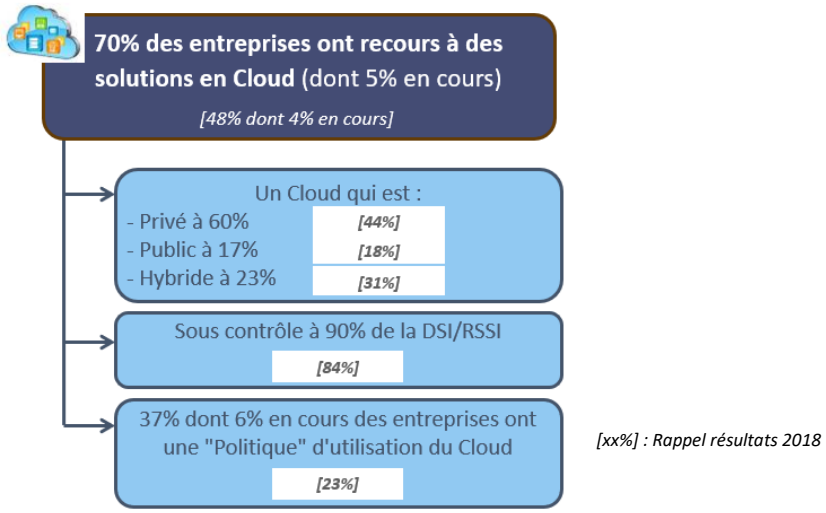


Figure 33 – Implication des différentes entités à la PSSI

L'année 2020 marque une explosion du recours aux services cloud par les entreprises : alors que moins de 50 % de celles-ci utilisaient le cloud sur le périmètre 2018, elles sont dorénavant 70 % à y recourir. Il est à noter que les chiffres de l'enquête basés sur l'année 2019 ne prennent pas en compte l'augmentation prévisible, liée à la crise du COVID-19.

On observe plus particulièrement une augmentation de l'utilisation de clouds privés au détriment des clouds hybrides, par rapport au périmètre 2018. Cette augmentation pourrait s'expliquer par un phénomène de défiance et de « repli sur soi » lié à la forte augmentation des menaces et des événements négatifs depuis 2018. En effet, 60 % des entreprises de notre échantillon utilisent un cloud privé en 2020, alors qu'elles n'étaient que 44 % en 2018. L'utilisation des clouds publics reste cependant constante par rapport au périmètre de 2018.

L'accroissement des menaces et des événements négatifs est corrélé avec une augmentation des investissements pour mettre en place les plans de mesures de sécurité :

- nous constatons un contrôle plus serré de la part des DSI et des RSSI. Ce niveau de contrôle, qui était de 84 % en 2018 est dorénavant de 90 % ;
- de manière concomitante, nous observons une augmentation notable du pourcentage d'entreprises ayant défini une « politique » d'utilisation du cloud. Elles sont 37 % en 2020 à la définir ou à l'avoir définie alors qu'elles n'étaient que 23 % en 2018, et le retard relatif que nous constations il y a deux ans est en train d'être rattrapé.

L'année 2020 est une année charnière pour l'utilisation du cloud par les entreprises. D'un côté, nous constatons une réticence à faire confiance à des fournisseurs externes, car les solutions proposées ne sont pas toujours évaluées comme suffisamment matures pour protéger les infrastructures au regard d'exigences de sécurité de plus en plus contraignantes. D'un autre côté, l'accélération des projets de transformation digitale associée à la crise sanitaire liée à la COVID-19 devraient catalyser la montée en puissance du cloud et du télétravail.

Thème 16 : Gestion des incidents liés à la sécurité de l'information

Des incidents collectés plus nombreux mais une résolution plus rapide

Les cellules de collecte et de traitement des incidents de sécurité de l'information sont de plus en plus adoptées par les entreprises, portant à 59 % le pourcentage d'organisations y ayant recours, avec un bond de 18 points par rapport à l'étude de 2018. En outre, même si la sécurité de l'information peut y est partagée avec d'autres fonctions, comme c'est le cas majoritairement (59 %) dans le secteur des transports et des télécoms, on notera tout de même qu'un tiers de ces entreprises possèdent une cellule dédiée, principalement dans le secteur des banques et des assurances.

Que ces cellules soient dédiées ou partagées avec d'autres fonctions dans l'entreprise, elles sont conformes au RGPD et une politique de sécurité de l'information est formalisée à 66 %.

Les incidents de sécurité relevés par ces cellules sont principalement liés :

- à l'informatique de gestion (76 %) ;
- à l'informatique des services généraux tels que caméras, badgeuse, serrure, etc. (66 %) ;
- aux autres formes d'informations (43 %) ;
- à l'informatique industrielle (SCADA) (37 %) ;
- aux processus (activités) (24 %).

Si 39 % des entreprises déclarent ne pas voir subi d'incidents avérés concernant la sécurité de l'information, celles ayant été touchées affichent un temps de résolution plus rapide que les années précédentes. En effet, l'incident le plus sévère a été résolu à 72 % en moins de 24 heures (70 % en 2018) et à 96 % en moins de 72 heures (86 % en 2018). Parmi ces entreprises, seuls 7 % ont déposé une plainte au cours de l'année (17 % en 2018) à la suite de la survenue de ces incidents sur le SI, et ce principalement dans le secteur de l'industrie et du BTP (11 %).

Une hiérarchie des incidents comparable avec les années précédentes

Le recensement des incidents peut s'apparenter à celui relevé lors de l'étude MIPS 2018 qui les classait en trois catégories :

- catégorie 1 : fréquence d'incidents (FI) > 20 % (4 types d'incidents) ;
- catégorie 2 : FI comprise entre 10 % et 20 % (3 types d'incidents) ;
- catégorie 3 : FI compris < 10 % (10 types d'incidents) ;

En faisant un zoom sur les deux premières catégories on s'aperçoit que les incidents les plus fréquemment signalés ont eu pour cause des :

- pertes de services essentiels telles que coupures d'électricité, d'eau, de climatisation, des services télécoms (29 %) ;
- pannes d'origine interne aussi bien matérielle que logicielle, entraînant l'indisponibilité du système (29 %) ;
- infections par virus sans que l'entreprise soit spécifiquement visée (22 %) ;
- vols ou disparitions de matériel informatique ou télécoms (21 %) ;
- erreurs d'utilisation de saisie, d'exploitation du système, etc. (19 %) ;
- erreurs de conception dans la réalisation ou la mise en œuvre des logiciels et procédures (13 %) ;
- attaques logiques ciblées de type destruction manuelle de données, déni de service, bombe logique, cheval de Troie, etc. (11 %).

Même si l'on constate des incidents moins importants lors de cette étude, il n'en reste pas moins que cinq d'entre eux ont subi une réelle augmentation.

Au cours de l'année 2019, votre organisme a-t-il subi des incidents de sécurité de l'information consécutifs à… ?

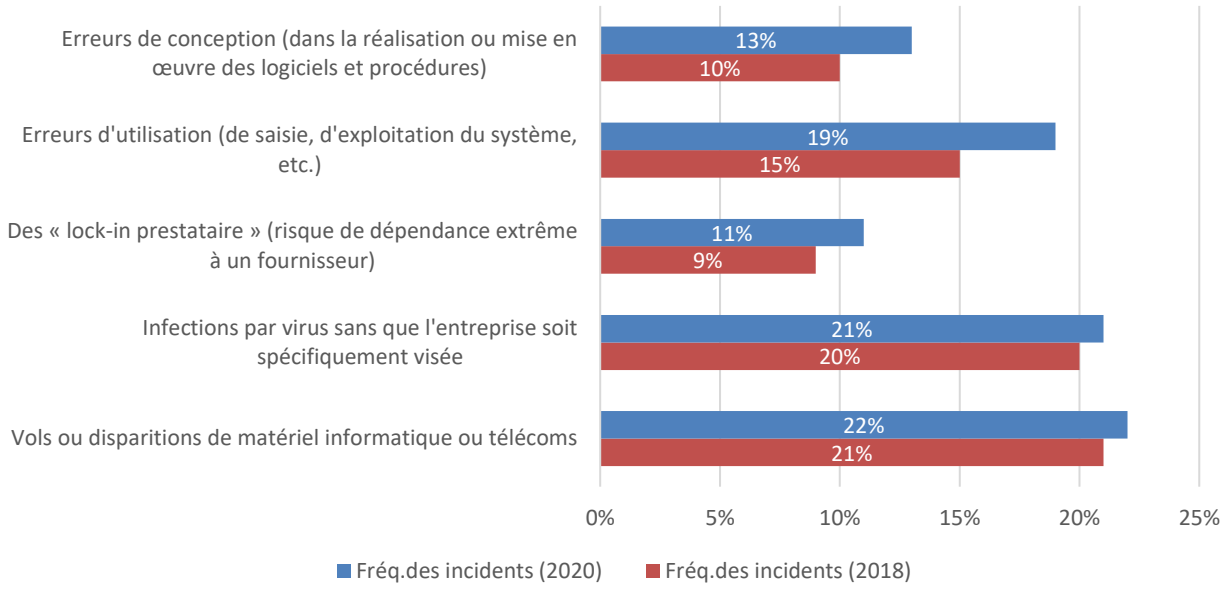


Figure 34 – Origine des incidents de sécurité de l'information

Le secteur de l'industrie et du BTP a pesé dans la répartition des incidents les plus fréquemment signalés et présentés précédemment, puisqu'il obtient souvent, et de très loin, la valeur maximum dans plusieurs domaines :

- pertes de services essentiels : 10 incidents tout comme le secteur du commerce ;
- pannes d'origine interne : 30 incidents, soit 200 % de plus que les suivants, les secteurs du commerce et des services ;
- erreurs d'utilisation : 100 incidents, soit 100 % de plus que le secteur du commerce ;
- erreurs de conception : 50 incidents, soit 108 % de plus que le secteur du commerce ;
- vols ou disparitions de matériel informatique ou télécoms : 100 incidents, soit 400 % de plus que le secteur des services qui se place deuxième ;
- infections par virus : 100 incidents, soit 11 % de plus que le secteur des services qui se place juste derrière et 400 % sur le troisième, le secteur des transports et des télécoms ;
- actes de chantage ou d'extorsion informatique : 50 incidents soit 67 % de plus que le secteur des services qui se place juste derrière et 2 400 % sur troisième, le secteur des banques et des assurances.

Le rançongiciel, vecteur d'attaque toujours aussi préoccupant

Parmi les sujets abordés dans le *Panorama de la cybercriminalité* du Clusif au cours des dernières années, le rançongiciel reste le vecteur d'attaques le plus préoccupant en 2019 pour les entreprises à 12 %. Sans surprise, le secteur des banques et des assurances se retrouve en tête, avec une entreprise sur quatre ciblées. C'est également le même ratio pour les entreprises de plus de 2 000 salariés.

Les sujets suivants ont été abordés dans le *Panorama de la cybercriminalité* du Clusif au cours des dernières années. Avez-vous été confrontés à l'un ou plusieurs de ces sujets en 2019 ?

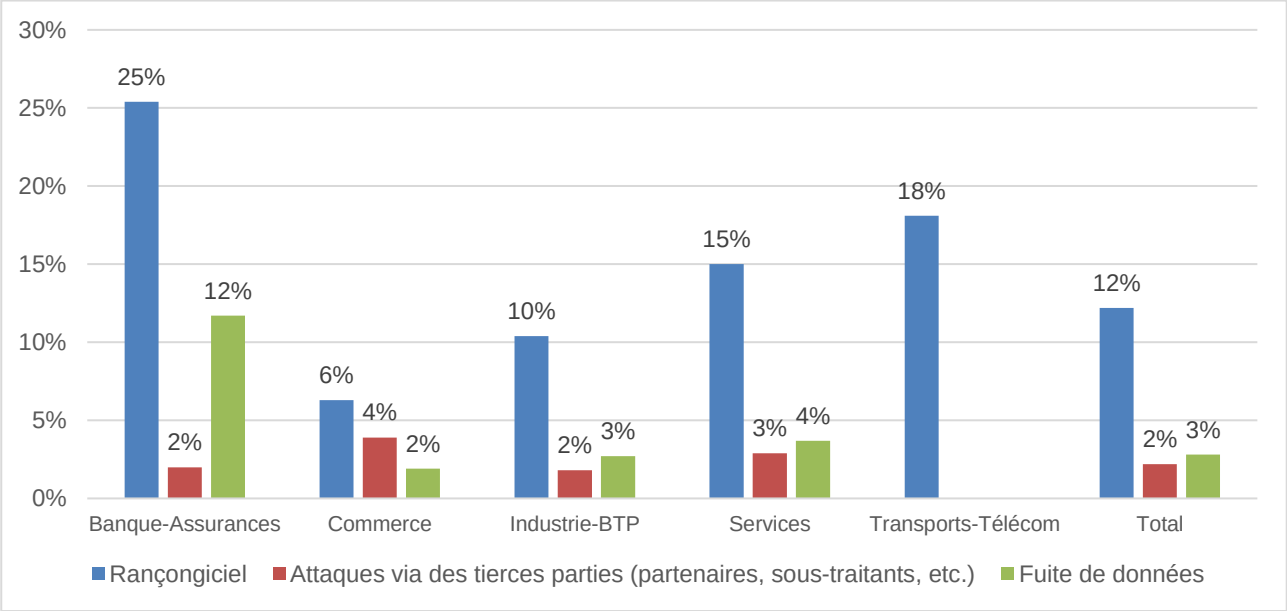


Figure 35 – Sujets identifiés dans le *Panorama de la cybercriminalité* 2020 vécus par les entreprises

« Ne payez pas la rançon. Le paiement ne garantit en rien le déchiffrement de vos données et peut compromettre le moyen de paiement utilisé. » Cette recommandation de l'Anssi semble désormais faire écho auprès des entreprises, puisque 100 % des victimes de rançongiciel n'ont, *a priori,* pas payé la rançon demandée. Pour les entreprises ayant répondu (35 %), l'impact d'une telle attaque est estimé à près de 2 000 k€ dans le secteur des services et toucherait les entreprises entre 250 à 1 999 salariés. Ils ne sont que 82 % à avoir pu récupérer leurs données et seulement 64 % à avoir communiqué sur le sujet.

Que ce soit par courriel (hameçonnage, *phishing)* ou par clé USB, pour ne retenir qu'eux, les entreprises ont identifié le vecteur d'entrée d'une attaque par rançongiciel à 71 % et à hauteur d'une entreprise sur deux dans le secteur de l'industrie et du BTP.

Les fuites de données dont ont été victimes les entreprises ne représentent quant à elle que 3 % des attaques subies et c'est une nouvelle fois le secteur des banques et des assurances qui est le plus touché, à hauteur de 12 %. De ces fuites, près d'une entreprise sur deux reconnaît qu'elles contenaient des données à caractère personnel et elles ne sont que 63 % à avoir fait une notification de violation de données personnelles conformément à l'article 33 du règlement général sur la protection des données (RGPD).

Impacts financiers des incidents

Plus d'une entreprise sur deux a évalué l'impact financier des incidents de sécurité. Pour les entreprises ayant subi un sinistre, la répartition du financement reste la même que dans l'étude précédente, alors qu'elles ne sont plus que 12 % contre 54 % en 2018 à ne pas connaître la manière dont ces sinistres sont financés.

À noter que 86 % des entreprises n'ont toujours pas souscrit à une cyberassurance, mais elles sont 37 % à posséder une police d'assurance, ce qui représente une progression de 12 points par rapport à l'étude de 2018. Cette police d'assurance prend en compte la valeur des informations perdues, altérées ou volées sur les smartphones et tablettes dans moins de un cas sur cinq.

Comment avez-vous traité l'impact financier de vos sinistres ?

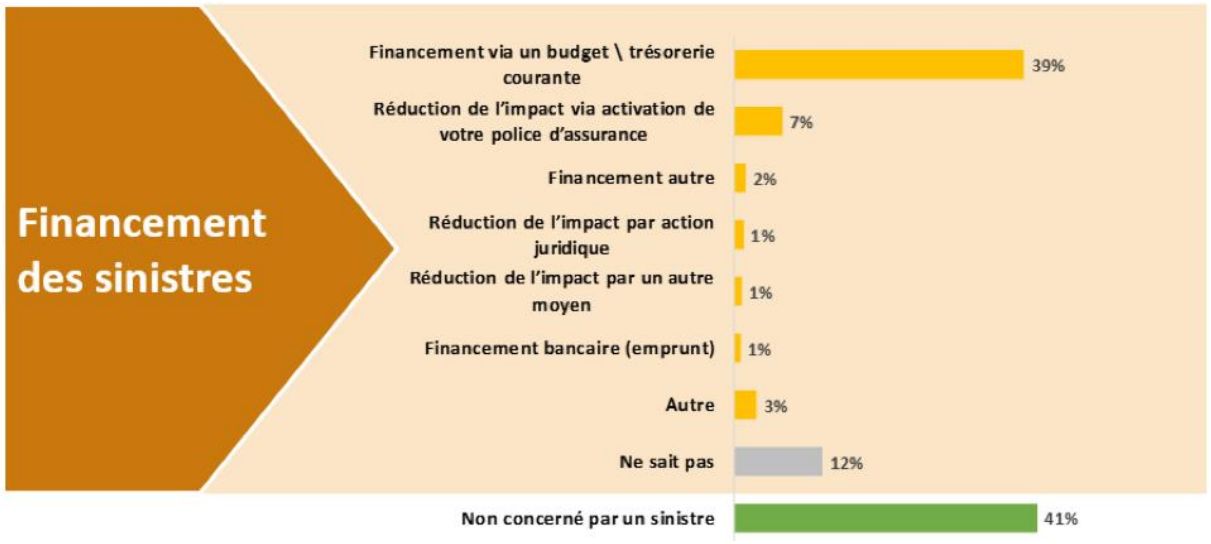


Figure 36 – Financement des sinistres

Que ce soit au travers d'une souscription à une cyberassurance ou à une police d'assurance, le secteur dont la préoccupation principale est de réduire l'impact financier reste incontestablement celui des transports et télécoms (44 %), très largement devant les autres puisqu'il devance de 17 points le suivant, le secteur des banques et des assurances.

Thème 17 : Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité

Une gestion de la continuité qui embarque davantage l'informatique industrielle

Le périmètre des plans de continuité d'activité (PCA) et plans de continuité informatique (PCI) couvrent désormais plus fréquemment l'informatique industrielle. En effet, dans la précédente étude MIPS 2018, seuls 19 % des PCA et PCI intégraient les environnements informatiques industriels alors qu'ils sont aujourd'hui pris en compte dans 28 % des cas.

La gestion de la continuité d'activité dans votre entreprise couvre-t-elle les scénarios suivants (plusieurs réponses possibles) ?

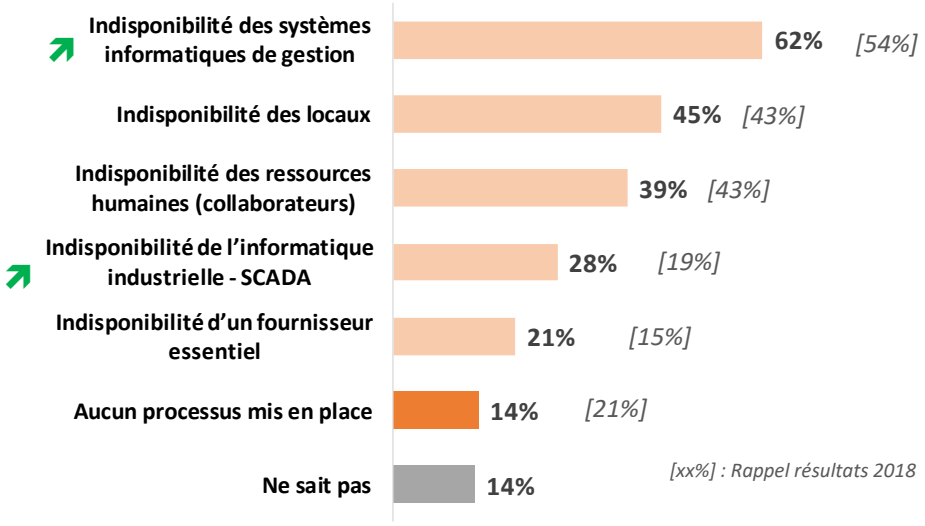
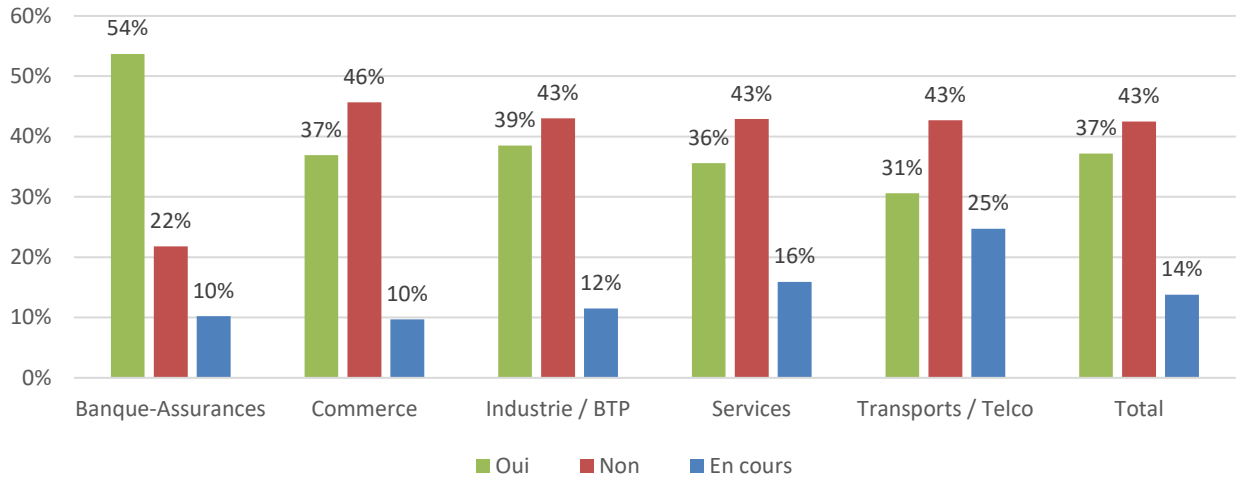


Figure 37 – Domaine de couverture de la gestion de la continuité

Seule la moitié des entreprises ont évalué les exigences métiers dans le cadre d'un BIA formel

Une démarche d'élaboration de PCA doit obligatoirement prendre en compte un bilan d'impact sur l'activité (*Business Impact Analysis* – BIA) formel. Or seule la moitié des répondants à l'enquête signalent que les exigences métiers ont été évaluées grâce à ce type de démarche. Il convient donc d'encourager les entreprises à progresser sur ce point.

Avez-vous évalué les exigences « métiers » en termes de DMIA* et de perte de PDMA dans le cadre d'un BIA*** formel ?**



** DMIA : Délai maximal d'interruption admissible (Recovery Time Objective – RTO)*
*** PDMA : Perte de données maximale admissible (Recovery Point Objective – RPO)*
**** BIA : Bilan d'impact sur l'activité (Business Impact Analysis)*

Figure 38 – Pourcentage d'entreprises engagées dans une démarche de BIA formel

La fréquence des tests progresse nettement pour être réalisés environ une fois par an

Point remarquable à signaler, plus de la moitié des entreprises réalisent des tests PCA/PCI une fois par an alors que l'étude 2018 indiquait que moins de 30 % des cas étaient concernés. Cette nette progression est encourageante dans la perspective de disposer de PCA opérationnel.

À quelle fréquence sont testés 1 les plans de continuité d'activité par les utilisateurs « métier » et 2/ / les plans de continuité informatiques ?

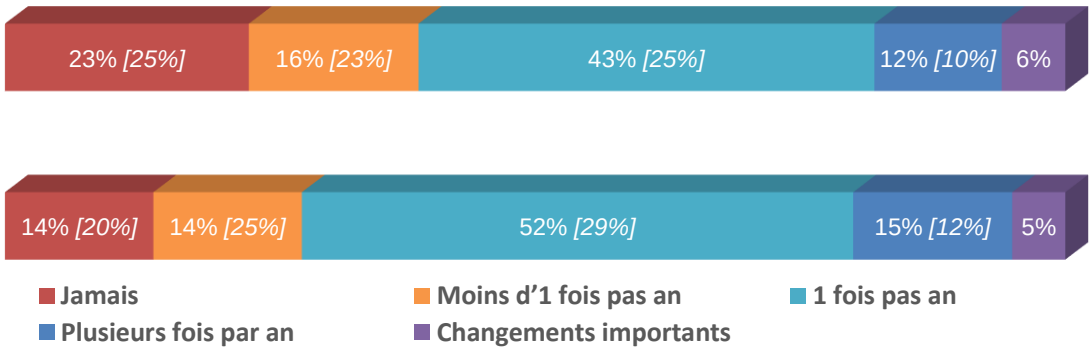


Figure 39 – Fréquence des tests

Thème 18 : Conformité

Ce thème aborde la conformité sous trois aspects :

- la conformité avec les obligations légales (RGPD, loi Informatique et Libertés) ;
- l'utilisation de tableaux de bord ;
- les audits de sécurité.

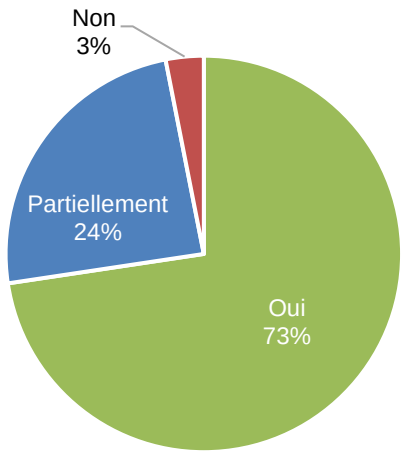
Conformité avec les obligations légales et réglementaires

L'édition 2020 de l'étude MIPS est la première depuis l'entrée en application, le 25 mai 2018, du règlement général sur la protection des données de l'Union européenne (RGPD), l'édition 2018 étant intervenue durant la période transitoire où le RGPD venait d'entrer en vigueur (25 mai 2016) sans être formellement applicable. Depuis la dernière édition, la loi Informatique et Libertés a également été révisée pour tenir compte du RGPD (1er juin 2019).

Alors que les dispositions du RGPD s'imposent depuis deux ans, la quasi-totalité des entreprises estiment être en conformité, totalement (73 %) ou partiellement (24 %).

Cela représente une évolution majeure depuis 2018, où 24 % des entreprises ne s'estimaient pas prêtes pour le RGPD, tandis que 22 % l'étaient totalement et 46 % partiellement.

Votre entreprise est-elle en conformité avec le RGPD* ?



** RGPD : Règlement général sur la protection des données (General Data Protection Regulation – GDPR)*

Figure 40 – Répartition du degré de conformité avec le RGPD

Si le degré de conformité est homogène, quelle que soit la taille des entreprises, on note que les entreprises qui s'estiment en retard sur la conformité se retrouvent essentiellement dans le secteur de l'industrie et du BTP où elles sont seulement 7 % à ne pas être en conformité. Cela s'explique sans doute en partie par le fait que ces secteurs traitent peu de données personnelles en dehors de celles de leurs salariés, moins stratégiques, ce qui peut rendre ces entreprises moins sensibles à la problématique de conformité.

La fonction de délégué à la protection des données (DPD/DPO)

Depuis 2018, la fonction de délégué à la protection des données (DPD, *Data Protection Officer* – DPO) est obligatoire dans un certain nombre de cas, et en tout cas fortement recommandée.

Dans ce contexte, seuls 57 % des entreprises indiquent avoir clairement identifié et attribué la fonction de DPD/DPO, et 9 % sont en cours.

La fonction de DPD/DPO est-elle clairement identifiée et attribuée ?

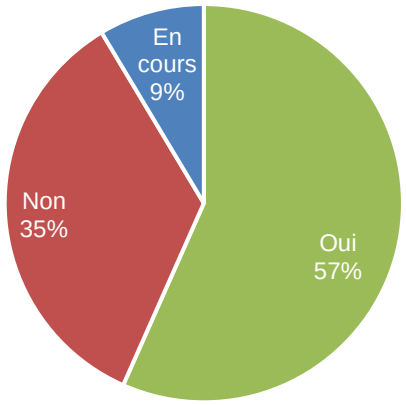


Figure 41 – Identification de la fonction de DPD/DPO

Sans surprise, ce sont les entreprises du secteur des banques et des assurances qui sont les plus nombreuses à avoir mis en place un DPD/DPO (84 %), les volumes de données personnelles et l'importance stratégique de leur protection expliquant cette démarche. *A contrario,* c'est dans le secteur de l'industrie et BTP que le DPD/DPO est le moins souvent identifié : 40 % des entreprises n'y ont ni identifié à ce jour de DPO ni entrepris de démarche en ce sens.

On note également que lorsqu'une PSSI a été formalisée, la fonction de DPD/DPO est plus souvent identifiée (66 %) que lorsqu'il n'y a pas de PSSI (32 %).

Lorsqu'un DPD/DPO a été identifié, il est majoritairement rattaché à la Direction générale (60 %), et dans une moindre mesure à la DSI (17 %). Toutefois, dans les entreprises de plus de 500 personnes, la Direction juridique est citée plus souvent que la DSI (18 % *vs* 7 % pour les entreprises de 500 à 1 999 salariés, 13 % *vs* 10 % pour celles de plus de 2 000 salariés).

Quel est le rattachement hiérarchique du DPD/DPO au sein de votre entreprise ?

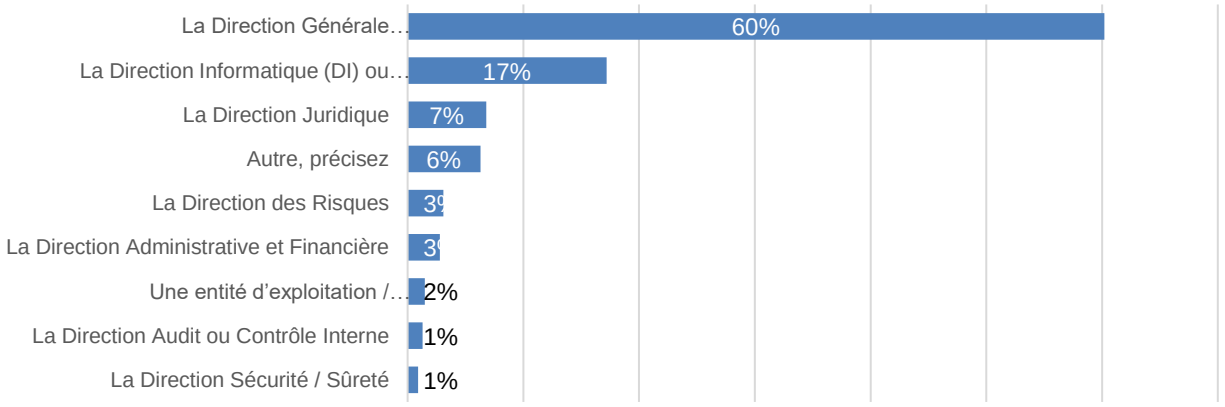


Figure 42 – Rattachement hiérarchique du DPD/DPO

Si, en moyenne, la Direction des risques est peu citée (3 %), le DPD/DPO lui est souvent rattaché dans le secteur des banques et des assurances (20 %) et celui des transports et télécoms (12 %). Cela correspond sans doute au fait que ces secteurs ont une plus grande culture de la gestion des risques.

Bien que la tenue du registre des traitements soit juridiquement dévolue au responsable de traitement, on sait que lorsqu'il est identifié, c'est au DPD/DPO que cette responsabilité est généralement attribuée.

Dans les cas où cette fonction n'existe pas dans l'entreprise, la tenue du registre est assurée majoritairement par la DSI (55 %) ou par le service juridique (17 %).

En l'absence de DPO/DPD, qui est en charge du registre des traitements dans votre entreprise ?

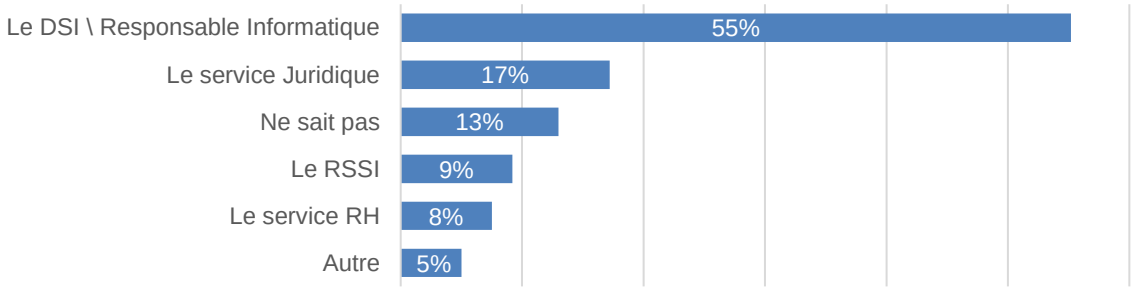


Figure 43 – Responsabilité des formalités (en l'absence de DPO/DPD)

On constate sur ce point des différences significatives selon les secteurs d'activité. Ainsi, le DSI est plus souvent cité dans le secteur des transports et des télécoms (69 %) et dans celui du commerce (63 %) que dans les autres secteurs. De même, le service juridique l'est plus souvent dans les secteurs des banques et des assurances (44 %), des services (25 %) et du commerce (29 %).

Utilisation de tableaux de bord de sécurité

L'utilisation de tableaux de bord reste très largement absente des questions de sécurité : une grande majorité des entreprises indiquent ainsi ne pas avoir mis en place d'indicateurs (70 %). Si ce chiffre est en léger recul, on peut noter qu'il n'évolue que très peu depuis 2014 (74 % en 2014, 73 % en 2016, 76 % en 2018).

Pour le tiers des entreprises qui utilisent des indicateurs, ceux-ci sont surtout de nature opérationnelle (67 %), ou concernent le pilotage des fonctions SSI (62 %) et, dans une moindre mesure, ils correspondent à des indicateurs stratégiques destinés à la Direction (45 %). On note une évolution continue de ces derniers, ce qui confirme l'intérêt croissant des directions générales, déjà observé en 2018.

Revue de la sécurité de l'information

La proportion d'entreprises (22 %) qui déclarent être concernées par des lois ou réglementations spécifiques en matière de sécurité SI (hors RGPD) est pratiquement constante depuis 2014.

Votre entreprise est-elle soumise à des lois et/ou réglementations spécifiques en matière de sécurité de l'information ?

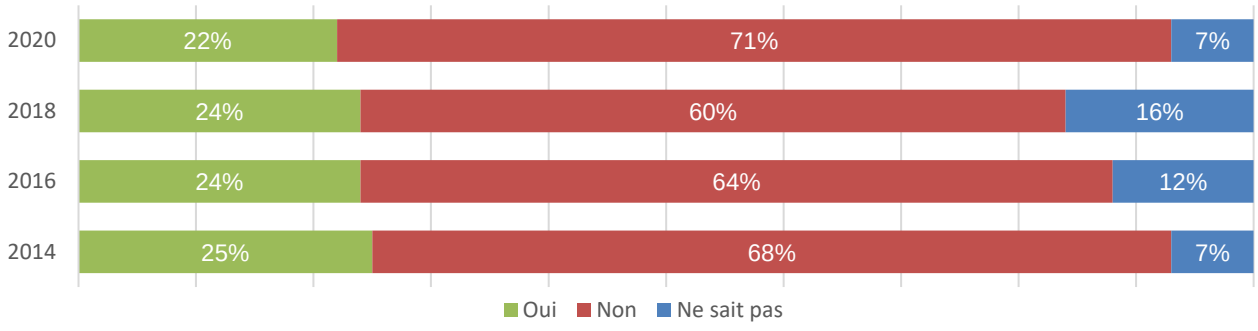


Figure 44 – Entreprises soumises à des lois/réglementations spécifiques pour la sécurité SI

On note toutefois une grande disparité dans les réponses apportées selon les secteurs. Ainsi, sans surprise, les banques et les assurances sont 48 % à déclarer être soumises à des textes spécifiques, malgré un taux de réponses incertaines de 24 %. Au contraire, le secteur du commerce indique, avec une grande certitude (1 % de « ne sait pas ») ne pas être soumis à des textes particuliers (81 %).

Votre entreprise est-elle soumise à des lois et/ou réglementations spécifiques en matière de sécurité de l'information ?

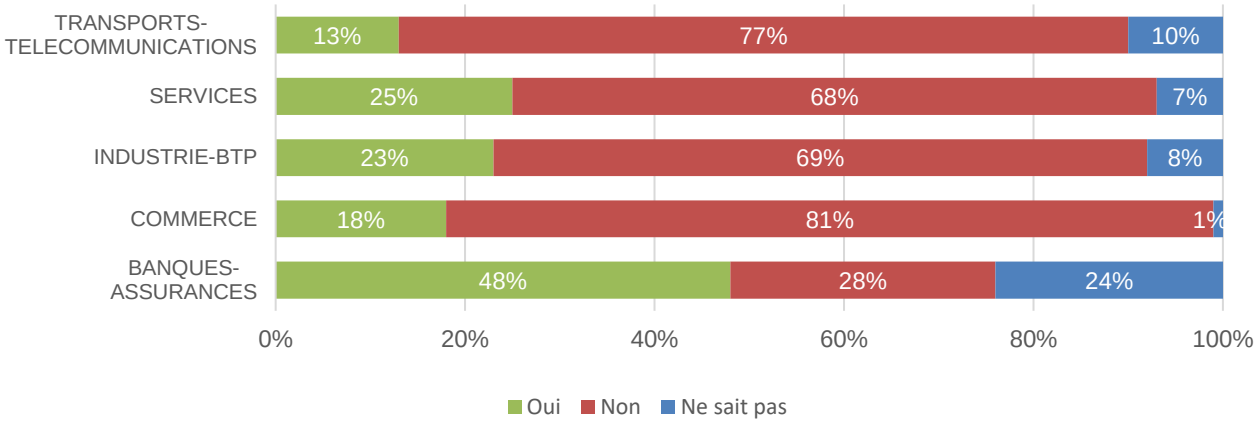


Figure 45 – Entreprises soumises à des lois/réglementations spécifiques pour la sécurité SI (par secteur)

Plus de 80 % des entreprises indiquent aujourd'hui procéder à des audits ou des contrôles de sécurité du SI, cette pratique étant en progression constante depuis 2014. Dans la quasi-totalité des cas, la fréquence de ces contrôles reste au maximum de cinq par an.

Le secteur des banques et des assurances se démarque logiquement avec au moins un contrôle effectué par an (84 % des cas), jusqu'à plus de cinq par an dans 16 % des entreprises.

Parallèlement, les grandes entreprises pratiquent des audits de manière quasi systématique (92 % contre 79 % en moyenne).

Combien d'audits ou de contrôles de sécurité du SI sont menés en moyenne au sein de votre entreprise sur une période de deux ans ?

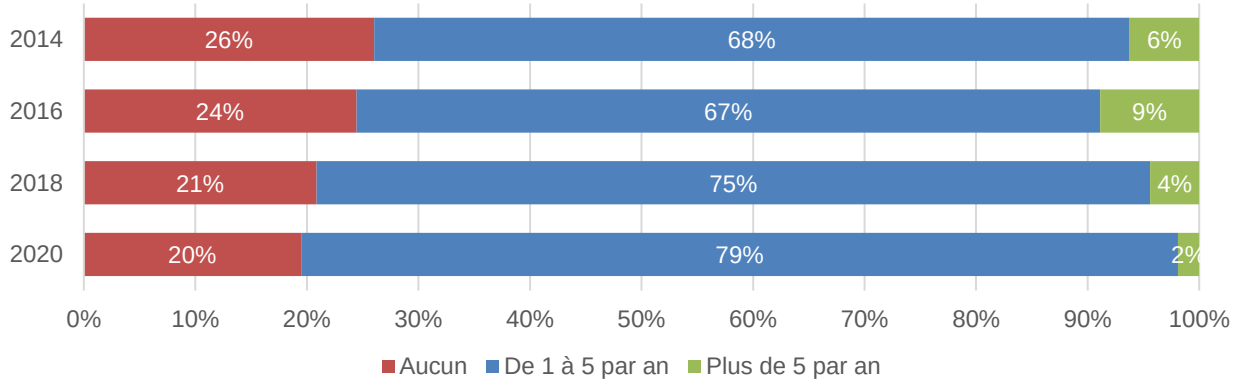


Figure 46 – Fréquence des audits de sécurité au cours des deux dernières années

La nature des audits a sensiblement évolué depuis 2018. Il s'agit en priorité de tests d'intrusion (68 % des cas contre 47 % en 2018). Viennent ensuite les audits organisationnels (58 % *vs* 39 %), de configuration (57 % *vs* 45 %), de continuité d'activité (45 % *vs* 32 %), les revues régulières des droits d'accès logiques (39 % *vs* 34 %), les audits physiques (35 %), les audits de code source (31 %) et les revues régulières des droits d'accès physiques (27 %).

En ce qui concerne leur motivation, ces audits répondent d'abord à une exigence contractuelle ou réglementaire (59 %) plus souvent citée dans une très large mesure que lors de l'édition 2018 (33 %). Les audits de routine (« sans motivation ») ont quant à eux quasiment disparu (4 % contre 24 % en 2018).

Quelles sont les principales motivations qui déclenchent ces audits ?

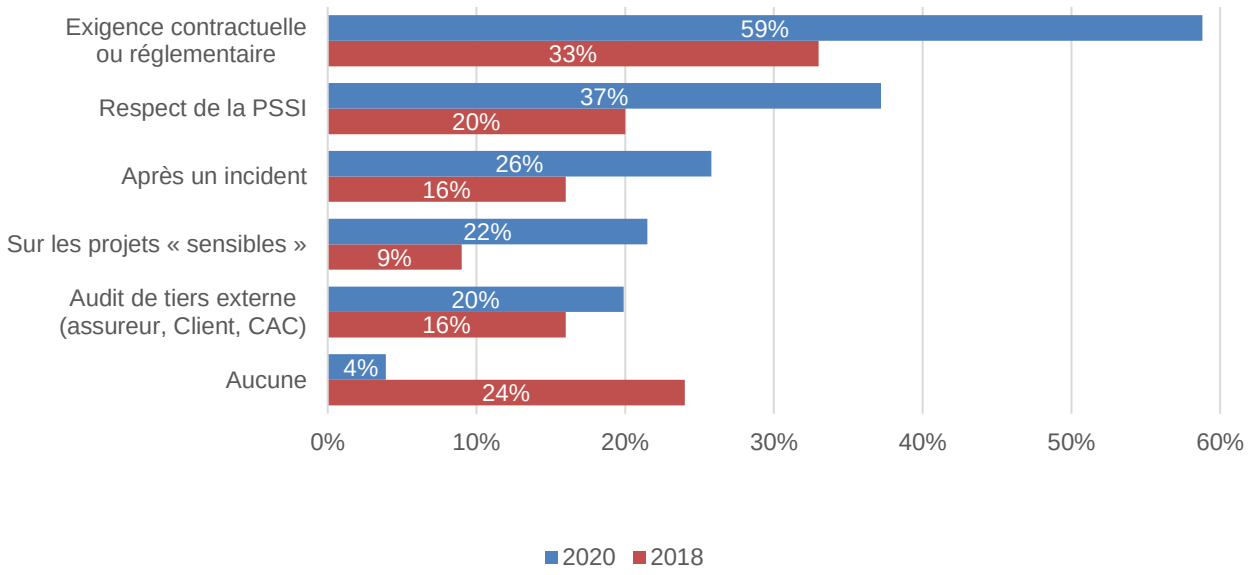


Figure 47 – Motivation des audits de sécurité

11 rue de Mogador

75009 Paris

France

✆ +33 1 53 25 08 80

clusif@clusif.fr

Téléchargez toutes les productions du Clusif sur

https://clusif.fr