ÉTUDE CLUSIF

Menaces informatiques et pratiques de sécurité en France

Édition 2020

- Les entreprises de plus de 100 salariés
- Les collectivités territoriales
- Les particuliers internautes

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.

Avant-propos

Dans ce contexte un peu particulier de crise sanitaire, le groupe de travail et de réflexion élargi nous livre son nouveau rapport d'étude des statistiques sur les pratiques de sécurité de l'information et de cybersécurité. Sans doute trop souvent oubliés des commentateurs de l'actualité, ces chiffres ne sont pas moins importants que ceux de la cybercriminalité et ceux, à venir, quantifiant les cyberattaques.

Je l'ai déjà évoqué dans une tribune, mais la vérité des chiffres ne vaut que le crédit que nous pouvons, par notre interprétation, leur donner. Je voudrais donc souligner ici tant la qualité de l'enquête réalisée par notre partenaire GMV Conseil que le remarquable travail d'interprétation et de commentaires fait par cet aréopage d'experts, qui est RSSI, qui est consultant qui est intégrateur/industriel. De cette mixité de sensibilité ressortent des consensus dans les interprétations. Bien sûr, cela reste une « vérité », celle du Clusif, alors à vous lecteurs, profanes ou experts, de vous faire votre propre analyse.

La matière est riche, les acteurs nombreux et la convergence des idées comme des vues ne sont jamais une évidence. Mais le Clusif s'est toujours appuyé sur ses adhérents, sur la richesse et la pluralité de leurs expériences ainsi que sur des experts externes pour analyser, commenter et mettre en perspective ces données, ces chiffres. Nous sommes très heureux de compter à nos côtés une structure qui doit être demain le point focal de toutes démarches pour toutes celles et tous ceux qui subissent les affres des cybercriminels : la plateforme Cybermalveillance.gouv.fr, dont je remercie ici l'implication, sur la thématique « Internautes », de son Directeur général, Jérôme NOTIN.

L'activité et l'actualité de la cybercriminalité nous imposent une nouvelle approche. Dans un monde où l'on pense que quatre mois d'une mise en suspens de la vie sociale et économique, au profit de notre santé, vont changer radicalement les choses, il nous faut sans doute nous aussi nous réinventer et évoluer avec ce possible changement annoncé. C'est pour cela que le Groupe de travail MIPS va changer de physionomie, de fréquence et de spectre. Mais je laisse à son animateur Lionel MOURER, le soin de dévoiler plus avant ces transformations à venir.

Je conclurai cette introduction, par de vifs remerciements à tous les membres, les experts extérieurs et aux trois animateurs des chapitres de l'étude, dont Cyril BRAS sur le thème Collectivités territoriales. Merci de votre implication et de votre travail dans les conditions de ces dernières semaines.

Jean-Marc GRÉMY

Président du Clusif

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…

Enfin, cette année comme depuis 2008, l'étude reprend le volet très complet consacré aux pratiques des particuliers utilisateurs d'Internet à domicile (998 répondants), en constante évolution au regard des nouveaux usages.

Cette synthèse reprend l'une après l'autre chacune des thématiques abordées et en précise les tendances les plus remarquables.

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…

Collectivités territoriales : une amélioration à géométrie variable, mais encore insuffisante

Pour la troisième fois, le Clusif s'intéresse à la façon dont les collectivités territoriales intègrent la cybersécurité dans leur fonctionnement. Pour cela un sondage a été réalisé auprès de 202 collectivités en début d'année 2020. Les résultats ainsi obtenus ont été redressés afin de correspondre à la réalité de la répartition des collectivités. Ces derniers ont ensuite été analysés par des experts provenant de différents horizons professionnels, mais aussi des collectivités territoriales françaises.

Il en ressort que les collectivités, avec l'appui de 70 % des directions générales ont progressé dans la formalisation de leur PSI ; cependant, cette dernière a encore du mal à sortir de la sphère DSI.

Corollaire de la PSI, la fonction de RSSI est présente dans la majorité des collectivités, mais il reste difficile pour beaucoup de la dédier à un poste à plein temps, ce qui a pour conséquence de placer le RSSI dans une position de juge et partie qui ne permet pas une réelle liberté de parole ou une évaluation correcte des enjeux par les dirigeants.

Bien qu'en amélioration, la SSI n'est pas encore l'affaire de tous et les moyens tant humains que financiers ne sont pas la plupart du temps à la hauteur des enjeux. Bien que le sentiment de dépendance au SI soit fort, le budget alloué à la cybersécurité reste la variable d'ajustement des DSI avec l'absence de budget dédié et/ou pérenne. Cependant, ce dernier est en augmentation par rapport à la précédente étude.

Du côté des ressources humaines (RH), la mise en place de chartes d'usage des SI continue de progresser même si les communautés de commune restent à la traîne. Il reste malgré tout difficile de gérer les départs ou les changements de poste. Un point remarquable concerne la mise en œuvre de programmes de sensibilisation pour les différentes populations, mais malheureusement sans pour autant en évaluer l'impact réel.

Du côté de l'inventaire des actifs, on note une progression importante, avec une proportion de collectivités l'ayant réalisé qui s'élève à 66 % mais ce progrès est à nuancer par les aspects de classification qui, lorsque celle-ci est en œuvre se limite bien souvent à la distinction entre sensible et non sensible. Il en est de même pour l'analyse des risques. Globalement, les risques sont identifiés, mais non formellement analysés. Ainsi, nous pouvons supposer que les plans de réduction des risques se basent sur une approche empirique.

La gestion des accès varie en fonction de la taille des collectivités ; encore une fois, les communautés de communes sont ici en retrait. En revanche, les méthodes d'authentification fortes tendent à s'homogénéiser et on constate que, globalement, les droits d'accès sont de mieux en mieux gérés avec la mise en place de procédures pour 68 % des collectivités, notamment pour les administrateurs. Des politiques de mot de passe sont mises en œuvre dans 65 % des cas étudiés.

Concernant la cryptographie, elle reste largement sous-utilisée. Lorsqu'elle est mise en œuvre, elle vise quatre objectifs : le chiffrement de données, l'authenticité, l'authentification ou la non-répudiation.

Les aspects relevant de la sûreté sont en très nette progression avec la mise en œuvre de plus en plus fréquente de dispositifs de contrôle d'accès et de vidéosurveillance combinés à de l'accueil physique. Il en est de même pour la protection des données, ces dernières étant de plus en plus déplacées vers des supports physiques amovibles.

Au niveau de la sécurité d'exploitation, des solutions classiques de protection sont en place (antivirus, antispam, pare-feu), mais on constate un retard important dans les capacités de détection. Les équipements mobiles restent également en retrait sur la mise en place de dispositifs de protection. Pour ce qui est de la gestion des vulnérabilités techniques, la veille est en forte progression mais n'est pas systématiquement en cohérence avec les systèmes implémentés dans les collectivités, ce qui n'a que peu d'impact sur la

formalisation de la gestion des correctifs de sécurité. Les délais de mise en œuvre restent faibles et ne se sont pas améliorés depuis la précédente étude.

Concernant la sécurité des communications, les SI s'ouvrent de plus en plus sur l'extérieur à partir d'un environnement maîtrisé au détriment du BYOD, qui est en régression. L'accès à Internet est aussi plus ouvert vers les réseaux sociaux ou les messageries instantanées externes, mais reste encore soumis à un filtrage d'URL dans 61 % des cas.

Aucune amélioration n'est à signaler dans la mise en place des concepts de bases de développements sécurisés, où c'est toujours le pragmatisme qui domine, ce qui se traduit par de faibles exigences dans les cahiers des charges s'expliquant en partie par l'absence de référent sécurité pour les développements.

La majorité des collectivités territoriales fait appel à l'infogérance, en particulier dans les communautés de communes. En revanche, même si des audits de sécurité sont mis en place pour s'assurer de la conformité, le contrôle s'appuie trop rarement sur l'utilisation d'indicateurs. Le recours aux services cloud progresse aussi, mais pas aussi vite que son encadrement.

Au niveau des incidents, les collectivités ont commencé à être touchées par les attaques par rançongiciels avec 30 % des conseils territoriaux et des villes impactés. Ce risque reste toutefois sous-évalué puisque 62 % des répondants l'estiment faible, alors que l'impact financier maximal observé dans l'étude s'élève à 400 k€. Autre point, la capitalisation sur les incidents n'est pas encore à l'ordre du jour, la priorité étant plutôt donnée à la remise en service qu'à l'analyse de l'attaque et la collecte d'éléments. Un point rouge concerne les systèmes de contrôle et d'acquisition de données en temps réel (*Supervisory Control And Data Acquisition* – SCADA) qui sont encore cette année les grands oubliés de la SSI alors que certaines activités pourraient relever de la LPM ou de la directive NIS.

Étant donné l'absence de capitalisation sur les incidents, la formalisation de la gestion de crise cyber reste là aussi très faible et inférieure aux pratiques observées en entreprise. La mise en œuvre de plans de conduite ou de reprise d'activité (PCA/PRA) ne concerne qu'un quart des collectivités avec une faible fréquence de tests de mise en pratique.

Cette édition est la première de notre série d'études à consacrer un volet aux collectivités territoriales depuis l'entrée en vigueur du RGPD. Globalement, les collectivités s'estiment être en conformité totale pour 34 % d'entre elles et partielle pour 59 %. La désignation d'un DPO étant obligatoire pour ce type de structures, 75 % indiquent s'être déjà acquittées de cette obligation et 10 % déclarent que la désignation d'un DPO en cours. Celui-ci est parfois mutualisé, notamment dans les communautés d'agglomération. S'il est principalement rattaché à la Direction générale (51 %), il est externalisé dans certains cas (19 %). Le référentiel général de la sécurité (RGS) n'est pas aussi bien suivi que le RGPD puisque 57 % des collectivités ont identifié totalement ou partiellement les services nécessitant une homologation. Pour ce qui est du suivi par TBSSI, 87 % des collectivités indiquent ne pas en avoir mis en place. En revanche, une progression s'est opérée depuis la précédente étude dans le domaine des audits, 56 % déclarant aujourd'hui en faire au moins un tous les deux ans. Ce sont surtout les exigences réglementaires (51 %) qui ont motivé cette évolution.

Pour conclure, nous retiendrons que la prise en compte des enjeux de cybersécurité reste très variable en fonction de la taille des collectivités, les communautés de communes étant souvent à la traîne. Il est évident que l'arrivée du RGPD a aidé à cette prise en considération ; néanmoins, le retard en la matière reste important. La gestion de la SSI est encore trop souvent sous pavillon DSI entraînant une situation de juge et partie pour le RSSI qui n'est pas toujours facile à gérer, et donc une liberté de parole amoindrie.

Depuis plusieurs mois, les collectivités se trouvent de plus en plus fréquemment confrontées à des actes de cybermalveillance qu'elles sous-estiment encore trop. La capitalisation des incidents et l'organisation de la réponse à incident sont encore trop faibles et nécessitent une plus grande allocation de moyens tant humains que financiers.

Même si, globalement, la situation s'améliore par rapport à l'étude précédente, les collectivités ont devant elles un chantier important pour que la cybersécurité soit perçue comme un gage de confiance dans l'usage des moyens numériques mis à la disposition des citoyens.

Internautes et les pratiques de sécurité : des constantes, parfois des progrès mais encore des axes d'amélioration…

L'étude 2020, toujours représentative de la population française, démontre que les téléphones mobiles sont aujourd'hui l'outil privilégié pour se connecter à Internet. Dans les foyers français, en dehors des ordinateurs, les télévisions et systèmes audio ainsi que les consoles de jeux restent les objets les plus connectés. L'Internet des objets où chaque foyer aurait des dizaines, voire des centaines de petits équipements connectés demeure théorique.

En parallèle, l'étude indique que le Wi-Fi est la technologie la plus utilisée par les internautes pour se connecter à Internet depuis leur domicile : 90 % y ont recours, ce taux se portant à 98 % pour les étudiants. Pour ceux qui n'utilisent pas cette technologie, ils sont plus d'un tiers (35 % en 2020 *vs* 24 % en 2018) à répondre qu'ils n'y ont pas recours « pour des raisons de sécurité » tandis qu'ils sont 26 % à expliquer qu'ils font ce choix « pour raisons de santé », alors qu'ils n'étaient que 12 % en 2018.

Sur les pratiques de navigation sur Internet, il est intéressant de noter que l'utilisation de services en ligne dits « communautaires » (covoiturage, location de logement entre particuliers…) connaît une progression de 9 points en 2020, passant de 38 % à 47 %. Les personnes seules en activité sont même 62 % à utiliser ces services « au moins parfois », suivies de près par les 15-29 ans (61 %) puis les CSP+ (59 %).

Depuis 2016, la perception des menaces sur la vie privée est stable : 69 % des sondés estiment qu'Internet met en danger leur vie privée, 88 % estiment qu'il est important de la protéger, dont 49 % vont jusqu'à penser que cela est très important. Malgré cela, seulement 46 % des personnes sondées vérifient régulièrement leurs paramètres de confidentialité sur les réseaux sociaux, avec un recul régulier de 2 % par an depuis 2016. Même constat à l'autre bout de l'échelle puisque les internautes sont 38 % à ne pas vérifier et modifier ces paramètres régulièrement, soit 8 points de plus depuis 2016 !

Concernant le risque sur les données des équipements, la tendance observée entre 2018 et 2020 est la même pour les utilisateurs de tablettes/mobiles et ordinateurs. La proportion de ceux qui estiment que le risque est « très important » sur leurs objets connectés fait toutefois plus que doubler entre 2018 et 2020 : de 8 % à 19 %. Par ailleurs, le nombre d'internautes étant dans l'incapacité d'appréhender le risque quand il s'agit d'objets connectés, même s'il se contracte fortement en 2020 (32 % *vs* 25 % en 2018), reste malgré tout 2,5 fois supérieur à celui des catégories précédemment étudiées.

À propos des menaces qui peuvent peser sur leur informatique personnelle, les internautes comprennent de mieux en mieux la nécessité de changer fréquemment leurs mots de passe, de ne pas utiliser le même partout et de privilégier une combinaison complexe de caractères. *A contrario,* l'absence de mise à jour de l'antivirus est de moins en moins perçue comme une menace. Ce constat à la baisse se fait sur tout ce qui pourrait s'apparenter à la mise en place de solutions techniques (antispam, antivirus, *firewall*…).

La part des internautes qui se sentent informés de leurs droits, malgré le nouveau cadre du RGPD, n'évolue que très peu entre 2018 et aujourd'hui, voire diminue pour certaines catégories. Le pari lancé dans l'étude en 2018 n'est donc pas encore gagné.

Lorsque les internautes subissent des dommages sur leurs équipements, ils font de plus en plus appel à des prestataires payants (37 % pour les ordinateurs contre 26 % en 2018, 36 % pour les mobiles/tablettes contre 21 % en 2018) : les bénévoles sont donc beaucoup moins sollicités.

D'une manière générale, la tendance des internautes qui ne se sentent pas en sécurité sur Internet est à la hausse depuis 2016. Ils étaient alors 27 % puis 30 % en 2018, pour atteindre 33 % en 2020.

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

REMERCIEMENTS **3**

AVANT-PROPOS **4**

SYNTHESE DE L'ETUDE **5**

Entreprises : « sécurité de l'information, tout le monde pense que c'est important, elle avance… mais les budgets restent précaires ! 5

Pour conclure… 9

SOMMAIRE **12**

LISTE DES FIGURES **14**

METHODOLOGIE **18**

LES ENTREPRISES DE PLUS DE 100 SALARIES **22**

Présentation de l'échantillon 22

Thème 5 : Politique de sécurité de l'information (PSSI) 24

Thème 6 : Organisation de la sécurité de l'information 27

Thème 7 : Sécurité des ressources humaines 30

Thème 8 : Gestion des actifs 32

Thème 9 : Contrôle d'accès 36

Thème 10 : Cryptographie 39

Thème 11 : Sécurité physique et environnementale 40

Thème 12 : Sécurité liée à l'exploitation 41

Thème 13 : Sécurité des communications 43

Thème 14 : Acquisition, développement et maintenance des systèmes d'information 44

Thème 15 : Relation avec les fournisseurs 46

Thème 16 : Gestion des incidents liés à la sécurité de l'information 49

Thème 17 : Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité 52

Thème 18 : Conformité 54

LES COLLECTIVITES **62**

Présentation de l'échantillon 62

Thème 5 : Politique de sécurité de l'information (PSI) 63

Thème 6 : Organisation de la sécurité de l'information 65

Thème 7 : La sécurité des ressources humaines 70

Thème 8 : Gestion des actifs 72

Thème 9 : Contrôle d'accès 76

Thème 10 : Cryptographie 79

Thème 11 : Sécurité physique et environnementale 80

Thème 12 : Sécurité liée à l'exploitation 82

Thème 13 : Sécurité des communications 86
Thème 14 : Acquisition, développement et maintenance du SI 87
Thème 15 : Relations avec les fournisseurs 89
Thème 16 : Gestion des incidents SSI 92
Thème 17 : Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité 95
Thème 18 : Conformité 96

LES INTERNAUTES 103

Présentation de l'échantillon 103
Partie I – Identification et inventaire ordinateurs et smartphones 103
Partie II – Usages de l'internaute 105
Partie III – Perception de la menace et sensibilité de l'utilisateur aux risques et à la sécurité de l'information 109
Partie IV – Moyens et comportements vis-à-vis de la sécurité informatique 118

Liste des figures

Figure 1 – Évolution du budget sécurité selon les secteurs d'activité 23
Figure 2 – Principaux freins à la conduite des missions de sécurité de l'information 24
Figure 3 – Entreprises ayant formalisé leur politique de sécurité 24
Figure 4 – Part des entreprises ayant mis à jour leur politique depuis moins de trois ans 25
Figure 5 – Entités impliquées dans la politique de sécurité de l'information 26
Figure 6 – Bases sur lesquelles ont été mises en place les mesures de sécurité 27
Figure 7 – Identification et attribution de la fonction de RSSI 27
Figure 8 – Rattachement du RSSI (lorsque la fonction est attribuée) 28
Figure 9 – Nombre de personnes rattachées au RSSI (en ETP) 28
Figure 10 – Temps passé par le RSSI à ses différentes tâches/activités 29
Figure 11 – Présence d'une charte informatique par taille d'entreprise 30
Figure 12 – Principaux moyens utilisés pour sensibiliser les collaborateurs 31
Figure 13 – Inventaire des actifs 32
Figure 14 – Classification des actifs 32
Figure 15 – Nombre de niveaux de sensibilité utilisés pour la classification des actifs 33
Figure 16 – Inventaire des risques 33
Figure 17 – Méthodes d'analyse de risques utilisées 34
Figure 18 – Mise en place d'un plan de réduction des risques 35
Figure 19 – Acceptation des risques résiduels et validation du plan d'action 35
Figure 20 – Évolution de l'usage des technologies et des approches de sécurisation 37
Figure 21 – Synthèse de l'usage des technologies et des approches de sécurisation 37
Figure 22 – Procédures de gestion des accès 38
Figure 23 – Usage de la cryptographie par catégorie d'entreprise 39
Figure 24 – Usage de la cryptographie par type d'entreprise 39
Figure 25 – Dispositifs de sécurité physiques en entreprise pour la protection des salles machines 40
Figure 26 – Protection contre les menaces « logiques » 41
Figure 27 – Prise en compte de la veille technologique 42
Figure 28 – Délais de mise en œuvre des correctifs 43
Figure 29 – Position de la PSSI concernant la sécurité des communications 44
Figure 30 – Mise en place de cycles de développement sécurisé par secteurs d'activité 45
Figure 31 – Méthodes de développement sécurisé 46
Figure 32 – Mise en infogérance (totale ou partielle) du SI 47
Figure 33 – Implication des différentes entités à la PSSI 47
Figure 34 – Origine des incidents de sécurité de l'information 50
Figure 35 – Sujets identifiés dans le *Panorama de la cybercriminalité* 2020 vécus par les entreprises 51
Figure 36 – Financement des sinistres 52
Figure 37 – Domaine de couverture de la gestion de la continuité 52
Figure 38 – Pourcentage d'entreprises engagées dans une démarche de BIA formel 53

Figure 39 – Fréquence des tests 54
Figure 40 – Répartition du degré de conformité avec le RGPD 55
Figure 41 – Identification de la fonction de DPD/DPO 55
Figure 42 – Rattachement hiérarchique du DPD/DPO 56
Figure 43 – Responsabilité des formalités (en l'absence de DPO/DPD) 56
Figure 44 – Entreprises soumises à des lois/réglementations spécifiques pour la sécurité SI 57
Figure 45 – Entreprises soumises à des lois/réglementations spécifiques pour la sécurité SI (par secteur) . 58
Figure 46 – Fréquence des audits de sécurité au cours des deux dernières années 58
Figure 47 – Motivation des audits de sécurité 59
Figure 48 – Fonctions des personnes interrogées 63
Figure 49 – Collectivités ayant formalisé leur politique de sécurité 63
Figure 50 – Part des collectivités ayant mis à jour leur politique de sécurité il y a moins de trois ans 64
Figure 51 – Entités ayant été impliquées dans la politique de sécurité 64
Figure 52 – Bases sur lesquelles repose la mise en place de mesures de sécurité de l'information 65
Figure 53 – Normes citées par les collectivités ayant déclaré s'appuyer sur des référentiels pour la mise en place des mesures de sécurité 65
Figure 54 – Part des RSSI dédiés à la fonction 66
Figure 55 – Rattachement hiérarchique du RSSI/RSI 67
Figure 56 – Sentiment de dépendance à l'informatique des collectivités 68
Figure 57 – Évolution du budget sécurité par rapport à l'année précédente 69
Figure 58 – Évolution du budget en fonction des postes (comparaison sur les trois études) 70
Figure 59 – Existence d'une charte d'usage du SI 70
Figure 60 – Destination de la charte d'usage du système d'information 71
Figure 61 – Les moyens de sensibilisation 71
Figure 62 – Procédure de suppression des droits d'accès et de restitution du matériel 72
Figure 63 – Inventaire des actifs 72
Figure 64– Classification des actifs 73
Figure 65 – Nombre de niveaux de classification de la sensibilité des actifs 73
Figure 66 – Inventaire des risques 74
Figure 1 – Part des collectivités ayant effectué, après leur inventaire, une analyse formelle des risques 74
Figure 68 – Méthodes d'analyse des risques utilisées 75
Figure 69 – Mise en place de plans de réduction des risques 75
Figure 70 – Acceptation des risques résiduels et validation du plan d'action 76
Figure 71 – Technologie/approche de sécurisation par type d'authentification 77
Figure 72 – Authentification – Focus sur les approches technologiques 77
Figure 73 – Authentification – Focus sur les modèles par habilitations/droits 78
Figure 74 – Procédure formelle de création, modification, et suppression de comptes utilisateurs 78
Figure 75 – Procédure spécifique pour les administrateurs ? 78
Figure 76 – Règles de constitution et de péremption des mots de passe 79
Figure 77 – Usage de la cryptographie par type de collectivité 79
Figure 78 – Collectivités déclarant protéger leurs données sur support physique 80

Figure 79 – Sécurisation de l'accès aux salles machines 81
Figure 80 – Contrôle d'accès et détection 81
Figure 81 – Types de contrôle d'accès 81
Figure 82 – Détection incendie/inondation 82
Figure 83 – Les outils traditionnels quasi généralisés désormais… 83
Figure 84 – Une plus grande diversité d'armes de sécurisation… 83
Figure 85 – Des veilles permanentes généralisées… 85
Figure 86 – La formalisation des procédures progresse péniblement… 85
Figure 87 – Position de la PSSI concernant la sécurité des communications 87
Figure 88 – Mise en place de cycles de développement sécurisé 88
Figure 89 – Existence d'un référent sécurité 88
Figure 90 – Réalisation de contrôle de code 89
Figure 91 – Collectivités ayant placé tout ou partie de leur système d'information en infogérance 90
Figure 92 – Existence d'audit sur les infogérances 90
Figure 93 – Recours des directions métiers et des utilisateurs à des services en cloud 91
Figure 94 – Encadrement du recours à des services en cloud 91
Figure 95 – Type d'événements, d'incidents 92
Figure 96 – Cellule de collecte et de traitement des incidents de sécurité de l'information 93
Figure 97 – Traitement des incidents par type de système d'information 94
Figure 98 – Durée maximale d'interruption de service 94
Figure 99 – Composition de la gestion de crise 95
Figure 100 – Pourcentage d'entreprises engagées dans une démarche de BIA formel 95
Figure 101 – Fréquence des tests 96
Figure 102 – Répartition du degré de conformité avec le RGPD 97
Figure 103 – Identification de la fonction de DPD/DPO 97
Figure 104 – Rattachement hiérarchique du DPD/DPO 98
Figure 105 – Niveau d'identification des SI concernés par le RGS 98
Figure 106 – Fréquence des audits de sécurité au cours des deux dernières années 99
Figure 107 – Types d'audits et de contrôles de sécurité du SI 100
Figure 108 – Motivations principales des audits 100
Figure 109 – Équipements des internautes en 2020 103
Figure 110 – Fréquence de connexion en mobilité avec son smartphone 104
Figure 111 – Les objets connectés chez les internautes en 2020 104
Figure 112 – Usages du Wi-Fi à domicile depuis 2010 105
Figure 113 – Stockage d'informations personnelles 106
Figure 114 – Usages de l'Internet en 2020 107
Figure 115 – Conditions exigées pour accepter un paiement en ligne 108
Figure 116 – Menace sur la vie privée par Internet : les convaincus 109
Figure 117 – Menace sur la vie privée par Internet : une prise de conscience qui se fait attendre 110
Figure 118 – Perception de la menace selon les équipements 111
Figure 119 – Perception de la menace sur les objets connectés 112

Figure 120 – Perception de la sécurisation des paiements en ligne 113
Figure 121 – Perception des risques liés au cloud 114
Figure 122 – Un sentiment de sécurité 114
Figure 123 – Classement des menaces 115
Figure 124 – Les facteurs qui participent à la perception de la menace 116
Figure 125 – Nature des incidents sur ordinateurs et tablettes/mobiles 117
Figure 126 – Nature et réponse à incident sur le cloud 118
Figure 127 – Moyen de protection 119
Figure 128 – Comportement et pratiques pour sécuriser les équipements et usages 120
Figure 129 – Exercice de leurs droits par les internautes 121
Figure 130 – Moyen de résolution des dommages pour les ordinateurs et mobiles/tablettes 122
Figure 131 – Moyen de résolution des dommages dans le cloud 122

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.

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 !

Le budget sécurité de l'information est-il en augmentation par rapport à l'année précédente ?

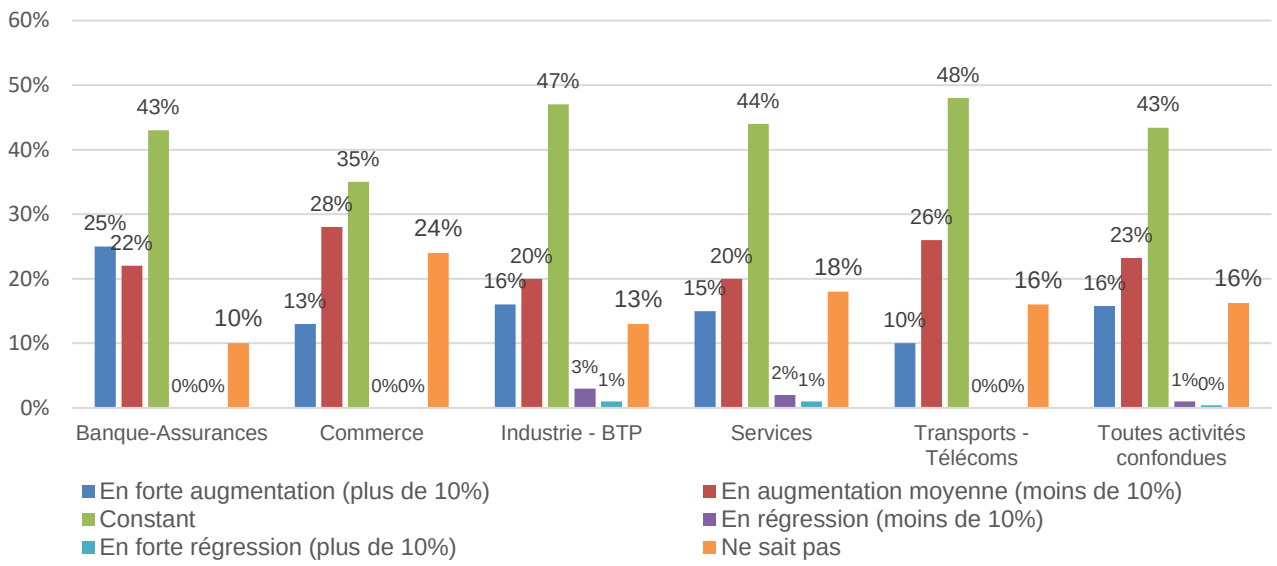


Figure 1 – Évolution du budget sécurité selon les secteurs d'activité

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 ?

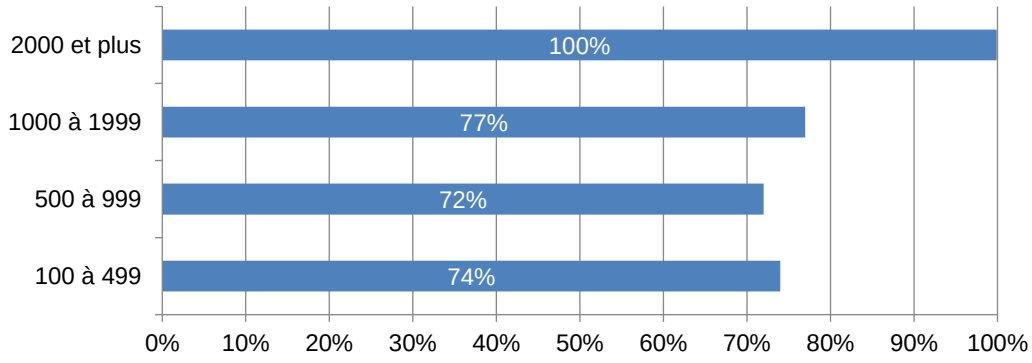


Figure 3 – Entreprises ayant formalisé leur politique de sécurité

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

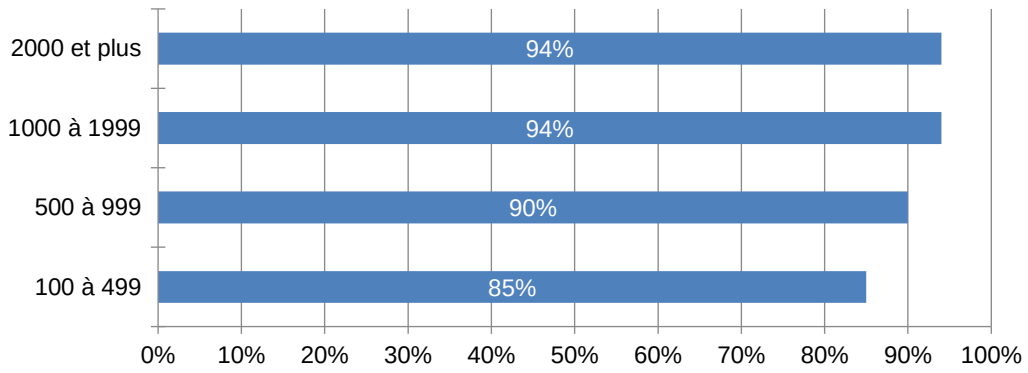


Figure 4 – Part des entreprises ayant mis à jour leur politique depuis moins de trois ans

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 %).

Quelles sont les entités de votre entreprise qui se sont impliquées dans l'élaboration de la PSSI ?

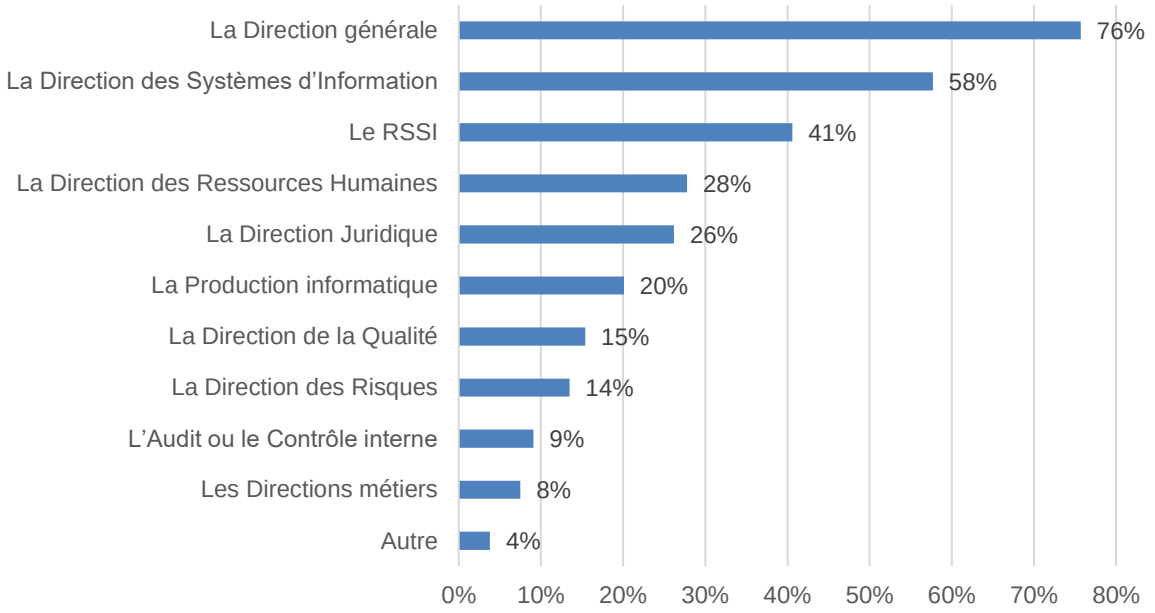


Figure 5 – Entités impliquées dans la politique de sécurité de l'information

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 %.

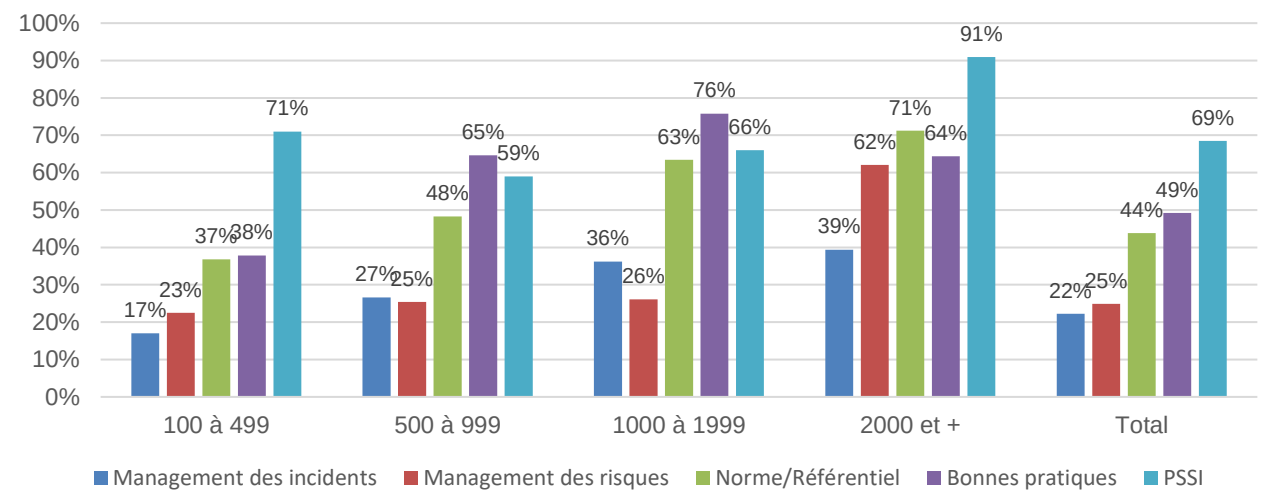


Figure 6 – Bases sur lesquelles ont été mises en place les mesures de sécurité

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.

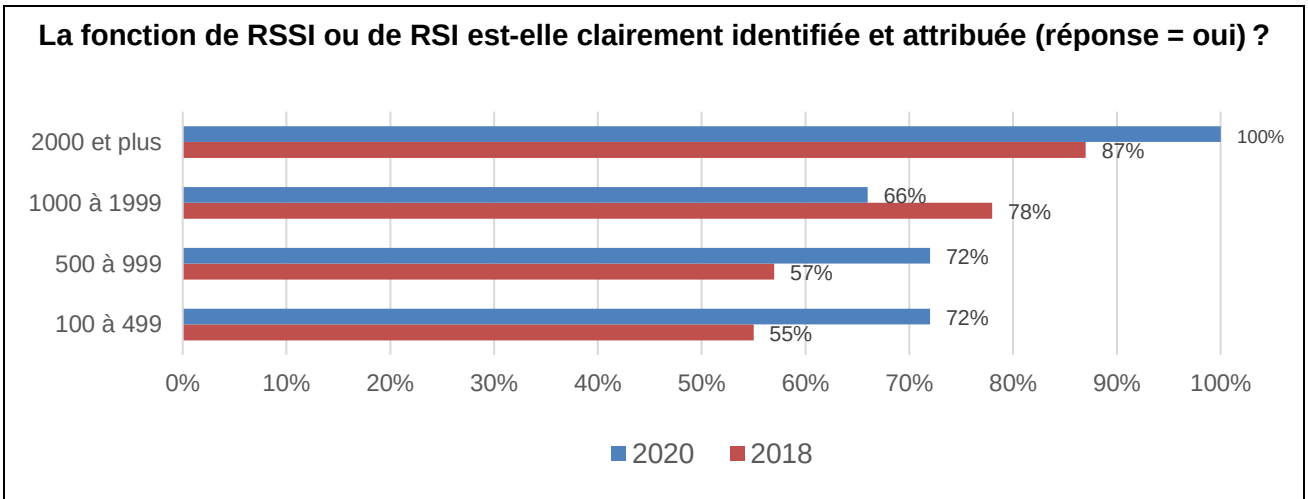


Figure 7 – Identification et attribution de la fonction de RSSI

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.

Quel est le rattachement hiérarchique du RSSI/RSI au sein de votre entreprise ?

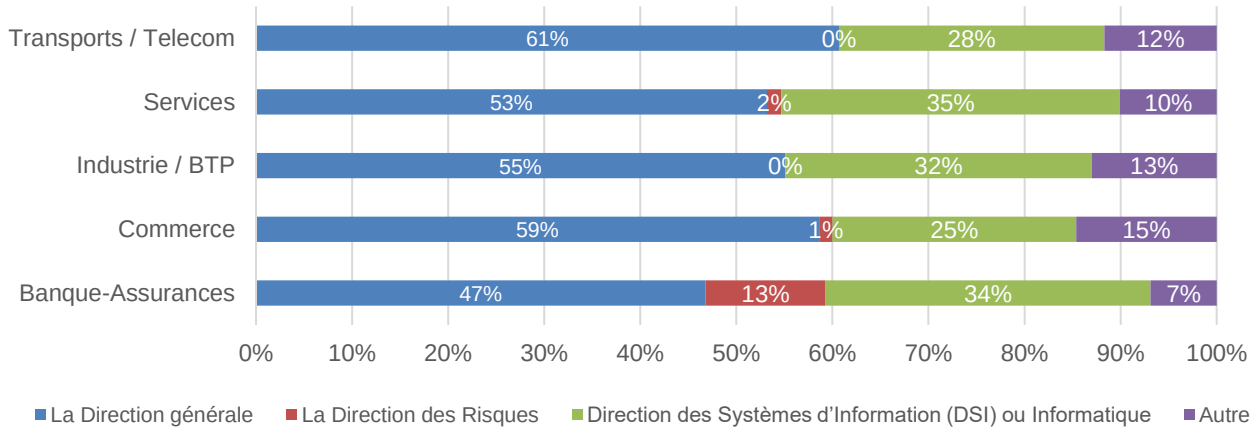
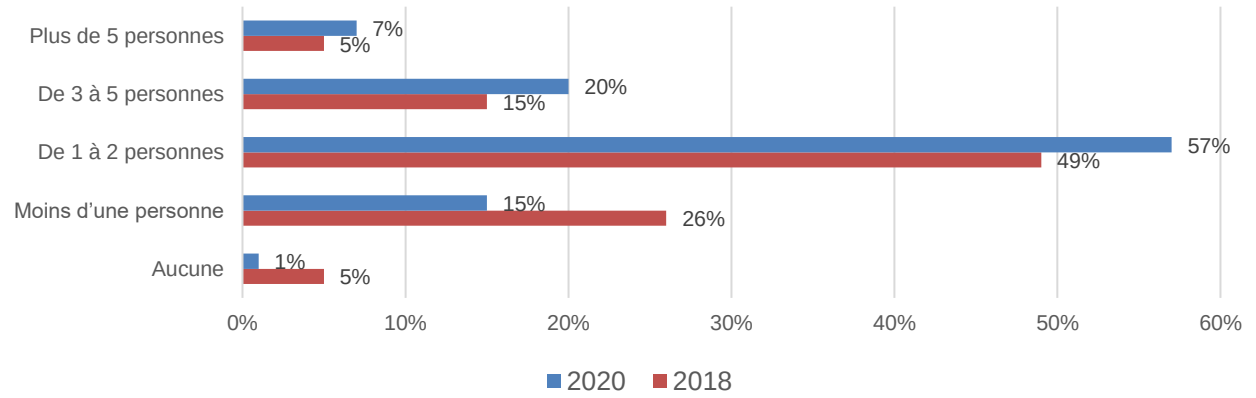


Figure 8 – Rattachement du RSSI (lorsque la fonction est attribuée)

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).

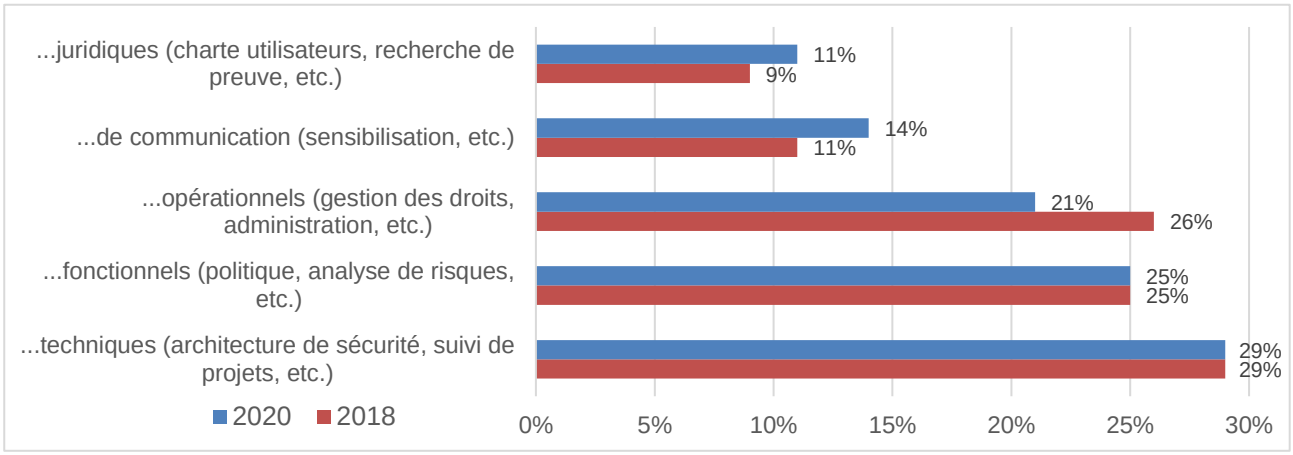


Figure 10 – Temps passé par le RSSI à ses différentes tâches/activités

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.

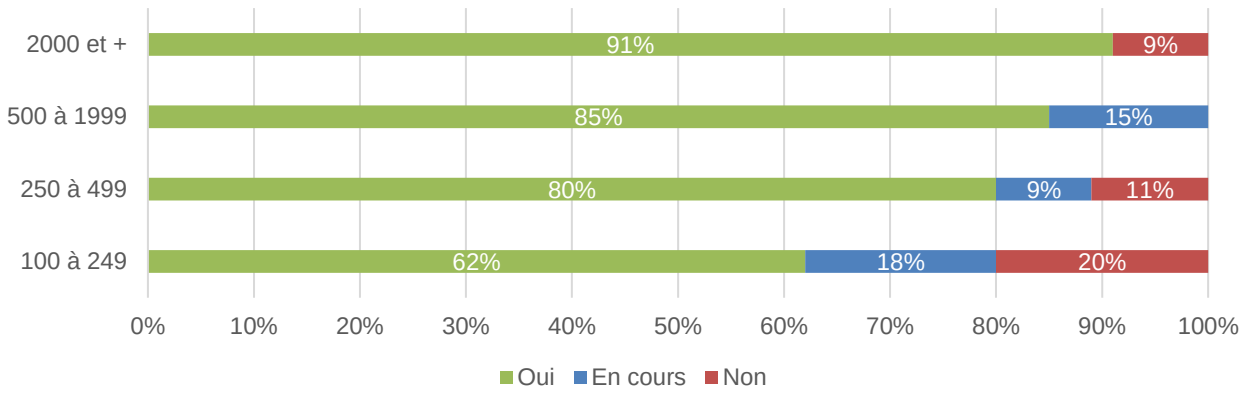


Figure 11 – Présence d'une charte informatique par taille d'entreprise

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.

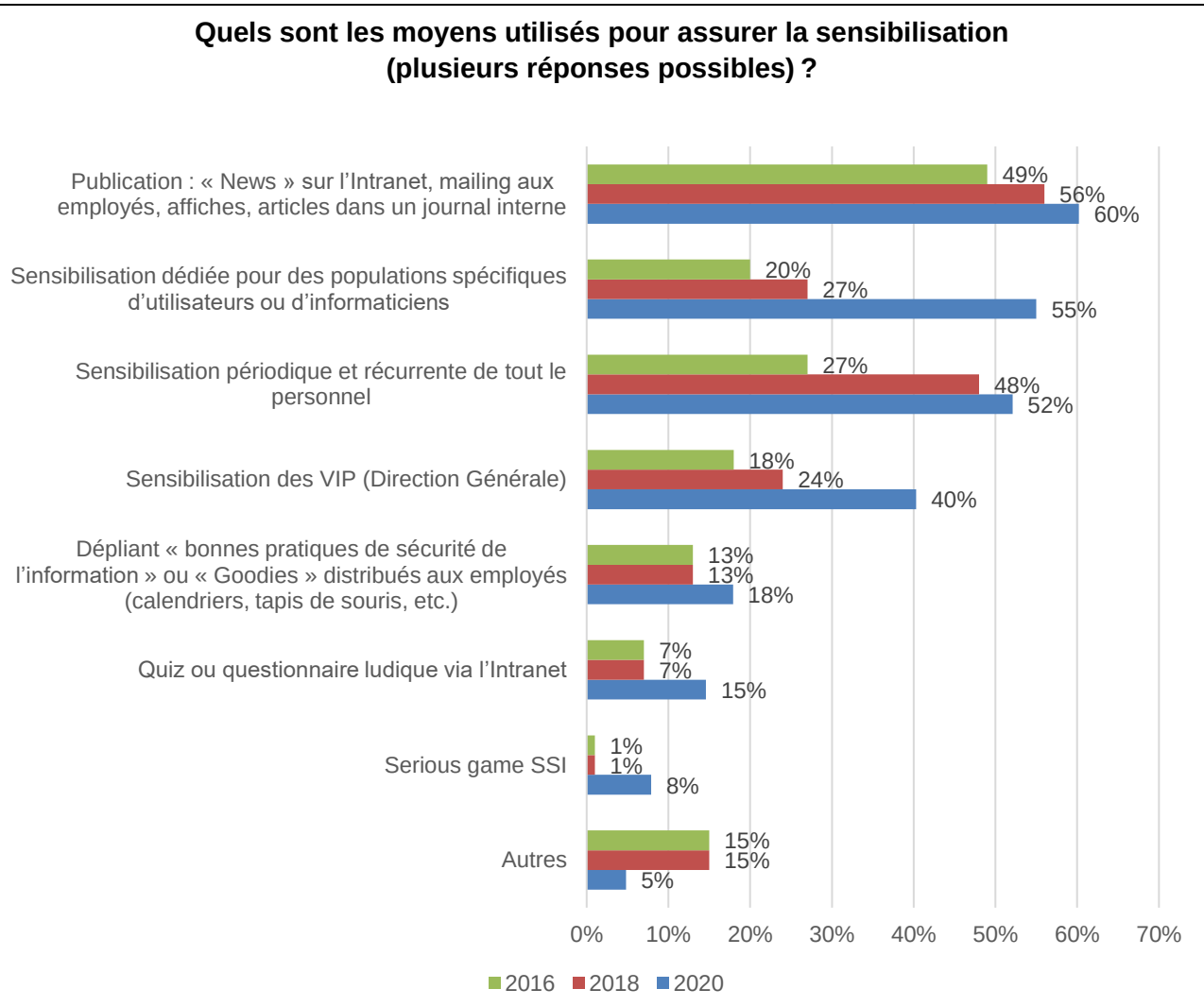


Figure 12 – Principaux moyens utilisés pour sensibiliser les collaborateurs

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.

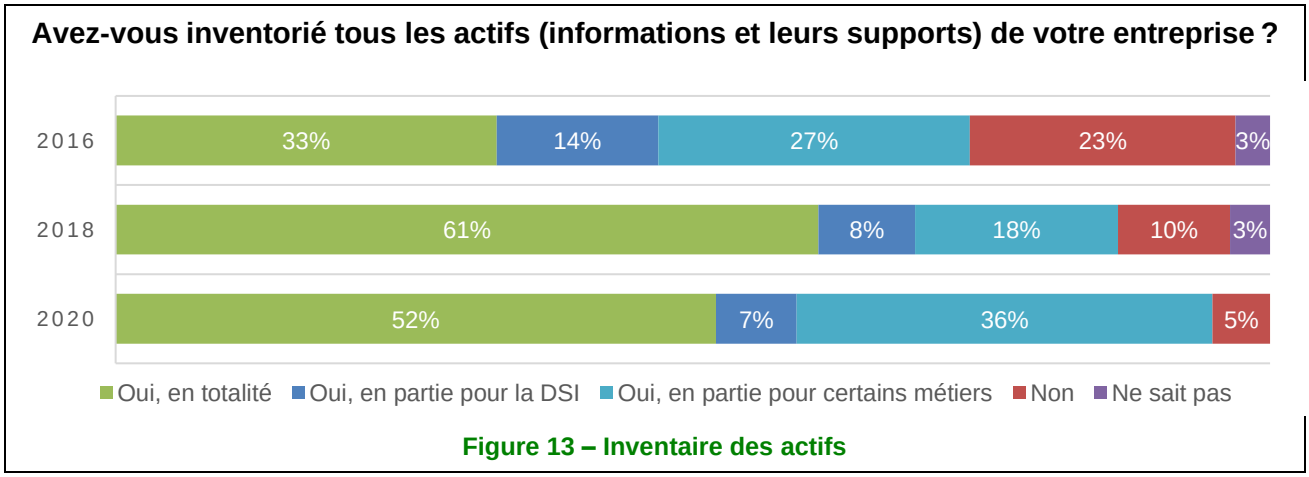


Figure 13 – Inventaire des actifs

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.

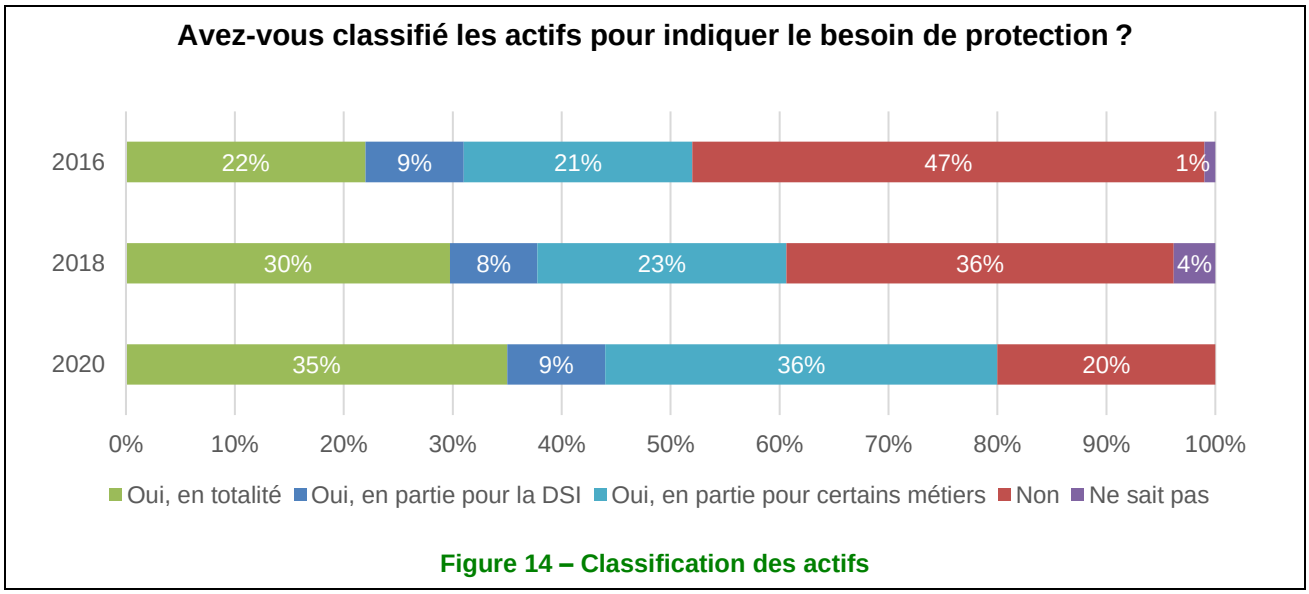


Figure 14 – Classification des actifs

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 ?

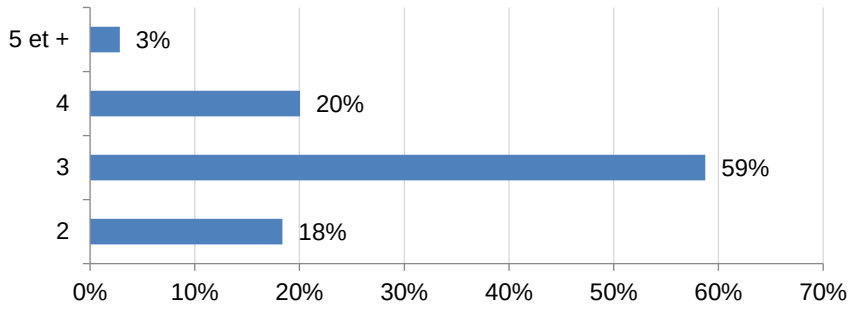


Figure 15 – Nombre de niveaux de sensibilité utilisés pour la classification des actifs

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 ?

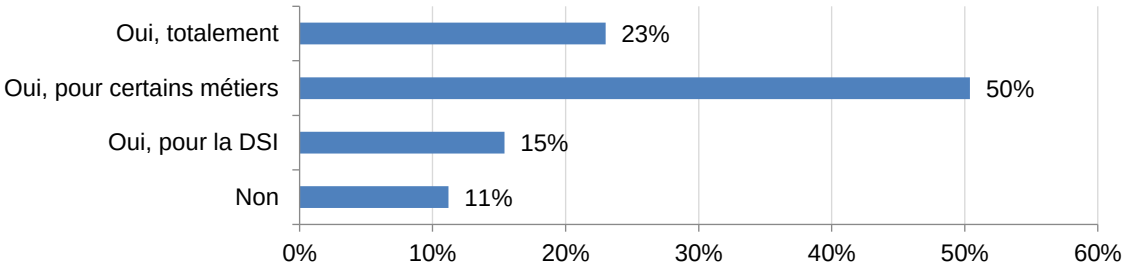


Figure 16 – Inventaire des risques

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 %

[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.

Inventaire partiel, pour la DSI	30 %
Inventaire partiel, pour certains métiers	38 %

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

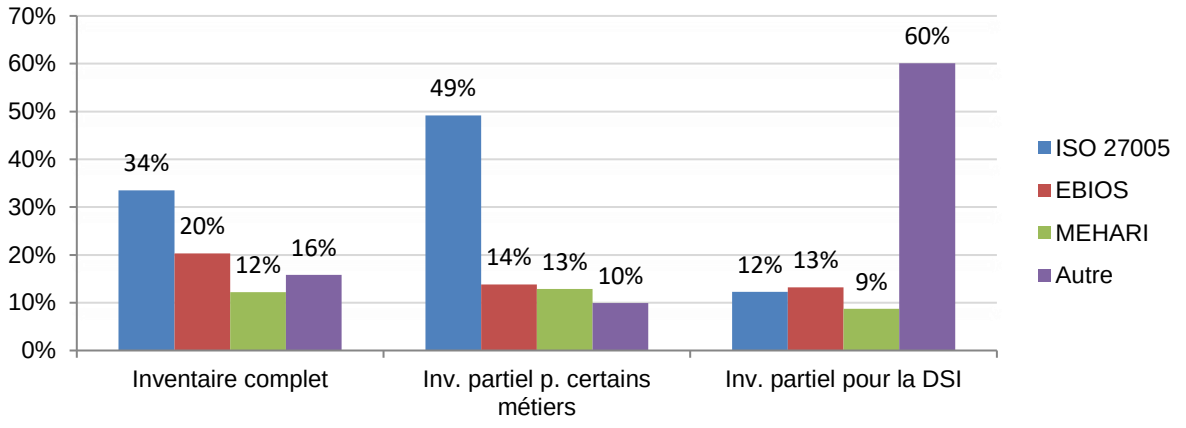


Figure 17 – Méthodes d'analyse de risques utilisées

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.

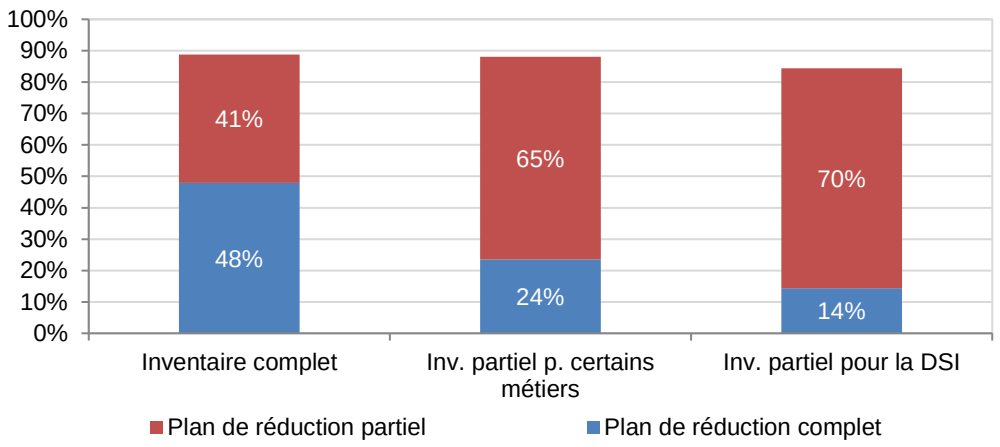


Figure 18 – Mise en place d'un plan de réduction des risques

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

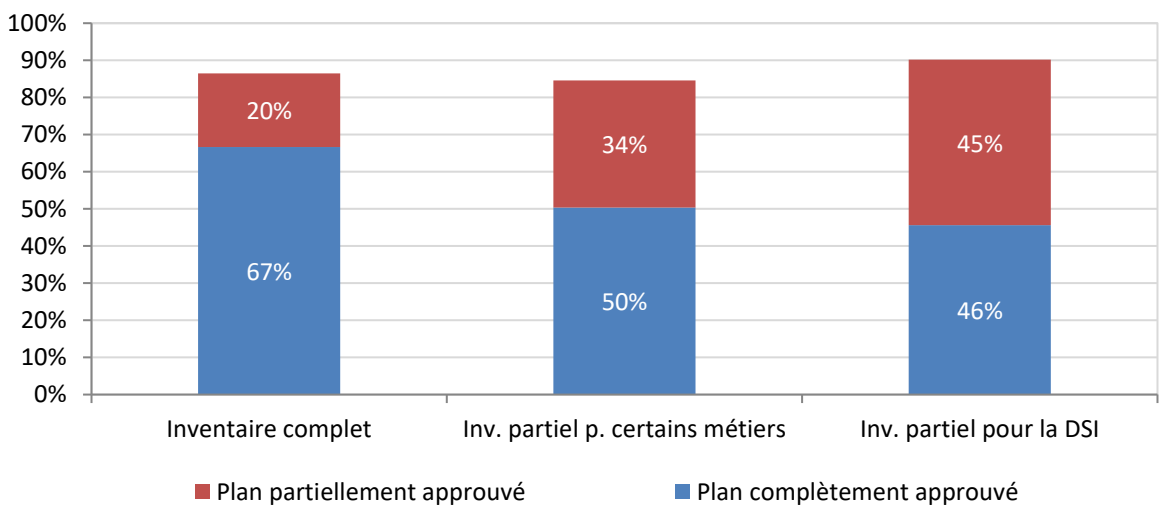


Figure 19 – Acceptation des risques résiduels et validation du plan d'action

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 Governance* – 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) ?

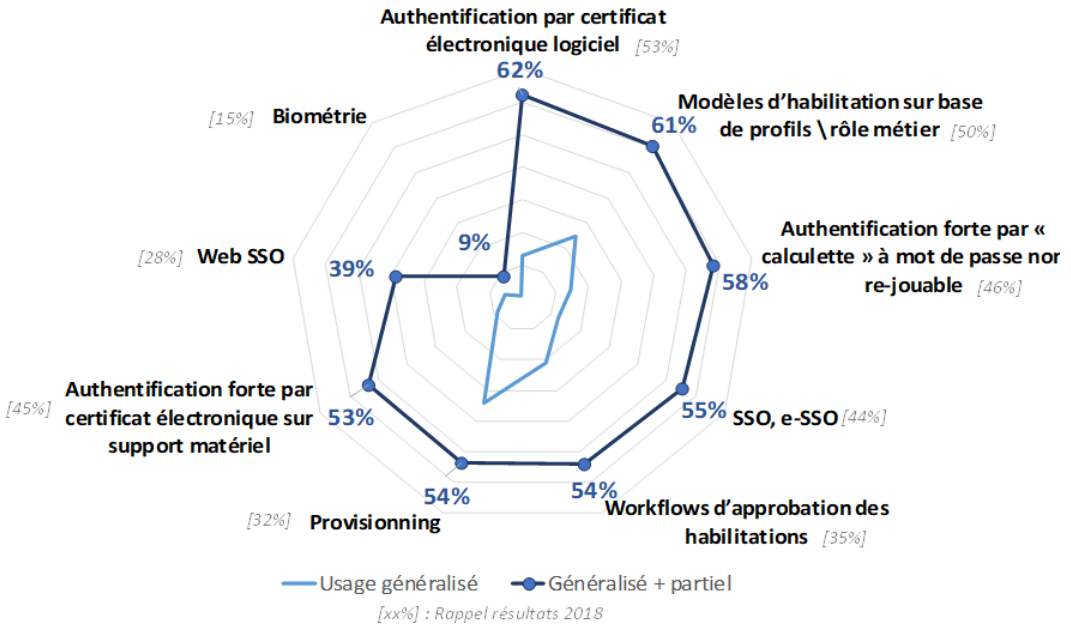


Figure 20 – Évolution de l'usage des technologies et des approches de sécurisation

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 %.

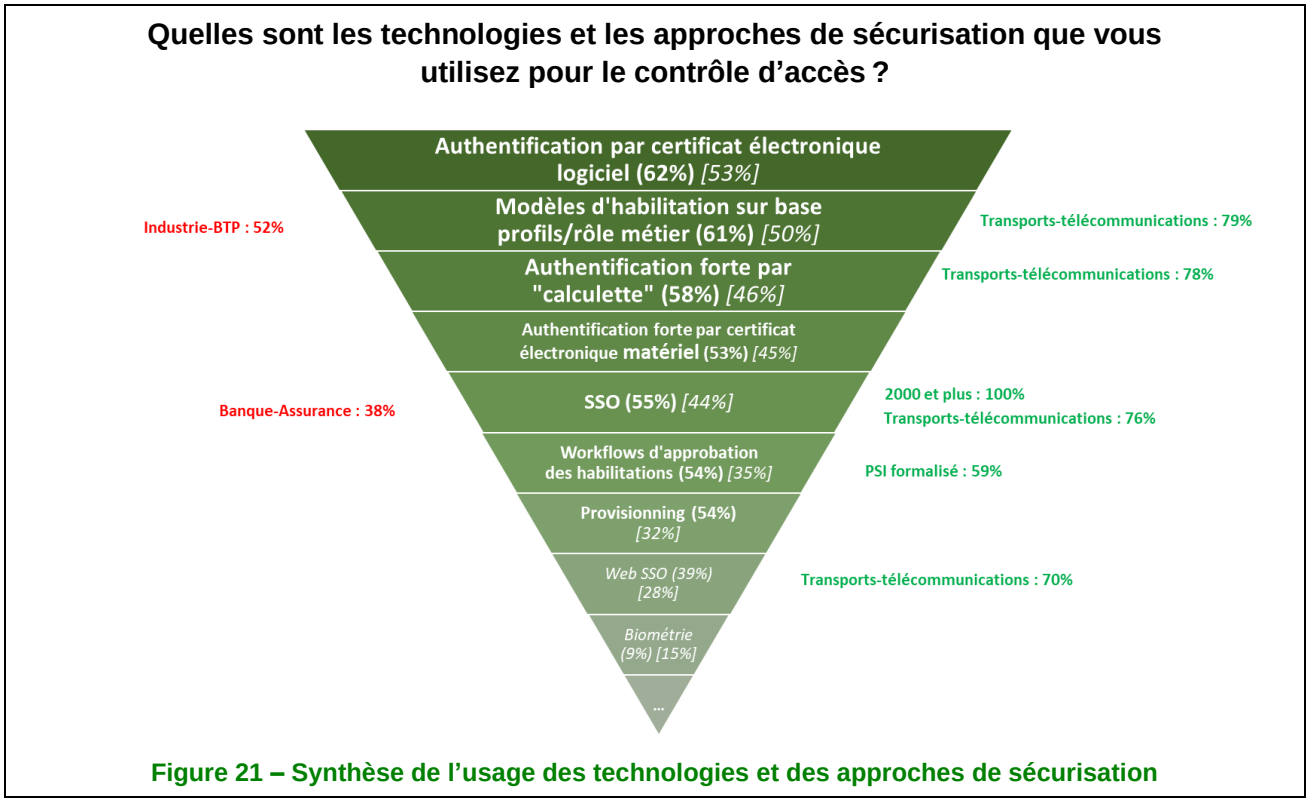


Figure 21 – Synthèse de l'usage des technologies et des approches de sécurisation

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) ?

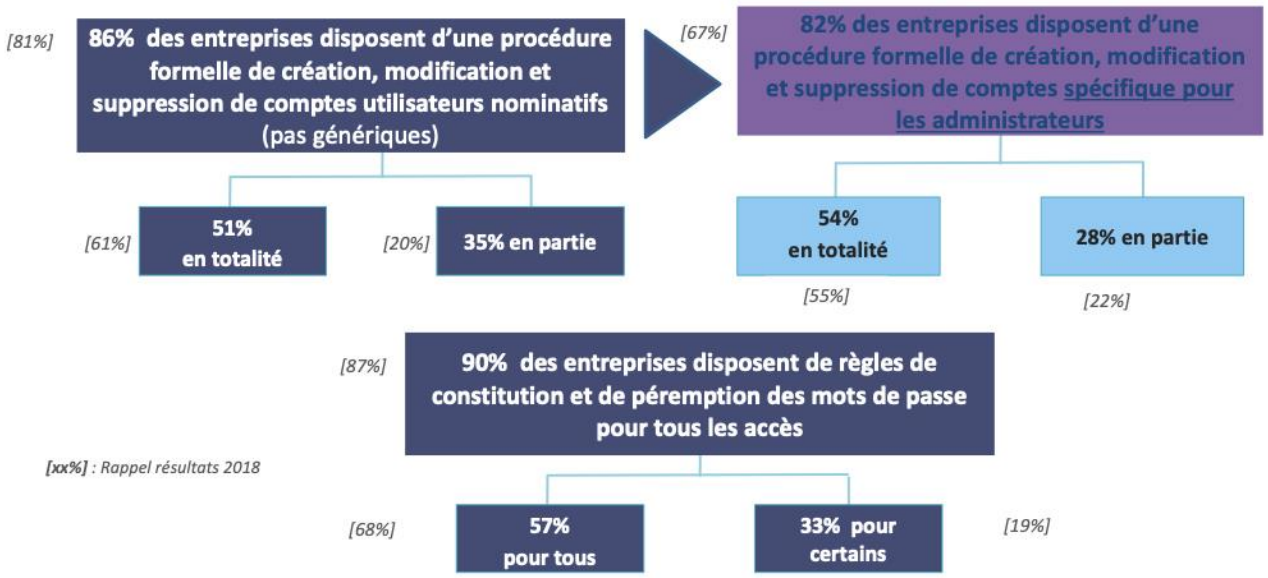


Figure 22 – Procédures de gestion des accès

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.

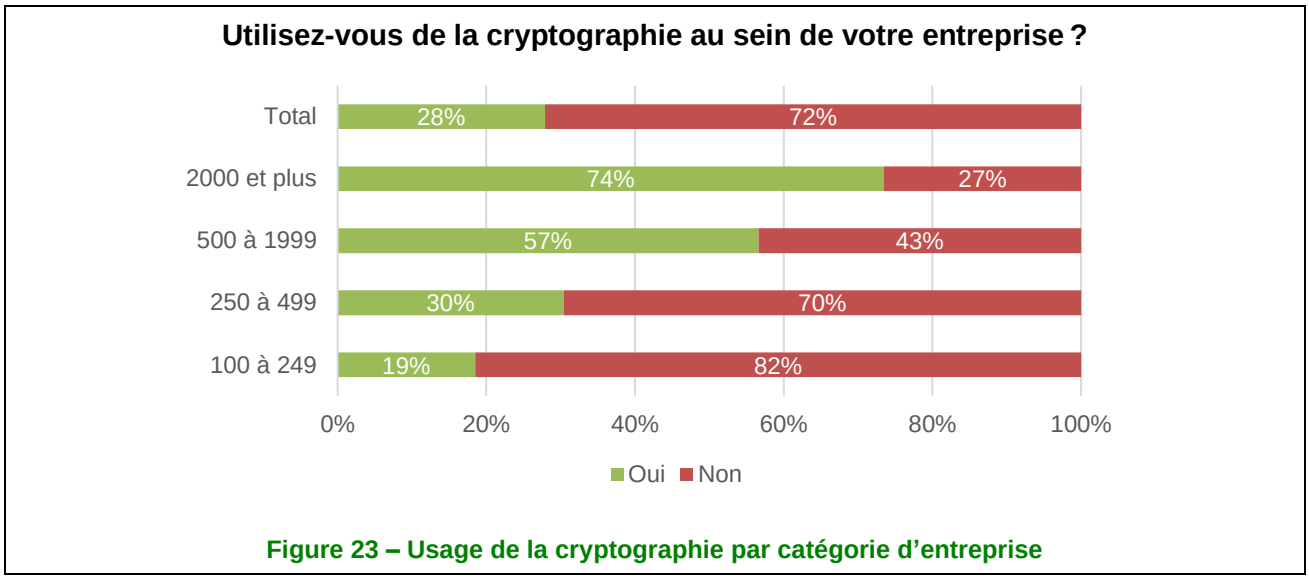


Figure 23 – Usage de la cryptographie par catégorie d'entreprise

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.

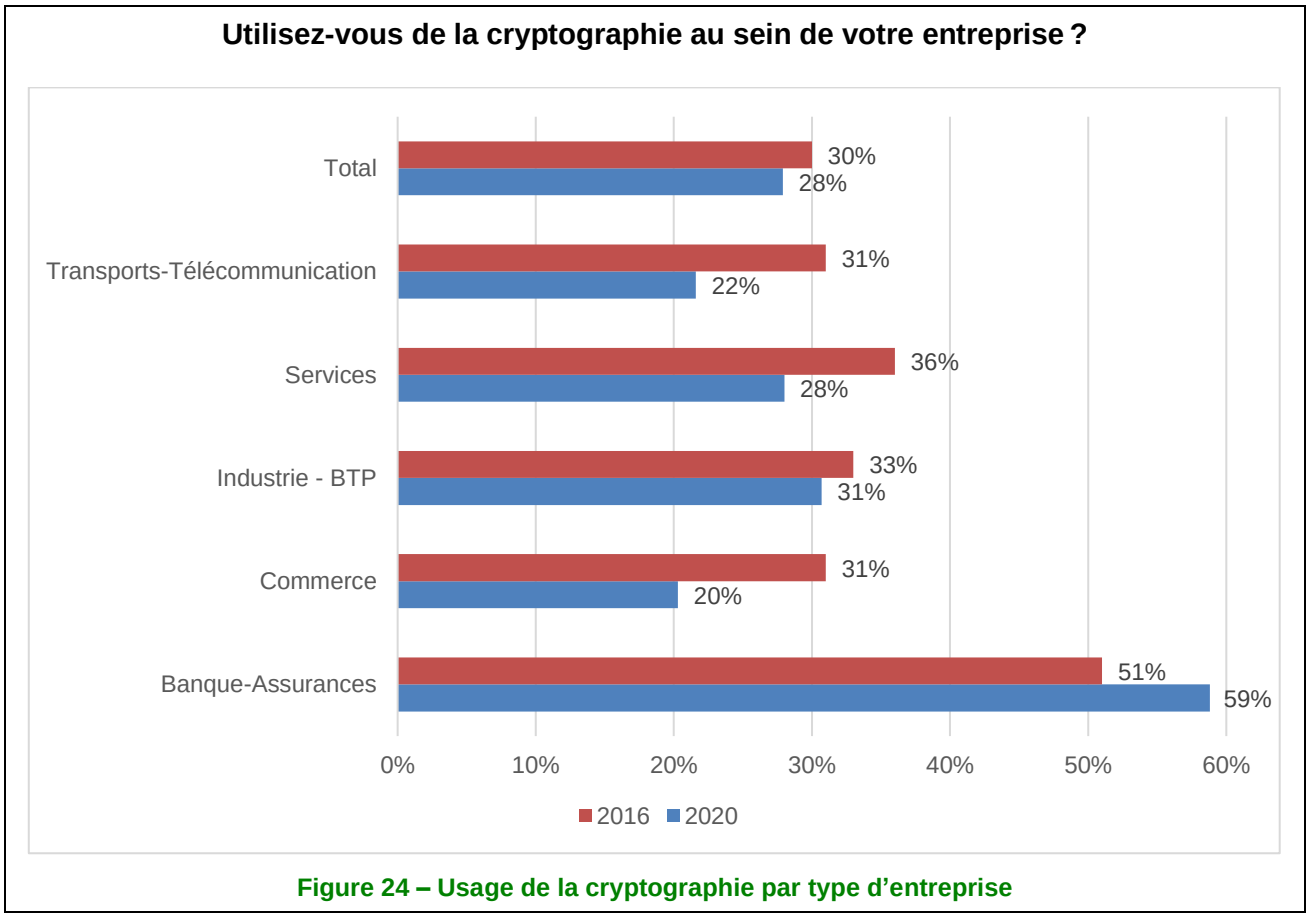


Figure 24 – Usage de la cryptographie par type d'entreprise

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 ?

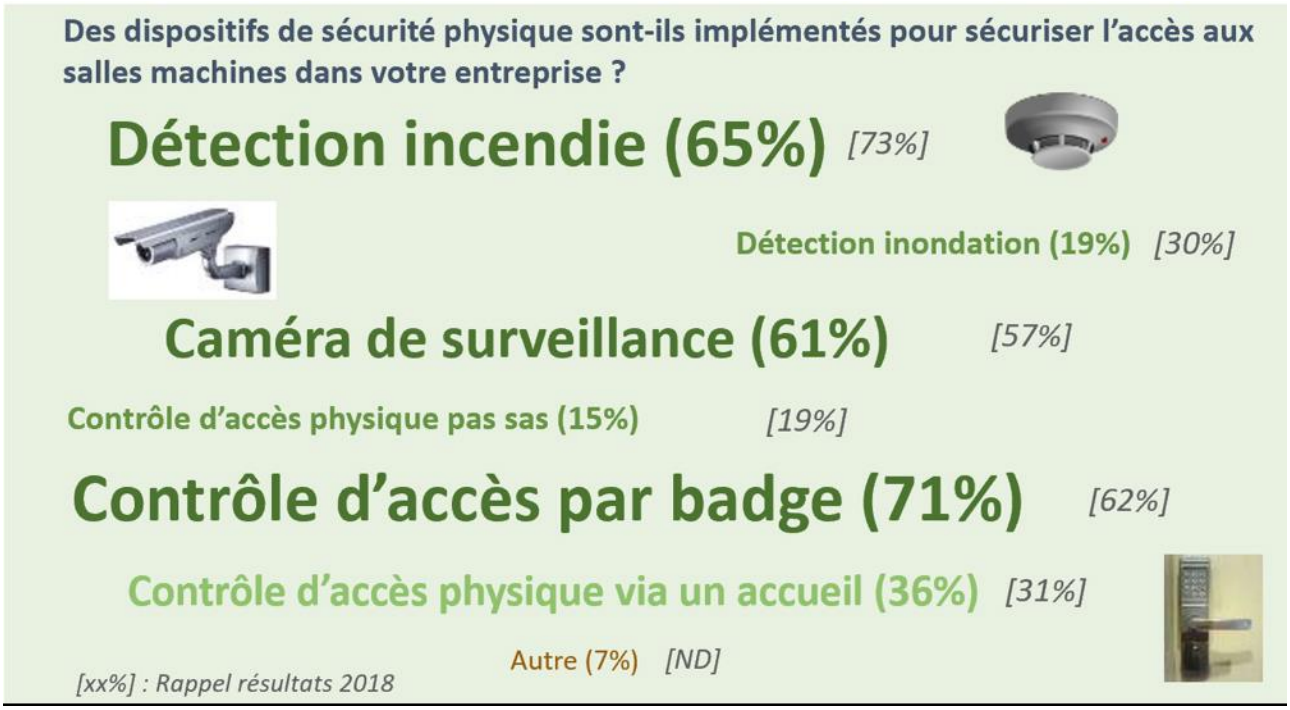


Figure 25 – Dispositifs de sécurité physiques en entreprise pour la protection des salles machines

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.

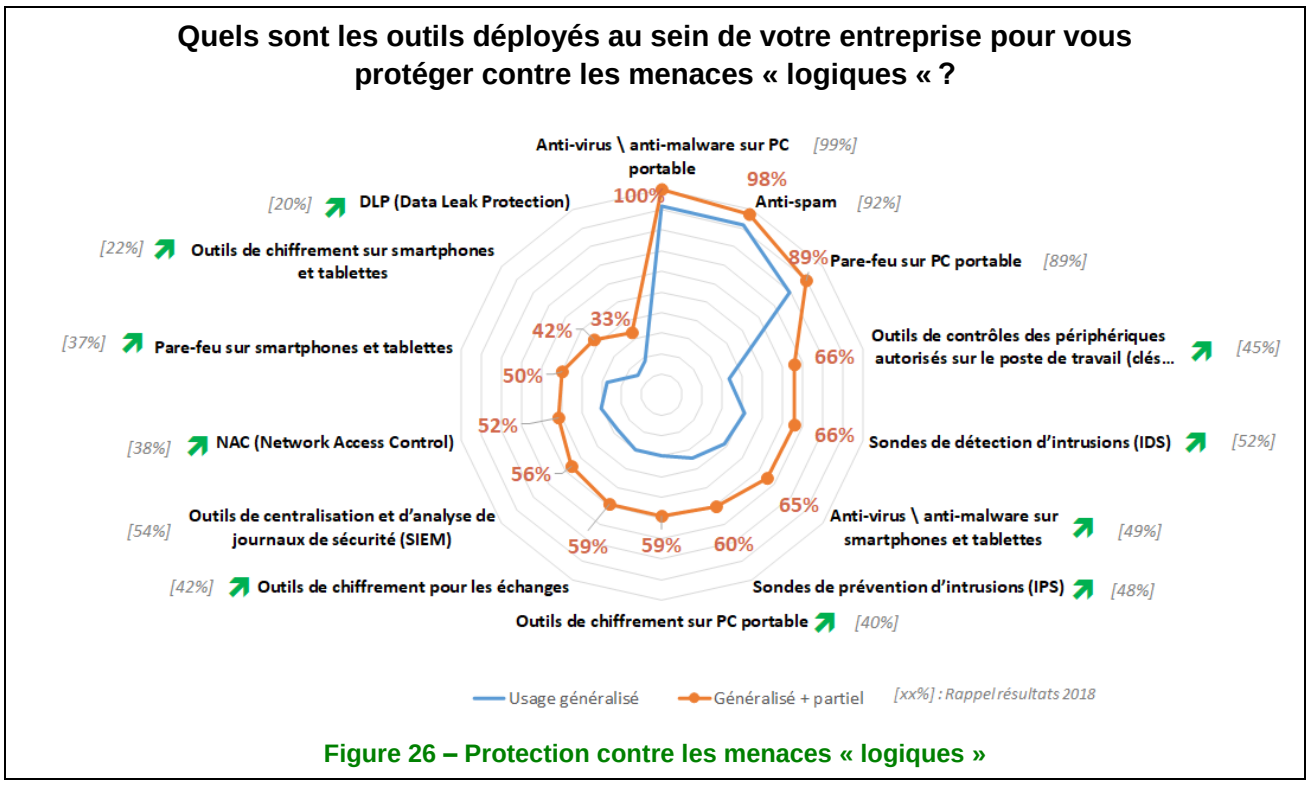


Figure 26 – Protection contre les menaces « logiques »

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).

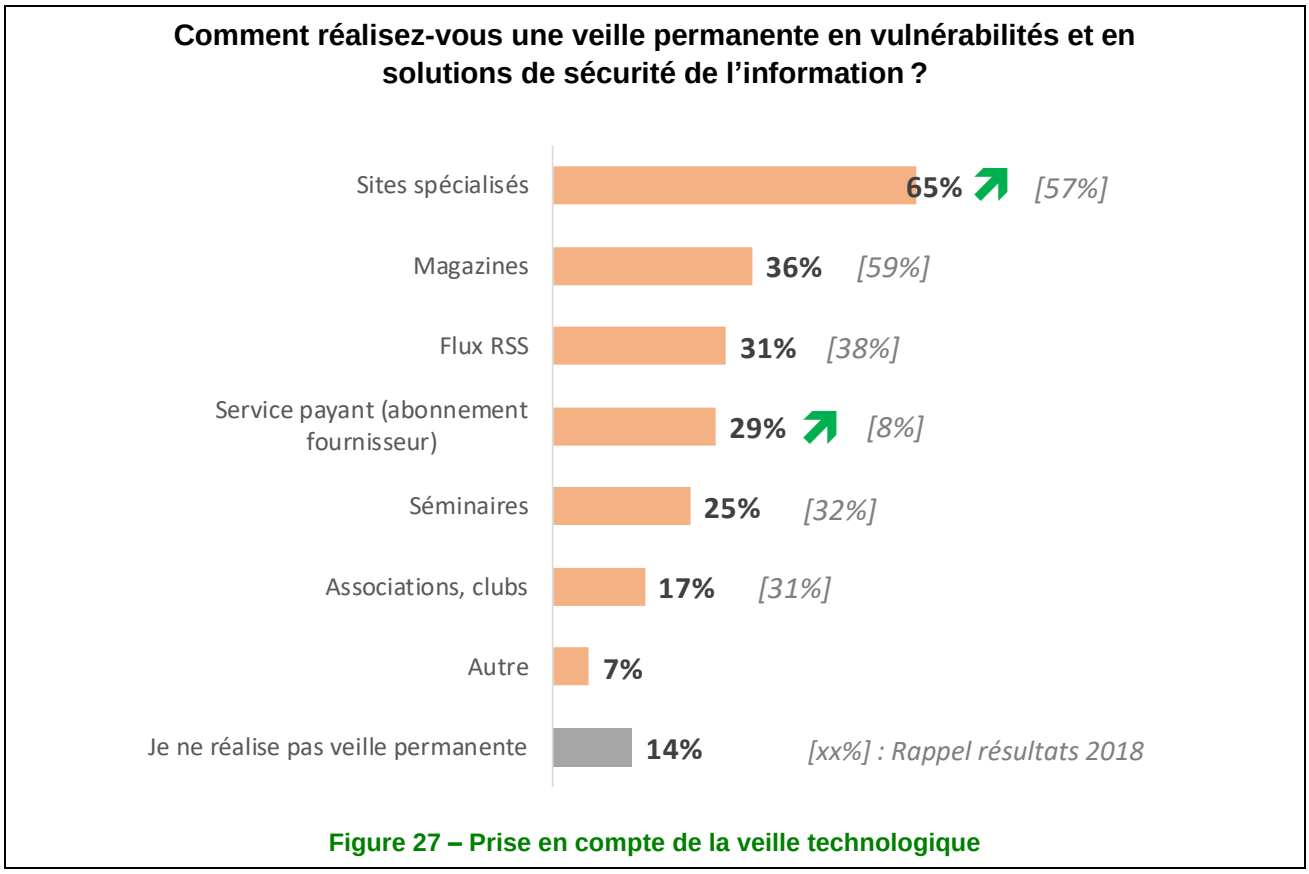


Figure 27 – Prise en compte de la veille technologique

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).

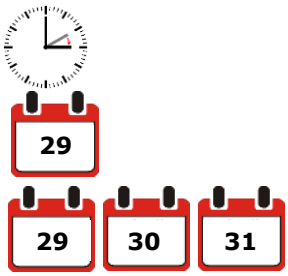
Faire de la veille, c'est bien… Déployer les correctifs, c'est mieux !

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 ?

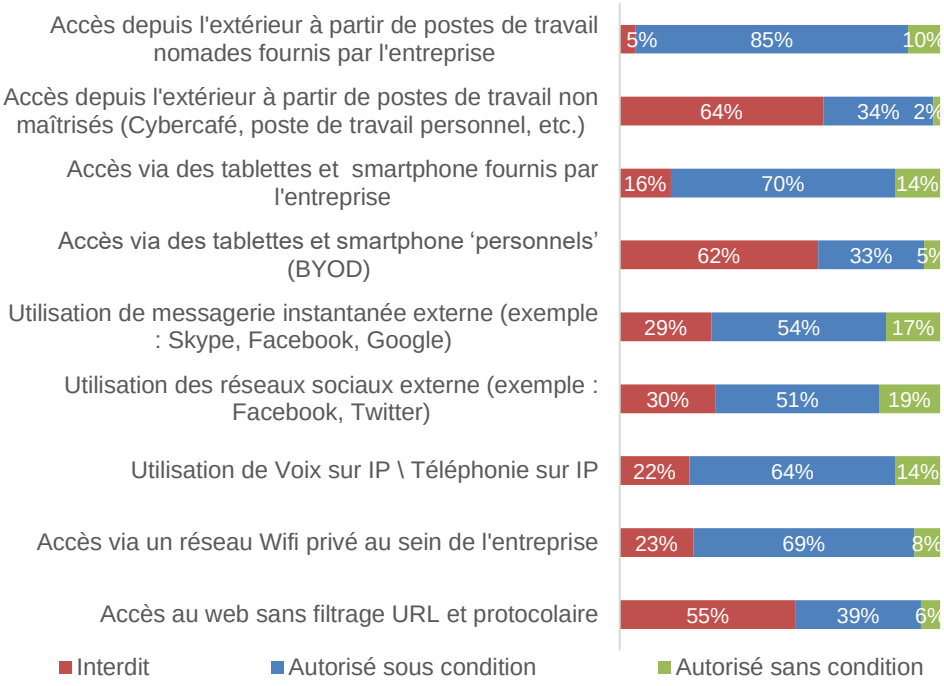


Figure 29 – Position de la PSSI concernant la sécurité des communications

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.

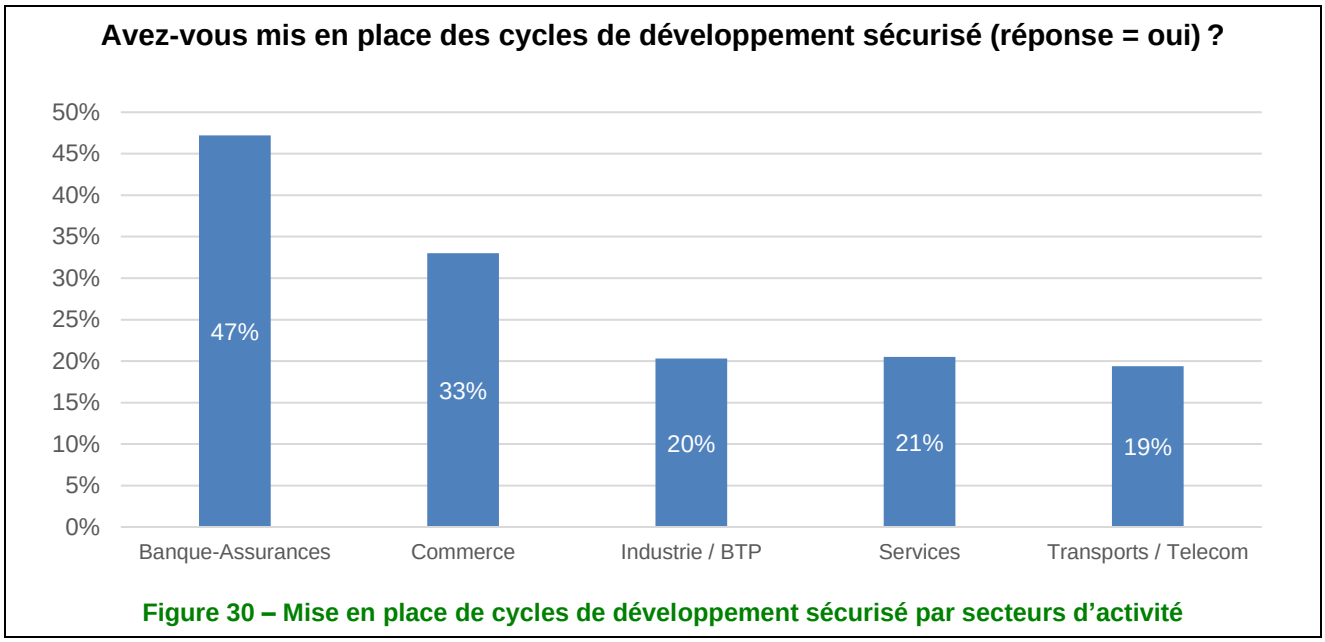


Figure 30 – Mise en place de cycles de développement sécurisé par secteurs d'activité

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.

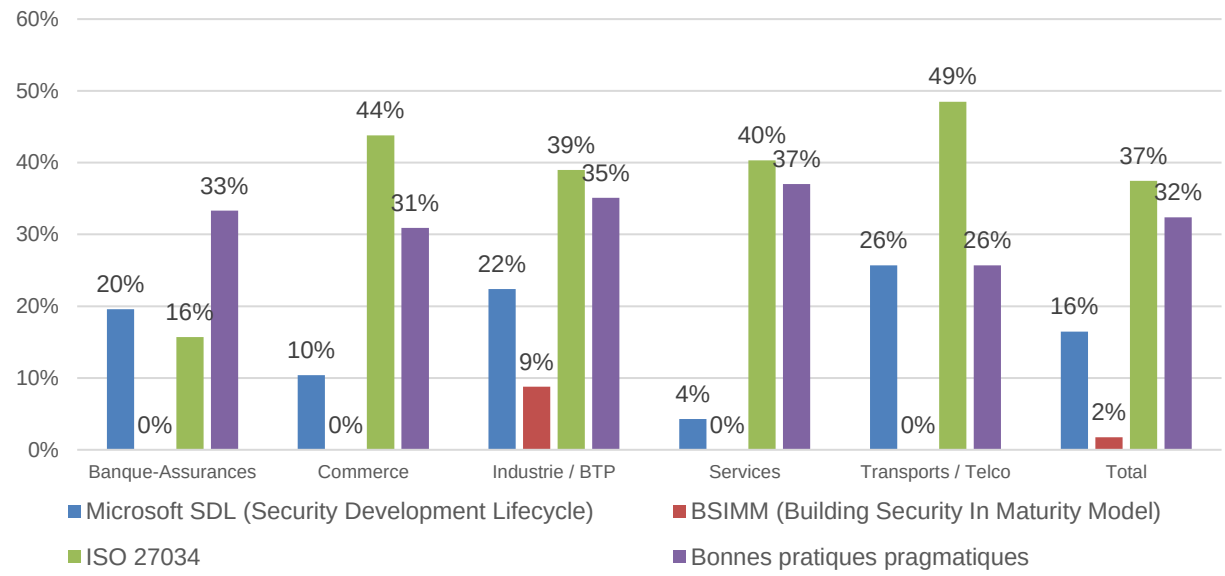


Figure 31 – Méthodes de développement sécurisé

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.

Avez-vous placé tout ou partie de votre SI sous contrat d'infogérance ?

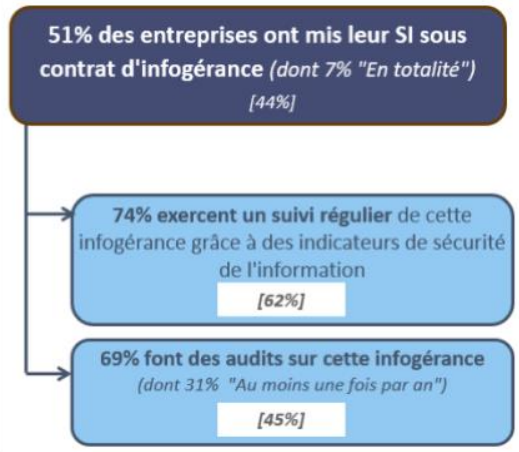


Figure 32 – Mise en infogérance (totale ou partielle) du SI

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 ?

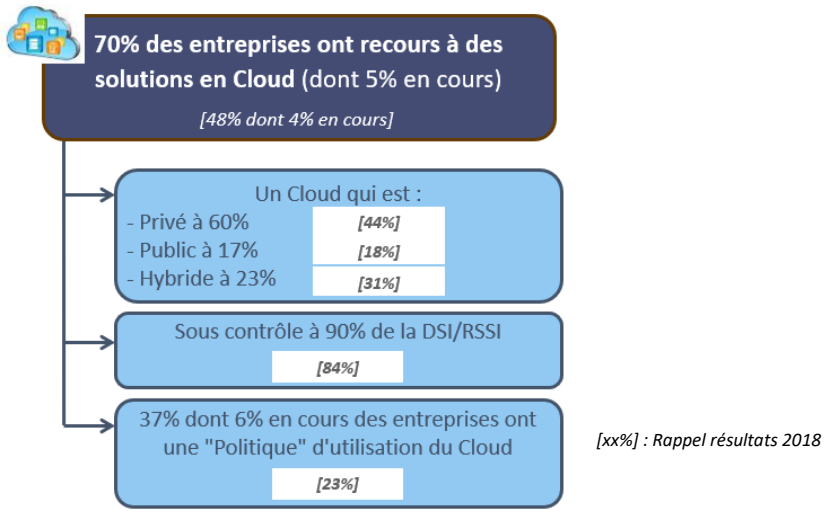


Figure 33 – Implication des différentes entités à la PSSI

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… ?

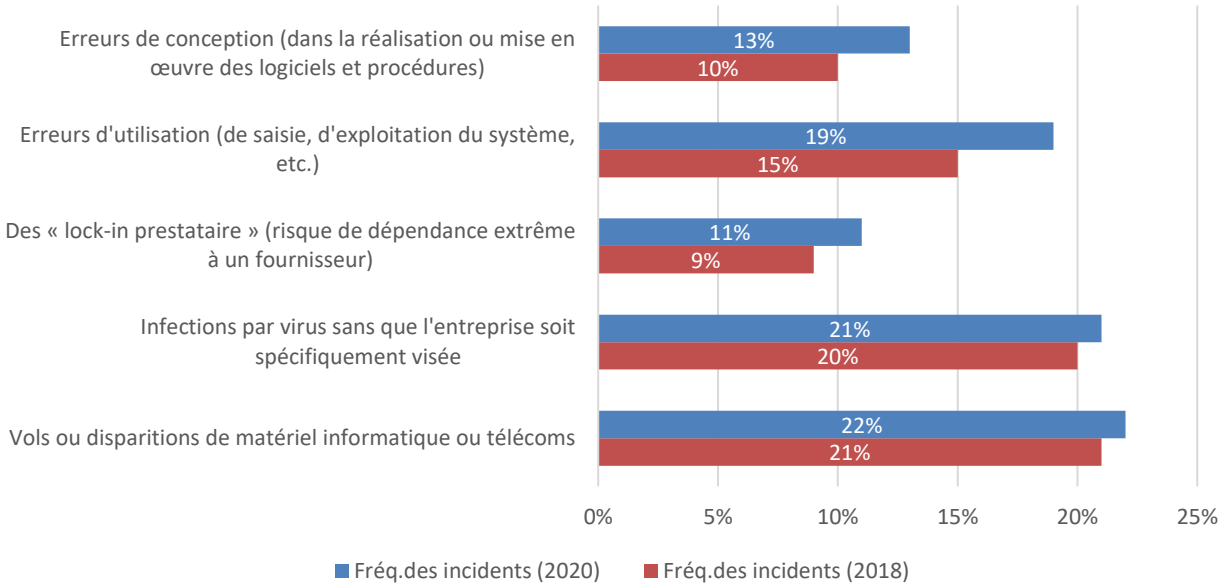


Figure 34 – Origine des incidents de sécurité de l'information

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 ?

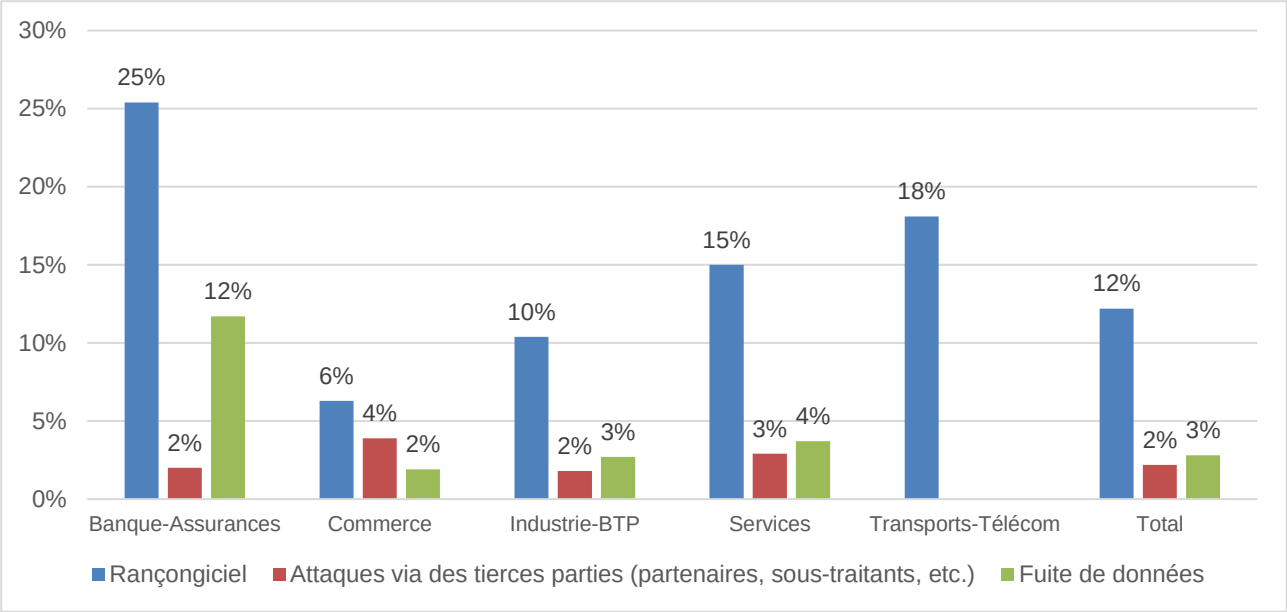


Figure 35 – Sujets identifiés dans le *Panorama de la cybercriminalité* 2020 vécus par les entreprises

« 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 ?

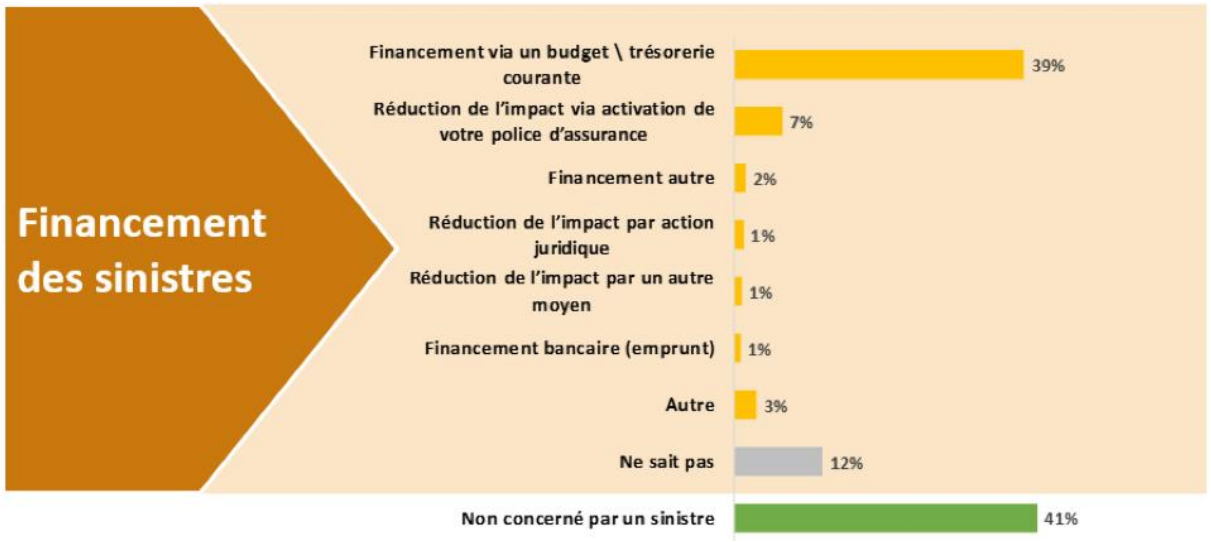


Figure 36 – Financement des sinistres

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) ?

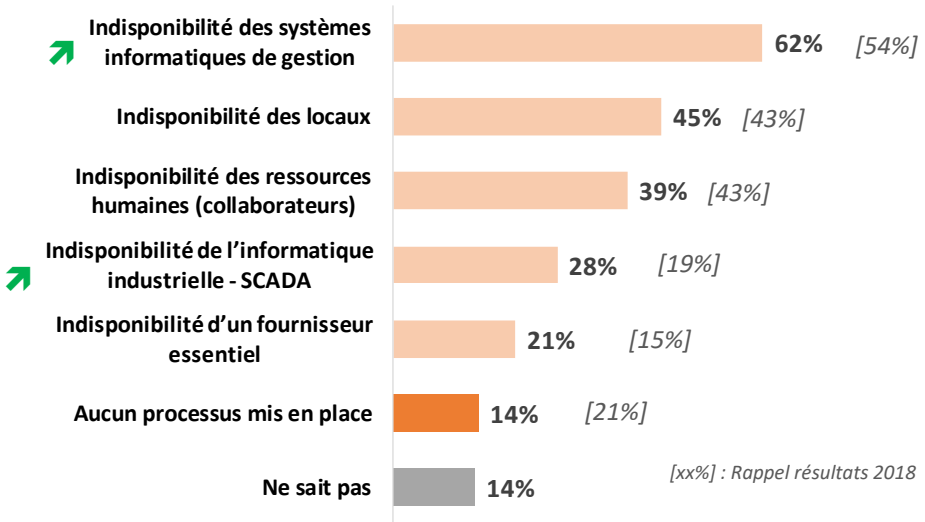
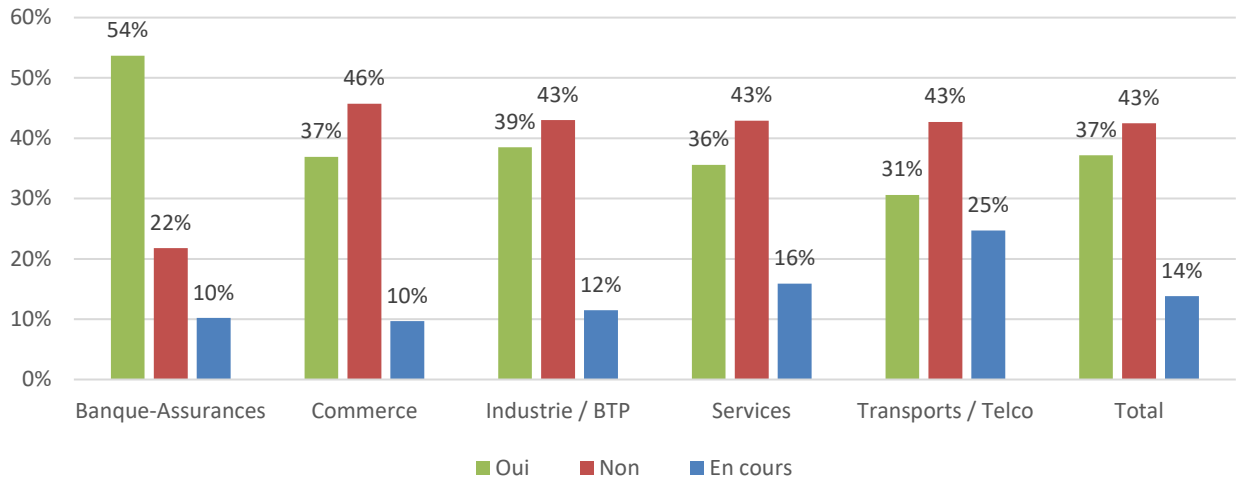


Figure 37 – Domaine de couverture de la gestion de la continuité

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 ?

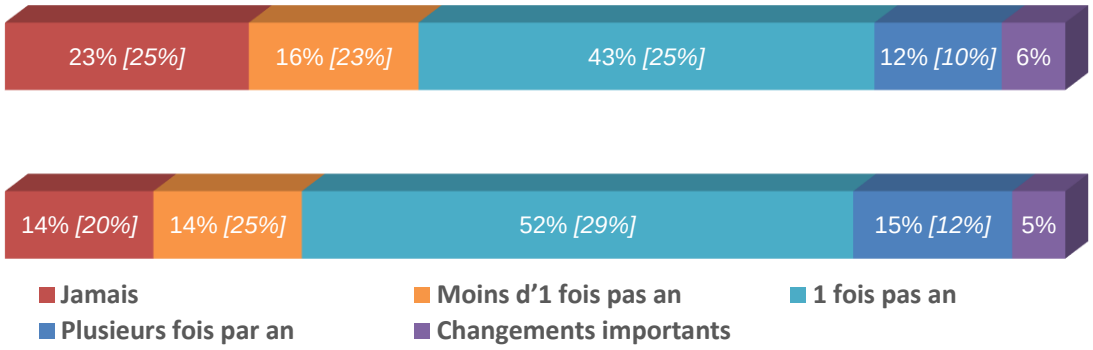


Figure 39 – Fréquence des tests

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.

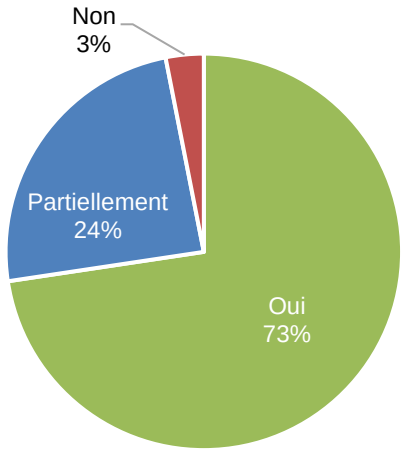
Conformité avec les obligations légales et réglementaires

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 ?

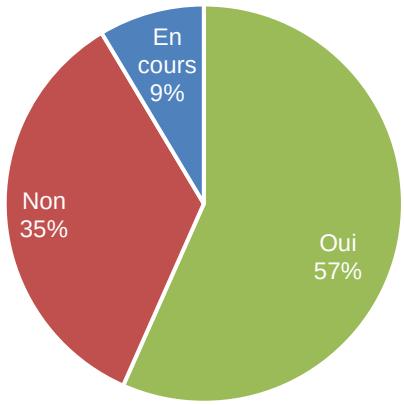


Figure 41 – Identification de la fonction de DPD/DPO

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).

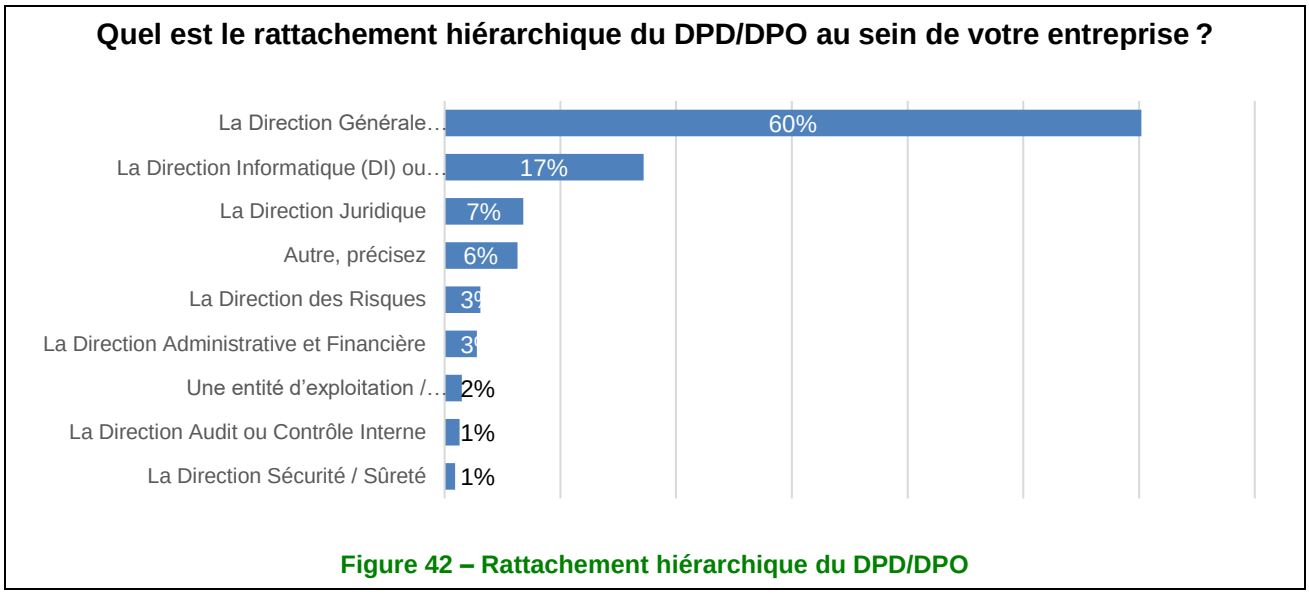


Figure 42 – Rattachement hiérarchique du DPD/DPO

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 %).

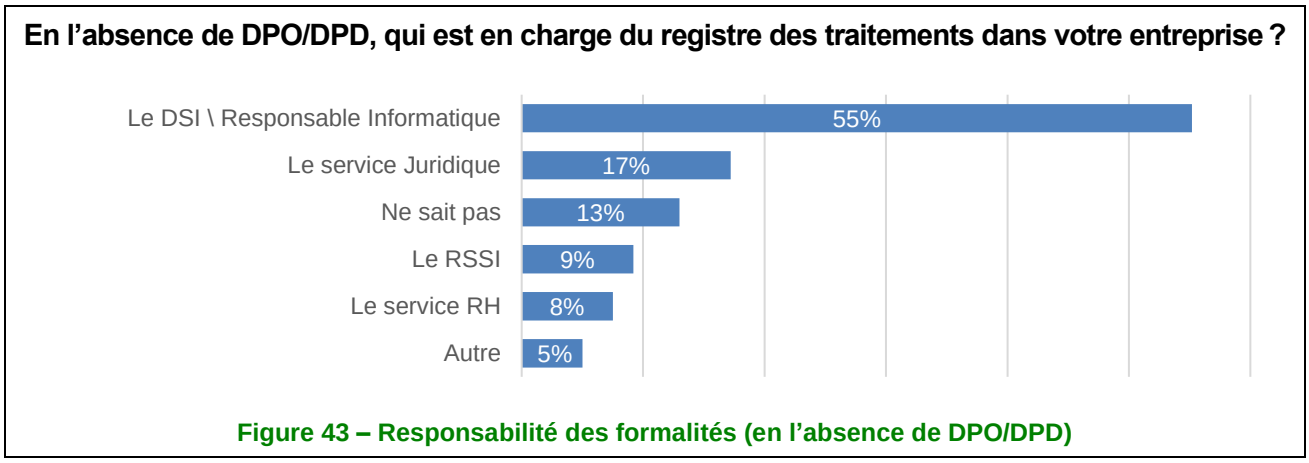


Figure 43 – Responsabilité des formalités (en l'absence de DPO/DPD)

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 ?

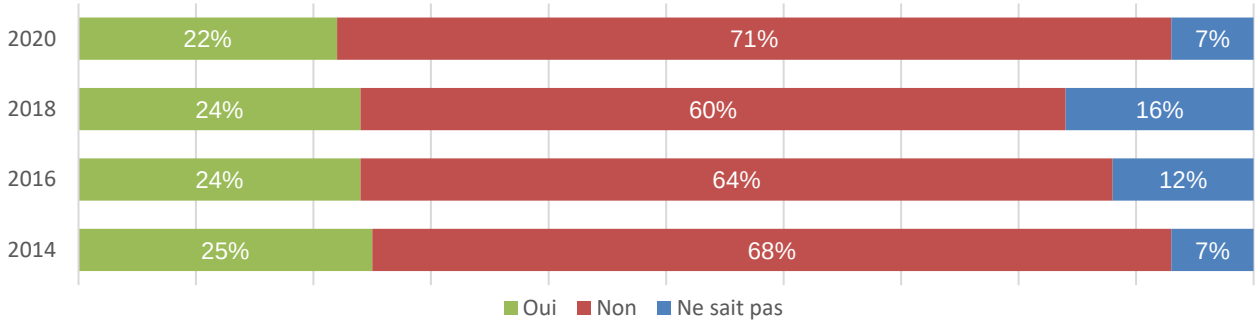


Figure 44 – Entreprises soumises à des lois/réglementations spécifiques pour la sécurité SI

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 %).

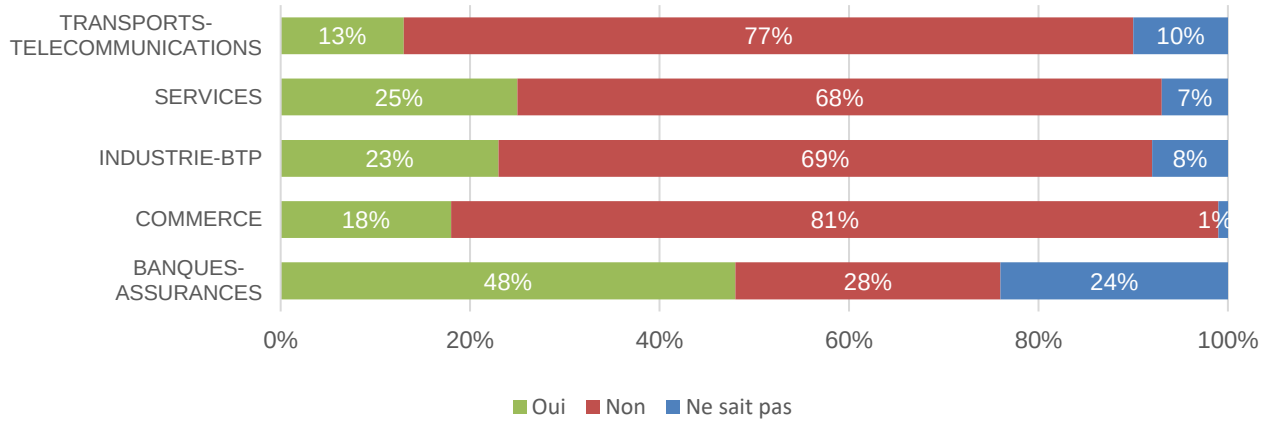


Figure 45 – Entreprises soumises à des lois/réglementations spécifiques pour la sécurité SI (par secteur)

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).

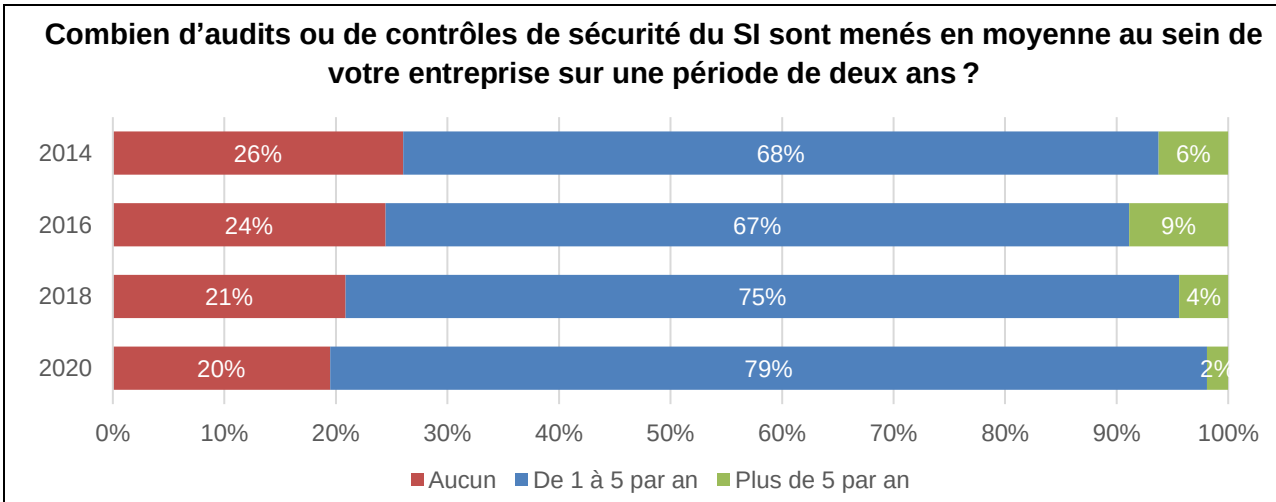


Figure 46 – Fréquence des audits de sécurité au cours des deux dernières années

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 ?

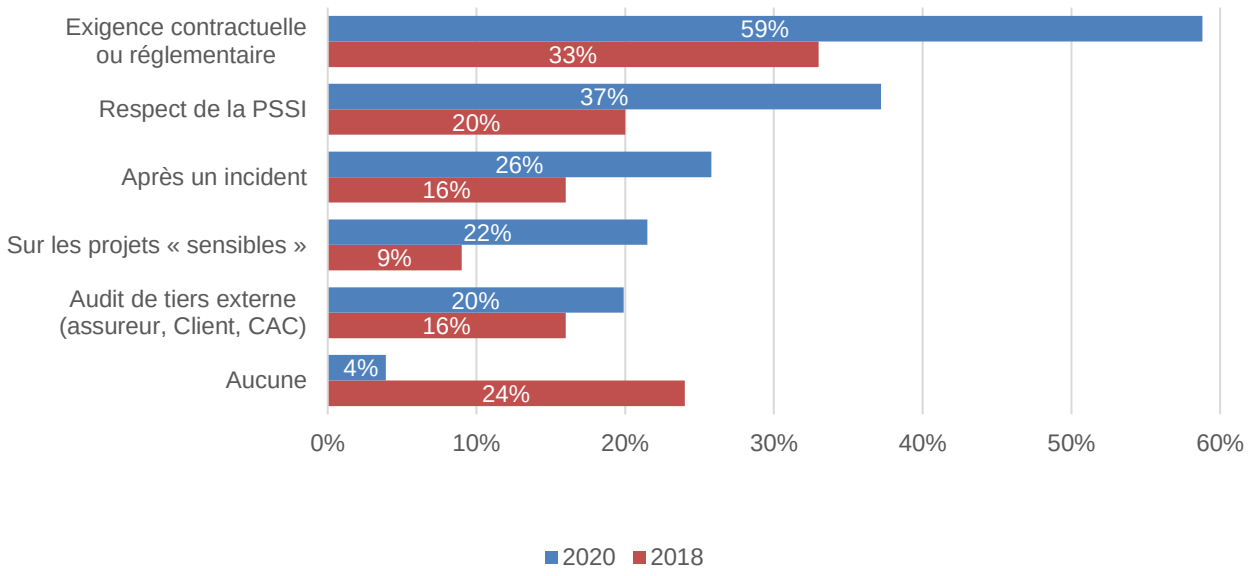


Figure 47 – Motivation des audits de sécurité

Collectivités territoriales

- Présentation de l'échantillon
- Thème 5 : Politique de sécurité de l'information (PSI)
- Thème 6 : Organisation de la sécurité de l'information
- Thème 7 : La 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 du SI
- Thème 15 : Relations avec les fournisseurs
- Thème 16 : Gestion des incidents SSI
- Thème 17 : Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité
- Thème 18 : Conformité

Les collectivités

Présentation de l'échantillon

Toujours des disparités entre les collectivités et un cadrage de la cybersécurité plus important

La cible de l'enquête MIPS de 2020 est identique à celle des études réalisées en 2012 et 2016. Il est donc possible de comparer les changements opérés au niveau de la prise en compte de la cybersécurité des collectivités territoriales. Depuis 2016, ces structures ont dû faire face à des changements réglementaires importants survenus en 2018, notamment :

- la loi de programmation militaire (LPM) qui a connu plusieurs phases de mise en œuvre en 2015 et 2019 ;
- le règlement général sur la protection des données (RGPD) ;
- la transposition de la directive NIS dans le droit français.

C'est surtout le RGPD qui a entraîné une prise de conscience de l'importance des données personnelles détenues par les collectivités, et ce, quelle que soit leur taille.

La cible de l'étude est constituée des collectivités territoriales suivantes :

- les communes de plus de 30 000 habitants ;
- les intercommunalités réparties entre :
  - les communautés de communes de plus de 10 000 habitants,
  - les communautés d'agglomération, communautés urbaines et les métropoles ;
- les conseils territoriaux regroupant les régions et les départements.

Sur quelque 1 260 collectivités de France métropolitaine interrogées, 202 ont répondu à la sollicitation du Clusif, soit un taux d'acceptation d'environ 16 %. Bien que ce taux soit faible, il reste possible d'observer les évolutions dans la prise en compte du sujet de la cybersécurité.

À l'instar de la précédente étude, la méthode des quotas a été utilisée ici. Pour représenter le plus fidèlement la réalité des collectivités territoriales françaises par rapport à celles ayant répondu à nos sollicitations, un redressement a été effectué. Ce dernier se présente de la façon suivante :

	Échantillon Clusif	%	Redressement	Données nationales Insee
Communes de plus de 30 000 habitants	31	15 %	➔	13 %
Communautés de communes de plus de 10 000 habitants	34	17 %	➔	55 %
Communautés d'agglomération, urbaines et métropoles	111	55 %	➔	26 %
Conseils territoriaux	26	13 %	➔	7 %
Total	**202**	**100 %**		

La cybersécurité relevant normalement du responsable de la sécurité des systèmes d'information (RSSI), c'est lui qui était ciblé en priorité pour répondre au questionnaire. À l'instar de 2016, 20 % en moyenne des

responsables interrogés assuraient cette fonction en 2019. Les réponses à ce questionnaire sont donc fournies par des personnes dont la fonction première et/ou exclusive n'est pas la cybersécurité.

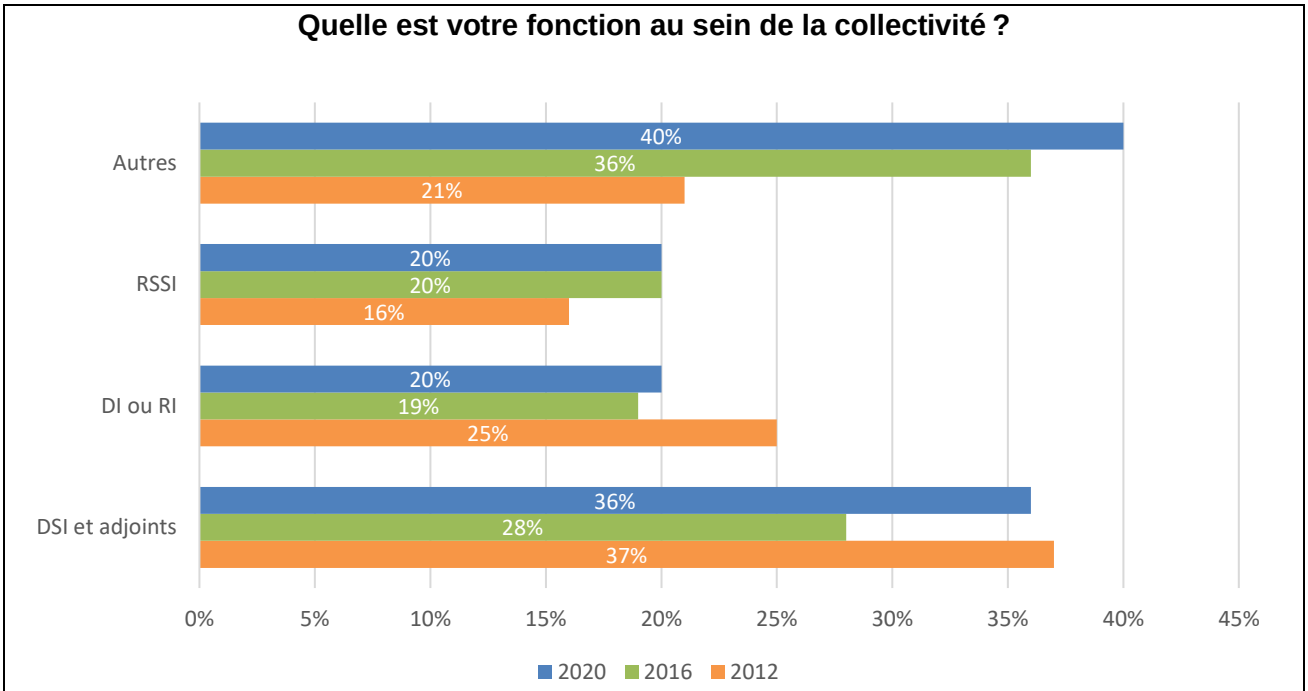


Figure 48 – Fonctions des personnes interrogées

Des disparités importantes concernant le RSSI persistent dans les différentes collectivités. Ce sont encore les conseils territoriaux qui sont les plus représentés par cette fonction avec 42 % des répondants, suivis par les communes (en hausse à 36 %), mais ce taux s'effondre ensuite pour les communautés d'agglomération/urbaines ou métropoles (18 %) et les communautés de communes, avec seulement 14 % des interrogés.

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

Progression de la formalisation

On observe une nette augmentation de la part des collectivités ayant formalisé leur PSI (52 % *vs* 32 % en 2016), et ce plus particulièrement pour les communautés de communes, qui étaient moins d'une sur quatre à avoir formalisé leur PSI lors de la dernière enquête.

Ce pourcentage varie désormais assez peu selon le type de collectivité.

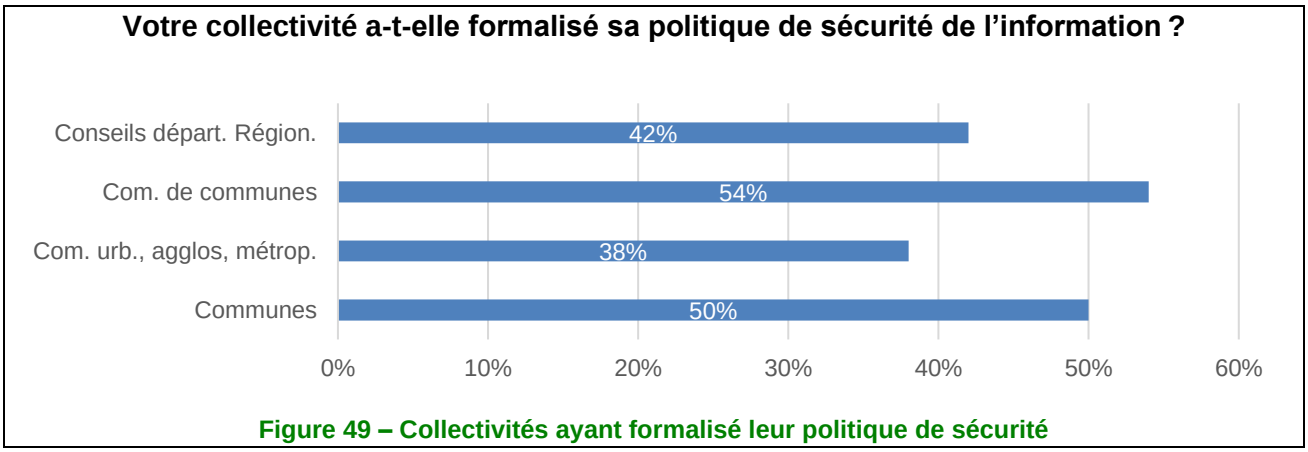


Figure 49 – Collectivités ayant formalisé leur politique de sécurité

De plus, la PSI est très majoritairement à jour, quel que soit désormais le type de collectivité.

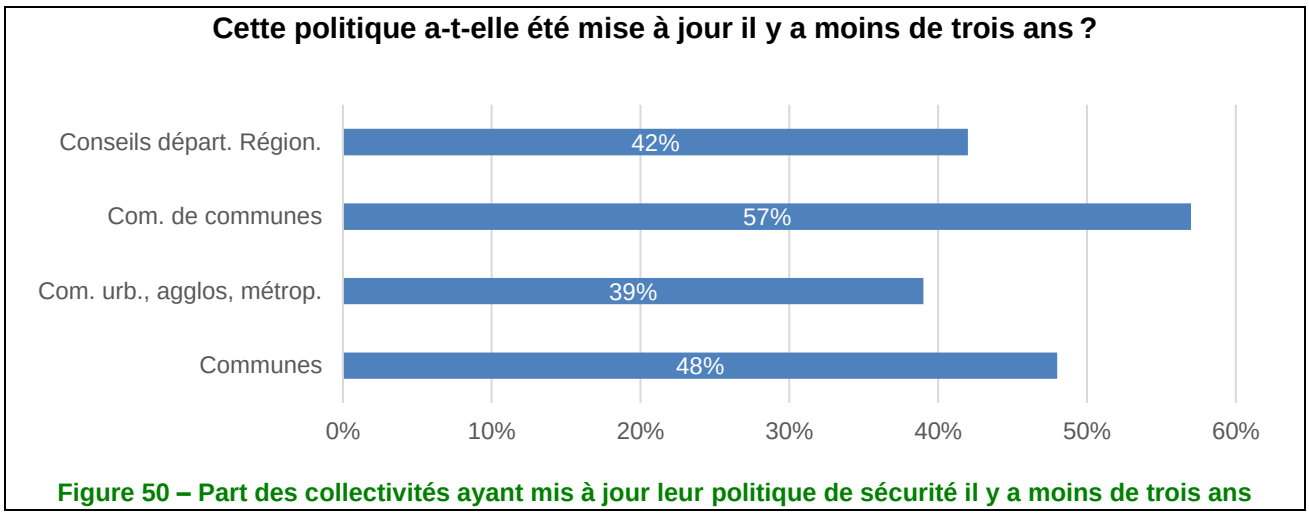


Figure 50 – Part des collectivités ayant mis à jour leur politique de sécurité il y a moins de trois ans

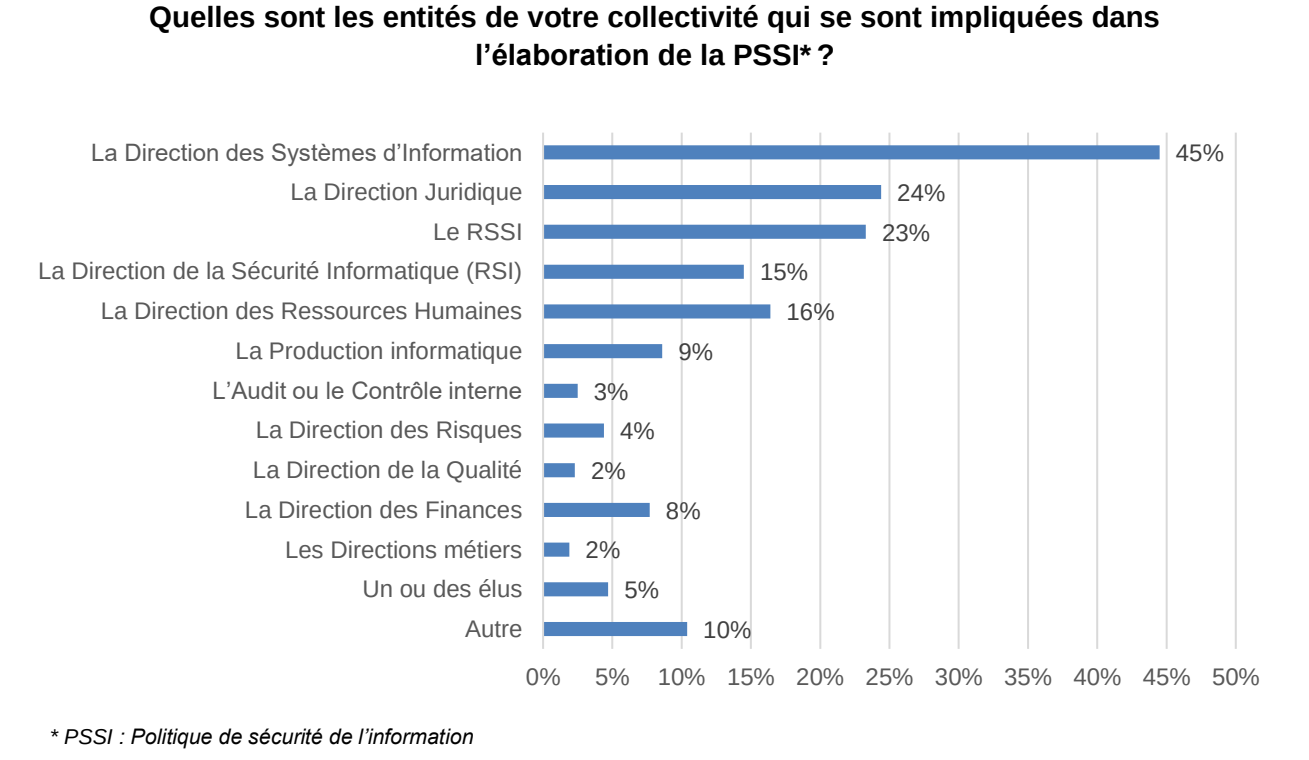
La PSI des collectivités territoriales reste moyennement soutenue par la Direction générale des services (pour environ 50 %, en légère régression).

Communication de la politique de sécurité de l'information

Cette politique de sécurité n'est toujours que moyennement diffusée à l'ensemble des parties prenantes (53 %, dont 23 % de manière proactive et explicite et 30 % uniquement pour information, sans accompagnement spécifique). Ce taux, s'il reste médiocre, est cependant en augmentation, puisqu'il n'était que de 43 % il y a quatre ans.

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

L'implication de la Direction générale des services s'affirme et est désormais citée par près de 70 % des collectivités, en très nette augmentation par rapport à 2016 (moins de 40 %).



** PSSI : Politique de sécurité de l'information*

Figure 51 – Entités ayant été impliquées dans la politique de sécurité

Bases sur lesquelles ont été mises en place les mesures de sécurité de l'information

Il ressort clairement de notre étude que la mise en place des mesures de sécurité est majoritairement basée sur une ou plusieurs normes, et ce dans une proportion quasiment identique, par souci de respecter les bonnes pratiques reconnues, la conformité à la PSI étant citée par 41 % des collectivités et le management des risques, par 14 % d'entre elles seulement.

Les mesures mises en place ont-elles été définies (citer – plusieurs réponses possibles) ?

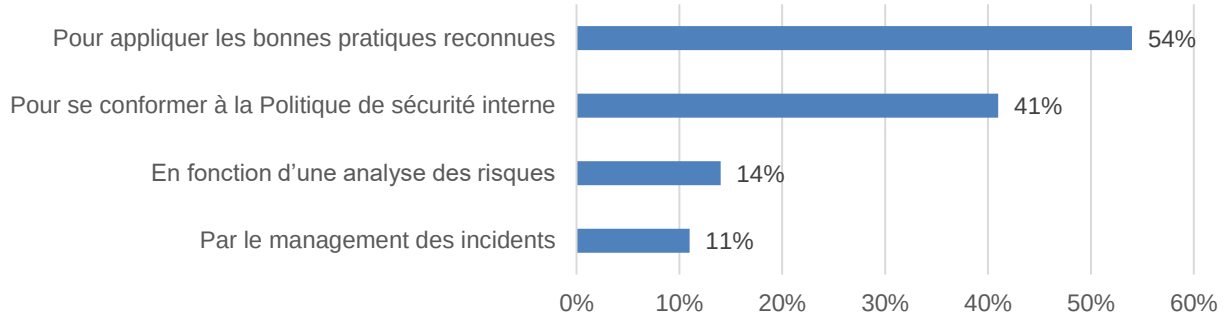


Figure 52 – Bases sur lesquelles repose la mise en place de mesures de sécurité de l'information

On note cependant que pour les collectivités s'étant appuyées sur une ou plusieurs normes, le RGPD arrive largement en tête et que les normes à spectre plus large sont assez peu référencées :

Les mesures mises en place ont-elles été définies (citer – plusieurs réponses possibles) ?

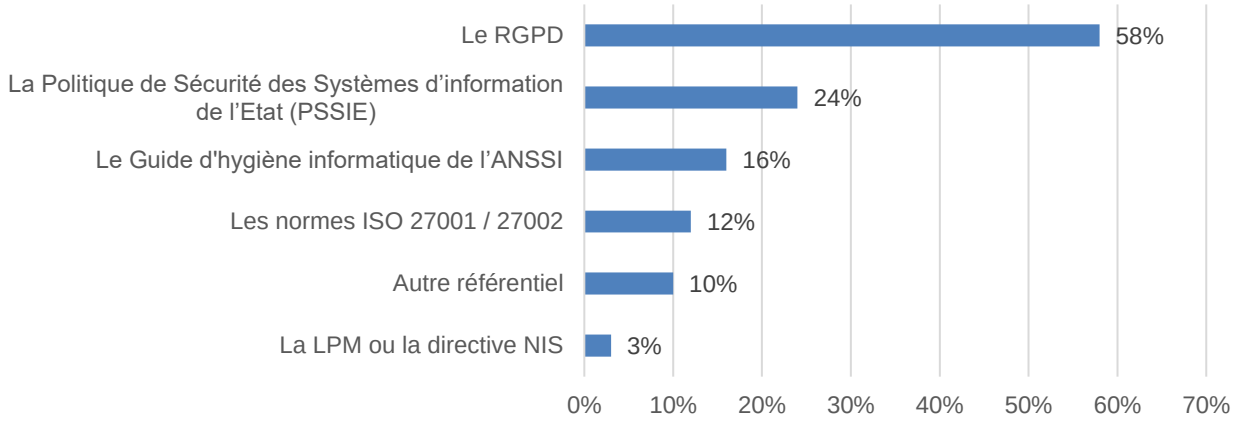


Figure 53 – Normes citées par les collectivités ayant déclaré s'appuyer sur des référentiels pour la mise en place des mesures de sécurité

Thème 6 : Organisation de la sécurité de l'information

RSSI : une fonction de mieux en mieux identifiée, mais encore réservée aux plus grandes structures

En quatre ans, l'identification de la fonction RSSI au sein des collectivités territoriales enregistre un net progrès puisqu'elles sont aujourd'hui 52 % à avoir identifié cette fonction contre 35 % en 2016, une infime proportion (1 %) déclarant « je ne sais pas ». La fonction de RSSI acquiert une bonne lisibilité d'autant que ce résultat n'est pas propre à un type de collectivité.

On note par ailleurs que la personne en charge de cette mission est dédiée à la fonction de RSSI dans 59 % des cas (contre 40 % en 2016) voire 67 % si on excepte les communautés de communes (CC) où ce taux se

situe en dessous des 50 %. Pour ces dernières, la faiblesse de ce résultat peut s'expliquer par une dotation de moyens plus modeste que pour les collectivités de type communauté d'agglomération ou urbaine.

Enfin, même si les communes affichent un bon résultat (88 %) concernant leur capacité à dédier une personne à la fonction de RSSI, on notera que seuls 8 % de celles qui ont répondu positivement à cette question ont moins de 30 000 habitants. Or selon le site officiel [8], en 2016 il y avait 35 431 (sur 35 885) communes de moins de 30 000 habitants et elles représentaient 61,3 % de la population.

Les bons résultats obtenus en matière de sécurité dans certaines collectivités doivent se rapporter aux enjeux liés à la population administrée. La protection n'est pas homogène

RSSI : dédier une personne reste une difficulté pour plus du tiers des collectivités territoriales

Concernant le non-cumul des fonctions, on note une amélioration par rapport aux chiffres de 2016 et 2012 sur l'ensemble des collectivités territoriales interrogées, et plus particulièrement les communes, où cette proportion augmente de manière spectaculaire. Sachant que 92 % de celles qui ont été interrogées ont plus de 30 000 habitants, on peut imaginer qu'elles disposent de services conséquents.

Les établissements publics de coopération intercommunale (EPCI) n'étant pas identifiés dans les enquêtes précédentes, on ne peut que constater les chiffres de 2020. Une différence apparaît en fonction de la taille des structures, les plus petites d'entre elles (communauté de communes) disposant *a priori* de moins de moyens leur permettant de détacher une personne pleinement à la fonction de RSSI.

De façon moins surprenante, on remarque une progression des conseils territoriaux. Il y a peut-être un effet dû à la loi NOTRe de 2016 qui a conduit à fusionner les régions, et donc à faciliter la mobilisation d'un équivalent temps plein (ETP) pour la SSI.

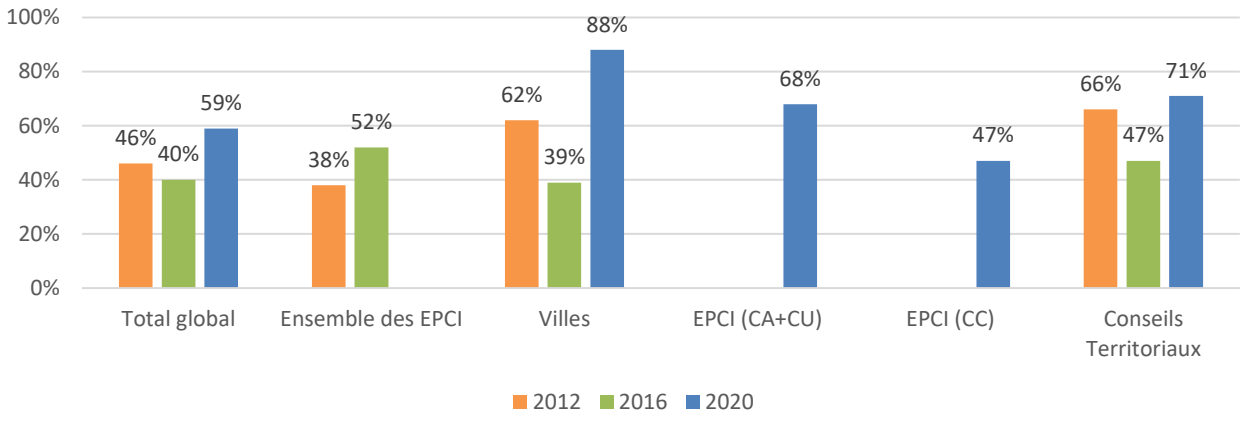


Figure 54 – Part des RSSI dédiés à la fonction

Dégager une personne dédiée pour assumer la fonction de RSSI se constate de plus en plus, mais dépend encore fortement de la taille des services.

RSSI : une fonction partagée avec ceux qui ont en charge le bon fonctionnement des SI, mais aussi avec des consultants externes

Si on affine les résultats en se demandant avec quelle(s) autre(s) fonction(s) se cumule(nt) celle de RSSI, on peut distinguer essentiellement les trois cas suivants : les DSI (42 %), les responsables informatiques (37 %) et les consultants externes (20 %).

Le cumul avec la fonction de DSI se rencontre majoritairement dans les EPCI, les conseils territoriaux et dans une moindre mesure les communes, celles-ci n'ayant pas toujours de DSI attitré. Cela semble d'ailleurs être confirmé par le fait que la plupart d'entre elles, la fonction de RSSI se cumule avec la fonction de responsable informatique.

[8] https://www.collectivites-locales.gouv.fr/files/files/statistiques/brochures/publication_globale_0.pdf

Enfin, notons que 7 % des collectivités s'appuient sur un consultant externe, excepté dans le cas des communautés de communes pour lesquelles ce taux s'élève à 28 %. Peut-être s'agit-il d'un compromis entre un manque d'effectif et/ou une carence de compétence en SSI ?

Dans le cas où la personne n'est pas entièrement dédiée aux missions de SSI (définition et contrôle de la PSSI…), le cumul majoritairement constaté avec celles relatives à la mise en œuvre de la PSSI peut interroger :

- ***sur la capacité des personnes à révéler des défaillances, des incidents ;***
- ***sur la bonne compréhension de l'enjeu de cette fonction par l'encadrement dirigeant.***

Rattachement du RSSI : un positionnement ne permettant pas une totale liberté de parole

De manière assez homogène le RSSI est, en fonction de la taille des services, rattaché à la DSI/DI (23 %) ou à la Direction générale des services (59 %).

Les exceptions qui se dégagent ne sont pas suffisamment significatives pour en déduire un résultat. En effet, sur l'ensemble des collectivités, de manière plus surprenante, 6 % des RSI sont rattachés à une direction administrative et financière et seuls 4 % de ceux en conseils régionaux ou territoriaux le sont à la Direction de la sécurité/sûreté (DGS).

Une comparaison avec les chiffres de 2016 montre globalement une diminution de la catégorie « autre » au profit des DSI et des DGS.

Quel est le rattachement hiérarchique du RSSI/RSI au sein de votre collectivité ?

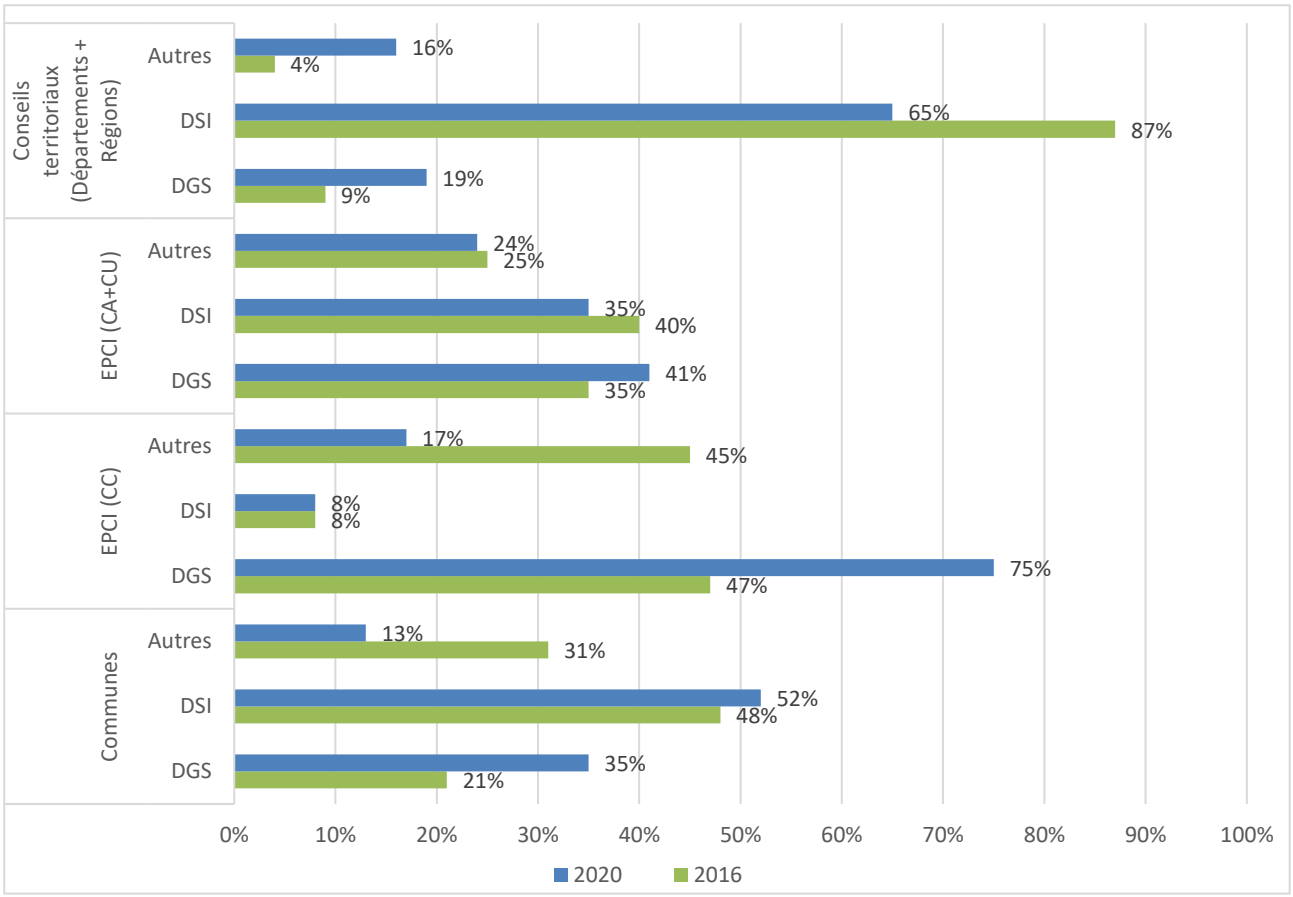


Figure 55 – Rattachement hiérarchique du RSSI/RSI

On pourrait au premier abord en conclure que le RSSI est rattaché à un niveau hiérarchique élevé et qu'il est de plus en plus reconnu. Mais compte tenu des réponses apportées à la question sur le cumul des fonctions, on peut douter de sa réelle liberté de parole sur, par exemple, les difficultés à mettre en œuvre la PSSI. En effet, 79 % des RSSI cumulent cette fonction avec celle de DSI ou de responsable informatique. Tout au plus

leur positionnement hiérarchique leur permet-il de demander des budgets supplémentaires en matière de sécurité.

Organisation transversale de la SSI : de nets progrès par rapport à 2016/des EPCI en retrait

En 2016, la part des collectivités territoriales ayant mis en place une organisation transversale (correspondants, réunions de pilotage, etc.) s'élevait à 12 %. En 2020, elle se monte à 30 %.

Se détachent de l'échantillon les communes avec un taux de 42 % de réponses affirmatives et les conseils territoriaux avec un taux de 54 %, les EPCI restant un peu en marge avec un taux d'environ 25 %.

On constate donc une nette amélioration, mais qui demeure insuffisante, pour considérer que la SSI est bien comprise comme étant l'affaire de tous.

Des effectifs consacrés à la SSI souvent insuffisants au regard des enjeux perçus pour les SI

Globalement, le nombre d'ETP mobilisés pour la SSI varie entre 0 et 5. Les tranches « moins de 1 ETP », « 1 à 2 ETP » et « 3 à 5 ETP » se répartissent équitablement au sein des communes et des EPCI de type communautés d'agglomération et communautés. Cette distribution laisse penser que le nombre d'ETP dépend directement de la taille des services et donc de l'usage de l'informatique, et qu'il n'appelle pas *a priori* de commentaire supplémentaire.

En revanche, de nouveau, on peut soupçonner un manque de moyens ou d'accès aux compétences requises pour les communautés de communes, puisque 51 % d'entre elles dégagent moins de 1 ETP et 11 %, plus de 3 ETP. Compte tenu des compétences qui leur sont dévolues et de leur fonction de guichet pour un certain nombre de services au public, on peut considérer qu'il s'agit d'un point à surveiller.

Pour les conseils territoriaux, compte tenu de l'importance des budgets qu'ils ont à gérer, notamment depuis la fusion des régions opérée en 2016, de la plus grande facilité à accéder à la compétence du fait de leur positionnement dans une ville départementale et/ou régionale, on peut s'étonner que 42 % des équipes SSI soient constituées de moins de 1 ETP. Cette situation des conseils territoriaux est d'autant plus surprenante que 73 % d'entre eux reconnaissent qu'une interruption des SI de plus de 24 heures a des conséquences graves sur leur activité.

Cette exigence de disponibilité des SI est d'ailleurs partagée de manière homogène par 77 % de l'ensemble des collectivités territoriales. Seuls 21 % considèrent qu'une indisponibilité de 48 heures est tolérable et 2 %, qu'une indisponibilité même de longue durée n'a pas de conséquences graves.

Une dépendance à l'informatique forte similaire à ce qui a été observé en 2016

La transformation numérique est en route dans les collectivités territoriales avec une part toujours plus importante de services assurés de façon dématérialisée. Il est donc naturel que la dépendance de ces dernières reste majoritairement forte.

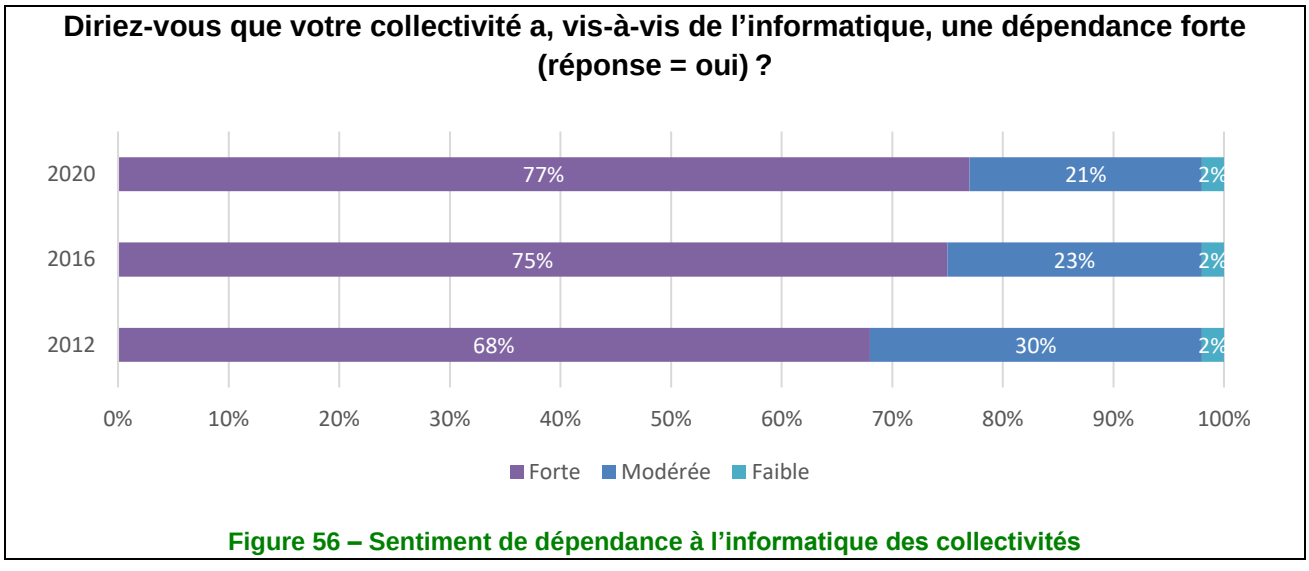


Figure 56 – Sentiment de dépendance à l'informatique des collectivités

Moyens consacrés à la sécurité de l'information par les collectivités

Une méconnaissance du budget alloué à la cybersécurité

Parmi les personnes interrogées, 63 % ignorent le montant du budget alloué à la cybersécurité de leur structure. Pour celles et ceux qui en ont connaissance, la plupart (57 %) refusent de le communiquer. Deux raisons peuvent être avancées pour expliquer une telle réticence :

- un montant peu élevé pourra indiquer que les investissements consentis ne sont pas à la hauteur des enjeux qui se posent en matière de cybersécurité ce qui fera de cette structure : soit pour les plus petites, une cible potentielle accessible à un pirate débutant, soit pour les plus grosses, un trophée pour hacker en mal de renommée ;
- un montant élevé pourra au contraire signifier que la collectivité a investi massivement à la suite d'une cyberattaque, sujet à propos duquel les victimes sont toujours peu enclines à communiquer.

Il devient donc difficile de tirer des enseignements à partir du panel restant, soit environ 33 collectivités. On constate néanmoins que le budget des conseils territoriaux est homogène (100 k€), qu'il est globalement faible pour les communautés d'agglomération et les métropoles (5 k€) et qu'il comporte des écarts importants entre les communes.

Le budget alloué à la cybersécurité, variable d'ajustement du budget des DSI ?

Pour la moitié des répondants, toutes collectivités confondues, le budget alloué à la cybersécurité est remis en cause d'une année sur l'autre. Il n'est sanctuarisé en totalité que pour 11 % d'entre elles et partiellement pour 23 %, 13 % n'étant pas en mesure de se prononcer. **Dans la majeure partie des collectivités, le budget cybersécurité n'est donc pas pérenne d'une année sur l'autre.**

Un budget en progression ou constant pour une majorité de collectivités

Par rapport aux précédentes études, le budget alloué à la cybersécurité reste constant pour la majorité des collectivités (45 % *vs* 67 % en 2016), mais la proportion de structures où ce budget est en hausse (forte ou moyenne) est en augmentation (41 % *vs* 18 % en 2016), ce qui pourrait trouver son explication dans une prise de conscience des enjeux liés à la cybersécurité. En effet, depuis l'étude MIPS de 2016, le monde numérique a été confronté à des cyberattaques d'ampleur qui ont été largement médiatisées (*Wannacry, Not Petya*…). Le cadre réglementaire a lui aussi fortement évolué. La prise en compte des obligations en matière de cybersécurité liées à la LPM a également eu un impact pour les collectivités désignées « opérateur d'importance vitale » (OIV). Enfin, l'arrivée du RGPD a fait apparaître les concepts de *Privacy by Design* et *Security by Default* qui imposent un ensemble de contraintes à l'ensemble des collectivités, et ce quelle qu'en soit leur taille.

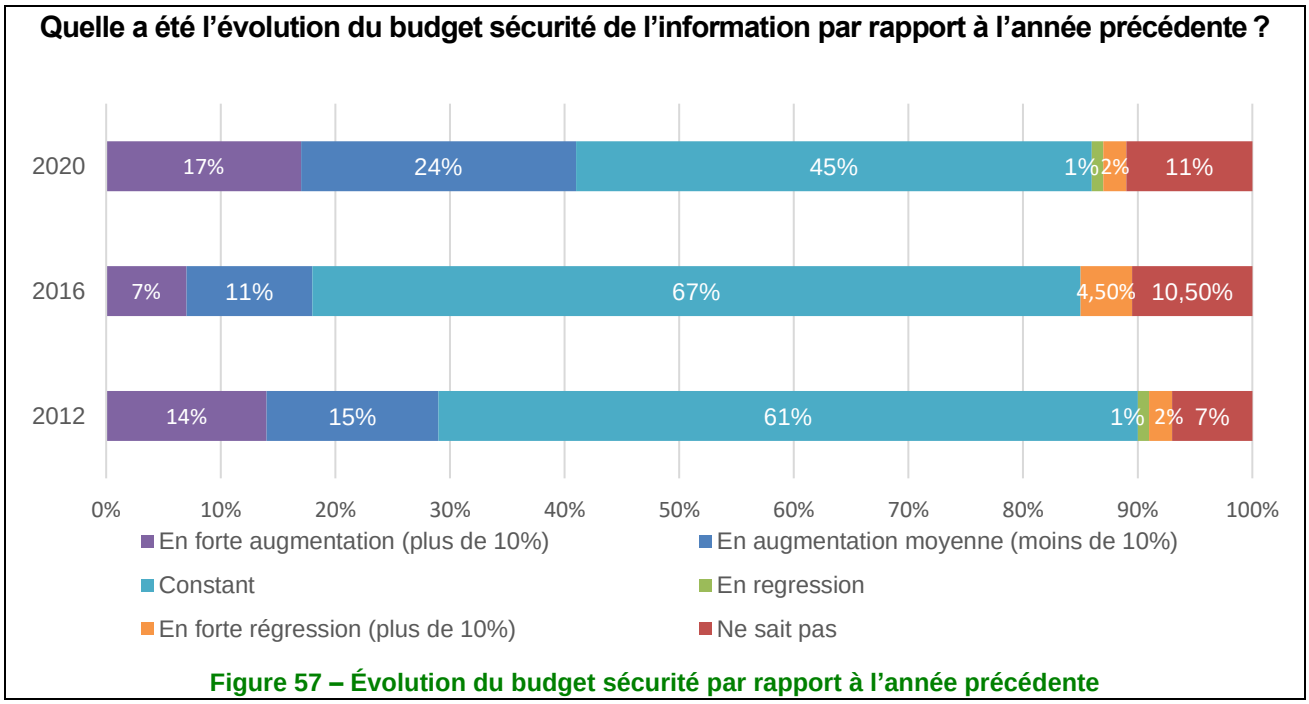


Figure 57 – Évolution du budget sécurité par rapport à l'année précédente

La cybersécurité ne se résume plus à la mise en œuvre de dispositifs techniques

Globalement, l'ensemble des dépenses budgétaires liées à la cybersécurité a augmenté, ce qui traduit une prise de conscience de l'impérieuse nécessité de protéger les SI des collectivités. Même si la mise en place de solutions (+ 20 points) reste le premier poste budgétaire dans les collectivités, nous pouvons remarquer une progression des dépenses en lien avec l'audit (+ 14 points), la mise en œuvre d'éléments organisationnels (+ 12 points) ou encore la formation (+ 7 points). Là encore, ces augmentations traduisent un changement de perception des enjeux en matière de cybersécurité qui ne sont plus désormais cantonnés à la mise en œuvre de solutions techniques. Tout cela est encore une fois à lier à la perception de la cybersécurité, soit par le prisme réglementaire, soit par celui de la réalité des cyberattaques.

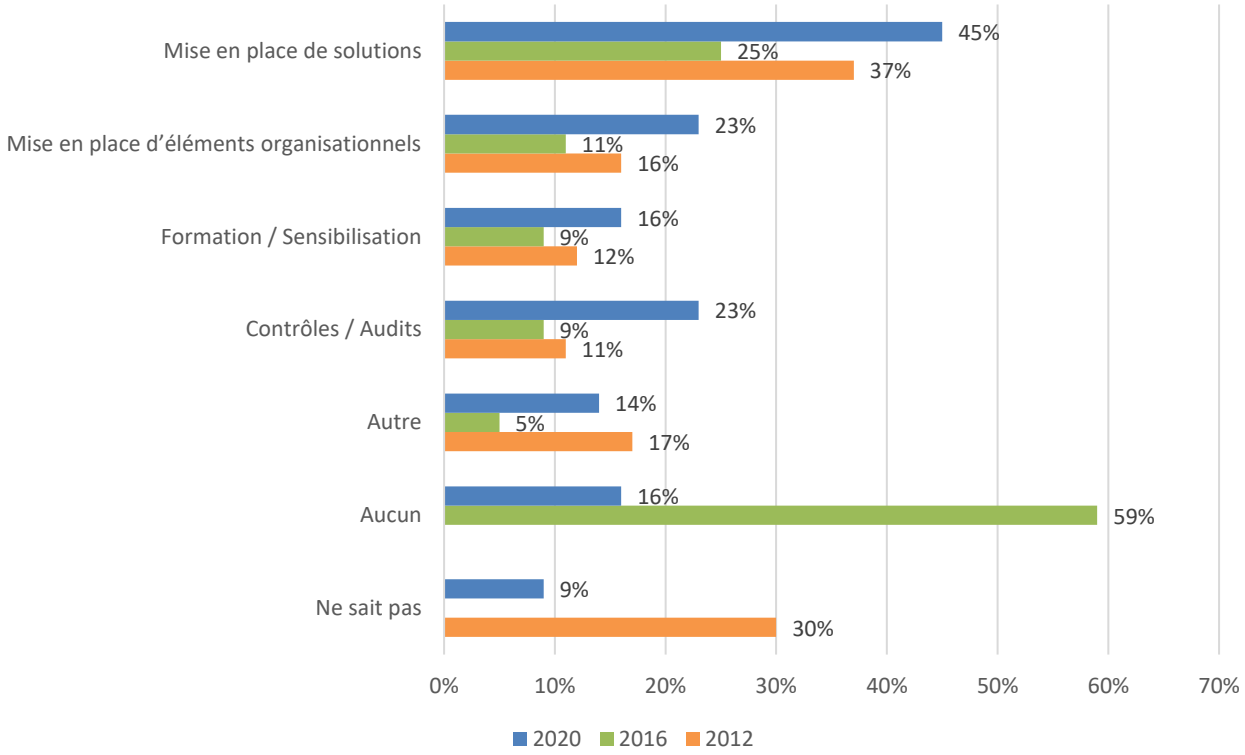


Figure 58 – Évolution du budget en fonction des postes (comparaison sur les trois études)

Thème 7 : La sécurité des ressources humaines

La charte d'usage du SI continue sa progression (+ 4 points depuis 2016) même si les communautés de communes restent à la traîne.

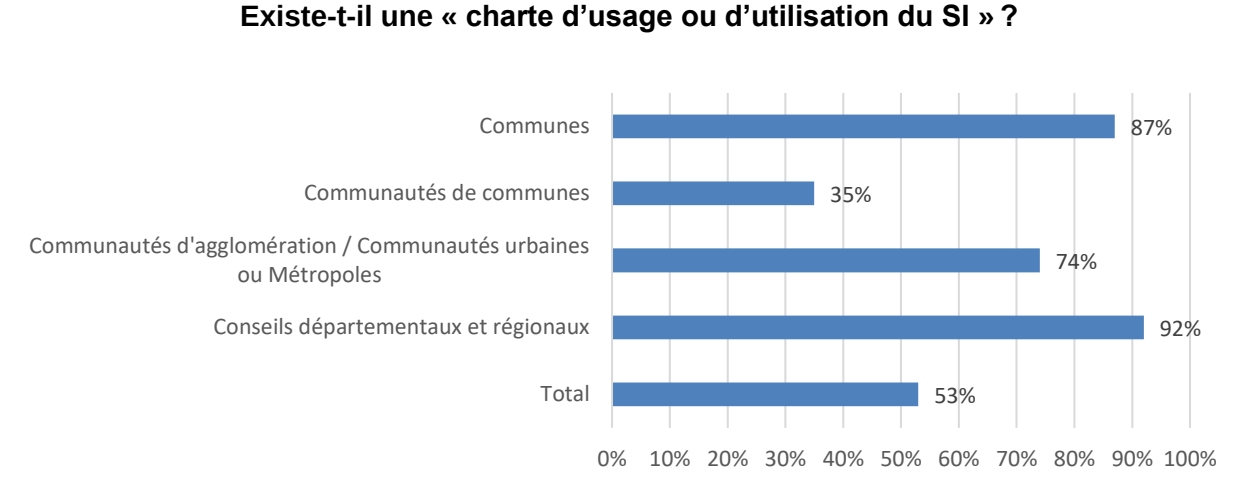


Figure 59 – Existence d'une charte d'usage du SI

La communication de la charte n'est pas égale pour toutes les populations d'usagers

La diffusion des règles de sécurité auprès du personnel reste élevée. Au fil du temps, cette pratique semble ainsi s'intégrer peu à peu dans la culture des organisations publiques. La nette progression de la sensibilisation des prestataires/fournisseurs (+ 9 points) semble être soutenue par les conseils départementaux et régionaux, établissements rompus à une gestion performante des contrats de service au sein desquels les exigences en termes de sécurité sont rigoureuses.

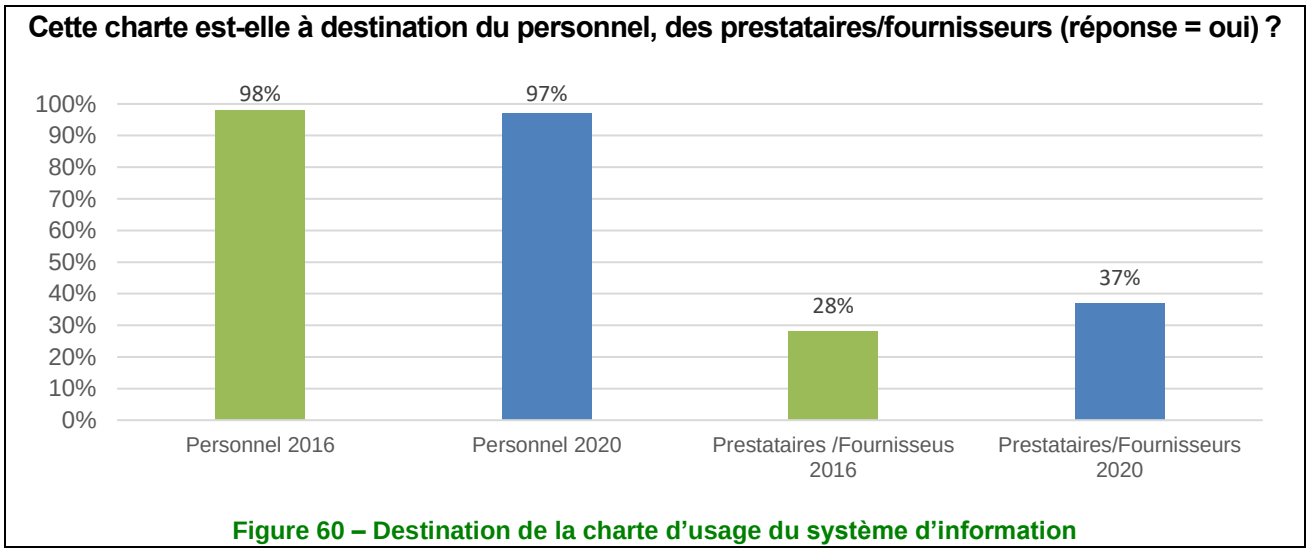


Figure 60 – Destination de la charte d'usage du système d'information

Des actions de sensibilisation récurrentes

En complément de la charte d'usage des SI, 48 % (+ 23 points depuis 2016) des collectivités ont mis en place des actions de sensibilisation auprès des utilisateurs ou sont engagées dans un tel processus. Ces actions deviennent largement récurrentes. On note un retour important des supports traditionnels. Sans doute trop chronographes et complexes à mettre en œuvre, les *serious games* sont quasi inexistants. Preuve que la sécurité des SI devient un sujet stratégique, les VIP sont spécifiquement sensibilisés dans deux cas sur cinq, ce qui représente 12 points de mieux qu'en 2016. Toutefois, seuls 37 % des collectivités ont mesuré l'impact de leur programme de sensibilisation.

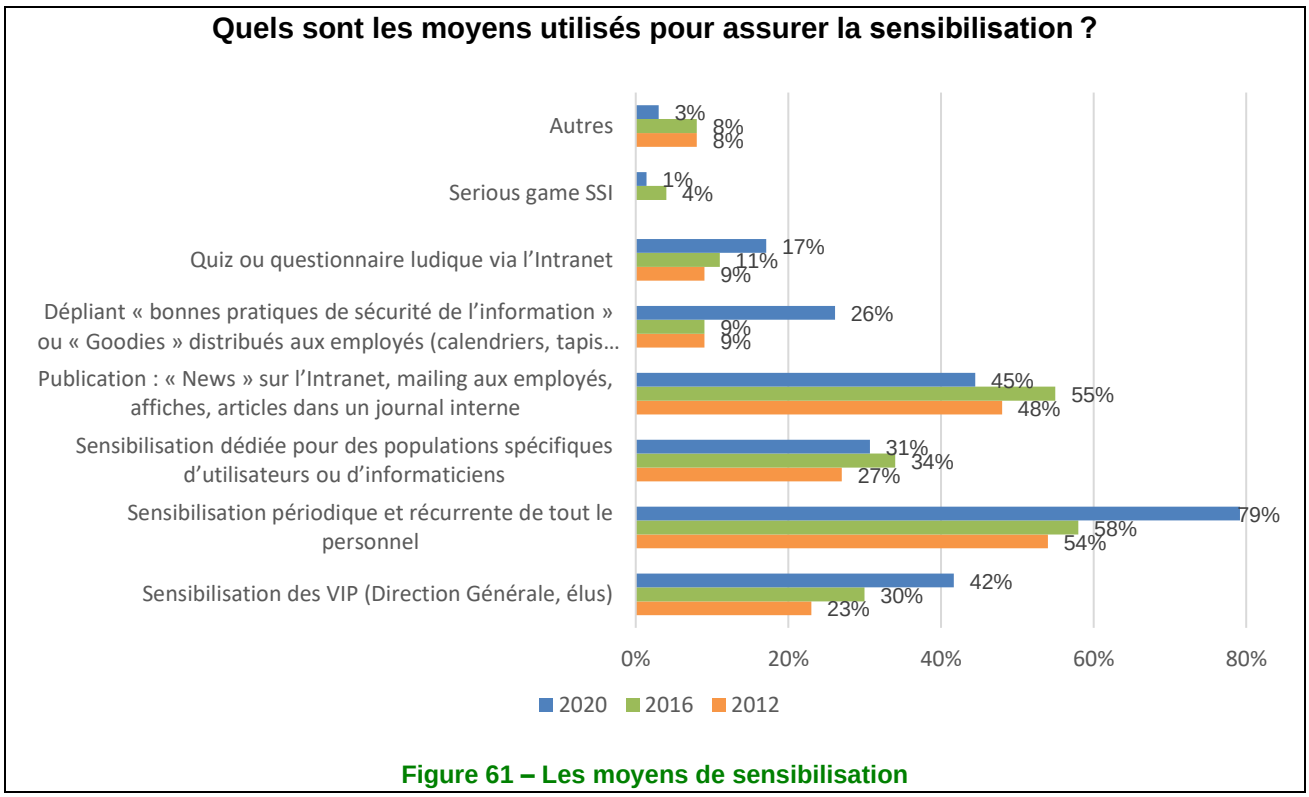


Figure 61 – Les moyens de sensibilisation

Une gestion des départs ou changements de poste toujours aussi complexe

Malgré les enjeux, le nombre de collectivités territoriales qui disposent d'une procédure formalisée pour la gestion des départs ou des changements de poste progresse très peu (+ 4 points par rapport à 2016). Toutefois, on peut espérer que le regain des « projets en cours » (+ 11 points) permettra d'améliorer la situation.

Existe-t-il une procédure pour gérer, en cas de départ ou mutation des collaborateurs, la suppression de tous les droits d'accès et la restitution du matériel ?

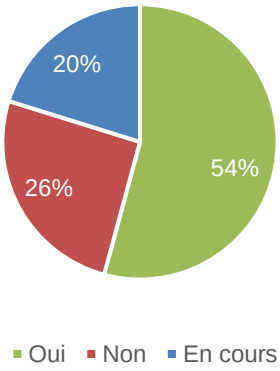


Figure 62 – Procédure de suppression des droits d'accès et de restitution du matériel

Thème 8 : Gestion des actifs

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

Le pourcentage de collectivités ayant réalisé un inventaire au moins partiel de leurs actifs informationnels progresse nettement et passe de 55 % à un peu plus de 90 %, marquant ainsi un progrès significatif en quatre ans, et ce, sans qu'il y ait de disparités notables en fonction des types de collectivités. Notons en particulier la forte progression des collectivités qui procèdent à un inventaire complet de leurs actifs (46 % en 2020, contre 22 % en 2016).

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

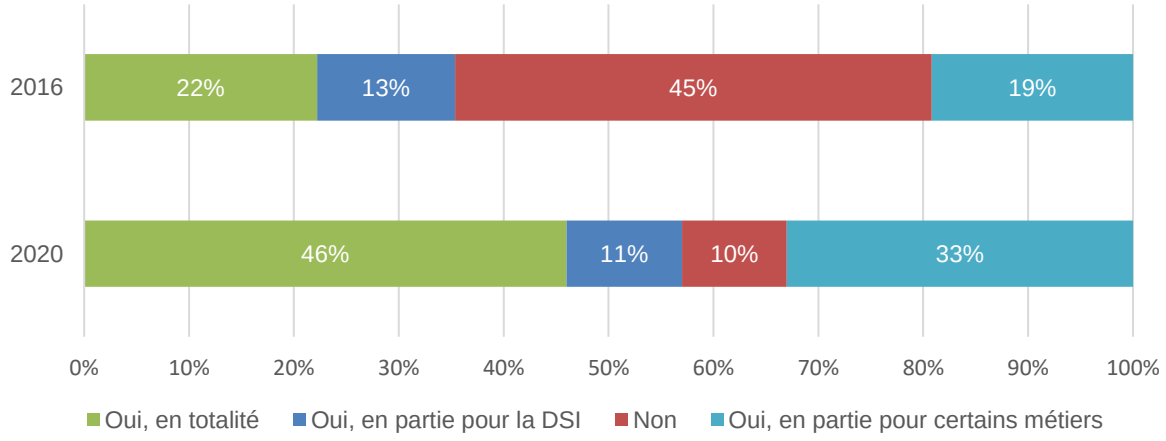


Figure 63 – Inventaire des actifs

La même croissance est constatée pour la classification des actifs : le nombre de collectivités ayant entrepris une classification, au moins partielle, de leurs actifs a presque doublé en quatre ans, pour atteindre 66 % en 2020 contre 35 % en 2016.

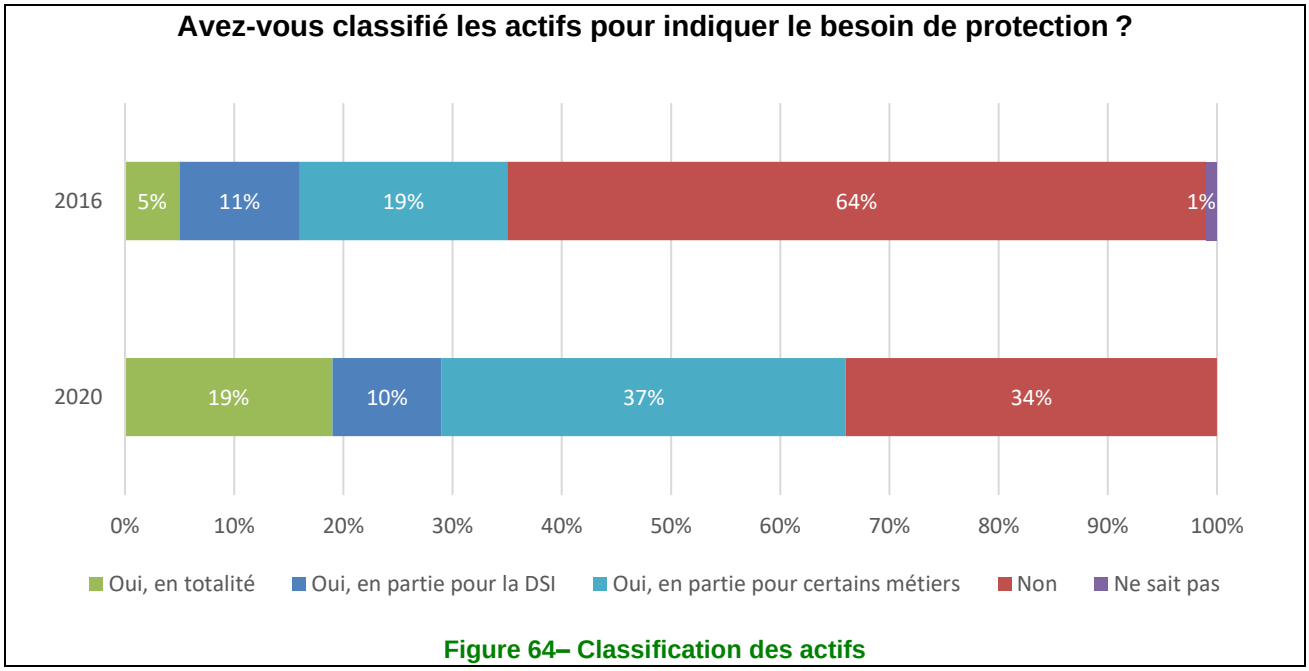


Figure 64– Classification des actifs

Toutefois, bien qu'ayant été multiplié par quatre depuis l'étude MIPS de 2016, le pourcentage de collectivités ayant classifié totalement leurs actifs demeure faible et n'atteint pas le seuil de 20 % sur l'ensemble de l'échantillon, ce pourcentage ne dépassant pas 10 % pour les communes, les communautés urbaines, d'agglomérations, les métropoles et conseils départementaux ou régionaux.

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

Le nombre de niveaux de sensibilité des informations le plus adopté (42 %) est de 2[9], suivi de 3 dans un peu moins de 35 % des cas. Il apparaît ainsi que pour 25 % des collectivités, la classification des actifs se limite à opérer une distinction entre sensible et non sensible !

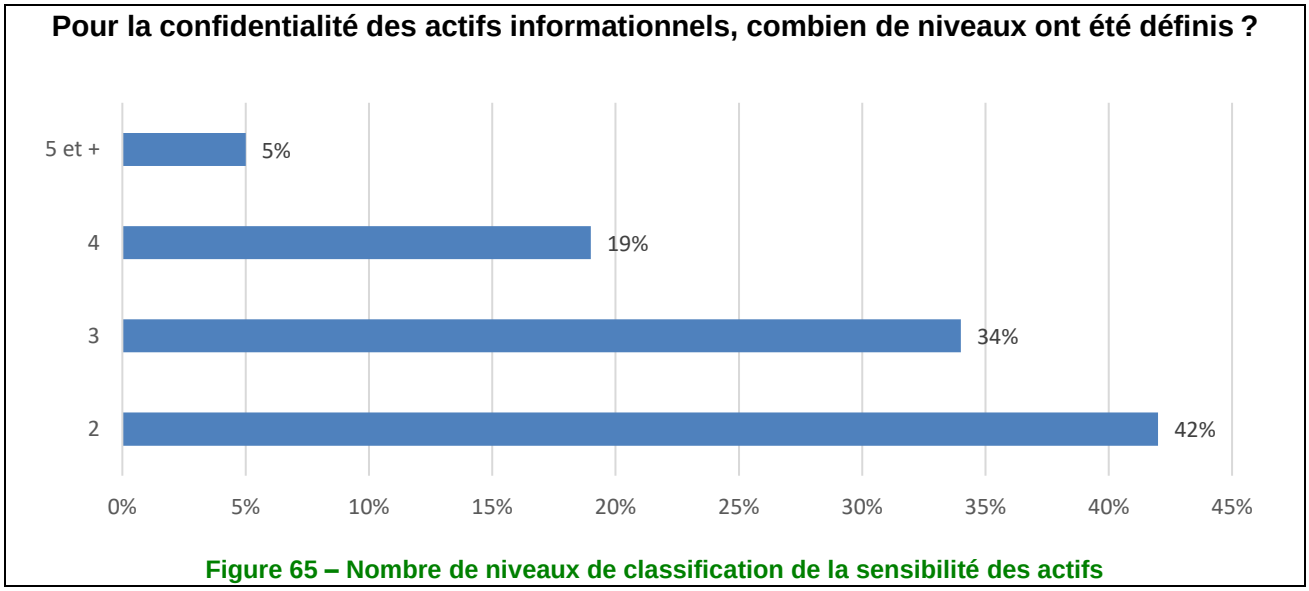


Figure 65 – Nombre de niveaux de classification de la sensibilité des actifs

[9] À noter que cette question a encore reçu quelques réponses anormales ou dénotant une mauvaise compréhension de la question posée (beaucoup de réponses « 0 », « 1 ») dont il n'a pas été tenu compte dans les pourcentages.

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

Un peu plus des trois quarts (76 %) des collectivités interrogées ont procédé à un inventaire au moins partiel des risques. Cependant, très peu (13 %) ont réalisé un inventaire complet de leurs risques.

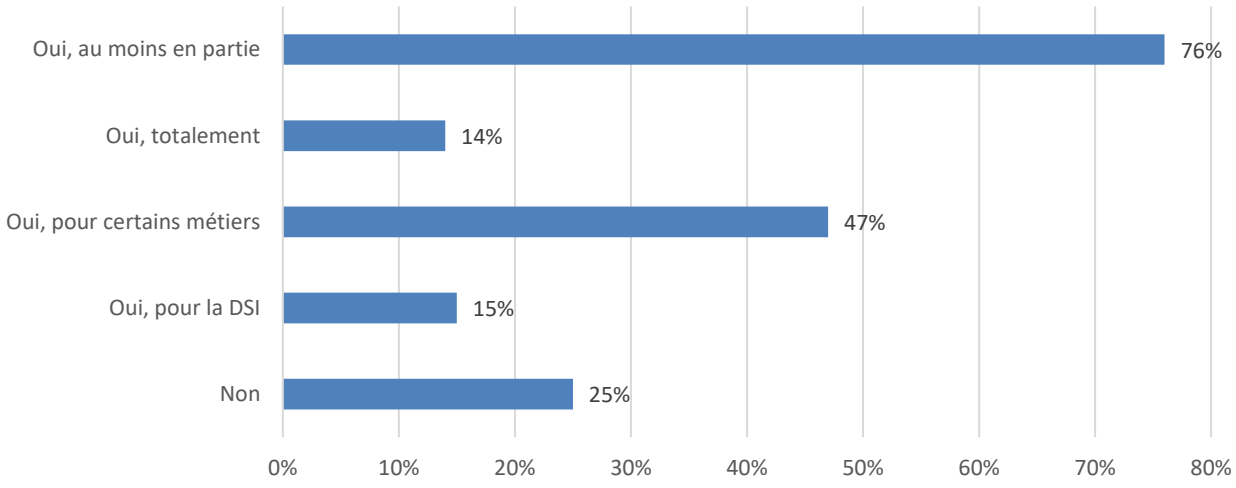


Figure 66 – Inventaire des risques

Notons que parmi les 13 % de collectivités qui ont procédé à un inventaire total de leurs risques, seuls 56 % ont réalisé une analyse formelle de ces derniers. Quant aux collectivités ayant fait un inventaire partiel de leurs risques, elles sont très peu à en effectuer une analyse.

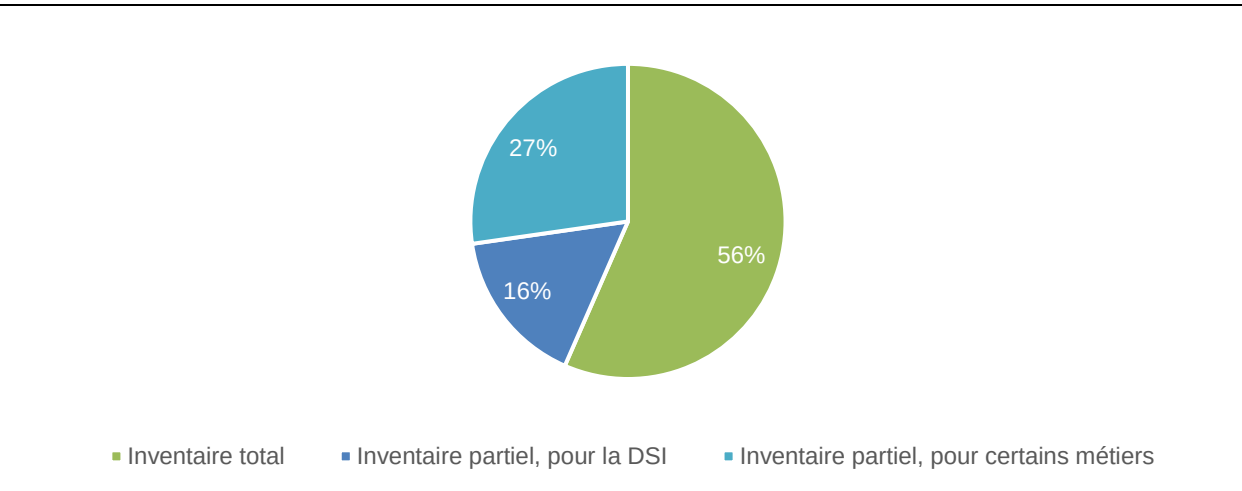


Figure 48 – Part des collectivités ayant effectué, après leur inventaire, une analyse formelle des risques

En d'autres termes, seulement 7 % des collectivités territoriales ont réalisé à la fois un inventaire complet et une analyse formelle de leurs risques.

Les méthodes utilisées pour cette analyse sont diverses, avec des différences notables selon le type d'inventaire effectué.

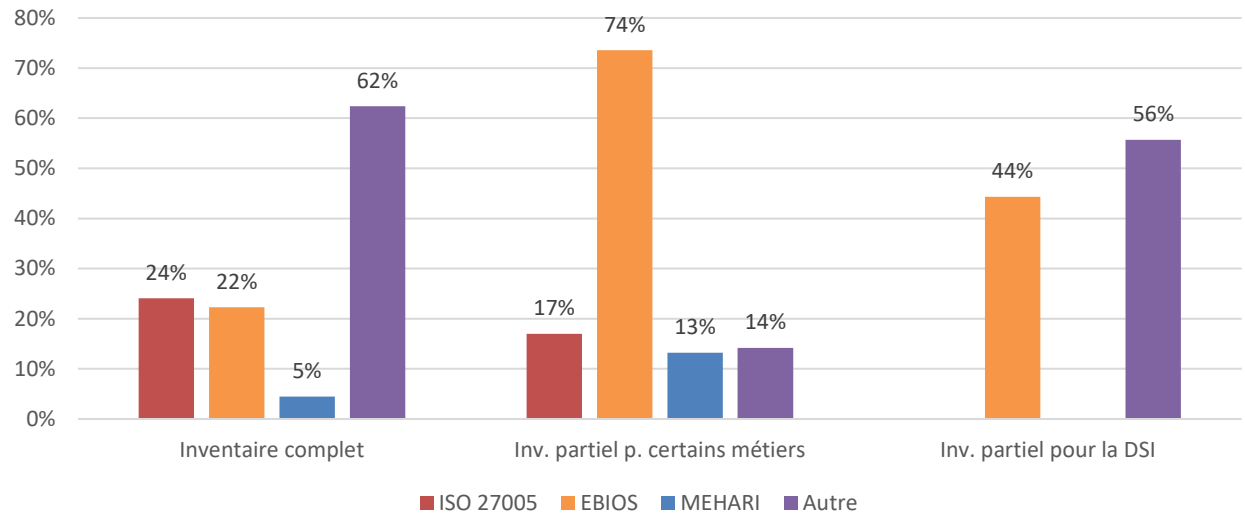


Figure 68 – Méthodes d'analyse des risques utilisées

Notons enfin que, lorsqu'elle est réalisée, l'analyse des risques l'est dans 65 % des cas par le RSSI ou le responsable informatique, ce qui n'est pas surprenant puisqu'il s'agit de leur domaine de compétence et de responsabilité.

Des plans de réduction des risques, même sans analyse formelle des risques

Bien que très peu de collectivités aient effectué un inventaire total et une analyse formelle de leurs risques (7 %), une grande majorité a mis en place un plan de réduction des risques, ce qui nous amène à penser que la plupart des collectivités traitent leurs risques de façon empirique.

Ainsi, les plans de réduction des risques mis en œuvre à la suite de leur inventaire – qu'une analyse formelle ait eu lieu ou non – restent stables et atteignent globalement, pour les plans au moins partiels, 67 %. Parmi les collectivités ayant fait un inventaire complet de leurs risques, 72 % ont élaboré un plan complet de réduction des risques.

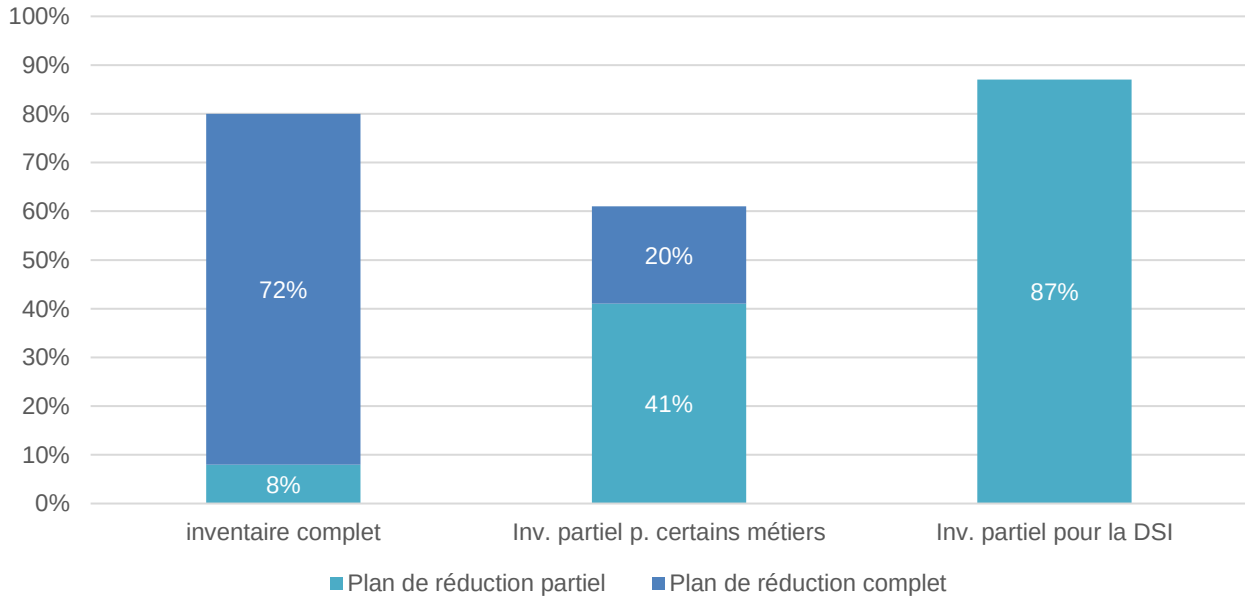


Figure 69 – Mise en place de plans de réduction des risques

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

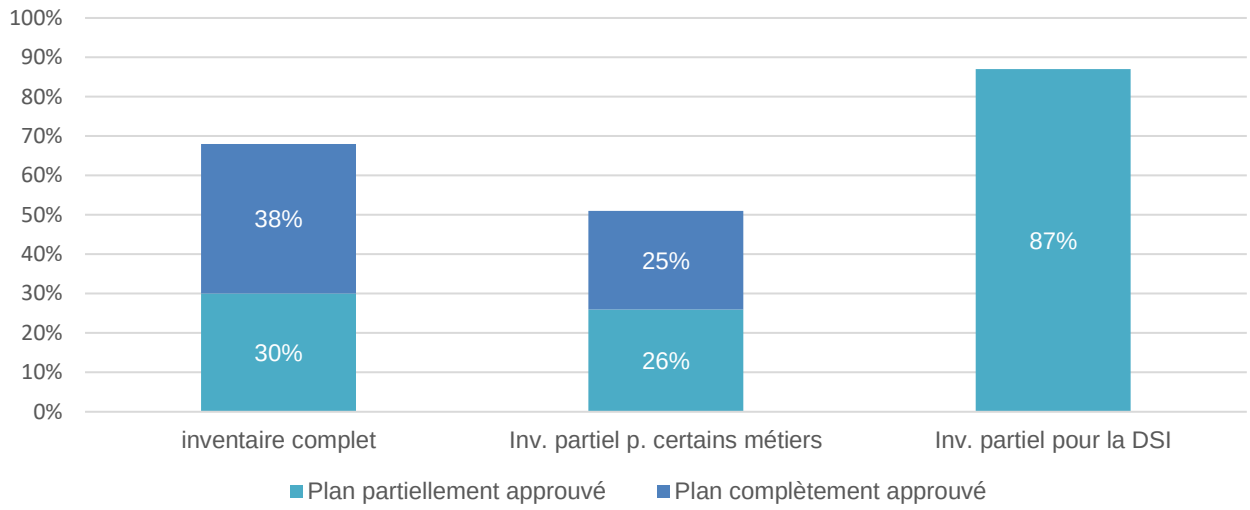


Figure 70 – Acceptation des risques résiduels et validation du plan d'action

Thème 9 : Contrôle d'accès

Technologie/approche de sécurisation

L'étude 2020 montre qu'une plus grande diversité d'outils est désormais en place pour les contrôles d'accès au sein des collectivités :

- les mots de passe non rejouables, en nette progression ;
- les habilitations sur base de profils, également en forte hausse.

Les communautés d'agglomération, les communautés urbaines et les métropoles restent les plus actives dans ce domaine, le fort accroissement de leur population tendant à jouer un rôle important dans le développement de ces technologies. *A contrario,* **les communautés de communes restent encore largement en retrait dans cette approche.** Ceci dénote soit que les enjeux ne sont pas encore pris en compte à la hauteur des risques actuels soit que l'équilibre territorial n'a pas encore été trouvé (problèmes de structure, d'approche, de moyens, etc.).

Une tendance à l'homogénéisation des moyens de contrôle d'accès

L'usage des contrôles d'accès reste très diversifié. Malgré un léger recul, avec respectivement 52 % et 49 % d'utilisation, **l'authentification forte par certificat électronique** sur support matériel et l'authentification par certificat électronique logiciel **restent les plus employées**, comme cela avait été le cas lors des précédentes études de 2012 et de 2016.

On observe une très forte augmentation (+ 18 points) de l'usage de **l'authentification forte par « calculette » à mot de passe non rejouable** par rapport à 2016.

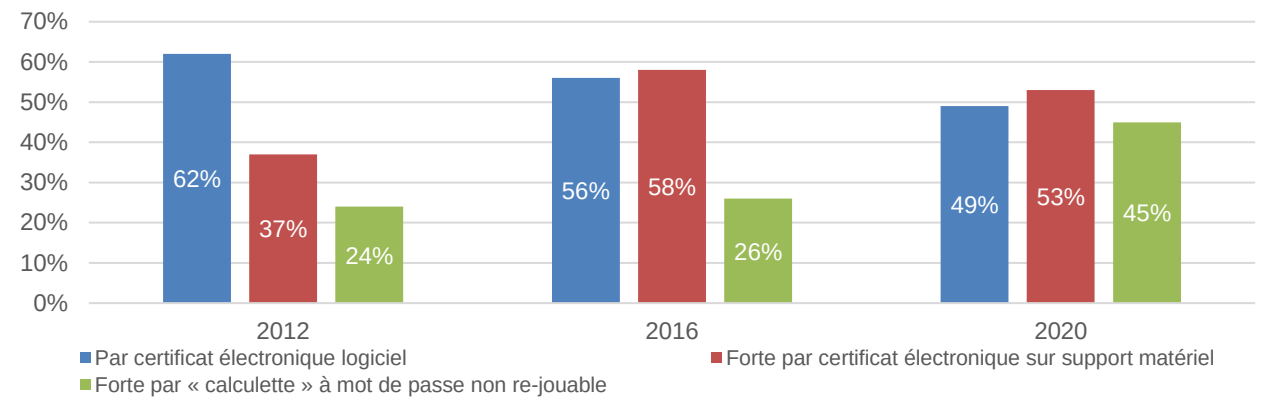


Figure 71 – Technologie/approche de sécurisation par type d'authentification

La progression des approches de type « SSO » reste à un niveau plus ou moins équivalent à ceux observés les années précédentes.

L'emploi des technologies basées sur la biométrie, d'un usage marginal (9 %), reste plébiscité par les plus grosses agglomérations, cependant cet usage est confronté à une réglementation encore très fragile à l'image de la judiciarisation de son emploi. Par ailleurs, les coûts de mise en œuvre pour les villes les plus modestes et soucieuses de la protection de la vie privée des concitoyens restent probablement une difficulté liée à son développement.

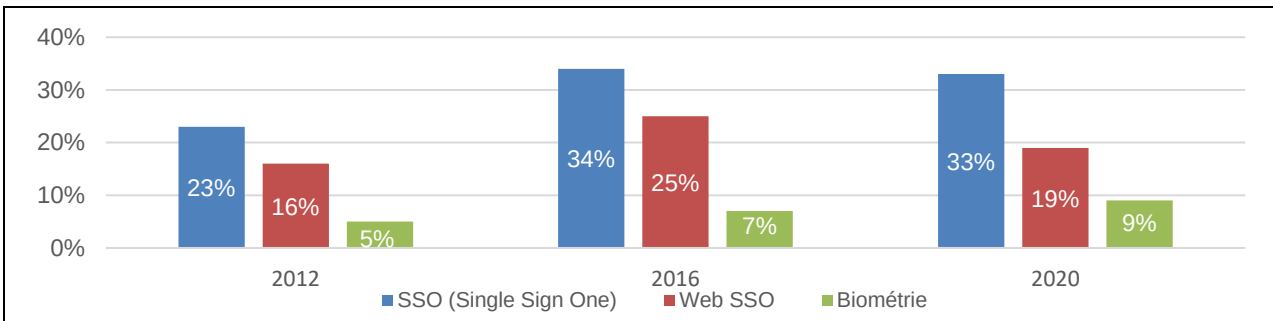


Figure 72 – Authentification – Focus sur les approches technologiques

L'automatisation des tâches contribue cette année encore à une meilleure gestion des droits d'accès

L'usage des **modèles d'habilitation sur base de profils/rôle métier** continue de progresser (+ 5 points), comme cela avait été le cas lors des études précédentes. Cette évolution se démarque par rapport aux *workflows* d'approbation des habilitations qui reculent très légèrement dans cette nouvelle étude (– 2 points).

Le *provisionning* continue quant à lui sa lente progression cyclique avec 25 %, soit une hausse de 1 point par rapport à 2016.

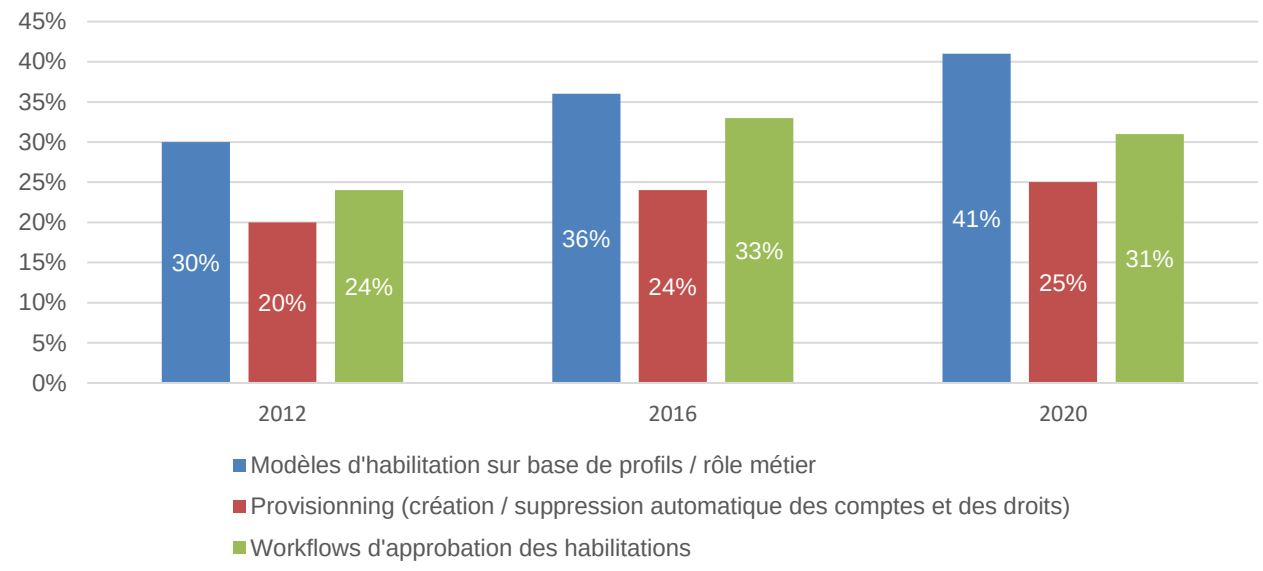


Figure 73 – Authentification – Focus sur les modèles par habilitations/droits

Procédures de gestion des accès : de nettes améliorations dans les procédures de gestion des utilisateurs

On note des progrès sur l'ensemble des procédures de gestion des utilisateurs, même si un tiers des collectivités reste à convaincre.

L'immense majorité (68 %) des collectivités locales déclare disposer d'une procédure formelle de création, modification et suppression de comptes utilisateurs nominatifs. La part des collectivités déclarant avoir une procédure formelle de création, modification et suppression de comptes utilisateurs nominatifs est donc en nette progression (+ 19 points par rapport à 2016), ce qui dénote une prise de conscience avérée sur ces aspects, comme les progrès à la hausse enregistrés pour les points précédemment évoqués.

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

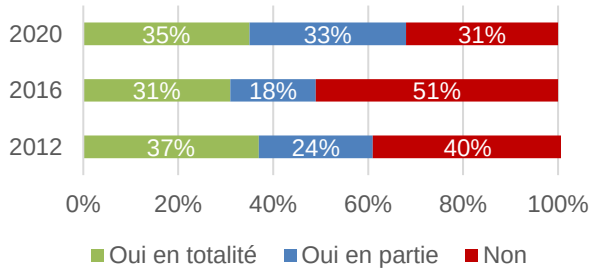


Figure 74 – Procédure formelle de création, modification, et suppression de comptes utilisateurs

Cette même procédure existe-t-elle spécifiquement pour les administrateurs ?

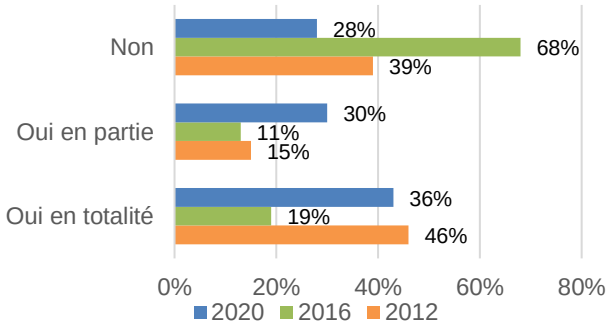


Figure 75 – Procédure spécifique pour les administrateurs ?

En corrélation avec le point précédent, **cette hausse est encore plus marquée lorsque l'on s'intéresse à la population sensible des « administrateurs » (+ 43 points).** Les collectivités apparaissent de plus en plus sensibilisées à l'importance de la mise en place de ces procédures sur les rôles essentiels de leurs activités :

- **35 % des collectivités locales déclarent disposer en totalité d'une procédure formelle** concernant les comptes utilisateurs. Ce chiffre est ramené à 33 % pour les communautés de communes ;

- **64 % des collectivités locales disposent de règles de constitution et de péremption des mots de passe pour tous les accès** (cumul des catégories « Oui, pour tous « et « Oui, pour certains »), soit une progression de 6 points par rapport à 2016. Ce chiffre est ramené à **56 % pour les communautés de communes** qui déclarent disposer de ces règles.

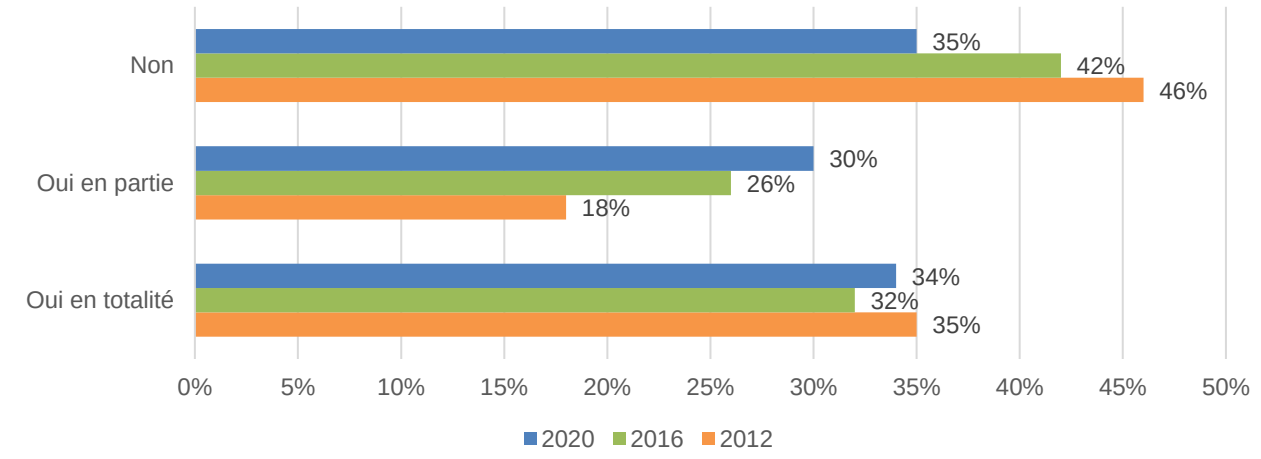


Figure 76 – Règles de constitution et de péremption des mots de passe

À nouveau, **les conseils départementaux et régionaux arrivent en tête des collectivités avec 65 % de « Oui pour tous »,** participant significativement à cette amélioration. Les communautés de communes restent quant à elles à un niveau relativement bas avec seulement **25 % de « Oui pour tous »**.

Thème 10 : Cryptographie

Les moyens de cryptographie n'arrivent toujours pas à percer, mais quand ils sont utilisés, ils participent fortement aux objectifs de sécurité

La cryptographie, moyen de sécurisation des données et de leur transport, reste largement sous-utilisée. Un peu plus d'un tiers (35 %) des collectivités déclarent l'utiliser, mais ce chiffre stable (– 4 points par rapport à l'étude 2016) recouvre une disparité de situations selon le type d'établissements.

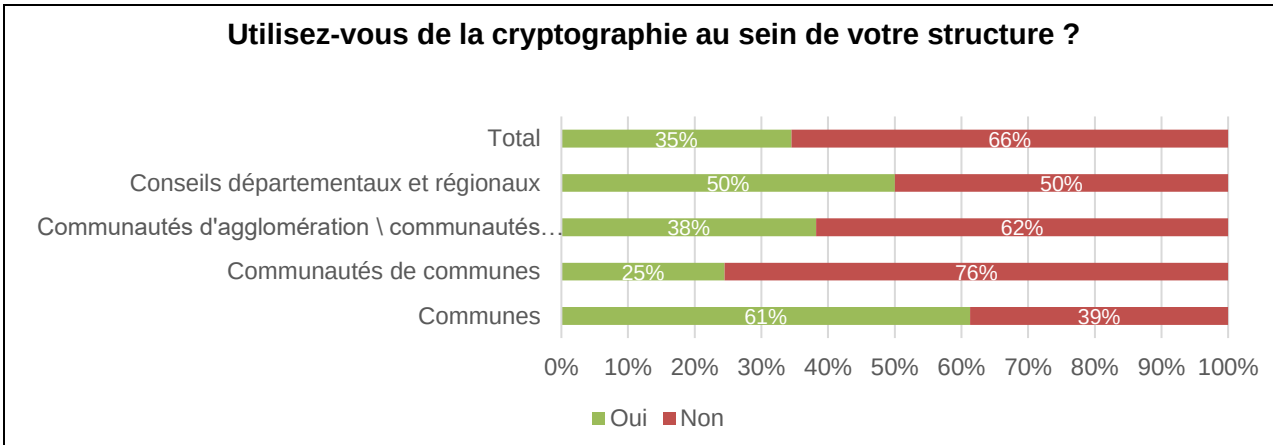


Figure 77 – Usage de la cryptographie par type de collectivité

Les communes sont en effet plus impactées par la dématérialisation de la chaîne comptable (PES v2) et du contrôle de légalité (@CTES), fonctions qui sont rarement mutualisées au sein d'une intercommunalité.

Lorsque cette technologie est utilisée, c'est largement la DSI (72 %) qui porte la responsabilité des moyens cryptographiques (attribution, révocation, destruction des clés). Dans 20 % des cas, ce service est assuré par une autre entité, en interne – Direction des affaires juridiques (4 %) ou Direction des ressources humaines (3 %) – ou délégué à un prestataire externe.

Quand les collectivités les mettent en œuvre, les moyens de cryptographie font l'objet d'un suivi formalisé (cycle de vie des certificats, clés, etc.) dans 55 % des cas. Par rapport à 2016, on note une très forte augmentation des moyens de cryptographie pour le chiffrement des données (84 %, + 65 points), l'authenticité de l'information (65 %, + 42 points), l'authentification des utilisateurs (60 %, + 36 points) ou la non-répudiation d'une action (20 %, + 15 points).

Thème 11 : Sécurité physique et environnementale

Les contrôles d'accès et la surveillance par caméra en très nette progression dans la plupart des collectivités territoriales

Les caméras de surveillance et les contrôles d'accès sont aujourd'hui couramment utilisés dans les collectivités territoriales. Tous les indicateurs progressent en ce qui concerne ces dispositifs implémentés, d'autant que les récentes règles de la Commission nationale de l'informatique et des libertés (Cnil) viennent encadrer la mise en place de l'ensemble de ces dispositifs, ce qui permet de garantir le respect des droits de chacun.

La protection des données sur support physique amovible (clé USB, bande, CD, papier, etc.) est, elle aussi, en nette progression : 60 % des collectivités locales déclarent ainsi protéger leurs données sur ce type de supports dans le cadre de la PSSI (+ 16 points par rapport à 2016), ce qui laisserait penser que celles-ci sont aujourd'hui plus sensibilisées à la protection des données sur supports physiques.

Ce sont les **communautés d'agglomération/communautés urbaines et les métropoles qui seraient les plus impliquées**, 71 % (+ 1 point par rapport à 2016) déclarent l'avoir intégrée.

Comme indiqué dans le graphique ci-dessous, **les communes seraient les plus démunies, plus de 65 %** d'entre elles indiquant ne pas encore protéger leurs données sur supports physiques.

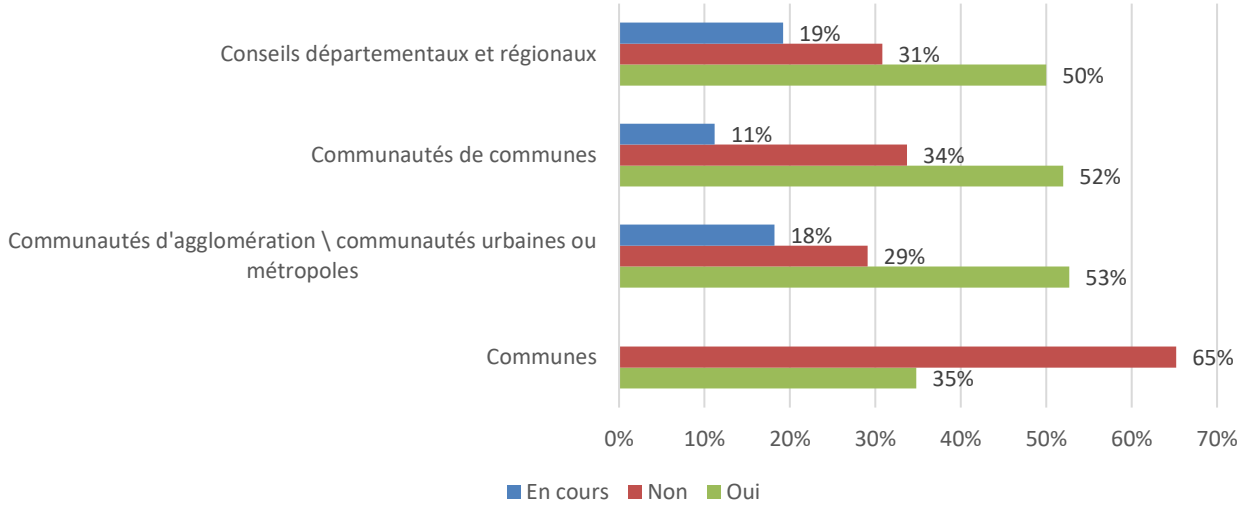


Figure 78 – Collectivités déclarant protéger leurs données sur support physique

La majorité (67 %) des collectivités locales déclarent avoir des dispositifs pour sécuriser l'accès aux salles machines, alors que ce chiffre n'était que de 50 % en 2016.

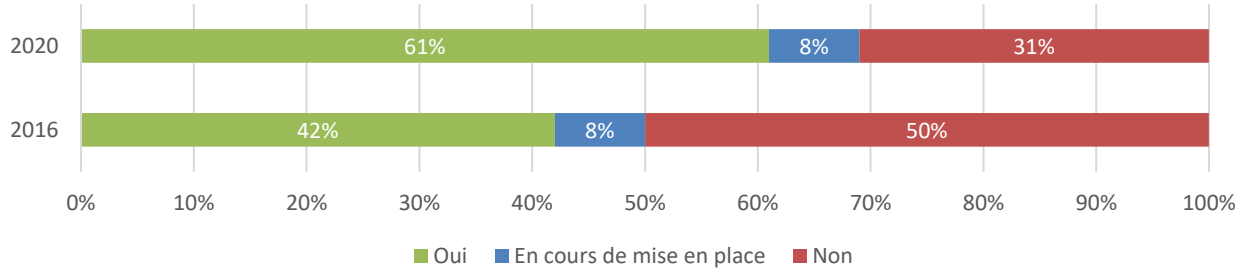


Figure 79 – Sécurisation de l'accès aux salles machines

Un système de détection incendie serait installé dans 49 % des cas. Les collectivités seraient, semble-t-il, moins vulnérables aux inondations, **12 % se protégeraient contre un dégât des eaux, une fuite des canalisations d'eau ou bien encore une montée des eaux.**

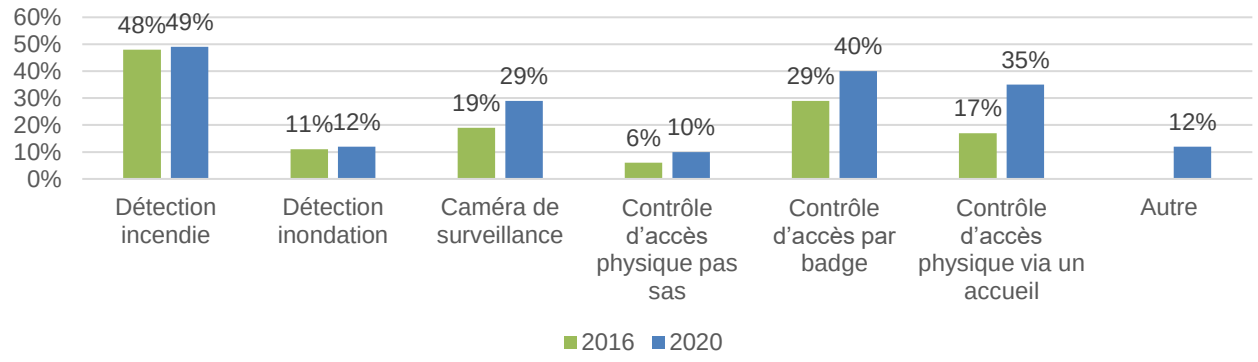


Figure 80 – Contrôle d'accès et détection

À noter, **le contrôle d'accès physique *via* un accueil subit la plus forte progression avec (35 %)**, soit 13 points de plus qu'en 2016.

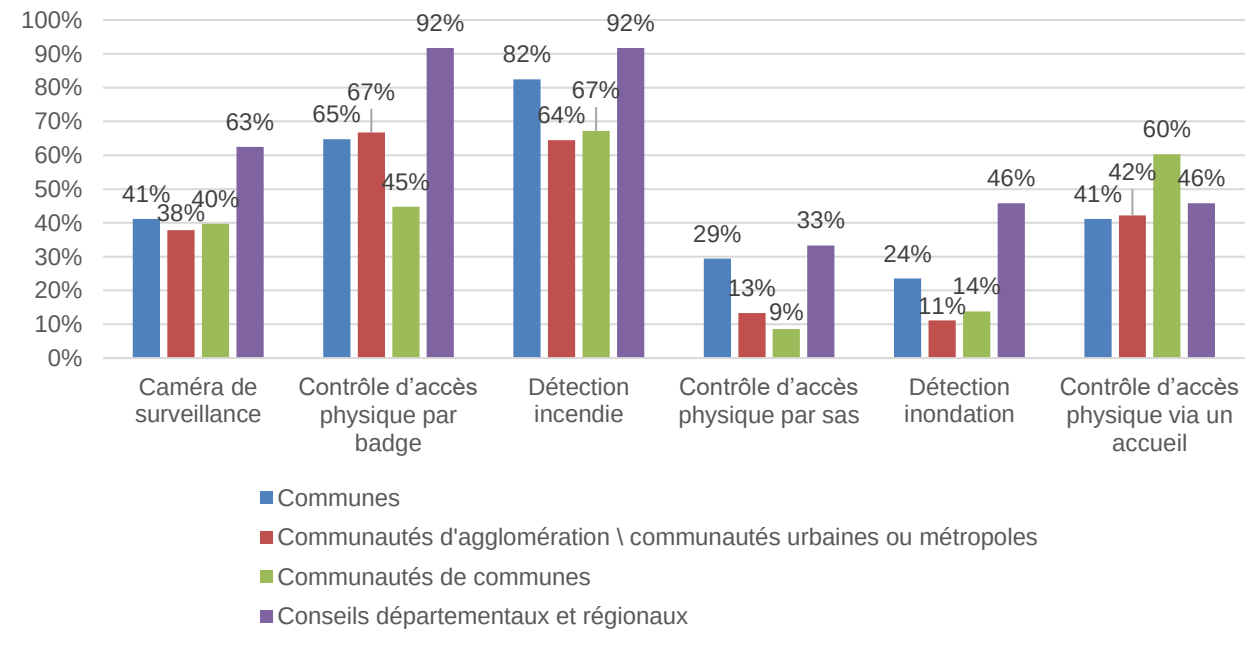


Figure 81 – Types de contrôle d'accès

Le contrôle d'accès par badge est le plus utilisé et serait souvent renforcé par un contrôle d'accès physique *via* un accueil ou bien des caméras de surveillance.

Dans plusieurs cas, **on observe des pratiques moins soutenues dans les communautés d'agglomération/communautés urbaines ou les métropoles**, contrairement à ce qui avait été observé en 2016.

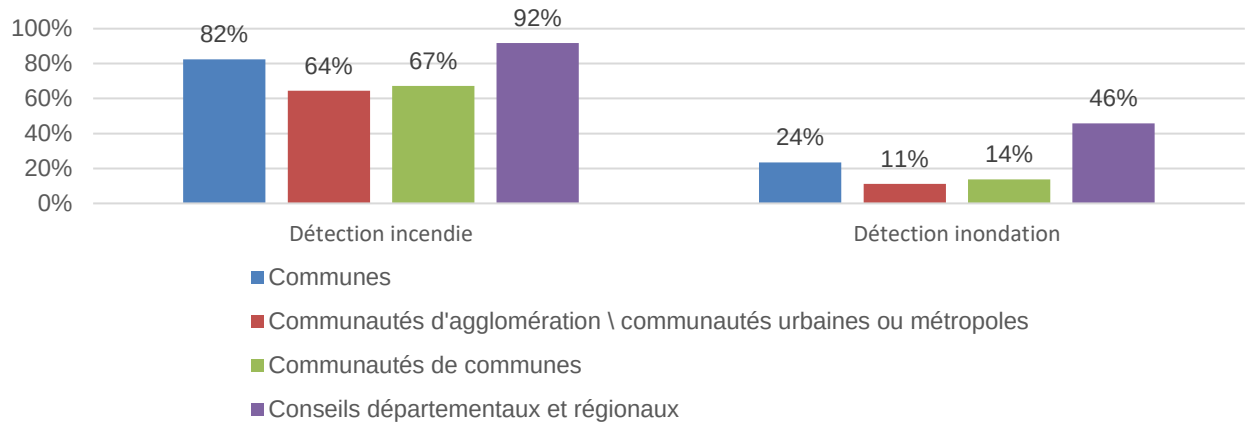


Figure 82 – Détection incendie/inondation

Thème 12 : Sécurité liée à l'exploitation

Protection contre les menaces « logiques » : une première barrière installée, une diversification de solutions engagée, mais encore trop en retard pour détecter et protéger

L'actualité en matière de cybersécurité a confirmé l'augmentation constante de la menace et des attaques, faisant de chaque acteur de notre société une cible potentielle. Ces dernières années, les collectivités, encore insuffisamment armées pour détecter et contenir des attaques parfois très virulentes sont passées de cibles potentielles à victimes avérées.

Souvent initiées de manière opportuniste, les intrusions dans un SI sont ensuite orchestrées de façon méthodique pour maximiser le bénéfice de l'attaquant en procédant à un vol de données suivi du déploiement d'un rançongiciel, rendant inopérant un maximum de systèmes.

Pour tenter d'y faire face, les collectivités ont mené une consolidation d'un premier niveau de sécurisation, centré sur les postes de travail. En effet, le déploiement des outils dits « classiques/traditionnels » pour la protection contre les codes malveillants connus (antivirus) ou le blocage des courriels indésirables (antispam) est devenu systématique. L'activation du pare-feu, bien que légèrement en retrait par rapport aux deux

précédentes solutions (82 % *vs* respectivement 96 % et 91 %) semble également perçue comme indispensable pour limiter, entre autres, les propagations latérales d'un attaquant.

Les outils traditionnels quasi généralisés

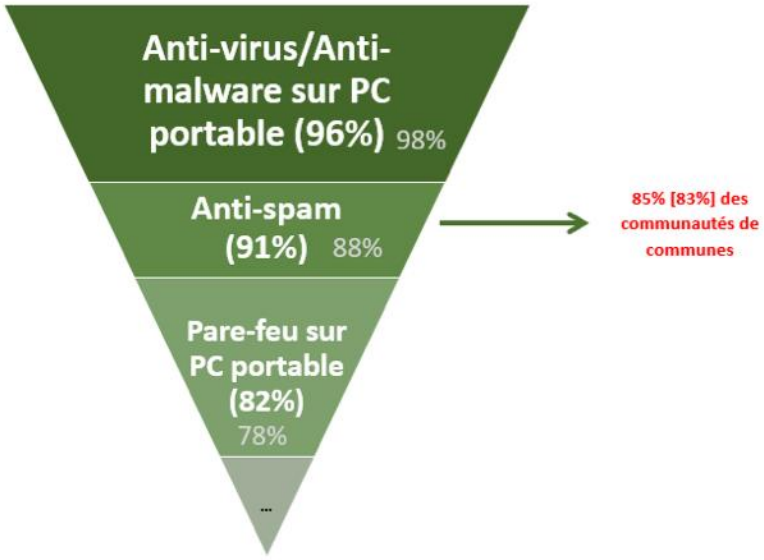


Figure 83 – Les outils traditionnels quasi généralisés désormais…

Ces premières solutions, installées et maîtrisées, représentent un début de réponse à la règle 14 « Mettre en place un niveau de sécurité minimal sur l'ensemble du parc informatique » du guide d'hygiène de l'Anssi[10]**.**

Les collectivités semblent avoir également engagé d'autres travaux de diversification des outils de sécurité.

Une plus grande diversité d'armes de sécurisation…

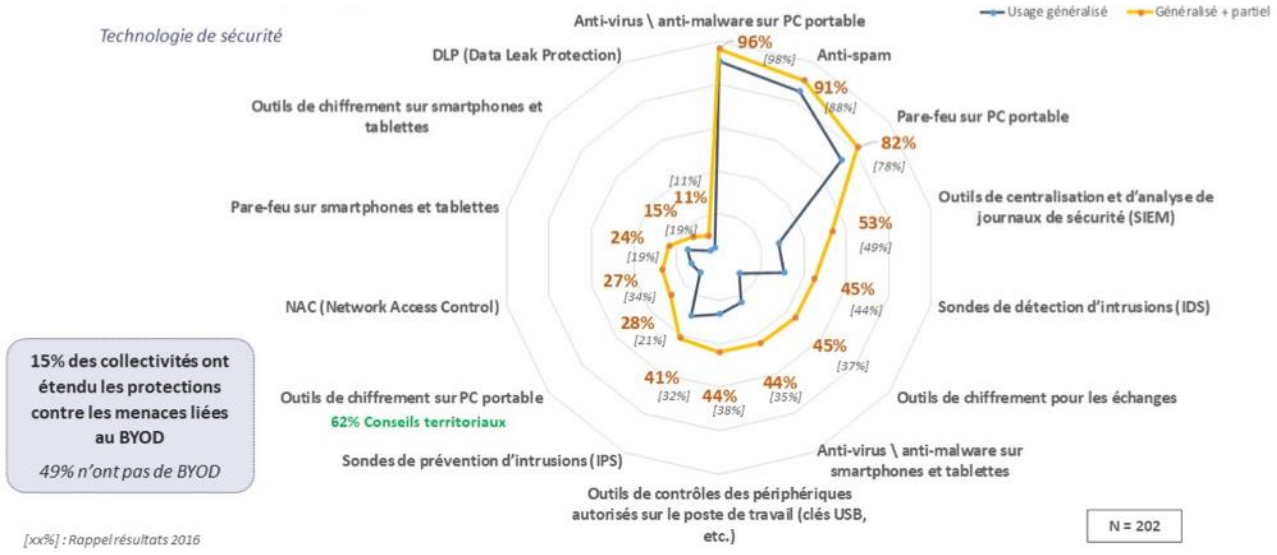


Figure 84 – Une plus grande diversité d'armes de sécurisation…

[10] https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf

Malgré l'effort réalisé sur les postes de travail des agents, on constate que les équipements mobiles (tablettes et smartphones), indispensables pour **favoriser la mobilité des agents**, restent en retrait au niveau de la sécurité malgré une évolution notable concernant la présence d'un antivirus de + 9 points.

Depuis l'entrée en vigueur du RGPD en 2018, les collectivités cherchent à répondre, avec leurs moyens, aux enjeux de sécurité, en particulier celui de la confidentialité des données. En effet, on note un usage renforcé du chiffrement, solution clé à la protection des données :

- chiffrement sur PC portable : + 7 points (par rapport à 2016), mais toujours très en retrait par rapport à la pratique en entreprise ;
- chiffrement pour les échanges : + 8 points.

Pour autant, les solutions pour se prémunir contre la perte de données (*Data Loss Prevention* – DLP), dont l'objectif est de prévenir la perte de données et d'en interdire les sorties non autorisées du SI, n'ont pas évoluées par rapport à 2016. Ce type de projet est coûteux et complexe à mettre en œuvre. Il nécessite de disposer d'une cartographie et d'une classification des données afin de déterminer celles à protéger et à surveiller prioritairement. Sujet d'autant plus complexe que les collectivités territoriales collectent, stockent et manipulent toujours plus de données, tout en répondant aux besoins de l'*open data*.

Concernant la supervision et la protection des événements sur le réseau, malgré un net recul des dispositifs NAC (– 7 points) permettant uniquement aux appareils autorisés de se connecter au réseau, les collectivités tentent d'améliorer leur capacité de détection et de blocage, respectivement par l'intermédiaire de sondes IDS (+ 1 point) et IPS (+ 9 points). Cette volonté d'être en mesure de repérer au plus tôt les attaques se traduit par le franchissement du cap de plus de la moitié (53 %) des collectivités ayant intégré un SIEM, mais, qui ne couvre généralement que partiellement la collecte des traces générées au sein de leur SI et encore trop peu leur analyse. Cela sera largement amplifié par les obligations imposées aux organisations qui sont/seront considérées comme OIV, en l'occurrence l'obligation de disposer d'un dispositif de surveillance permettant d'identifier les incidents impactant leur système d'information d'importance vitale (SIIV).

Les collectivités semblent donc évoluer et s'armer en diversifiant leurs solutions de sécurité, mais cette démarche tardive prend beaucoup de temps et nécessite des ressources et de l'expertise qui font souvent défaut. De fait, les collectivités sont encore très exposées aux risques cyber et auront encore du mal à prévenir et détecter la menace qui progresse, se spécialise et s'intensifie. À titre de comparaison, les chiffres concernant les technologies de sécurité des collectivités, malgré une légère évolution positive, n'atteignent pas ceux constatés en 2016 pour les entreprises, ce qui représente un retard de près de cinq ans. Il devient urgent d'identifier les freins au déploiement de ces solutions nécessaires à une protection efficace des équipements et des données constituant les SI de nos collectivités.

La gestion des vulnérabilités technique : malgré un processus de veille qui s'installe, la formalisation des procédures et des déploiements des correctifs

Les vulnérabilités techniques sont de potentiels points d'entrée, des opportunités de propagation ou encore des « munitions » pour un attaquant pour réaliser différentes attaques à l'encontre du SI d'une collectivité : vol de données, déni de service, destruction, etc.

En conséquence, les collectivités se doivent d'être en mesure d'identifier les vulnérabilités de leurs systèmes puis, dans un délai raisonnable et cohérent par rapport aux risques induits, de remédier, le cas échéant, à ces faiblesses détectées.

Pour être en mesure de réaliser cela, il faut se tenir informé des nouvelles vulnérabilités découvertes, de l'évolution des scénarios d'attaque, mais également des solutions de sécurité. Cette activité de veille apparaît en nette progression, passant d'à peine 50 % en 2016 à 88 % en 2020. La médiatisation et la récurrence des attaques sont probablement un facteur de ce phénomène ; pour autant, la veille reste empirique, consistant à collecter des informations sur des sites, magasines ou flux RSS spécialisés.

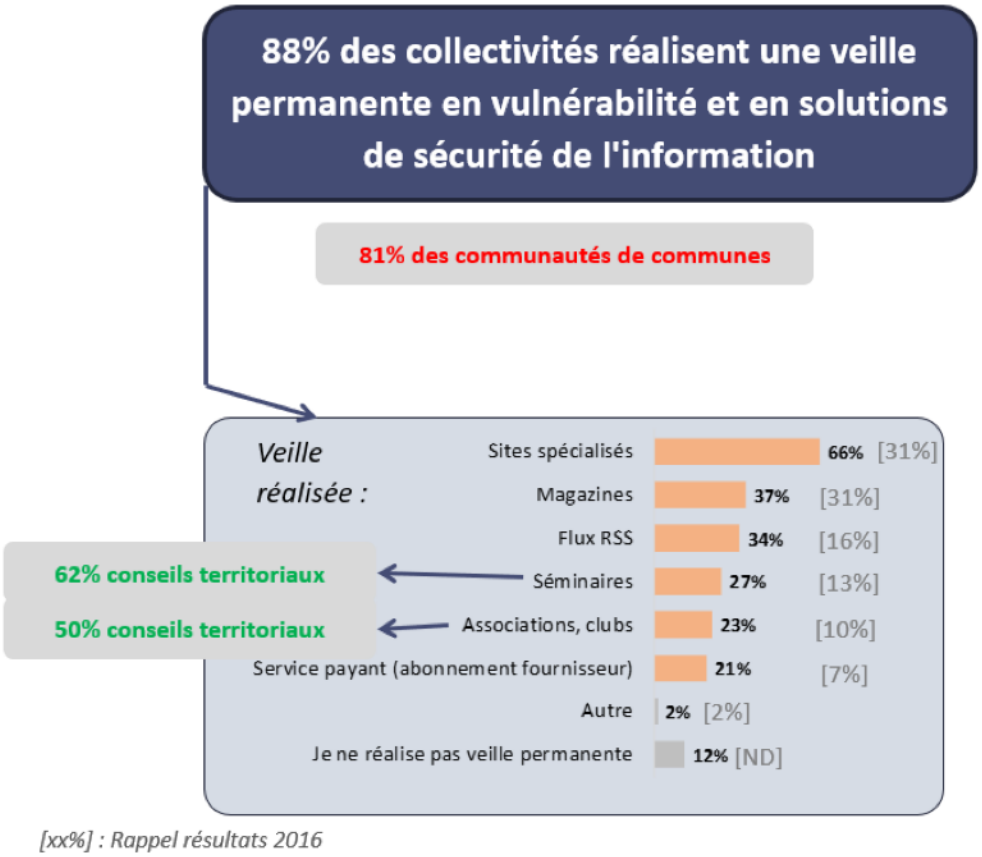


Figure 85 – Des veilles permanentes généralisées…

Le processus de veille n'est pas systématiquement défini en cohérence avec les systèmes implémentés dans les collectivités.

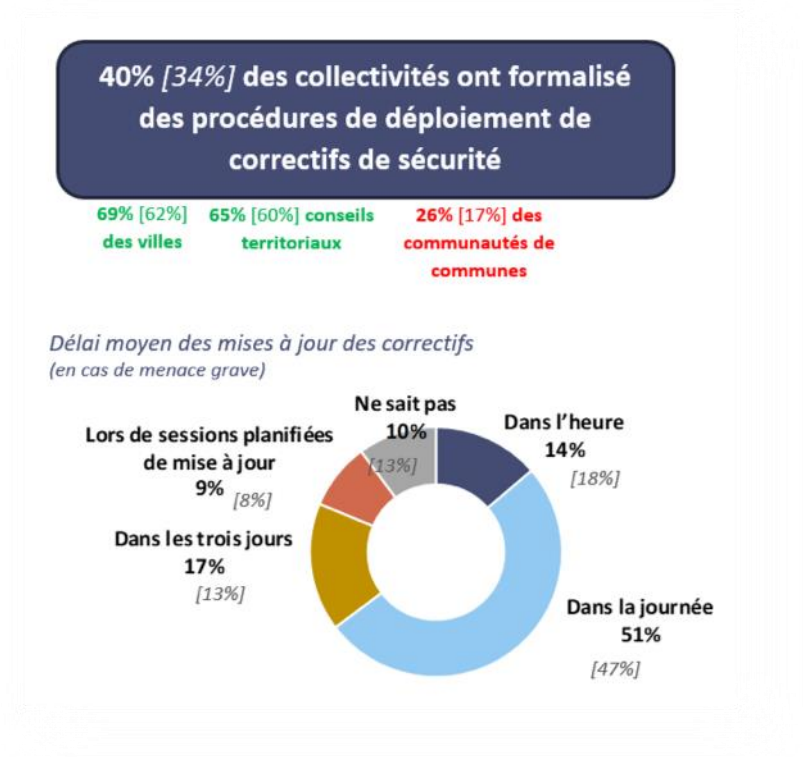


Figure 86 – La formalisation des procédures progresse péniblement…

Du côté des procédures associées à la gestion des correctifs de sécurité, la mise en place de la veille technologique n'a pas eu un impact direct sur la progression, qui n'est pas aussi marquée, passant péniblement de 34 % en 2016 à 40 % quatre ans plus tard. À l'instar de ce que nous avions constaté en 2016, des disparités entre types de collectivités sont toujours très présentes. En effet, malgré une augmentation plus significative au niveau des communautés de communes, + 9 points atteignant 26 %, ce type de collectivité reste nettement en retrait par rapport, par exemple, aux communes avec 69 %.

Ce constat de la difficulté à traiter la gestion des correctifs de sécurité est confirmé par les délais de réactivité qui ne se sont pas spécialement améliorés, voire ont légèrement régressé au niveau du déploiement dans l'heure en cas de menace grave (– 4 points).

Des efforts sont à noter sur le périmètre de la sécurité liée à l'exploitation, mais cela reste encore trop timide pour répondre aux problématiques et enjeux actuels et à venir. La difficulté à disposer de ressources humaines compétentes, formées à la cybersécurité et pérennes, associée à des capacités salariales plus faibles que dans le privé limite fortement les possibilités de recrutement dans les collectivités.

Thème 13 : Sécurité des communications

Ouverture accrue des SI à l'extérieur, accompagnée d'une méfiance accrue vis-à-vis des équipements non maîtrisés (BYOD)…

Par rapport à l'enquête précédente, l'accès aux SI depuis l'extérieur par des équipements maîtrisés (fournis par les collectivités) augmente significativement.

En 2020, 83 % des collectivités autorisent l'accès aux SI depuis l'extérieur par un poste maîtrisé, contre 74 % en 2016.

À l'inverse l'autorisation de l'usage d'un poste non maîtrisé est en baisse. Il est autorisé par 33 % des collectivités en 2020 contre 40 % en 2016.

Pour l'accès aux SI depuis des tablettes et des smartphones, le même constat se retrouve. Leur usage quand c'est la collectivité qui les fournit est en augmentation, passant de 66 % en 2016 à 75 % en 2020. Cependant l'autorisation de l'usage des tablettes et des smartphones non fournis par les collectivités (BYOD) baisse quant à lui fortement : 31 % les autorisent en 2020 contre 46 % en 2016.

L'utilisation de la messagerie instantanée et des réseaux sociaux est de plus en plus tolérée aujourd'hui, l'autorisation de l'usage de la messagerie instantanée passant de 64 % en 2016 à 79 % en 2020, et celle des réseaux sociaux, de 66 % à 86 %.

L'acceptation de l'usage de la VoIP et de la téléphonie sur IP augmente de 25 % pour s'établir à 81 % en 2020 contre 56 % en 2016, de même que celle du Wi-Fi qui progresse à 76 % en 2020 contre 68 % en 2016.

Enfin, l'autorisation de l'accès au Web sans-filtrage d'URL connaît une légère hausse pour atteindre 39 % en 2020 contre 34 % en 2016. La part des collectivités qui l'autorisent sans condition est de 13 %.

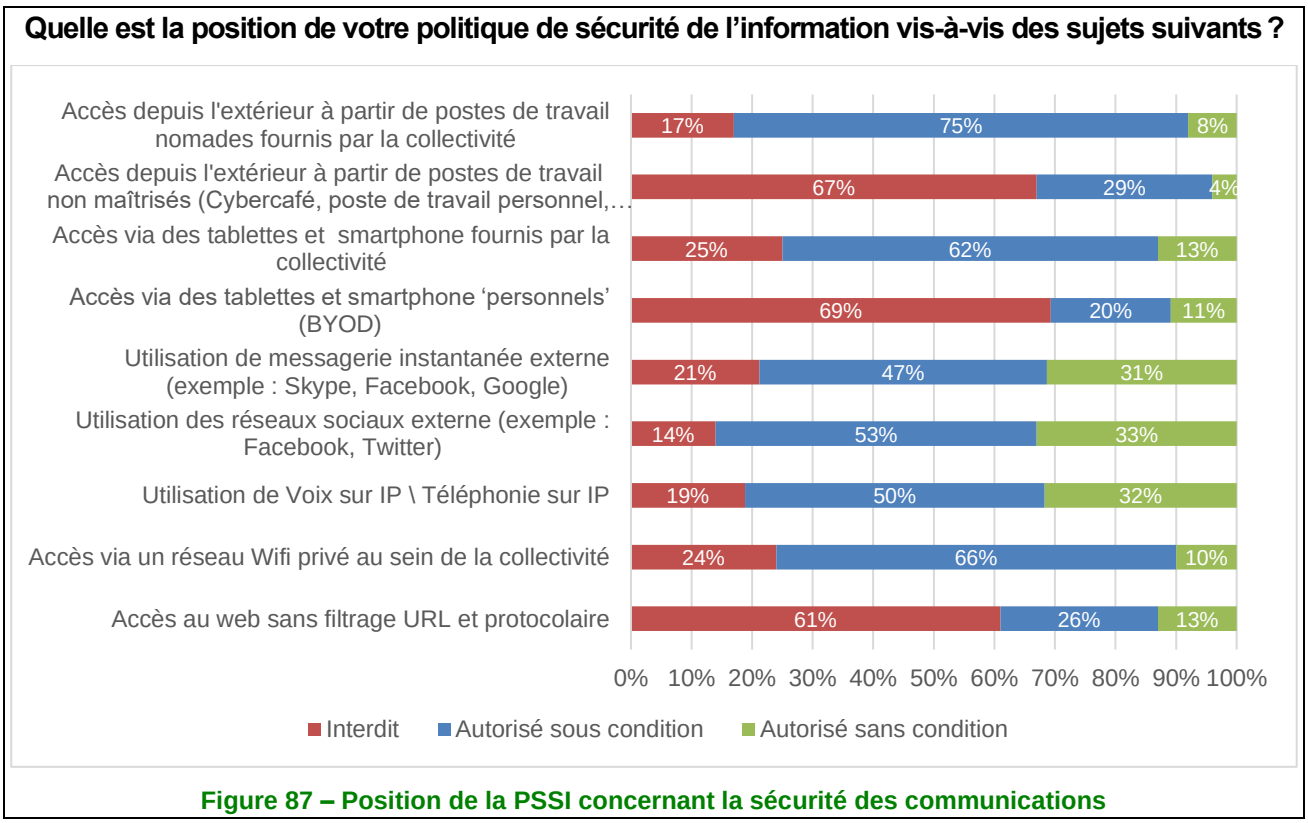


Figure 87 – Position de la PSSI concernant la sécurité des communications

Thème 14 : Acquisition, développement et maintenance du SI

Les concepts de développement sécurisé toujours pas mis en œuvre

Le constat relatif à l'absence de développeur dans les collectivités territoriales dénoncée dans l'étude MIPS de 2016 reste tout à fait d'actualité en 2020. Il permet d'expliquer le fait que les concepts de base de sécurité en développement ne soient majoritairement pas mis en œuvre avec une constance sur les trois études. Les DSI privilégient alors les solutions « sur étagère » ou le recours à des prestataires en développement.

L'absence de connaissances dans le développement sécurisé a pour conséquence des exigences minimalistes dans les cahiers des charges. Les éditeurs de progiciels ne sont alors pas contraints par des exigences de sécurité et les solutions développées peuvent présenter des failles ou des usages dangereux. Comme la majorité des collectivités expriment peu d'exigences, lorsqu'une vient à se poser, la structure se heurte soit à une absence de réponse, soit à un coût exorbitant pour y répondre…

Se pose ainsi la question : quel est le socle minimal d'exigence portant sur la SSI, entre autres, qu'il apparaît impératif d'exiger fermement dans un cahier des charges quitte à risquer un retour infructueux ? Cette question peut être posée sous une autre forme : quelles sont les exigences en matière de SSI dont le non-respect fait courir un risque estimé supérieur au risque de non-réponse ? Tant que chaque collectivité n'aura pas pris conscience de l'existence de cette question et n'aura pas fourni de réponse claire et ferme, aucun éditeur ou développeur spécialisé n'aura d'intérêt, notamment financier, à travailler de façon pertinente la sécurité de ses applications.

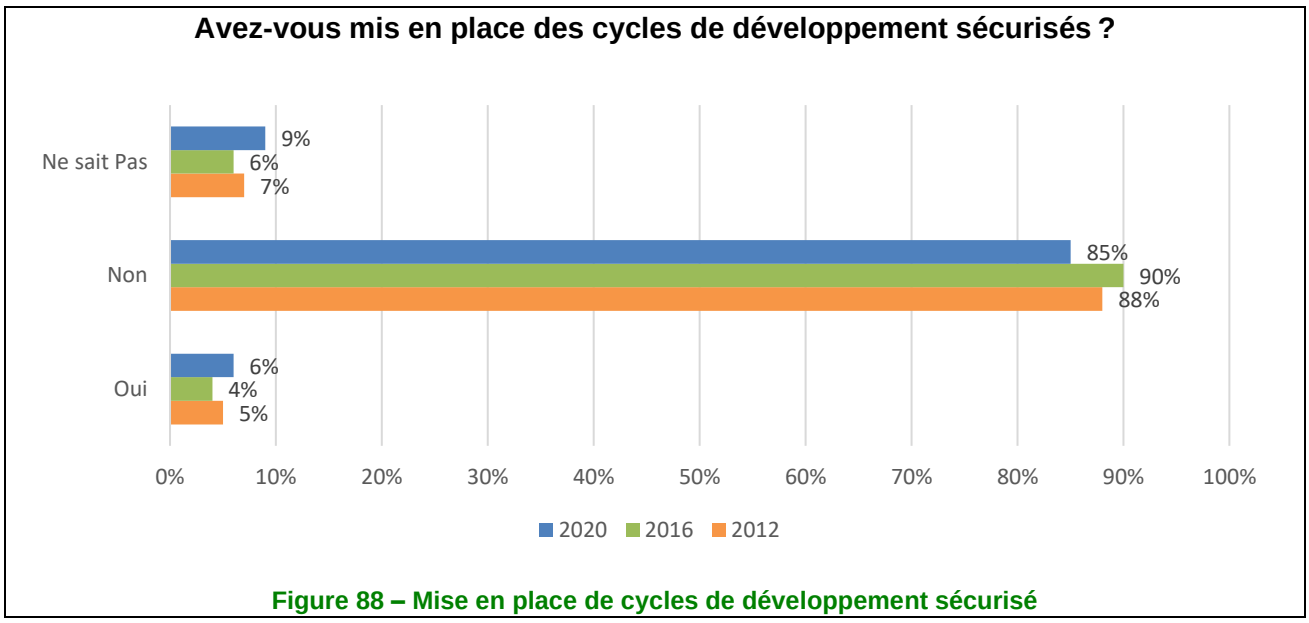


Figure 88 – Mise en place de cycles de développement sécurisé

Pour la faible part de collectivités indiquant mettre en œuvre du développement sécurisé, c'est le pragmatisme qui domine dans 65 % des cas, plutôt que le recours à des référentiels ou des normes.

Absence de référent sécurité pour les développements entraînant une absence de contrôle

Corollaire de ce que nous évoquions en début de thème, les collectivités sont globalement démunies concernant la présence d'un référent définissant les règles et bonnes pratiques de développement.

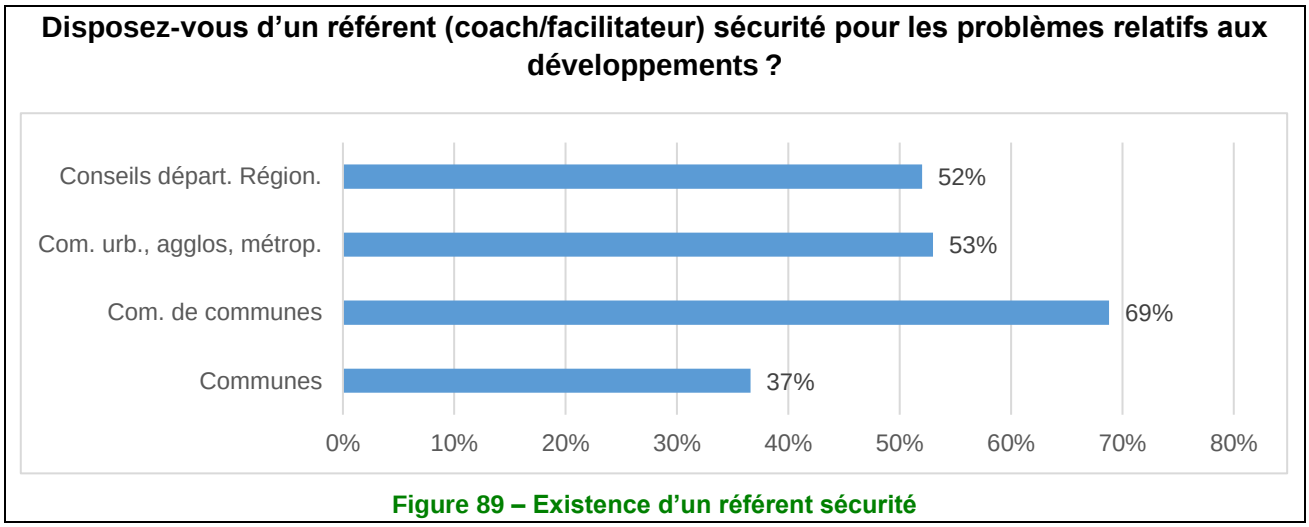


Figure 89 – Existence d'un référent sécurité

Cette situation entraîne inévitablement une absence de contrôle sur les applications internes pouvant conduire à des lacunes importantes de sécurité (failles, utilisation de protocoles non sécurisés…).

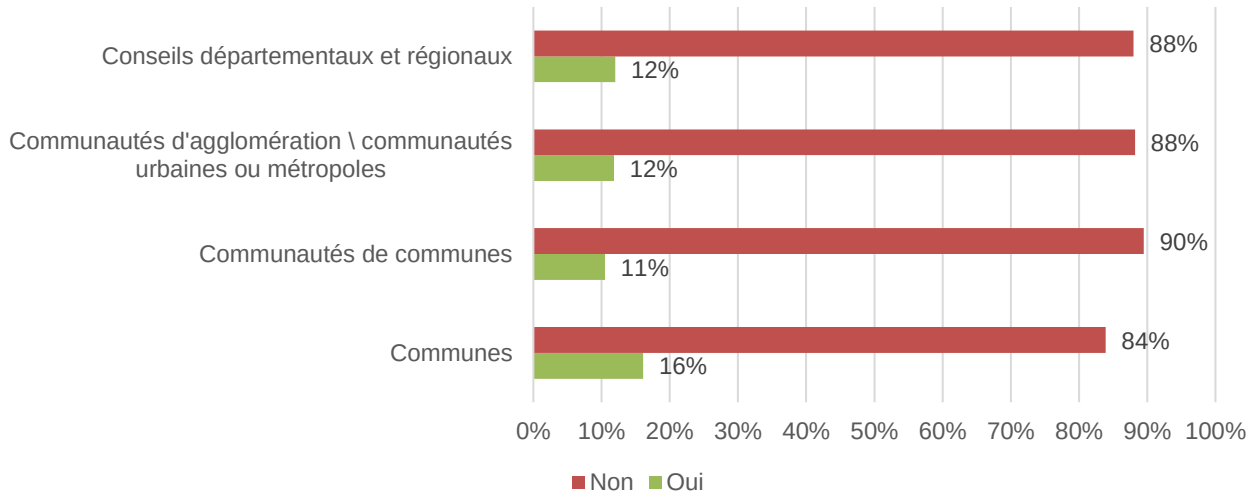


Figure 90 – Réalisation de contrôle de code

Le fait qu'il n'existe pas de fonction dédiée au contrôle de la sécurité du code semble déterminer l'absence de mise en œuvre de ces contrôles. Ce problème pourrait être partiellement contourné par deux possibilités qui *de facto* ne semblent pas exploitées : le transfert de cette tâche aux spécialistes du génie logiciel et l'utilisation d'applications capables de contrôler automatiquement la qualité du code, y compris sur les aspects sécurité.

Cette situation de non-contrôle peut également laisser supposer que les principes de *DevOps* ne sont pas ou peu mis en œuvre au sein des collectivités, ou tout du moins pas jusqu'au concept de *DevSecOps*.

Par ailleurs, la relative homogénéité des résultats ci-dessus incite à penser que la prise en compte de la SSI dans les développements n'est pas une affaire financière (toutes les tailles de collectivités répondant de manière homogène), mais plus une question d'absence de prise de conscience de ce besoin.

Thème 15 : Relations avec les fournisseurs

Le recours à l'infogérance concerne désormais la majorité des collectivités territoriales, avec en tête les communautés de communes

Alors qu'il y a quatre ans se posait la question d'un retour à l'internalisation à la suite d'une baisse du recours à l'infogérance, on assiste en 2020 à un doublement des collectivités déclarant recourir à l'externalisation de leur SI par rapport à 2016. Elles sont désormais 60 % à la confier à un prestataire externe, que ce soit en partie (43 %) ou en totalité (17 %). L'externalisation partielle reste donc bien plus importante que l'infogérance totale.

Les collectivités ayant recours à l'externalisation représentent 69 % des communautés de communes, 53 % des communautés d'agglomération, 52 % des conseils départementaux et régionaux ainsi que 37 % des communes.

Avez-vous placé tout ou partie de votre système d'information sous contrat d'infogérance (réponse = oui) ?

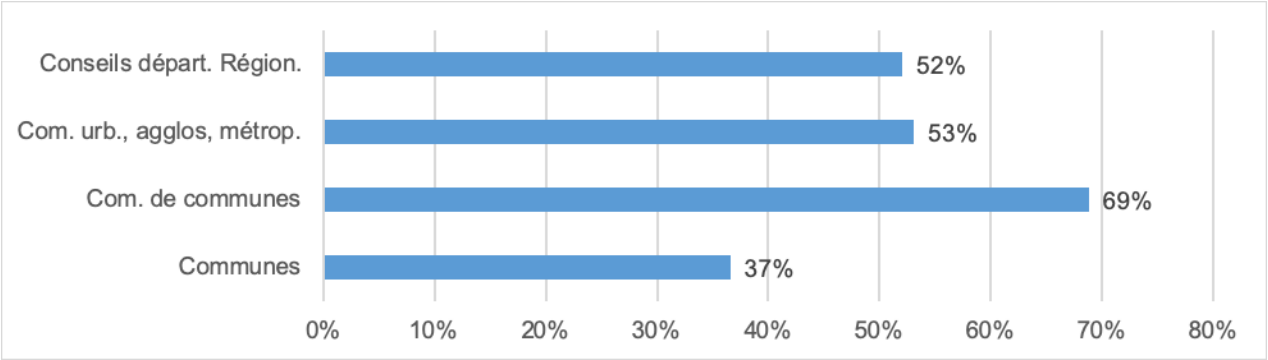


Figure 91 – Collectivités ayant placé tout ou partie de leur système d'information en infogérance

L'externalisation de la totalité du SI concerne 25 % des communautés de communes qui sont des collectivités de plus petite taille et demeure faible pour les communes (3 %), les conseils départementaux et régionaux (4 %) et les communautés d'agglomération (6 %).

L'externalisation partielle du SI demeure également plus faible dans les communes (33 %) que dans les autres formes de collectivités (44 % à 48 %).

Le contrôle de l'infogérance progresse : *via* les audits, mais pas *via* les indicateurs

Ce doublement de la surface des déclarations de recours à l'infogérance s'accompagne d'une progression sensible de son contrôle *via* des audits de sécurité (51 % des collectivités en 2020 contre 35 % en 2016). Ce recours aux audits de sécurité est majoritairement le fait des communes à 73 %, contre 46 % à 50 % pour les autres types de collectivités.

Effectuez-vous ou faites-vous effectuer des audits sur cette infogérance (sécurité technique des matériels, sécurité des informations transmises ou stockées, continuité d'activité…) ?

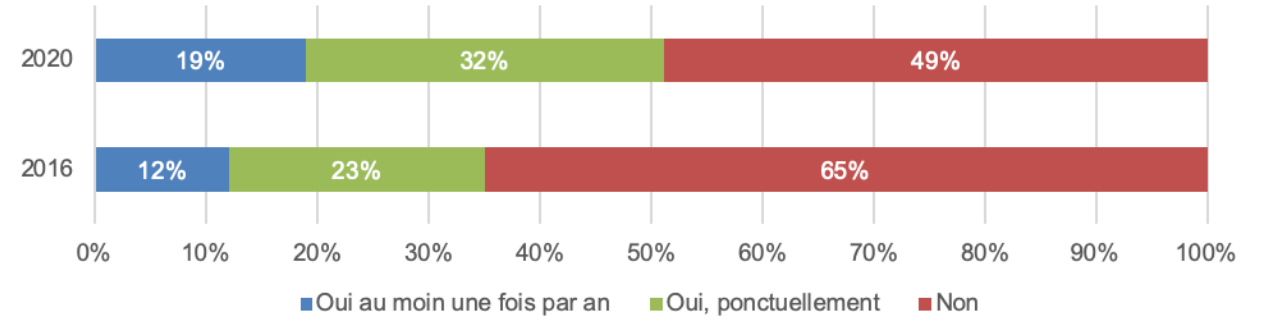


Figure 92 – Existence d'audit sur les infogérances

Cependant le recours aux indicateurs de sécurité de l'information pour contrôler l'infogérance, même s'il reste plus courant que le recours aux audits, il ne progresse pas pour autant (57 % en 2020 contre 61 % en 2016) ; il concerne la majorité (60 %) des communes et des communautés de communes.

Le nombre de collectivités ayant passé tout ou partie de leur SI sous infogérance et sans contrôles *via* des indicateurs et/ou des audits a par conséquent sensiblement augmenté depuis 2016.

Le recours à des services cloud progresse également bien plus vite que son encadrement

La progression du recours aux services cloud se confirme (+ 20 points entre 2016 et 2020 après une progression de + 23 points de 2012 à 2016) et 62 % des collectivités y ont désormais recours, *via* les directions métiers et/ou utilisateurs des collectivités et majoritairement en cloud privé (61 %), contre 18 % pour le cloud public et 21 % pour l'hybride.

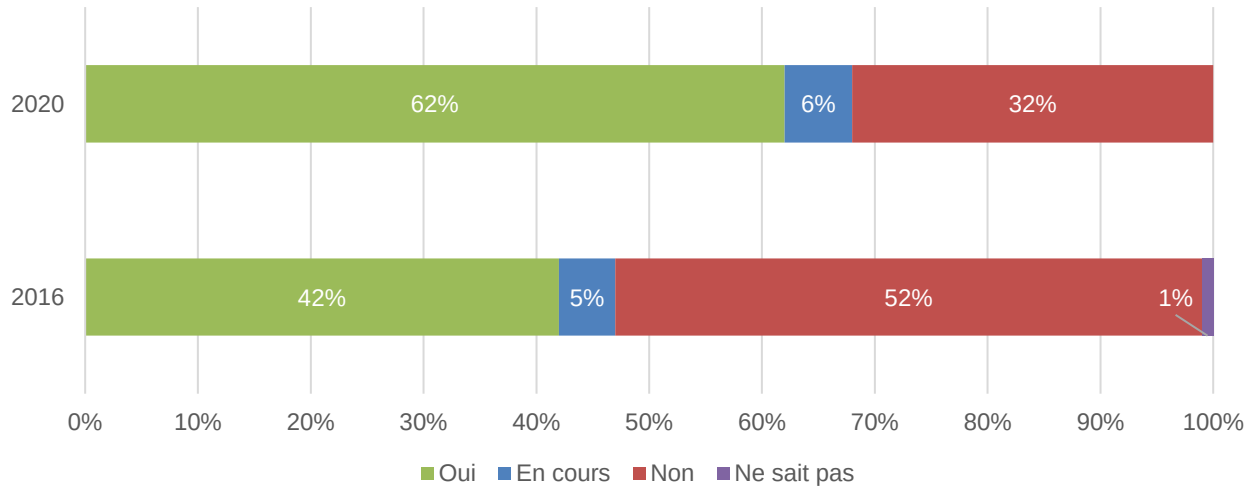
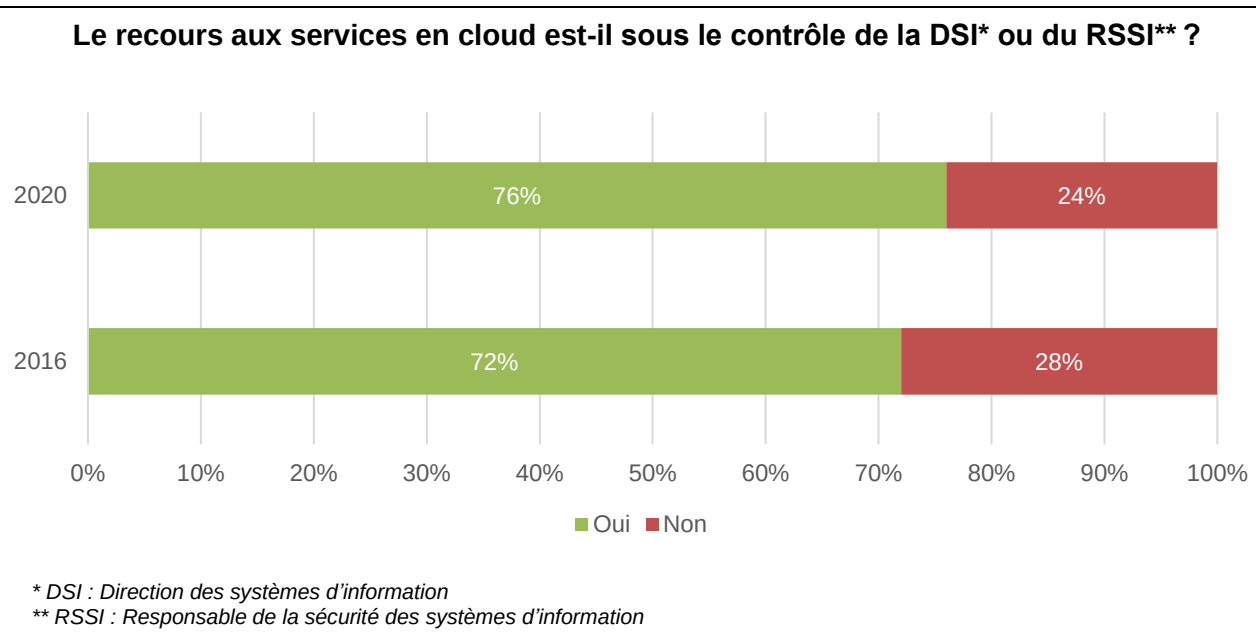


Figure 93 – Recours des directions métiers et des utilisateurs à des services en cloud

A contrario, le niveau d'encadrement du recours aux services cloud progresse assez peu, ce qui conduit mécaniquement à augmenter la surface du SI qui n'est pas contrôlée. En effet, dans 24 % des cas (contre 28 % en 2016), l'usage du cloud n'est pas sous le contrôle du DSI ou du RSSI. De plus, dans 79 % des cas (81 % en 2016), il n'y a pas de politique cloud existante ou en cours pour expliquer ce qui est autorisé ou ce qui ne l'est pas.



** DSI : Direction des systèmes d'information*
*** RSSI : Responsable de la sécurité des systèmes d'information*

Figure 94 – Encadrement du recours à des services en cloud

Thème 16 : Gestion des incidents SSI

L'arrivée des rançongiciels dans les SI de collectivités territoriales

Par rapport à la précédente étude, nous constatons une recrudescence des incidents liés à la perte de services essentiels (+ 15 points) qui constitue la principale cause d'incidents identifiée pour la plupart des collectivités. Les pannes d'origine interne représentent la seconde source d'indisponibilité des SI avec une faible variation par rapport à 2016 (+ 1 point).

La nouveauté réside dans les actions extérieures. Si les contaminations par virus ont été divisées par deux, les attaques par rançongiciel ont commencé à toucher les collectivités avec près de 30 % des conseils territoriaux et des villes impactés.

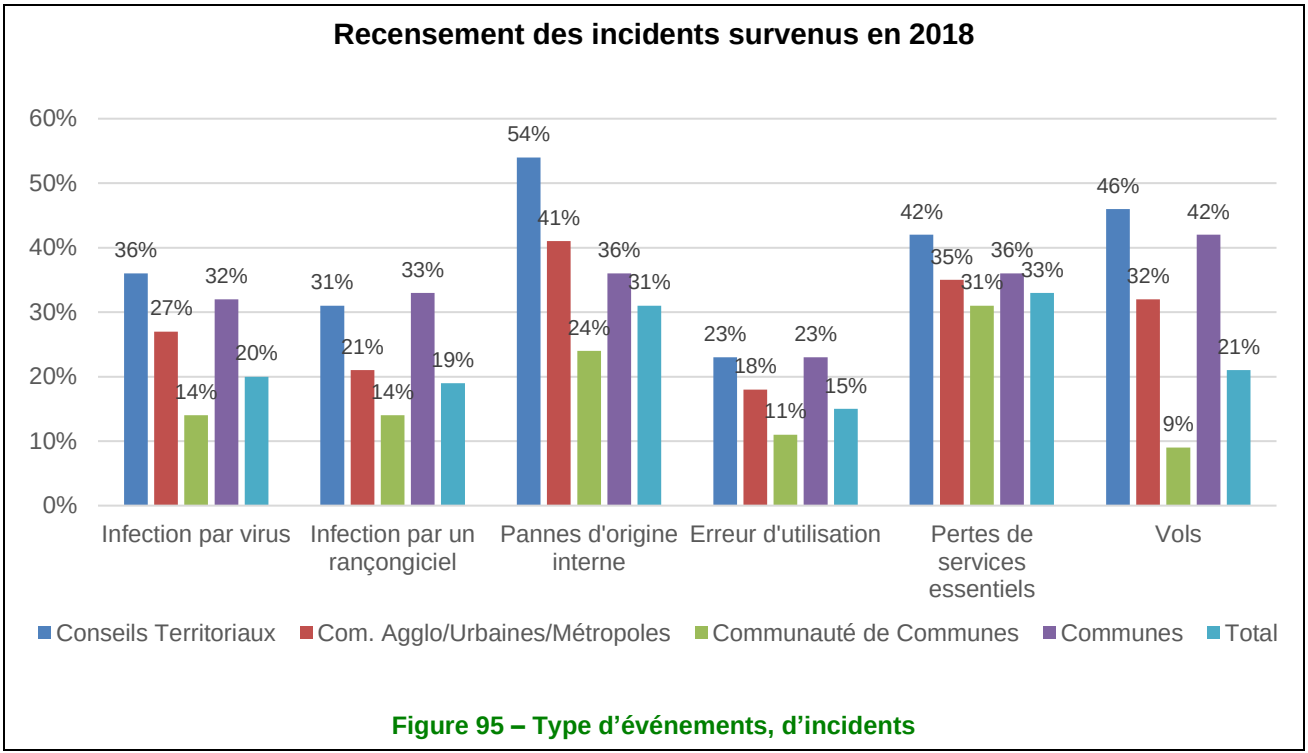


Figure 95 – Type d'événements, d'incidents

Cependant, le risque associé aux rançongiciels demeure sous-évalué puisque 62 % des répondants estiment qu'il est faible. Cela peut s'expliquer par le faible impact constaté pour 79 % d'entre eux qui ont réussi à récupérer leurs données et identifier le vecteur d'entrée. Toutefois, cet enthousiasme est à nuancer puisque sur le panel consulté, **l'impact total maximal observé pour une communauté de commune s'élève à 400 k€**.

Concernant la transparence sur les incidents, une majorité (53 %) de collectivités ne communiquent pas sur les attaques par rançongiciel subies.

De manière générale, la survenance d'un incident de sécurité n'est pas encore associée à la nécessité de déposer plainte. Seulement 10 % déclarent en avoir déposé auprès des services de police ou de gendarmerie au cours de l'année passée (diminution de 3 points par rapport à 2016). Plusieurs explications peuvent être avancées. La première concerne l'habilitation pour réaliser cette opération au nom de la collectivité. Ce type de dépôt de plainte est bien souvent technique et la perception sur l'opportunité de cette démarche au regard du temps qu'elle mobilise la relègue alors au second plan. La seconde explication qui complète la première raison tient dans le fait que le dépôt de plainte reste une étape chronophage et difficile. Il est essentiel d'avoir établi des liens au préalable avec les autorités afin que la plainte soit bien enregistrée et que les éléments techniques puissent être communiqués.

La capitalisation sur les incidents n'est pas encore à l'ordre du jour

Le précédent rapport faisait état d'une régression depuis 2012 de la gestion des incidents de sécurité, tendance qui reste globalement stagnante. Une grande majorité de collectivités ne dispose pas de cellule de

gestion des incidents affectant le système d'information que l'on pourrait identifier sous le terme de « tierce maintenance sécurité » (TMS). Actuellement, la plupart des DSI ou services informatiques fonctionnent avec le binôme tierce maintenance applicative (TMA) et tierce maintenance exploitation (TME), dont le but est le maintien en condition opérationnelle (MCO) des installations et autres applicatifs, alors que la TMS vise le maintien en condition de sécurité (MCS). Le MCO et le MCS peuvent porter des objectifs contraires et compte tenu de la charge des équipes composant les services informatiques, il est facile d'en déduire que la priorité est donnée à la production. Il n'y a donc pas de capitalisation des incidents frappant une collectivité.

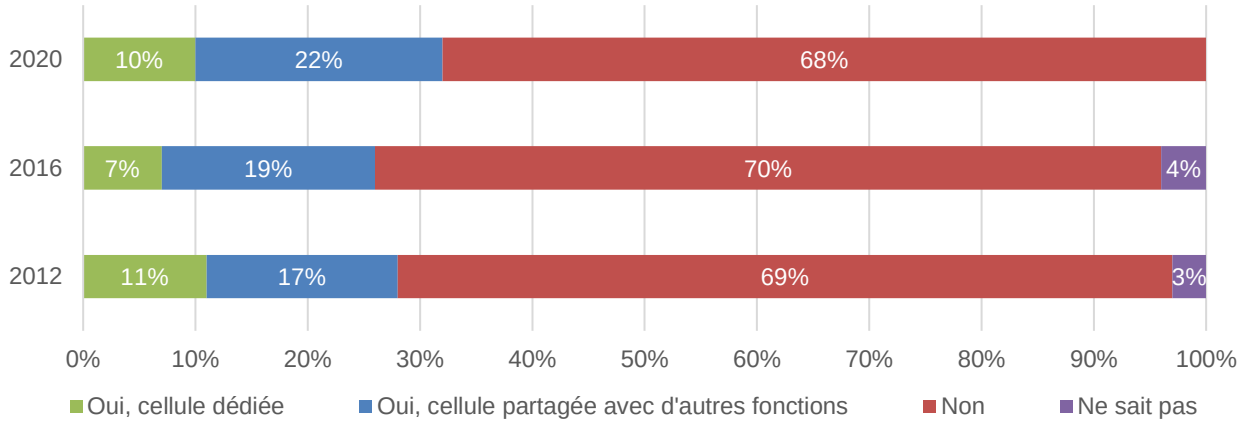


Figure 96 – Cellule de collecte et de traitement des incidents de sécurité de l'information

Les systèmes SCADA restent encore négligés

Si la gestion des incidents affectant les systèmes bureautiques est couverte à 79 %, ce taux tombe à 57 % pour la partie relevant des moyens généraux (caméras, badgeuses…). La situation est encore pire pour les systèmes industriels qui équipent bon nombre de collectivités. Seuls 11 % des cellules de gestion des incidents traitent ceux relevant des systèmes de contrôle et d'acquisition de données en temps réel (*Supervisory Control and Data Acquisition* – SCADA).

Pourtant, ces systèmes sont de plus en plus ciblés lors des attaques et sont souvent mal configurés, car opérés par des automaticiens ne disposant pas de la culture informatique idoine et encore moins en matière de SSI. Autre point important, nombre d'activités de ces systèmes s'inscriront tôt au tard dans le cadre des opérateurs de services essentiels (OSE) apparus avec la transposition en droit français de la directive NIS quand ils ne sont pas déjà désignés OIV. Ce dernier point devrait se traduire à l'avenir par une évolution des statistiques de traitement des incidents de sécurité de l'information dans les systèmes industriels (type SCADA).

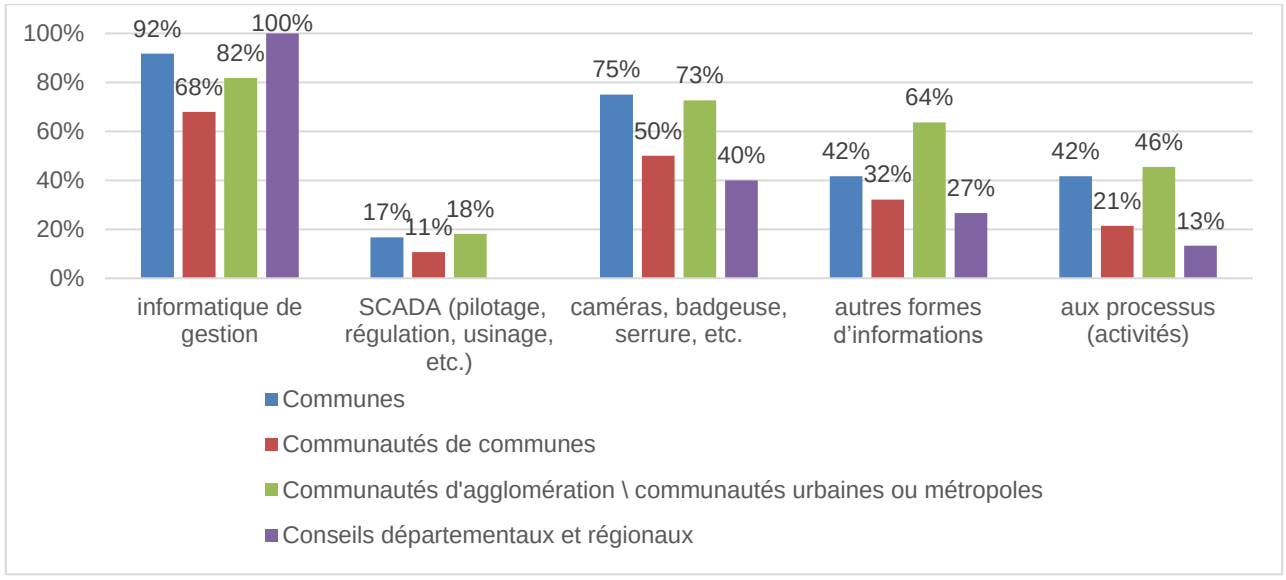


Figure 97 – Traitement des incidents par type de système d'information

Une évaluation des conséquences encore difficile

Comme évoqué auparavant, la gestion des incidents n'est pas adressée avec les moyens adéquats dans de nombreuses collectivités. Il n'y a donc rien d'étonnant à ce que 38 % des collectivités ignorent l'impact sur la production d'un incident de sécurité. En conséquence, 80 % des collectivités ne procèdent pas à une évaluation de l'impact financier des incidents et seulement 11 % disposent d'une police d'assurance. Là encore, la mise en place d'une assurance spécifique cyber nécessite en amont d'avoir réalisé une analyse des risques pesant sur la collectivité, seuls les risques résiduels pouvant être déportés vers une assurance

La problématique de l'assurance en cybersécurité est un sujet en soi, qui mériterait un article intégralement consacré à cette question. Il est néanmoins possible d'identifier plusieurs causes probables de ce peu de souscription à une police d'assurance dédiée :

- la question étant récente les produits sont également récents ;
- leur réel fonctionnement en cas de dégât a donc peu été éprouvé ;
- les décideurs et prescripteurs sont peu au fait de l'existence même de telles possibilités ;
- ce type de produit ne pourrait s'appuyer que sur des infrastructures correctement montées et tenues à jour, voire validées par l'assureur, faute de quoi ce dernier pourrait refuser l'indemnisation en cas d'incident.

Tous ces paramètres et d'autres encore pourraient expliquer le faible taux de souscription à ces produits spécialisés.

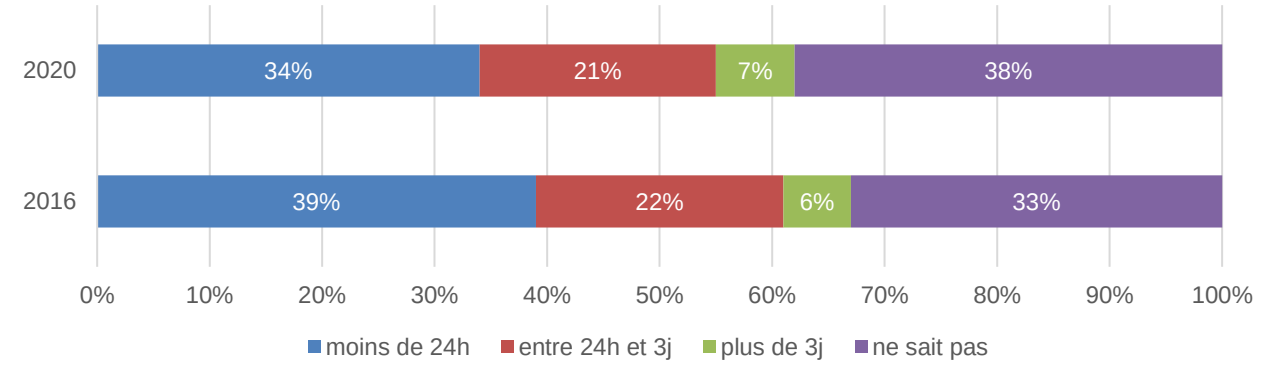


Figure 98 – Durée maximale d'interruption de service

Le réglementaire une ouverture au changement ?

L'arrivée du RGPD en mai 2018 a-t-elle permis une prise de conscience concernant les enjeux cyber ? Ce n'est pas si sûr. Là encore, 63 % des collectivités jugent l'importance d'une fuite de données comme faible et seulement 4 % déclarent en avoir subi. Pourtant, dans 83 % des cas, des données personnelles étaient concernées…

Comme nous l'avons observé pour la gestion des incidents SSI, le traitement des incidents affectant les données personnelles n'entraîne pas systématiquement un signalement à la Cnil (68 %), mais une meilleure réaction pour le dépôt de plainte (54 %). La question des parties prenantes impliquées dans la gestion d'un incident affectant les données personnelles peut expliquer en partie ce fait. Le délégué à la protection des données (DPD, *Data Protection Officer* – DPO) pouvant être juriste ou tout du moins avoir une appétence pour les considérations juridiques plus importantes qu'une équipe technique de DSI. La mise en œuvre actuelle et à venir de la directive NIS, qui devrait toucher les collectivités au cœur de leurs activités historiques (gestion des réseaux, gestion de la circulation, etc.) sera l'occasion de vérifier le poids des aspects réglementaires comme moteur du changement.

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

Une absence de formalisation de gestion de crise qui reste forte

Près de trois quarts des collectivités ne disposent pas d'un dispositif de gestion de crise formalisé. Les communautés de communes sont en retrait sur cette thématique par rapport aux entreprises.

Le recours aux services en cloud est-il sous le contrôle de la DSI ou du RSSI ?

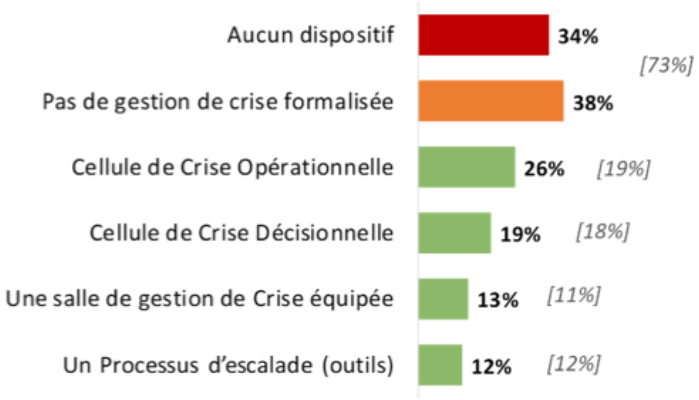


Figure 99 – Composition de la gestion de crise

Moins de 30 % des collectivités ont évalué les exigences métiers dans le cadre d'un BIA formel

Certes, les résultats de l'enquête concernant la thématique des bilans de l'impact sur l'activité (BIA) sont en progression par rapport à l'étude MIPS de 2016, mais un faible nombre de collectivités s'engagent dans une démarche de plan de continuité d'activité (PCA) avec un BIA prenant en compte les exigences métiers.

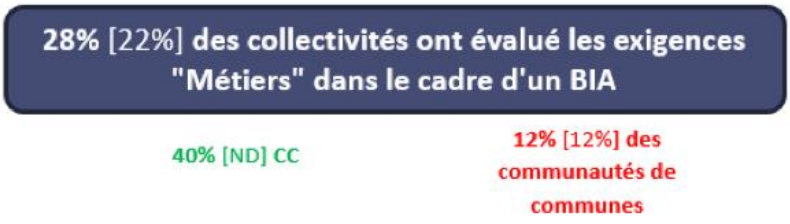


Figure 100 – Pourcentage d'entreprises engagées dans une démarche de BIA formel

Des plans de continuité davantage testés, mais loin d'être systématiques

Avec environ un quart des collectivités réalisant des tests de plan de continuité/plan de reprise d'activité (PRA) une fois par an, la fréquence des tests reste faible et en retrait par rapport aux entreprises.

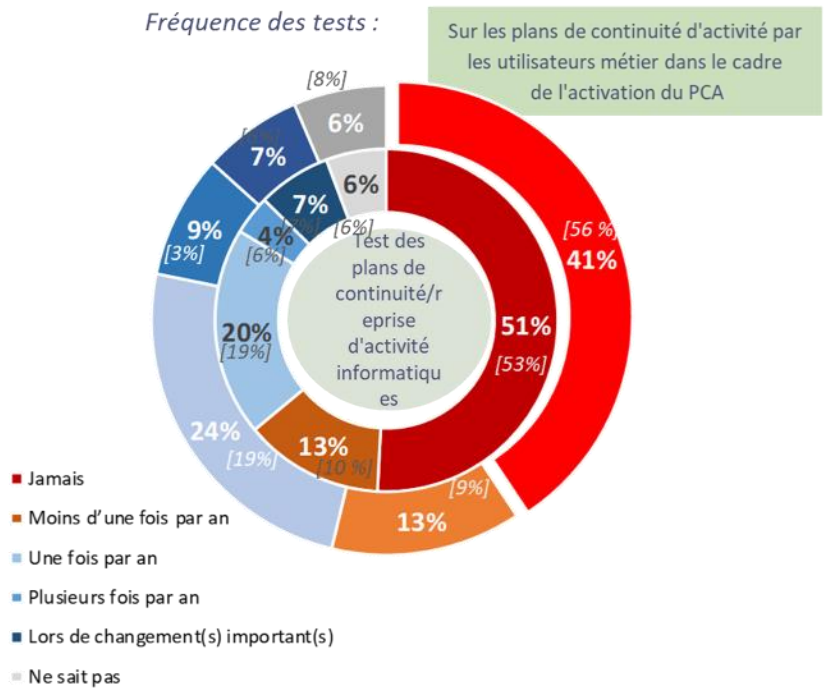


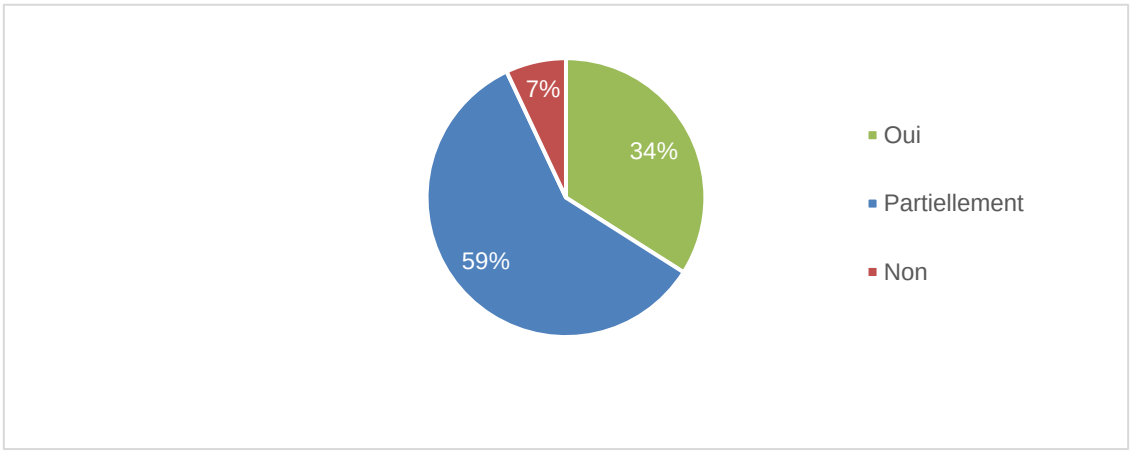
Figure 101 – Fréquence des tests

Thème 18 : Conformité

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 RGPD de l'Union européenne, l'édition 2018 étant intervenue durant la période transitoire ou 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 collectivités estiment être en conformité, totalement (34 %) ou partiellement (59 %). Alors que les entreprises estiment l'être totalement (73 %) ou partiellement (24 %), on peut penser que cette différence d'estimation est due au fait que la désignation d'un DPD/DPO étant obligatoire pour les entités publiques, ces délégués ont donné des réponses « plus honnêtes » sur le niveau réel de leur conformité,



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

Figure 102 – Répartition du degré de conformité avec le RGPD

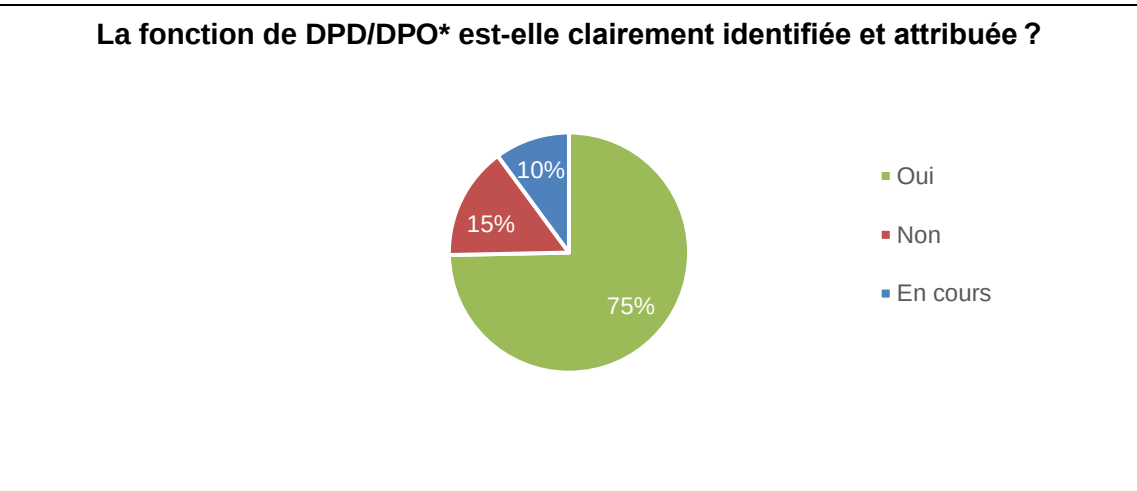
La fonction de délégué à la protection des données (DPD/DPO)

Depuis l'entrée en application du RGPD le 25 mai 2018, la fonction de DPD/DPO est obligatoire dans tous les organismes publics. Toutes les collectivités devraient donc désormais en avoir désigné un.

Pourtant, seuls 75 % des collectivités indiquent s'être acquittées de cette obligation. Dans 10 % des cas, la désignation est en cours. Restent 15 % des collectivités qui n'ont pas de DPD/DPO, même pressenti.

Si les désignations ont été effectuées dans la totalité des conseils régionaux et départementaux, c'est dans les communautés de communes que la situation est la moins aboutie, avec 23 % de désignations absentes. Il faut sans doute tempérer cette observation par le fait que les communautés de communes sont des structures de taille modeste, qui ont peu de traitement spécifique. La plupart des données sont traitées au niveau des communes associées, où le taux de désignation est, en revanche, très élevé (97 %).

Par ailleurs, les communautés d'agglomération, qui sont des structures de plus grande taille, ont également un taux de désignation élevé (82 % effective, 15 % en cours). De plus en plus, elles offrent également un service de DPO mutualisé à leurs communes associées.



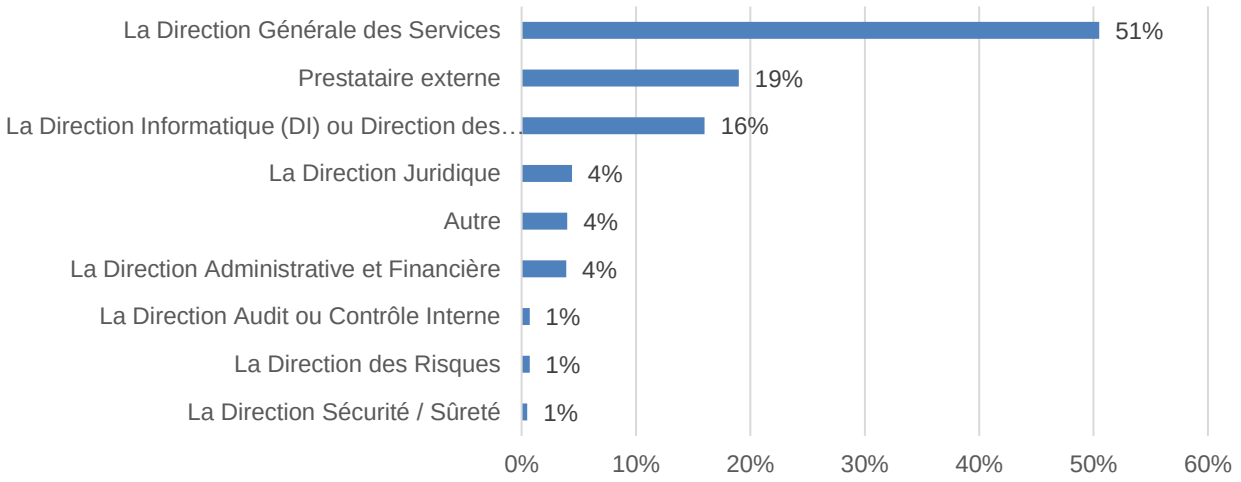
* DPD : Délégué à la protection des données (Data Protection Officer – DPO)

Figure 103 – Identification de la fonction de DPD/DPO

Dans la moitié des cas, le DPD/DPO est rattaché à la Direction générale des services. La fonction est externalisée dans 19 % des cas, auprès de prestataires spécialisés ou mutualisés avec les intercommunalités

ou des centres de gestion. Il est parfois rattaché à la DSI (16 %), et plus rarement à la Direction juridique ou la Direction administrative et financière.

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

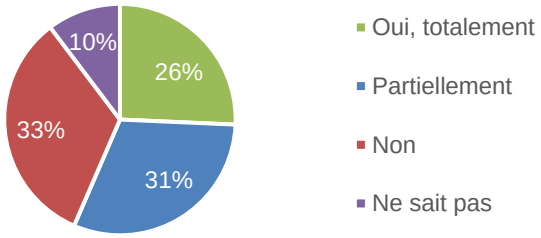


** DPD : Délégué à la protection des données (Data Protection Officer – DPO)*

Figure 104 – Rattachement hiérarchique du DPD/DPO

En ce qui concerne la conformité au référentiel général de sécurité (RGS), 57 % des collectivités ont identifié, totalement ou partiellement, les SI qui nécessitent une homologation. Un tiers n'ont pas effectué cette identification, et 10 % des personnes interrogées n'ont pas été en mesure de répondre.

Les SI nécessitant une homologation RGS* sont-ils tous identifiés ?



** RGS : Référentiel général de sécurité*

Figure 105 – Niveau d'identification des SI concernés par le RGS

Parmi les collectivités qui ont identifié les SI concernés, 78 % ont procédé, en totalité (57 %) ou partiellement (21 %), à l'homologation RGS.

On peut remarquer que le taux de conformité au RGS (78 % des 57 % de collectivités qui ont identifié les SI concernés, soit 45 %) est très inférieur à la conformité au RGPD, alors que le RGS est très antérieur (2010). Est-ce lié à une moindre médiatisation du RGS, ou aux risques de sanction du RGPD ?

Utilisation de tableaux de bord de sécurité

Le niveau d'utilisation de tableaux de bord reste très faible : 87 % des collectivités indiquent ne pas avoir mis en place d'indicateurs,

Les collectivités qui utilisent des indicateurs constituent donc un échantillon très limité. Leurs indicateurs sont surtout de nature opérationnelle (73 %) et dans 17 % des cas (– 13 points par rapport à l'étude de 2016) ils servent au pilotage des fonctions SSI. Pour 26 % (+ 5 points par rapport à l'étude de 2016), il s'agit d'indicateurs stratégiques utilisés par les instances de direction.

Les indicateurs les plus suivis sont : la conformité avec la politique de sécurité de l'information (64 %, soit un bond de 44 points par rapport à l'étude de 2016), le nombre d'incidents sur une période (48 %), les vulnérabilités détectées (46 %) et la cartographie des risques (38 %).

Revue de la sécurité de l'information

Une évolution majeure est observée sur ce point depuis l'édition 2016 de l'étude. Alors que plus de la moitié des collectivités ne procédaient à aucun audit de leur SI, 56 % déclarent aujourd'hui en réaliser au moins un tous les deux ans.

Cela semble indiquer une prise de conscience accrue de la sensibilité des SI, et de l'importance de prévenir les risques.

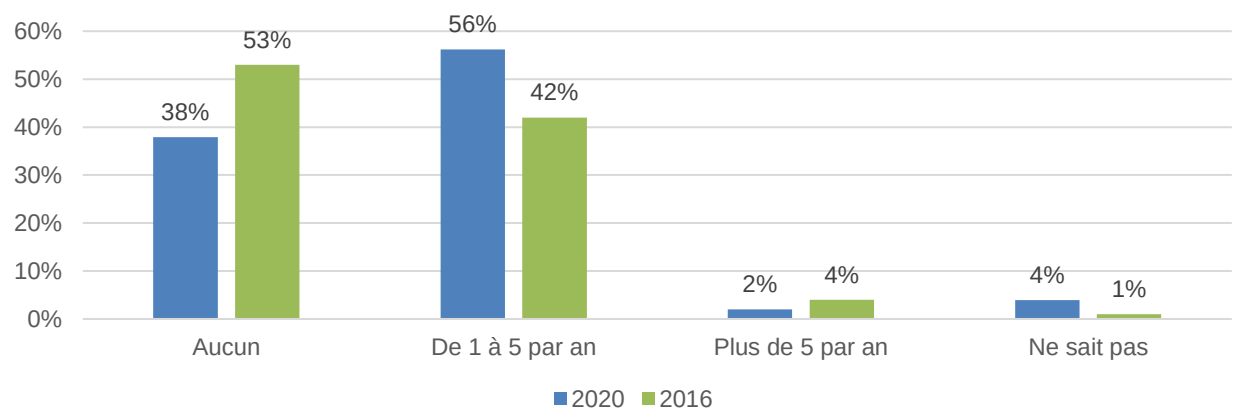


Figure 106 – Fréquence des audits de sécurité au cours des deux dernières années

Comme en 2016, les audits sont principalement techniques (architecture, configuration, intrusion). On note en revanche une bien meilleure connaissance de la nature des audits, ce qui semble indiquer une plus grande maîtrise de ce type de processus.

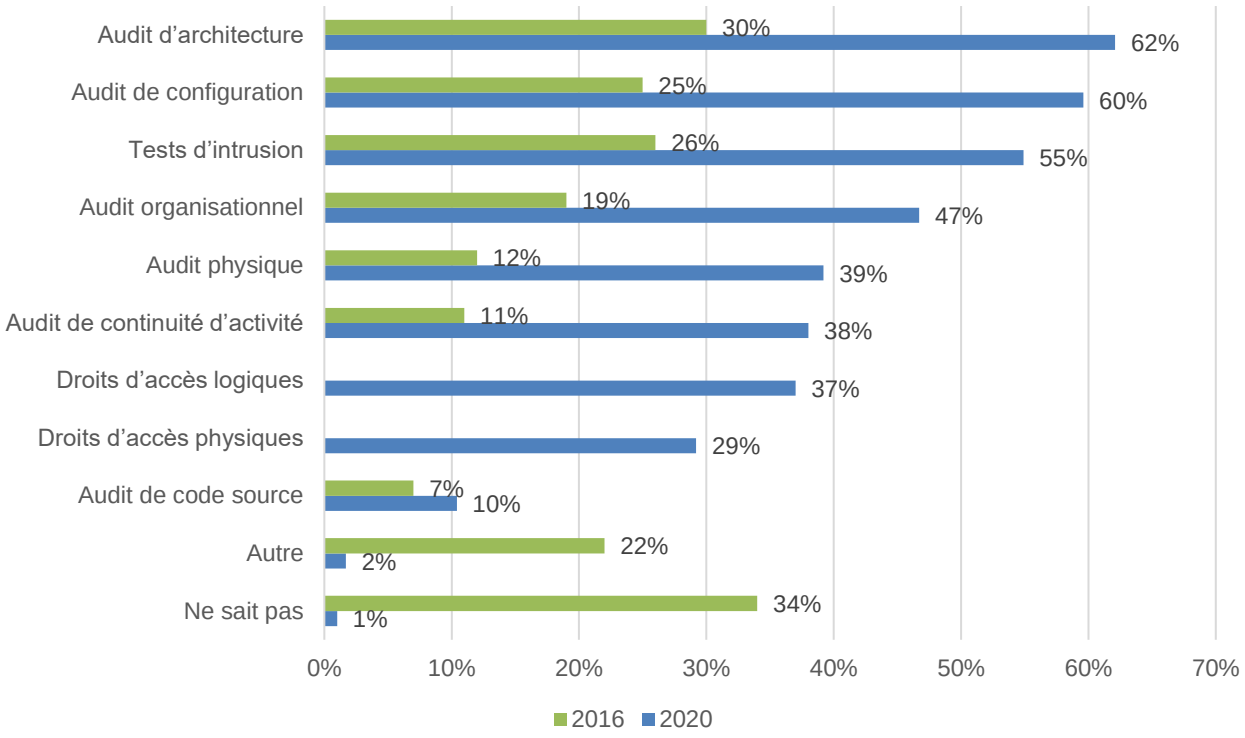


Figure 107 – Types d'audits et de contrôles de sécurité du SI

La motivation des audits est devenue très largement induite par les exigences contractuelles ou réglementaires (51 %) et, dans une moindre mesure, par la PSSI (31 %). Les incidents sont toujours un facteur déclenchant (23 %).

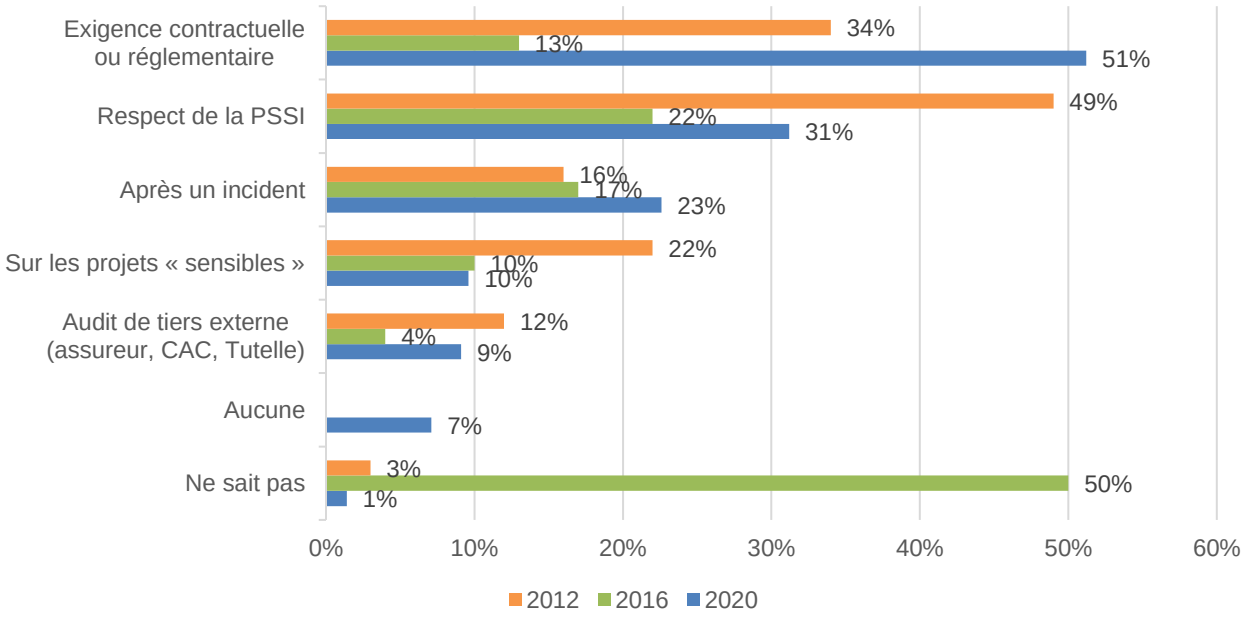


Figure 108 – Motivations principales des audits

Internautes

- Présentation de l'échantillon
- Partie I – Identification et inventaire ordinateurs et smartphones
- Partie II – Usages de l'internaute
- Partie III – Perception de la menace et sensibilité de l'utilisateur aux risques et à la sécurité de l'information
- Partie IV – Moyens et comportements vis-à-vis de la sécurité informatique

Les internautes

Présentation de l'échantillon

Pour cette étude 2020, 998 internautes de 15 ans et plus ont été sondés. Afin d'avoir une appréciation la plus fine possible de leurs usages, leur perception de la menace et leurs comportements, les chiffres ont été redressés sur les données statistiques nationales. On trouve donc :

- 52 % de femmes et 48 % d'hommes ;
- 41 % ont moins de 45 ans, 31 % plus de 60 ans ;
- 55 % d'actifs et 45 % de retraités, élèves/étudiants et sans profession ;
- 38 % ont des enfants (couples ou parents isolés).

Partie I – Identification et inventaire ordinateurs et smartphones

Le smartphone fait dorénavant seul la course en tête, l'ordinateur fixe continue sa chute

En 2020, le smartphone confirmant les prédictions annoncées dans le rapport de 2018 est dorénavant le moyen privilégié des internautes français pour consulter l'Internet, progressant encore de 5 points par rapport à 2018 pour atteindre 87 %. Il domine de la tête et des épaules les ordinateurs portables et les tablettes, dont les usages et le taux d'équipement moyen des foyers restent à peu près constants depuis 2016.

Le nombre moyen de smartphones par internaute français est en très forte progression et passe de 1,19 à 1,41 en deux ans (comparativement, il était passé seulement de 1,13 à 1,19 entre 2016 et 2018).

Quels équipements (professionnels ou personnels) utilisez-vous pour vous connecter à Internet à votre domicile ?

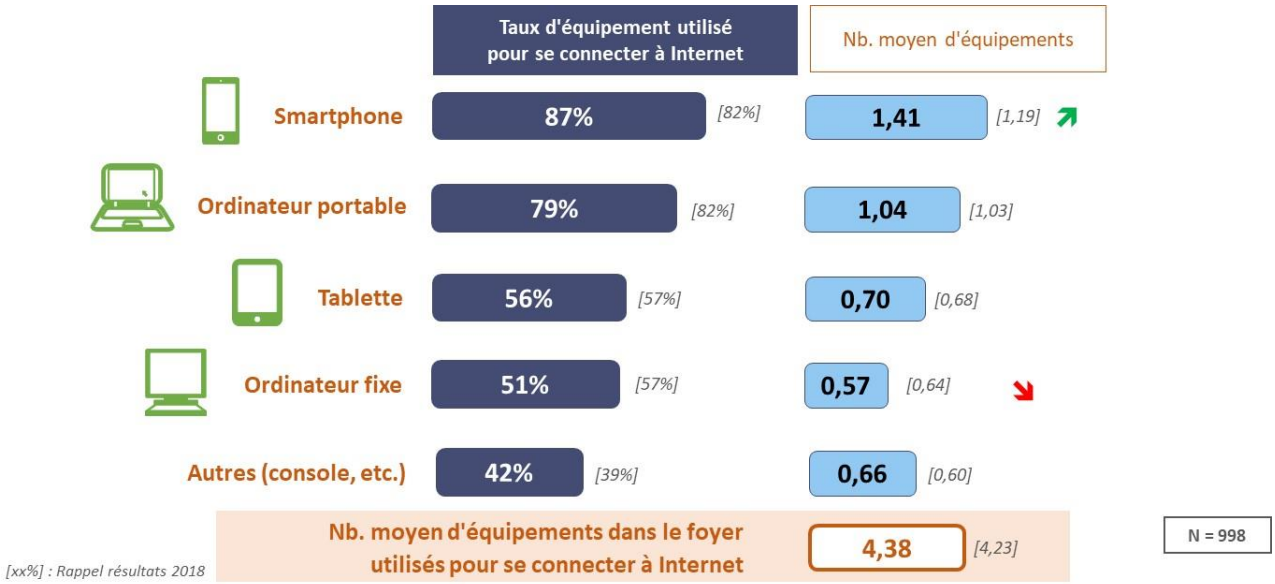


Figure 109 – Équipements des internautes en 2020

L'ordinateur fixe suit la tendance inverse, amorcée depuis 2014, puisqu'il n'est cité que par 51 % des internautes comme moyen de consulter l'Internet, perdant encore 6 points par rapport à 2018 ; le nombre moyen d'équipements par personne est par ailleurs, lui aussi, toujours en baisse.

La connexion des internautes en mobilité se généralise

En 2020, le nombre moyen d'internautes indiquant se connecter en dehors de leur domicile, même rarement, est constant comparativement à 2018, mais il est à noter que ceux qui le font « encore rarement » sont moins nombreux qu'en 2018 (17 % *vs* 23 %) et que les rangs de ceux qui disent se connecter souvent ont grossi (+ 4 points pour atteindre 37 %).

En dehors de votre domicile, vous connectez-vous à Internet avec un ou plusieurs équipements mobiles (ordinateur portable, tablette, smartphone) ?

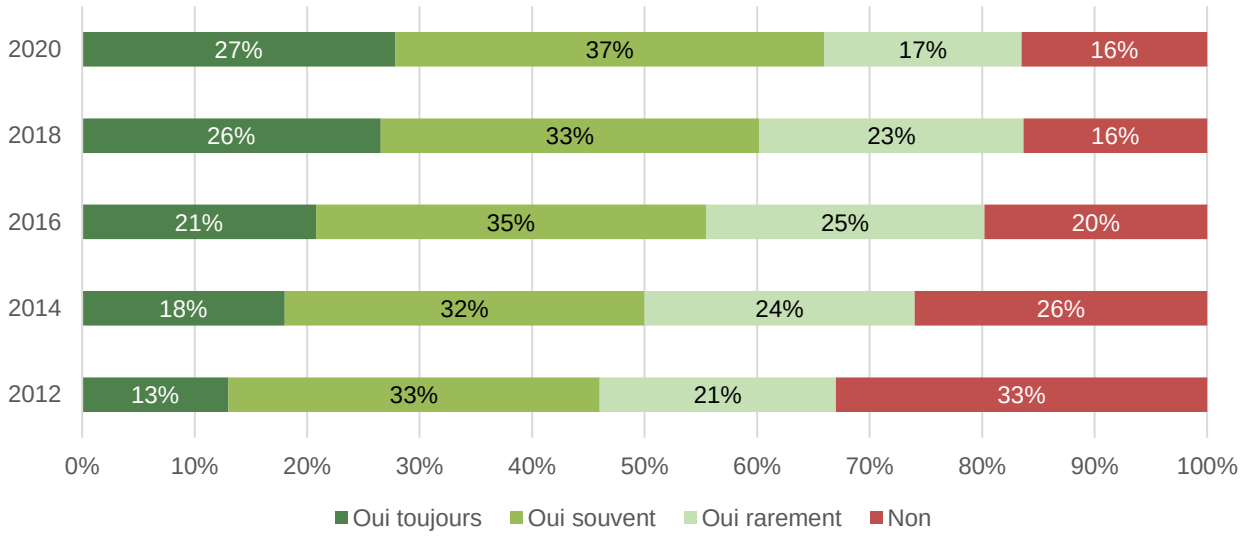


Figure 110 – Fréquence de connexion en mobilité avec son smartphone

Cette tendance est encore plus prononcée chez les personnes âgées de 19 à 44 ans (ils sont plus de 80 % à le faire toujours ou souvent), mais elle ne dépend pas de la catégorie sociale. Seuls les retraités et les personnes sans profession ne suivent pas cette évolution.

Les objets connectés du quotidien sans surprise

Internet des objets : qu'est-ce qui est connecté chez vous ou dans votre sphère personnelle ?

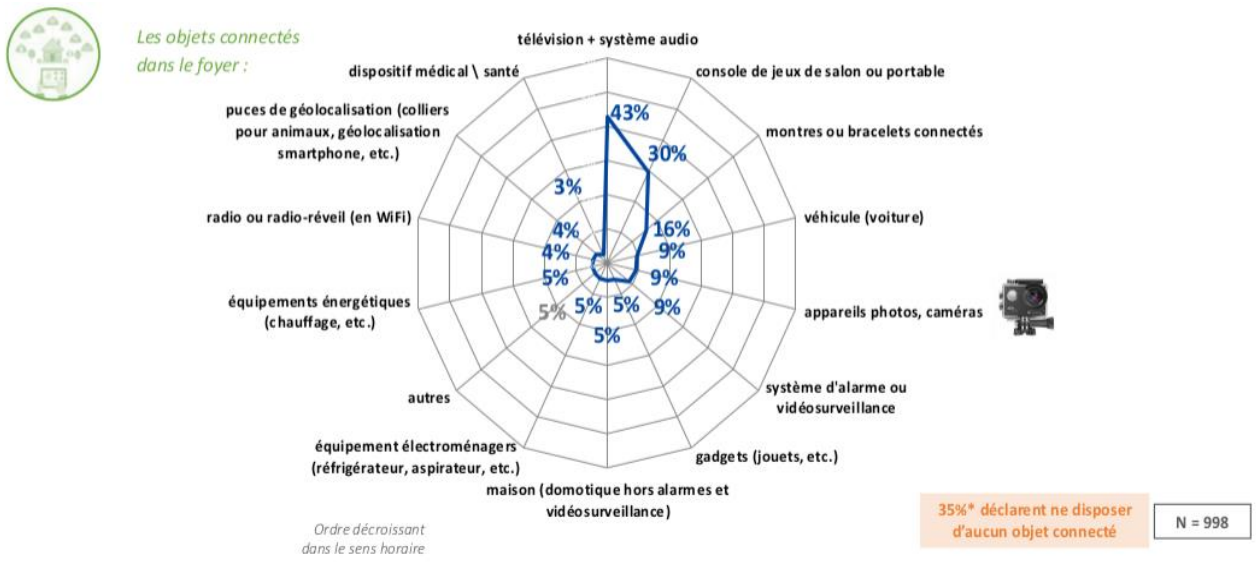


Figure 111 – Les objets connectés chez les internautes en 2020

En moyenne, on recense 1,5 objet connecté par foyer en 2020, 70 % des sondés en ayant moins de 5 (les jeunes générations sont 38 % à en détenir entre 5 et 10) et, comme lors des études précédentes, les objets figurant sur les trois marches du podium sont, dans l'ordre : les téléviseurs et systèmes audio, les consoles de jeux et les bracelets et montres connectés. Il faudra probablement attendre l'arrivée de la 5G et de ses Internet des objets (*Internet of Things* – IoT) associés pour observer de fortes évolutions dans ce domaine.

Partie II – Usages de l'internaute

La connexion depuis le domicile *via* Wi-Fi, quoi d'autre ?

L'accès à Internet se fait souvent et très souvent depuis le domicile où 9 personnes sur 10 ont alors recours au Wi-Fi. Les étudiants sont même 98 % à privilégier ce mode de connexion (+ 3 points par rapport à 2018).

Ces chiffres sont constants par rapport à 2018. Le confort apporté par les débits proposés, l'utilisation d'équipements mobiles dépourvus d'autres moyens de connexion font donc du Wi-Fi le champion toutes catégories de la connexion à l'Internet depuis son domicile.

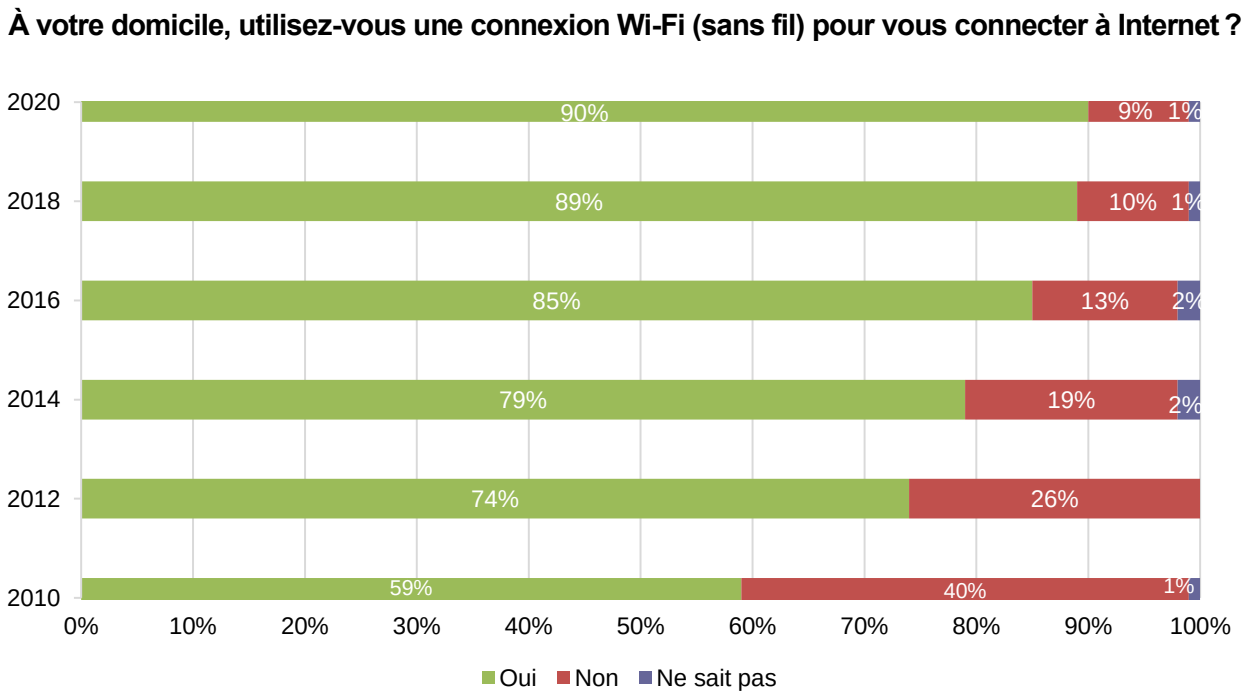


Figure 112 – Usages du Wi-Fi à domicile depuis 2010

L'absence de la technologie Wi-Fi dans les objets connectés du quotidien ayant fortement baissé, elle est de moins en moins invoquée par les sondés comme raison de ne pas s'en servir (28 % en 2018 contre 19 % en 2018). Corrélativement, les deux raisons majeures invoquées par les récalcitrants à ce mode de connexion, soit la sécurité et la santé, font un bon en avant conséquent : ils sont en effet plus d'un tiers (35 % en 2020 contre 24 % en 2018) à répondre ne pas l'utiliser « pour des raisons de sécurité » tandis qu'ils sont 26 % à y renoncer « pour des raisons de santé » alors qu'ils n'étaient que 12 % en 2018.

Hors du domicile, on observe une progression de l'accès à Internet, particulièrement en mobilité complète, qui gagne 4 points pour atteindre 30 % en moyenne des sondés en 2020. La catégorie d'âge 15-29 ans est toujours la plus importante à être connectée souvent et très souvent de la sorte, malgré un léger recul (53 % en 2020 contre 58 % en 2018).

Interactions personnel/professionnel, usages et stockage : pas d'évolutions

En matière de stockage d'informations à caractère personnel sur ses équipements personnels, il n'y a pas d'évolution franche à constater sur le type des documents stockés ni sur leur moyen de stockage, qui se fait majoritairement sur ordinateur. Y compris sur les offres de cloud, qui avaient pourtant connu une certaine augmentation entre 2016 et 2018 (+ 6 points), elle a d'ores et déjà atteint un palier à 33 % d'usage. Les 15-

29 ans, les employés et les élèves étudiants arrivent premiers *ex aequo* avec 46 % des sondés parmi ces trois catégories qui ont recours au cloud pour stocker leurs données.

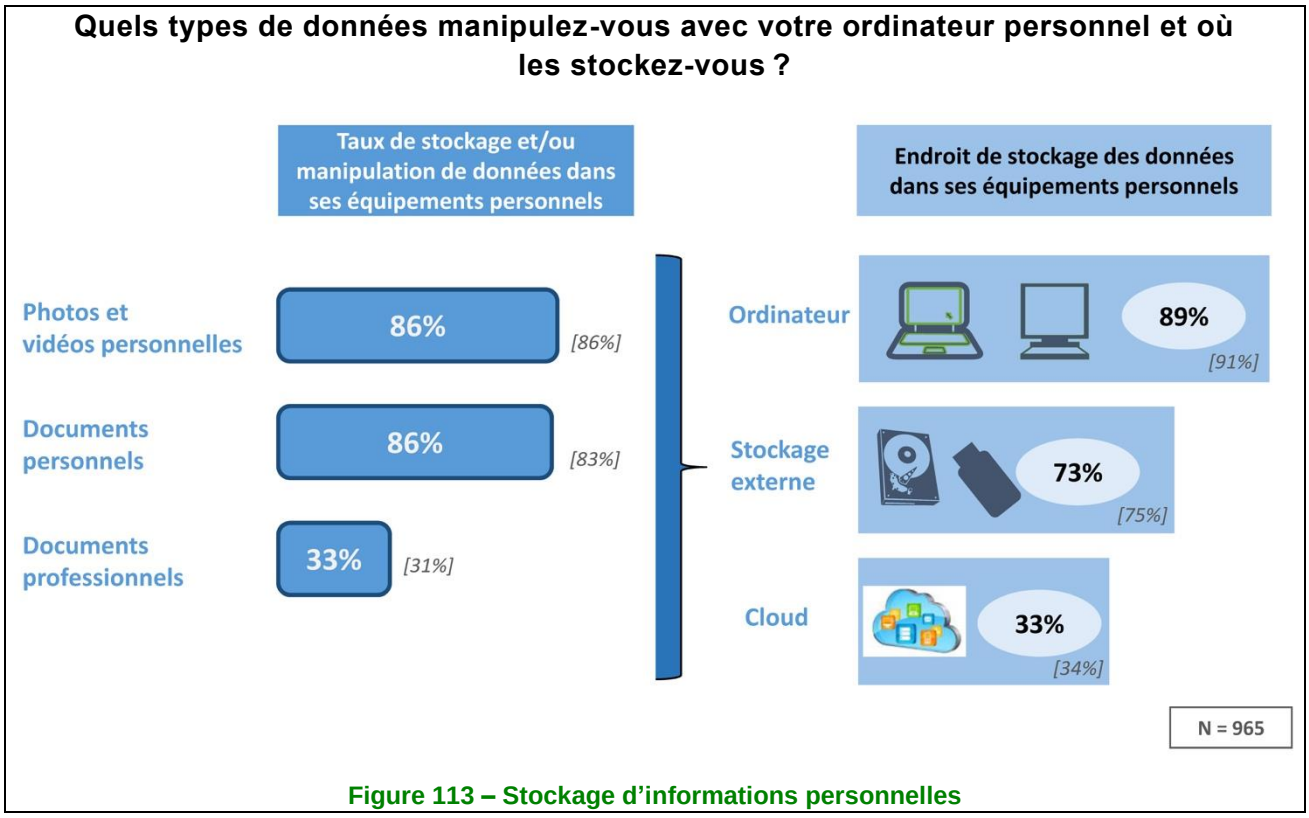


Figure 113 – Stockage d'informations personnelles

À noter : le mode de stockage sur support externe déporté chez un tiers (famille, ami) a également fait l'objet d'une question dans l'étude MIPS 2020, où il apparaît encore peu usité en moyenne (un peu moins de 14 %). Les commerçants, artisans et chefs d'entreprise se démarquent pourtant avec un taux d'adoption de ce système de stockage à 31 % ; ils sont également la catégorie de sondés recourant le plus massivement (81 % contre 33 % pour la moyenne de la population sondée) à l'usage de leurs équipements personnels pour y stocker des documents professionnels.

En ce qui concerne les usages de matériel personnel à des fins professionnelles, on n'observe pas de changement de comportement pour la moyenne des internautes par rapport à 2018 (36 %). Ce sont les étudiants (69 %) et les artisans, commerçants et chefs d'entreprises (63 %) qui sont les plus nombreux à indiquer faire usage de cette pratique, suivis de près par les jeunes urbains et les CSP+ (42 % de CSP+, 55 % de 15-29 ans et 45 % de Franciliens).

L'utilisation de l'accès Internet personnel pour se connecter à distance au réseau de son entreprise connaît peu de variations en moyenne, seule une augmentation importante étant à signaler chez les artisans, commerçants et chefs d'entreprise qui le font dorénavant très souvent (34 % en 2020 contre 16 % en 2018) plutôt que souvent (10 % en 2020 contre 25 % en 2018).

Les usages d'Internet : pas de nouveautés, mais quelques usages en hausse

Concernant les usages d'Internet, pas de révolution en 2020 ! Celui-ci se veut de plus en plus pratique, confirmant la tendance observée en 2018 (sa fréquence d'utilisation passe en moyenne de 53 % à 68 % entre les deux études) et son utilisation comme mode de communication progresse par rapport à son usage purement récréatif.

En effet, les moyens de communication en direct (chat, messagerie, etc.) passent de 65 % en 2018 à 72 % en 2020.

À titre personnel, sur Internet (sur smartphone ou ordinateur), quelles sont vos habitudes ?

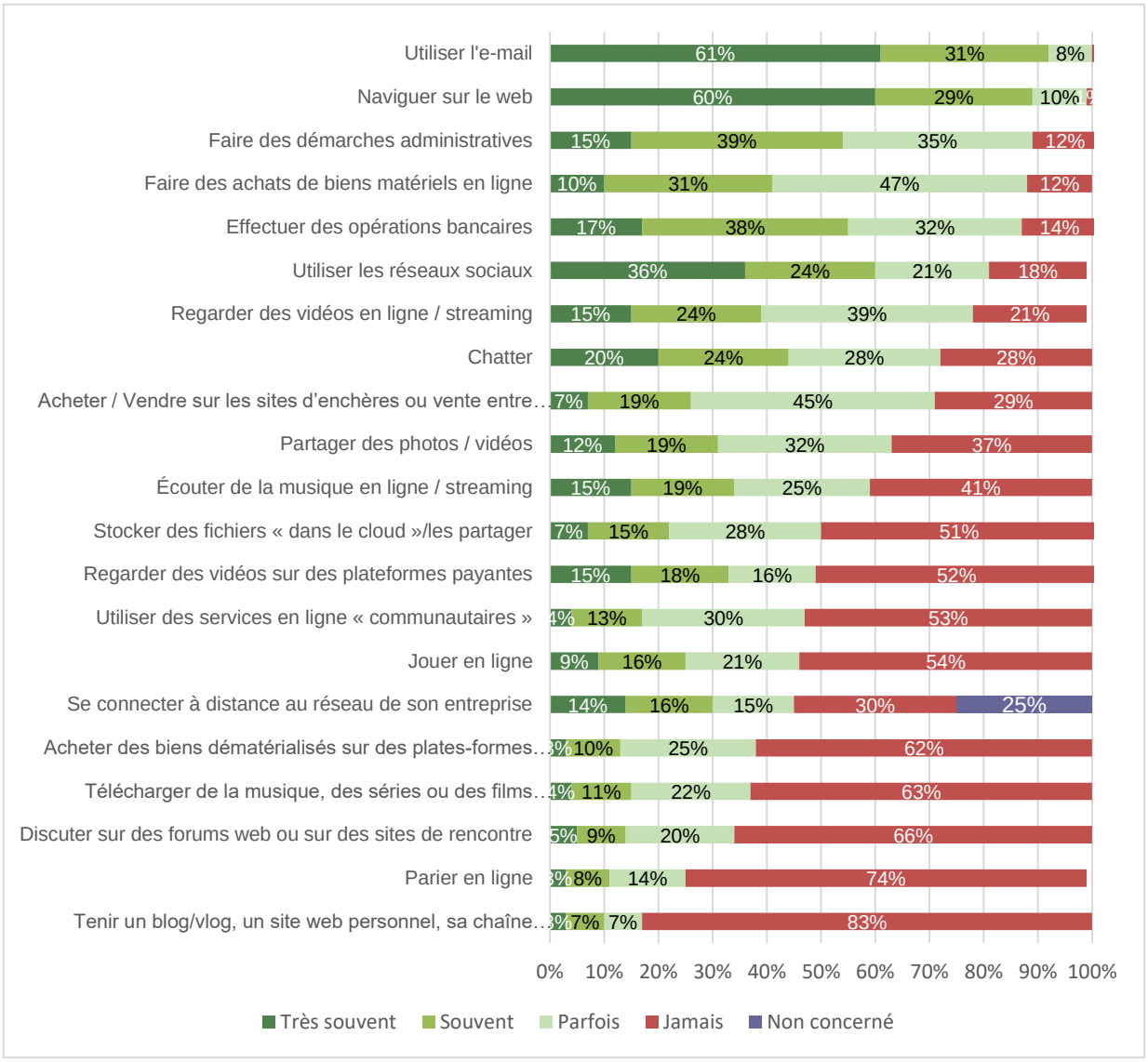


Figure 114 – Usages de l'Internet en 2020

En ce qui concerne les usages purement pratiques, il est intéressant de noter que l'utilisation de services en ligne dits « communautaires » connaît une progression de 9 points, passant de 38 % à 47 %. Les personnes seules en activité sont même 62 % à utiliser au moins parfois ces services, suivis de près par les 15-29 ans (61 %) puis les CSP+ (59 %).

Rappelons que le sondage a été réalisé début 2020 au sortir d'une période d'actualité sociale mouvementée, cette progression sera donc à vérifier lors de la prochaine étude.

Toujours d'un point de vue pratique, les internautes sont 86 % en moyenne (96 % pour les professions intermédiaires) à déclarer effectuer des opérations bancaires « au moins parfois » sur Internet (+ 3 points par rapport à 2018). Ils sont également toujours plus nombreux à effectuer leurs démarches administratives en ligne, 89 % (95 % pour les couples sans enfants) déclarant le faire « au moins parfois » en 2020 contre 85 % en 2018.

De nouveaux usages font également leur apparition dans le questionnaire en 2020 :

- le visionnage de vidéos en ligne sur des plateformes payantes, qui a déjà conquis presque un internaute sur deux (48 % en moyenne déclarant le faire très souvent, souvent ou parfois). Les couples avec enfant y recourent pour 62 %, les 15-29 ans à 81 % ;

- le pari en ligne, qui reste plus confidentiel, seulement pratiqué par un quart des internautes de « très souvent » à « parfois » en moyenne. C'est un usage plutôt masculin, 35,6 % des hommes y ayant recours contre seulement 16 % des femmes.

Il sera intéressant d'analyser l'évolution de ces usages sur les années à venir.

Parmi ceux dorénavant bien ancrés dans les habitudes des internautes, on trouve l'acte d'achat sous toutes ses formes (bien matériel, neuf ou d'occasion, ou dématérialisé). Cet usage connaît néanmoins un certain recul, passant de 67 % à 55 % entre 2018 et 2020.

Le paiement d'achats en ligne progresse sur terminal mobile, mais toujours avec condition

La principale évolution à retenir est le fait que les internautes sont moins réticents à effectuer le paiement de leurs achats en ligne avec leur tablette ou leur téléphone mobile plutôt que depuis un PC fixe ou un ordinateur portable. Les 15-29 ans l'ont largement adopté ; ils ne sont en effet plus que 18 % à ne pas envisager un paiement sur leur tablette ou téléphone mobile contre 33 % en 2018.

La part des sondés réticents au paiement en ligne baisse de 10 points (passant de 51 % à 41 %) tandis que les personnes qui envisagent d'y avoir recours si des conditions sont remplies sont dorénavant plus nombreuses (+ 10 points).

Le paiement en ligne sur ordinateur fixe ou mobile reste stable, 70 % des internautes n'utilisant cette solution pour leurs achats que sous conditions également.

L'acte de paiement en ligne *via* un autre type d'objet connecté (TV, console) est encore relativement confidentiel, 70 % des personnes interrogées n'y ayant jamais recours et plus deux tiers l'ayant expérimenté, uniquement sous certaines conditions.

Parmi les conditions suivantes, lesquelles exigez-vous pour accepter de payer en ligne ?

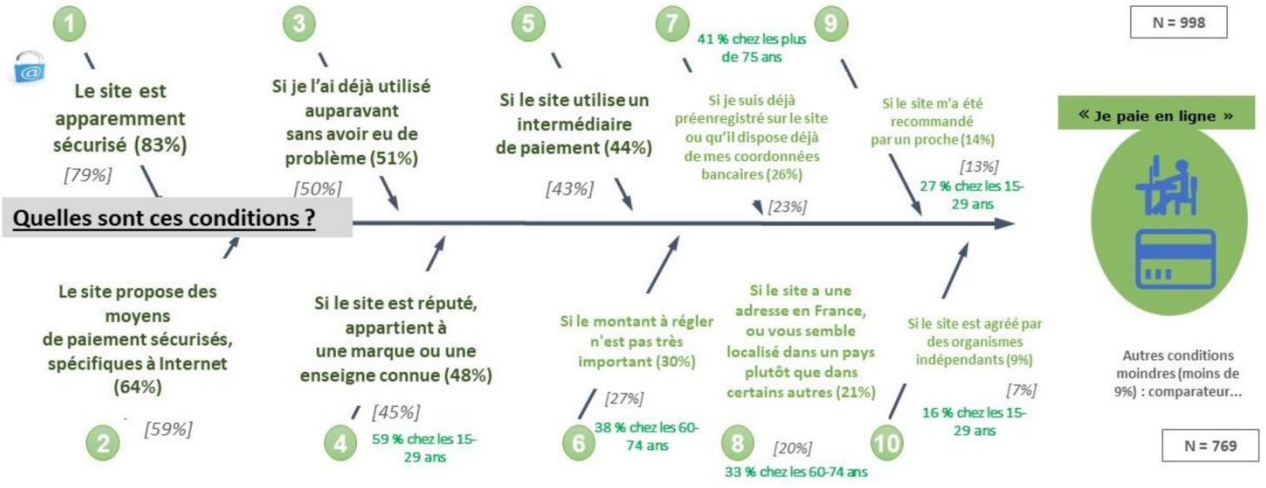


Figure 115 – Conditions exigées pour accepter un paiement en ligne

Les conditions les plus citées et qui continuent leur progression sont la sécurité « apparente » du site web (+ 4 points, pour atteindre 83 % en 2020) ou des moyens de paiement proposés par ce site (64 % en 2020 contre 59 % en 2018). La condition de réputation du site web marque le pas sauf chez les 15-29 ans, passant de 54 % à 59 % entre 2018 et 2020.

La condition d'avoir ses informations bancaires préenregistrées afin de faciliter l'achat reste une spécificité des retraités et des personnes de plus de 75 ans (41 % contre 26 % pour la moyenne des internautes français) et des hommes, qui sont 34 % à apprécier ce type de facilité.

La divulgation d'informations personnelles : une question de confiance

Concernant le remplissage de formulaire contenant des informations personnelles, la notion de « confiance » progresse encore par rapport à 2018 pour atteindre 70 % des personnes interrogées en moyenne.

Aucun des élèves/étudiants sondés n'accepte d'ailleurs de le faire sans condition, et ils sont 85 % à ne le faire que s'ils ont « confiance ».

En comparaison avec l'étude précédente, les 15-29 ans semblent être plus sensibles à ces aspects. En 2020, ils ne sont dorénavant plus que 13 % à les fournir sans condition, contre 25 % en 2018. Les artisans, commerçants et chefs d'entreprise parcourent quant à eux le chemin inverse, puisqu'ils sont 25 % en 2020 à le faire sans condition alors qu'ils n'étaient que 14 % en 2018.

Les plus réticents sont les cadres supérieurs qui sont 27 % à ne jamais remplir ce genre de formulaires, contre 20 % en moyenne pour l'ensemble des personnes interrogées.

Partie III – Perception de la menace et sensibilité de l'utilisateur aux risques et à la sécurité de l'information

Menace de la vie privée sur Internet : une insouciance toujours présente

Depuis 2016, la perception des menaces sur la vie privée est stable : 69 % des sondés estiment qu'Internet met en danger leur vie privée et 88 % considèrent qu'il est important de protéger leur vie privée, dont 49 % vont jusqu'à penser que cela est très important, ce qui représente 1 point de plus pour chacun des trois chiffres cités par rapport à la perception de 2018. Cette stabilité se retrouve aussi lorsque l'on aborde la perception du danger d'Internet pour les mineurs, puisque les sondés estiment en 2020 à 94 % que cette population est exposée.

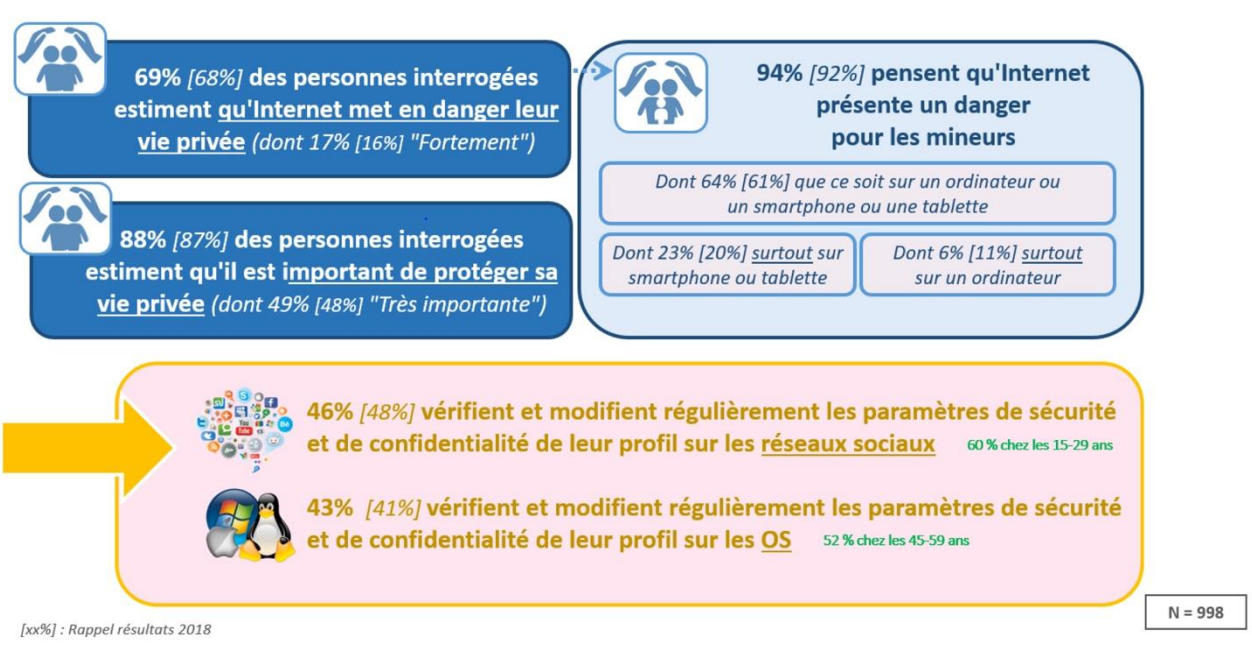


Figure 116 – Menace sur la vie privée par Internet : les convaincus

Même constat à l'opposé, puisque de moins en moins de personnes (26 %) pensent qu'Internet ne met pas leur vie privée en danger, soit un recul constant de 2 points par rapport à 2018 et même 4 points par rapport à 2016. En 2020 comme en 2018, ce sont les ouvriers, avec 10 % qui sont les plus représentatifs de cette catégorie.

Cette tendance se confirme également dans la perception de ceux qui pensent qu'il n'est pas important de protéger sa vie privée, puisqu'ils ne sont plus que 12 % en 2020 là où ils étaient 13 % en 2018. En tête de

cette catégorie se trouvent les ouvriers, avec 18 % des réponses données. Les cadres supérieurs, qui arrivaient en tête en 2018 avec 20 % ne sont plus que 15 % en 2020.

Si la prise de conscience des menaces qui pèsent sur leur vie privée est bien ancrée chez les sondés, force est de constater que cela n'est pas forcément suivi d'effet lorsqu'il s'agit de faire le nécessaire pour se protéger, puisque, globalement, on constate une érosion plus que significative dans la revue et la modification des paramètres de sécurité des réseaux sociaux et des systèmes d'exploitation (OS).

Concernant la sécurisation du profil des internautes sur les OS, même si un regain sensible se fait sentir, puisque l'on passe d'un taux de 41 % en 2018 à 43 % en 2020, c'est un peu l'arbre qui cache la forêt : seulement 46 % des personnes sondées vérifient régulièrement leurs paramètres de confidentialité sur les réseaux sociaux, ce qui représente un recul régulier de 2 % par an depuis 2016. Même constat à l'autre bout de l'échelle, puisque les internautes sont 38 % (+ 8 points par rapport à 2016) à ne pas vérifier et modifier ces paramètres régulièrement.

De même, 48 % des sondés ne vérifient pas et ne modifient pas régulièrement ces paramètres sur les OS, ce taux dépassant ainsi, pour la première fois depuis 2016, celui des internautes qui le font. Là encore, la progression est notable, puisque « seulement » 41 % ne le faisaient pas en 2016.

Les 15-29 ans utilisent presque tous les réseaux sociaux et les 45-59 ans ont vécu la naissance de l'informatique grand public. Ces derniers, contrairement aux générations Y et Z, ont appris à se servir d'un ordinateur et pas seulement à consommer l'informatique. C'est donc sans surprise que ce sont majoritairement les 15-29 ans (60 %) qui s'intéressent aux paramètres de sécurité des réseaux sociaux et les 45-59 ans (52 %) qui sécurisent les systèmes d'exploitation.

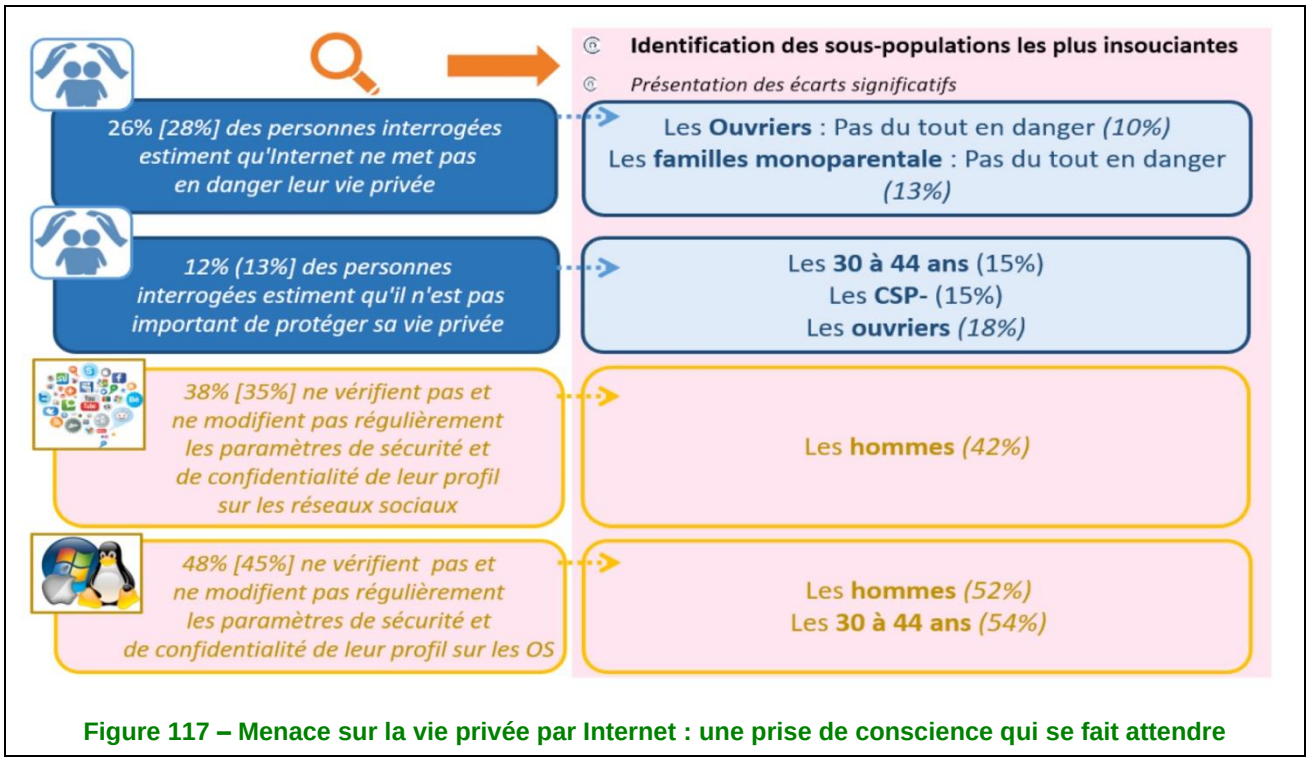


Figure 117 – Menace sur la vie privée par Internet : une prise de conscience qui se fait attendre

La perception du risque pesant sur les données est en hausse en 2020

Faisant écho aux précédents résultats et à la perception d'insécurité de la vie privée sur Internet, les personnes sondées sont en phase pour affirmer que, quel que soit l'équipement utilisé, le risque qui pèse sur les données est bien réel et suit globalement la même répartition qu'en 2018, même s'il existe une forte disparité de cette perception selon les équipements utilisés : les utilisateurs de tablettes/mobiles sont ainsi 63 % à estimer que les risques sur les données sont importants ou très importants, contre 54 % d'utilisateurs d'ordinateurs.

À l'opposé, seulement 26 % des sondés estiment ne courir aucun risque ou se trouver face à des risques peu importants en utilisant des tablettes/mobiles, alors qu'ils sont 37 % dans le même cas lorsqu'il s'agit d'un ordinateur.

Ce podium est le même qu'en 2018 et 2016 et l'écart de ressenti entre les deux populations est toujours important, même s'il tend à se réduire (de 16 % en 2016 à 11 % en 2020).

Une autre tendance vient confirmer ce qui a été vu précédemment, à savoir une hausse prononcée et globale de la perception du risque entre 2018 et 2020 : elle passe de 50 % à 64 % sur tablettes/mobiles et de 47 % à 54 % sur ordinateurs.

Enfin, la part des personnes qui ne sont pas capables d'estimer le risque encouru se réduit pour les utilisateurs de tablettes/mobiles, passant de 19 % en 2018 à 10 % en 2020 et rejoignant presque celle des utilisateurs d'ordinateurs (qui passent de 10 % en 2018 à 9 % en 2020).

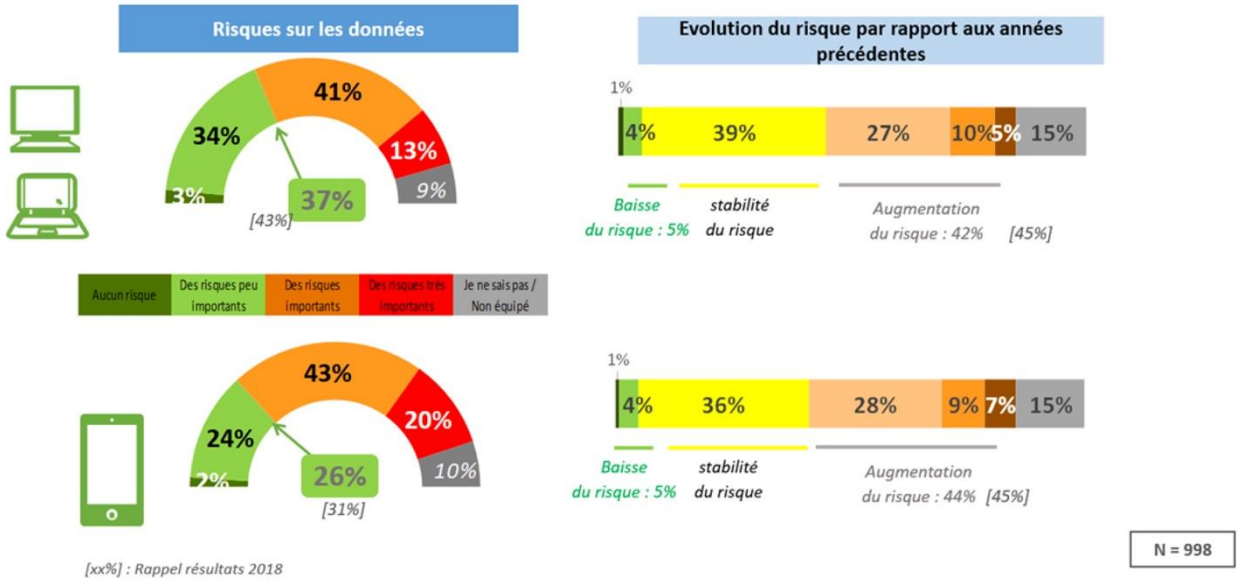


Figure 118 – Perception de la menace selon les équipements

Un quart des internautes dans l'incapacité d'estimer s'il existe un risque pour les données avec les objets connectés

En ce qui concerne l'appréhension du risque sur les objets connectés, la tendance observée entre 2018 et 2020 est la même que pour les utilisateurs de tablettes/mobiles et ordinateurs. Ceux qui pensent qu'il existe un risque « important ou très important » sur les données dépassent (50 %) ceux qui estiment que le risque est « peu important ou nul » (25 %) et leur taux augmente par rapport à 2018 (respectivement 36 % et 32 %).

Deux nombres sont toutefois remarquables :

- la proportion des sondés qui estiment que, lorsqu'il s'agit d'objets connectés, le risque sur les données est « très important » puisqu'il fait plus que doubler entre 2018 et 2020 passant de 8 % à 19 % ;
- le nombre d'internautes étant dans l'incapacité d'appréhender le risque quand il s'agit d'objets connectés, même s'il se contracte fortement en 2020 (32 % *vs* 25 % 2018), reste malgré tout 2,5 fois supérieur à celui des catégories précédemment étudiées.

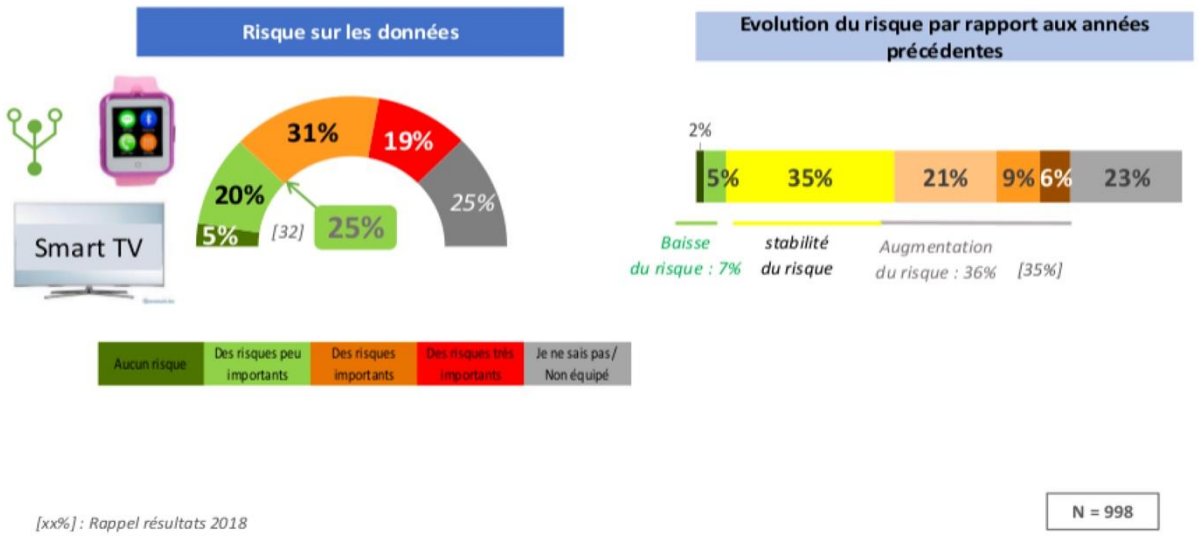


Figure 119 – Perception de la menace sur les objets connectés

L'ordinateur perçu comme l'équipement le plus sûr pour payer en ligne

Comme en 2016 et en 2018, les internautes pensent que l'ordinateur est plus sécurisé que les tablettes/mobiles lorsqu'il est question de payer en ligne, même si leur proportion se réduit notablement depuis le dernier sondage, passant de 39 % en 2018 à 33 % en 2020.

Toutefois, ce taux rejoint celui des internautes qui pensent que les ordinateurs et les tablettes/mobiles se valent en termes de sécurisation pour les paiements en ligne. Ils sont 34 % en 2020, une variation à la hausse négligeable sur deux ans puisqu'ils étaient 32 % en 2018 et 2016.

Enfin, en 2020, seuls 4 % des internautes (3 % en 2016 et 2018) pensent que le paiement via mobiles sont plus sécurisés qu'avec un ordinateur.

Pensez-vous que le paiement sur Internet est aussi sécurisé depuis un ordinateur et depuis un smartphone ou une tablette ?

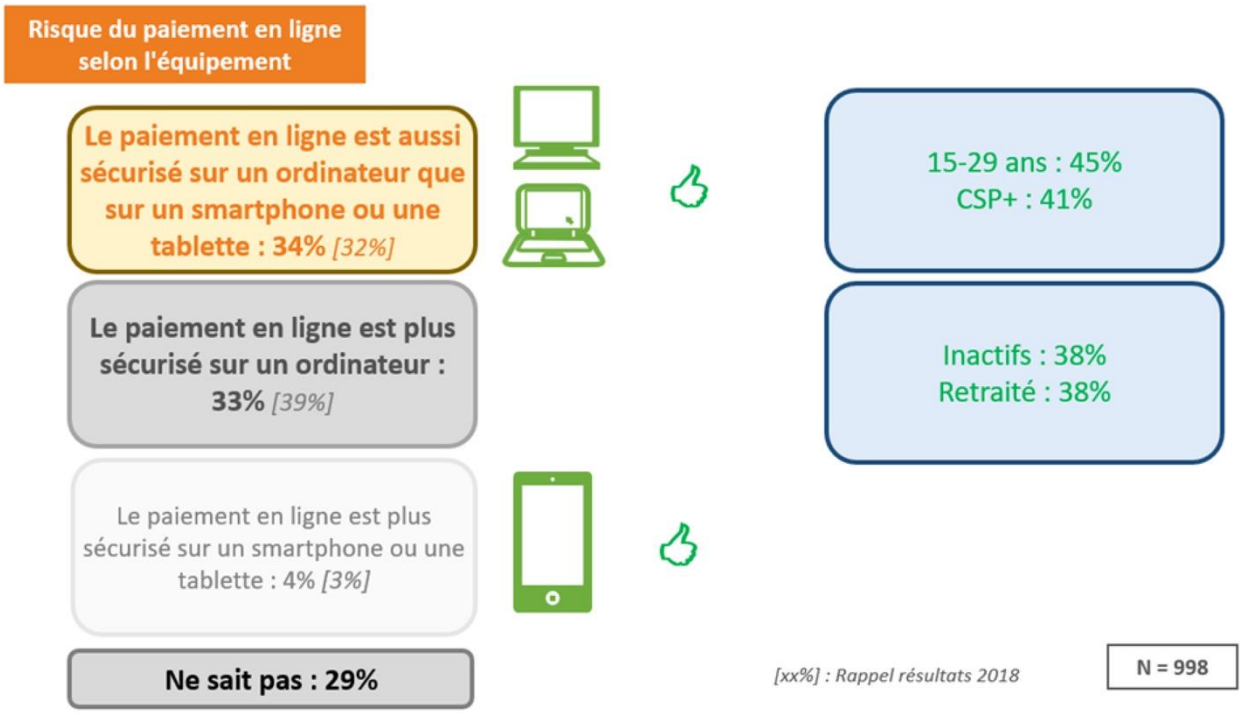


Figure 120 – Perception de la sécurisation des paiements en ligne

Un tiers des internautes ne savent toujours pas si le cloud est plus risqué que l'hébergement local

La part des internautes qui ne se sentent pas en capacité d'évaluer le risque du cloud comparé à celui d'un hébergement local est encore plus importante que pour les objets connectés ou le paiement en ligne : 32 % sont dans ce cas, ce taux étant stable depuis 2016, aussi bien pour la perte ou la destruction des données que pour l'atteinte à la confidentialité de ces dernières.

Les sondés pensent à parts quasi égales que le cloud est aussi sécurisé que l'hébergement local, avec un léger avantage pour la perte ou la destruction des données (31 % contre 29 % pour la confidentialité), cette tendance se maintenant, là aussi, depuis 2016.

Lorsqu'il s'agit de prendre parti pour l'une ou l'autre des solutions, les internautes se répartissent de la même manière depuis 2016 concernant le risque de perte ou de destruction de données : ils pensent en effet que l'hébergement local est plus risqué que le cloud, avec un taux quasi stable à 24 % en 2020. *A contrario,* une tendance à la baisse se dégage depuis 2016 chez les internautes qui pensent que le risque lié au stockage local est moindre que le celui lié au cloud, passant de 17 % en 2016 à 13 % en 2020. De fait, l'écart entre ces deux groupes augmente et s'élève à présent à 11 points.

En ce qui concerne le risque lié à la confidentialité des données, bien que les résultats soient en dents de scie depuis 2016, il reste établi que les internautes pensent qu'il est plus important dans le cas du cloud que de l'hébergement local. Avec un écart de 5 points enregistré entre les deux groupes, en 2020, les internautes sont désormais 17 % à penser que le risque est plus élevé si l'hébergement est local et 23 % s'il est assuré dans le cloud. Ils étaient respectivement 19 % et 20 % en 2018 et 18 % et 22 % en 2016.

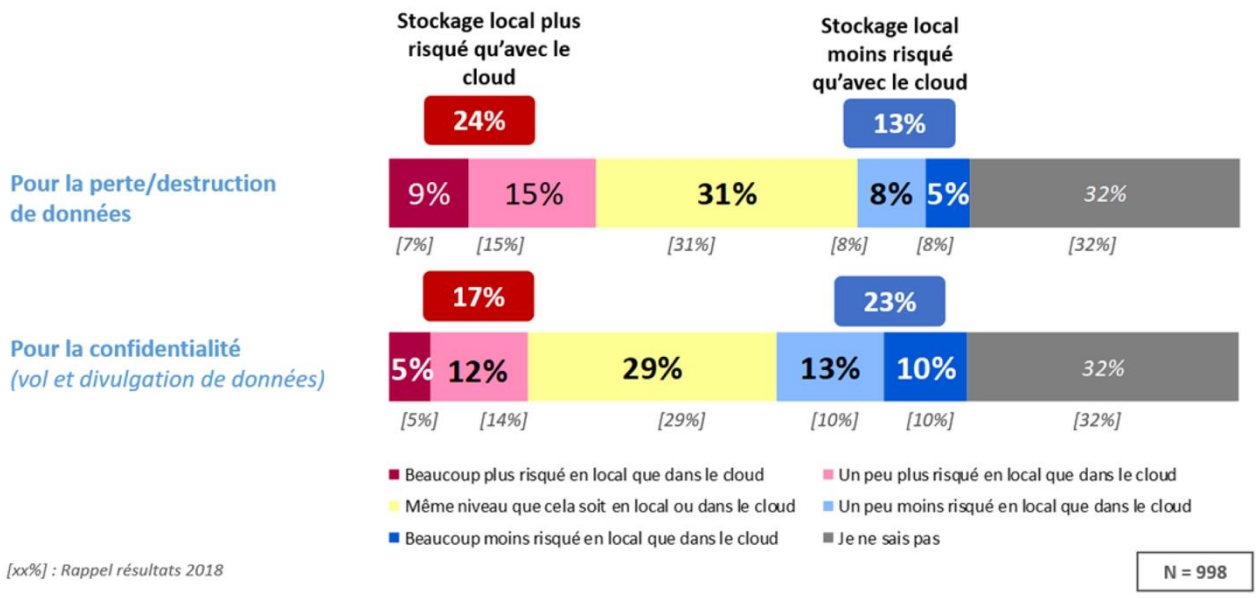


Figure 121 – Perception des risques liés au cloud

À la baisse depuis 2016, moins de deux personnes sur trois se sentent en sécurité sur Internet

À l'image du ressenti de la menace sur la vie privée et la confidentialité des données évoqué en début de chapitre, la part des internautes qui ne se sentent pas en sécurité sur Internet est à la hausse depuis 2016.

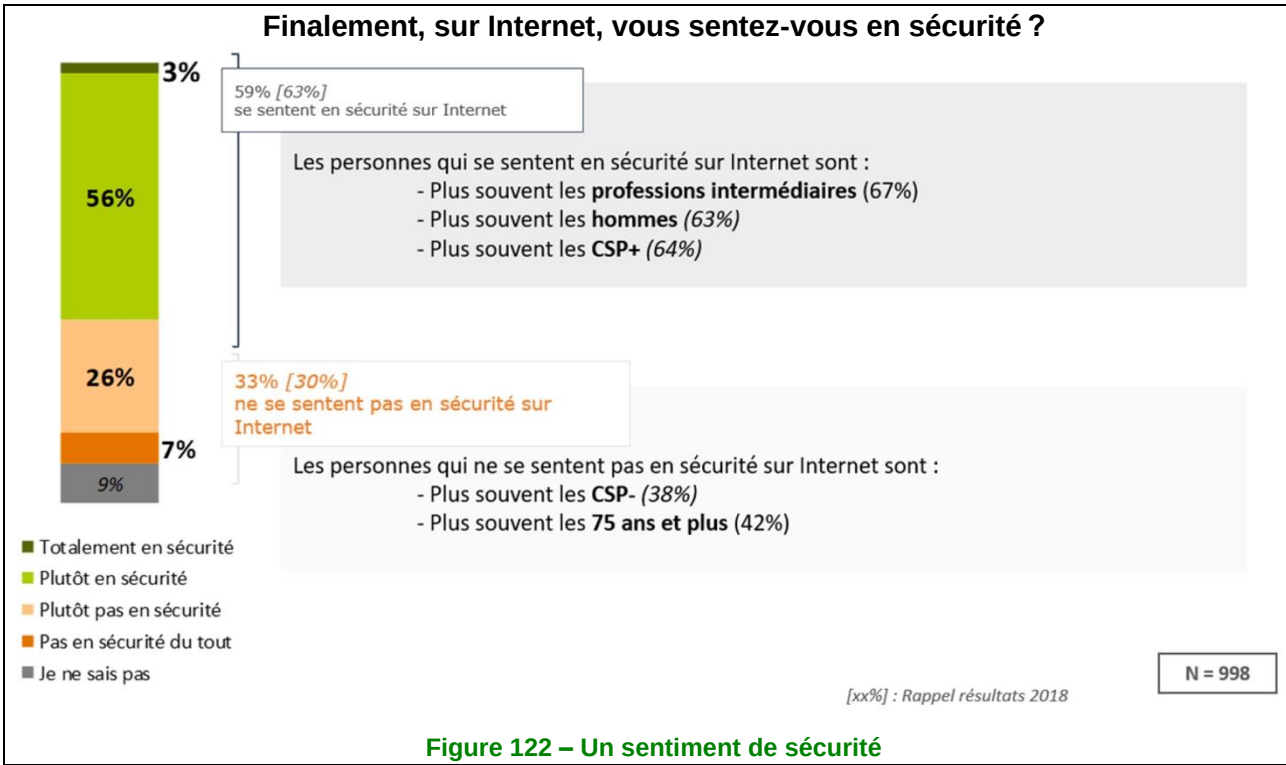


Figure 122 – Un sentiment de sécurité

Ils étaient alors 27 % puis 30 % en 2018, pour atteindre 33 % en 2020. À l'autre extrémité, et même si, *a contrario,* la tendance est à la baisse depuis 2016, une majorité d'internautes se sent encore plutôt ou totalement en sécurité sur Internet, puisqu'ils sont 59 % en 2020 contre 63 % en 2018 et 66 % en 2016.

C'est donc un constat paradoxal, puisqu'il était observé en début de ce chapitre que 68 % des personnes estiment qu'Internet met en danger leur vie privée.

La perception des menaces est à la hausse

La perception par les internautes de l'origine des menaces, en 2020, est soit à la hausse soit équivalente sur tous les points évoqués en 2018. Plus particulièrement, trois considérations passent au-dessus de 4,5 sur une échelle de 5. Il s'agit de :

- la présence de logiciels espions sur smartphone ou tablette ;
- les escroqueries liées aux réseaux sociaux ;
- les messages indésirables envoyés sur messagerie.

Aux extrémités de cette échelle, on retrouve en tête les menaces liées aux logiciels malveillants et, dans le bas du classement, des menaces liées à des causes non malveillantes.

En dehors de ces cas, deux grandes familles se distinguent :

- au-dessus de 4,5 :
  - les menaces qui pèsent sur la vie privée,
  - les menaces qui s'appuient sur les escroqueries ;
- au-dessous de 4,0 :
  - les menaces qui pèsent sur les données,
  - l'intrusion.

Les plus grosses progressions en 2020, avec 0,3 point, sont la perte des documents personnels (4,4) et le piratage des objets connectés (4,0).

Enfin, un scénario de menace fait son entrée dans cette édition 2020. Ayant marqué l'actualité des particuliers en 2019, le « chantage à la webcam » a retenu l'attention des internautes avec 3,9.

Parmi cette liste de menaces qui peuvent peser sur votre informatique personnelle, merci d'indiquer si vous considérez personnellement qu'elle peut, en l'absence de protection adaptée, représenter un risque nul, peu important, important ou très important

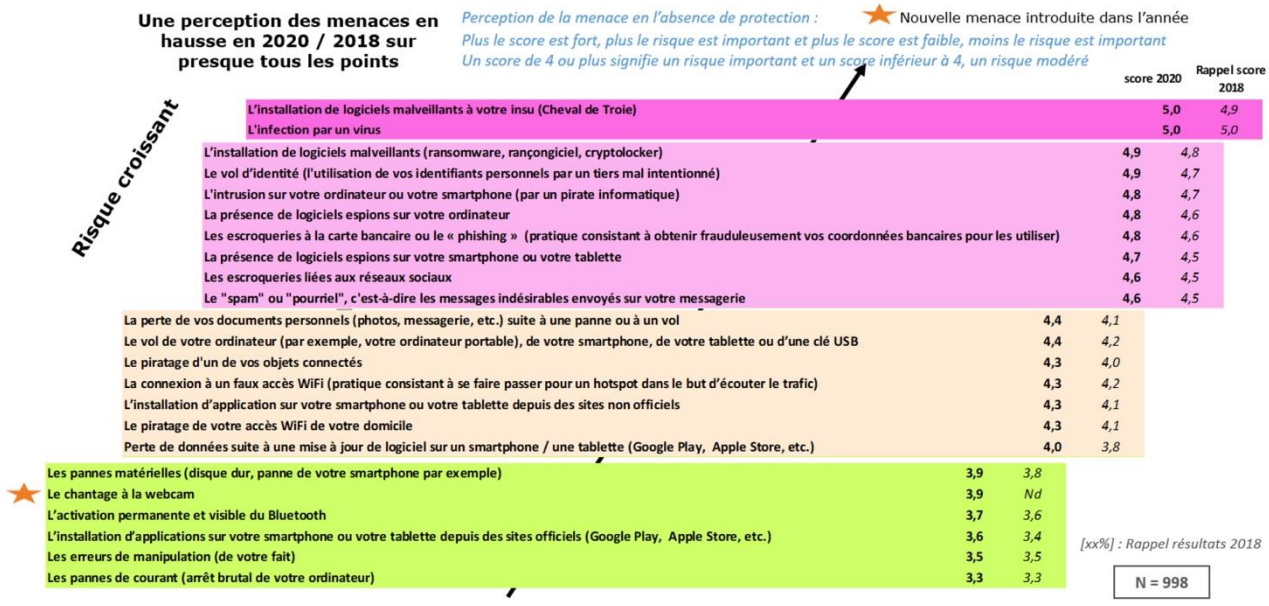


Figure 123 – Classement des menaces

Une prise de conscience de l'importance du traitement des mots de passe ?

Contrairement à ce qui vient d'être vu, les éléments qui influencent les scénarios de menaces stagnent ou baissent dans la majorité des cas. Malgré tout, quelques facteurs se retrouvent à la hausse parfois de façon prononcée. C'est le cas de l'absence de mise à jour des mots de passe qui fait un bond de 0,5 point en 2020 passant de 4,6 en 2018 à 5,1.

Le sujet des mots de passe progresse dans sa globalité puisque l'utilisation d'un mot de passe simple et la reprise systématique du même mot de passe augmentent tous les deux de 4,8 en 2018 à 5,0 en 2020.

Sont également en hausse :

- la divulgation de ses coordonnées sur Internet (de 4,9 à 5,1) ;
- l'absence de mise à jour de son système d'exploitation (de 4,3 à 4.5) ;
- l'absence de mise à jour du navigateur (de 4,0 à 4.1).

A contrario, l'absence de mise à jour de l'antivirus est à la baisse et passe de 5,1 en 2018 à 5,0 en 2020. Ce constat à la baisse se fait également sur tout ce qui pourrait s'apparenter à la mise en place de solutions techniques (antispam, antivirus, firewall…).

Parmi cette liste de situations et de pratiques, pouvez-vous indiquer si elle est de nature à augmenter les risques très fortement, fortement, faiblement ou pas du tout ?

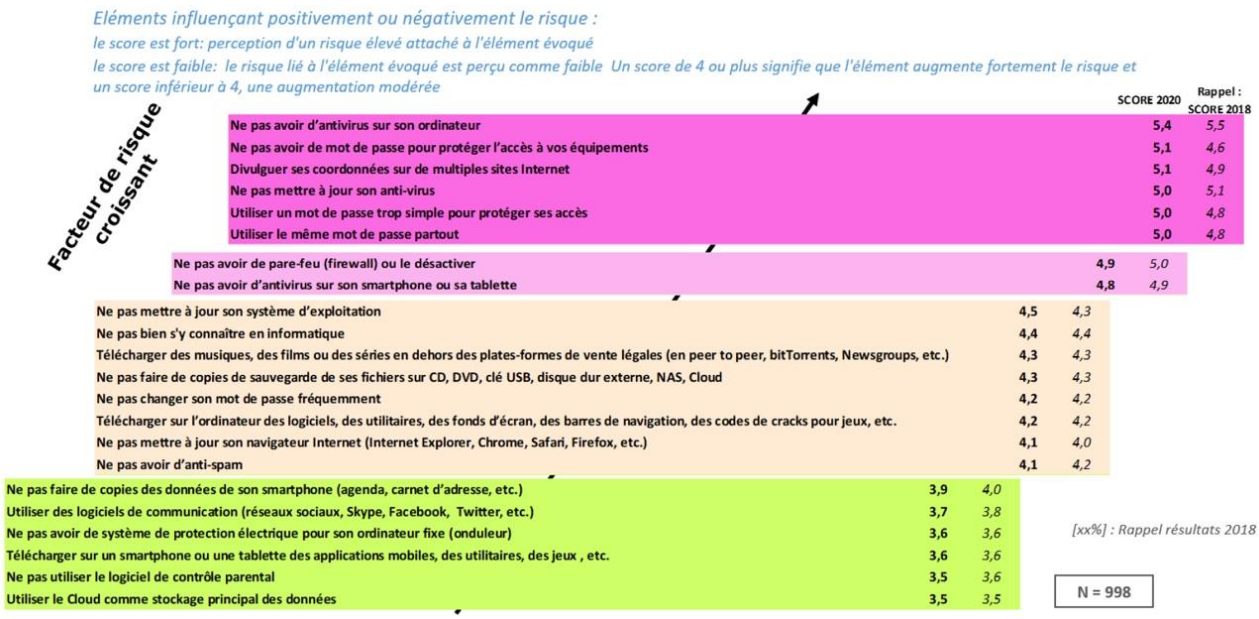


Figure 124 – Les facteurs qui participent à la perception de la menace

Une nette hausse des rançongiciels à l'origine de la perte des données sur ordinateurs

Concernant le taux d'incidents (perte ou vol de données), la tendance est indéniablement à la baisse depuis 2016, et ce quel que soit l'équipement utilisé :

- sur **ordinateur**, 14 % des internautes ont subi ce type de désagrément en 2020 contre 16 % en 2018 et 19 % en 2016 ;
- sur **tablette ou mobile,** ils sont 9 % en 2020, ce qui représente 3 points de moins par rapport à 2018 et 2016 (12 %) ;
- dans le **cloud,** 5 % des internautes ont été touchés en 2020 contre 9 % en 2018 et 8 % en 2016.

Les raisons de l'origine des incidents sont diverses, mais plusieurs points remarquables apparaissent.

Pour les tablettes/mobiles

- Le taux des incidents liés au matériel ou à un logiciel malveillant n'a pas évolué sur deux ans (respectivement 37 % et 24 %).
- Avec 37 %, les incidents liés aux problèmes matériels restent majoritaires. Cette catégorie recouvrant entre autres la perte, la casse et le vol, il est facile d'attribuer ce constat à la petitesse et au nomadisme des équipements concernés.
- Après avoir chuté en 2018 à 15 %, le taux des incidents liés à un dysfonctionnement logiciel repart à la hausse à 24 %, dépassant le taux de 2016 (21 %).
- La part des internautes ne connaissant pas la nature de l'incident se réduit de 20 % à 17 %, les tablettes et les mobiles étant le seul équipement à enregistrer une baisse dans cette catégorie en 2020.

Les ordinateurs

- Globalement, les variations sont en dents de scie depuis 2016. Le taux des internautes qui ne savent pas expliquer pourquoi un incident a eu lieu est la seule exception où une tendance à la hausse apparaît, passant respectivement de 18 % à 21 % de 2016 à 2018 pour atteindre 29 % en 2020.
- Les incidents liés aux logiciels malveillants font un bond de 10 points, passant de 27 % en 2018 à 37 % en 2020, mais restant toutefois en deçà de ce qui était observé en 2016 (42 %).
- On observe une augmentation des incidents liés à un dysfonctionnement logiciel (24 % en 2020 contre 18 % en 2018), leur taux dépassant celui de 2016 qui s'évaluait à 19 %.
- Quant aux incidents liés aux erreurs de manipulation ou affectant le matériel, ils se contractent fortement en 2020, passant respectivement de 34 à 19 % et de 30 à 22 %. Cela représente perte de 4 points pour chacun d'entre eux depuis 2016, où ils étaient à 23 et 26 %.

Dans les 24 derniers mois, avez-vous subi une perte ou un vol des données qui étaient stockées localement sur votre ordinateur, localement sur votre smartphone ou votre tablette ?

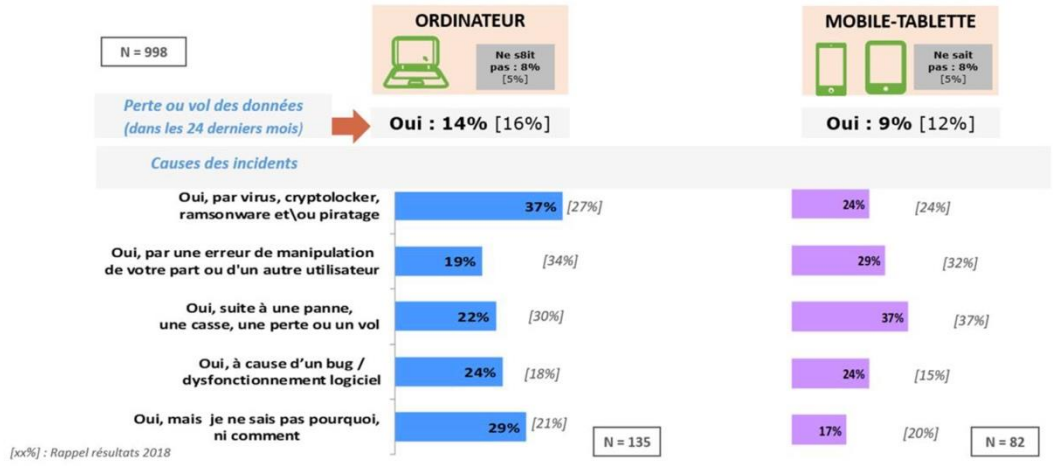


Figure 125 – Nature des incidents sur ordinateurs et tablettes/mobiles

Le changement des conditions d'utilisation des services, première cause de la perte des données des internautes sur le cloud

Avec les arrêts ou les modifications de services cloud populaires ainsi que les nombreux incidents ayant émaillé ces services et dont la presse se fait régulièrement l'écho, deux nouvelles catégories font leur apparition dans le sondage 2020 pour les incidents cloud ayant entraîné la perte de données :

- le changement des conditions d'utilisation d'un service (arrêt pur et simple, modification des règles d'utilisation, etc.) ;
- le dysfonctionnement d'un service.

L'apparition de ces nouvelles catégories interdit *de facto* la comparaison de ces résultats avec ceux des études précédentes ; toutefois, force est de constater que le taux d'incidents liés à un changement de condition d'utilisation fait une entrée remarquée, puisqu'avec 28 %, c'est la première cause, en 2020, des incidents cloud ayant entraîné des pertes de données chez les internautes sondés. Les autres causes sont en forte baisse, mais, comme pour la catégorie « ordinateur », la proportion des internautes ne sachant pas quelle est

l'origine de l'incident est en forte augmentation, passant de 11 % en 2018 à 22 % en 2020, dépassant même les 20 % de 2016.

Dans les 24 derniers mois, avez-vous subi une perte ou un vol des données qui étaient stockées dans le cloud ?

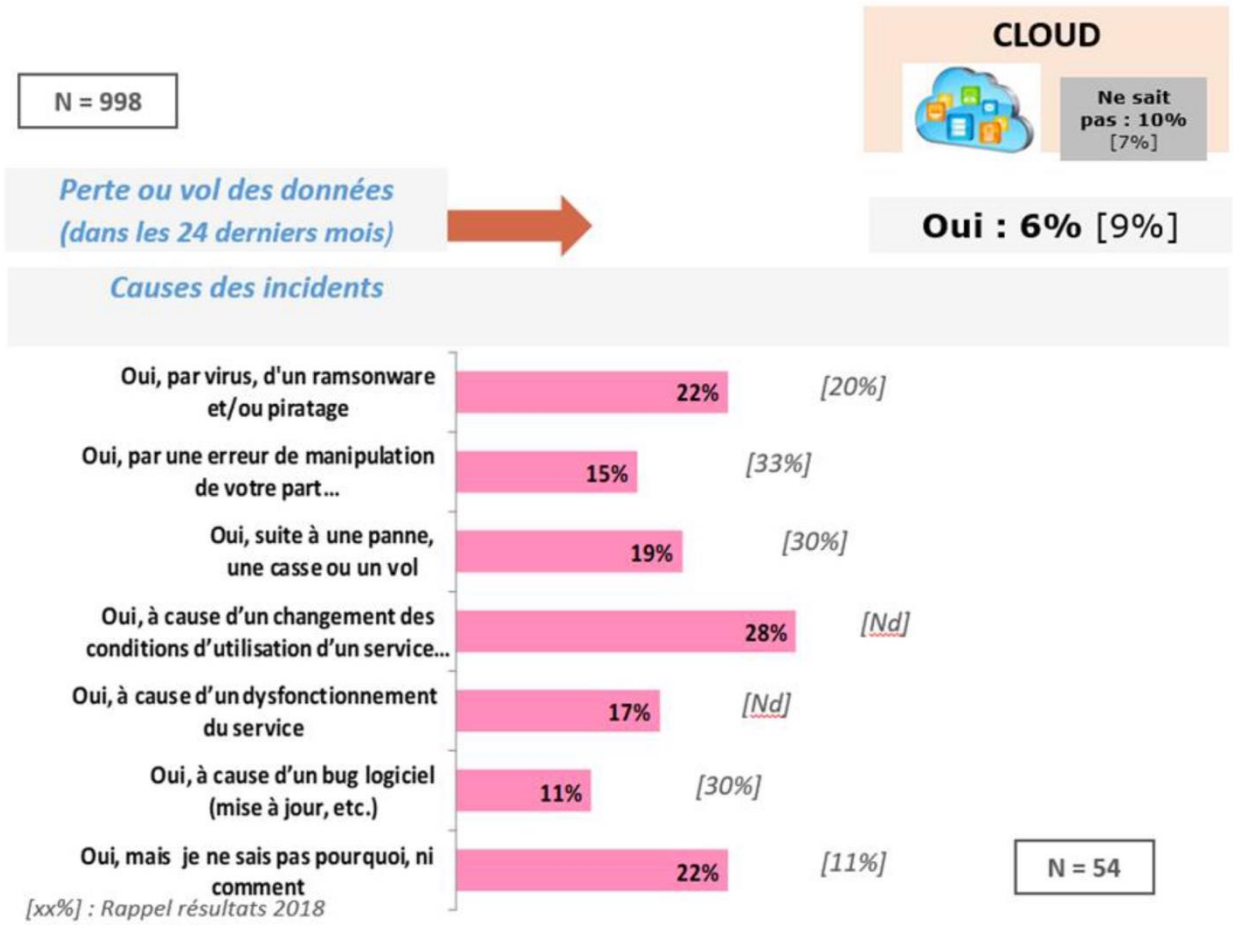


Figure 126 – Nature et réponse à incident sur le cloud

Partie IV – Moyens et comportements vis-à-vis de la sécurité informatique

Une baisse des moyens historiques de protection des équipements

La tendance relevée les années précédentes se confirme : les internautes s'équipent de moins en moins de solutions disponibles depuis de nombreuses années.

Ainsi, en 2016, 66 % des internautes équipaient leurs ordinateurs de packs de sécurité, contre 59 % en 2018 et 50 % actuellement. La baisse est encore plus notable concernant les antivirus qui étaient présents sur 88 % des ordinateurs en 2018 contre 80 % aujourd'hui, et sur 58 % des équipements mobiles en 2018 contre 53 % aujourd'hui. L'utilisation de pare-feu sur les postes passe de 77 % en 2018 à 70 % actuellement.

Les seules progressions, amorcées lors de la précédente étude concernent l'utilisation d'un mot passe au démarrage (+ 2 points sur les ordinateurs et + 9 points sur les équipements mobiles), d'un système d'authentification forte (respectivement + 15 points et + 4 points) et de moyens biométriques (+ 6 points et + 9 points), ces dernières technologies étant plus récentes.

Quels moyens de protection utilisez-vous pour garantir la sécurité de votre ordinateur/de votre smartphone ou de votre tablette ?

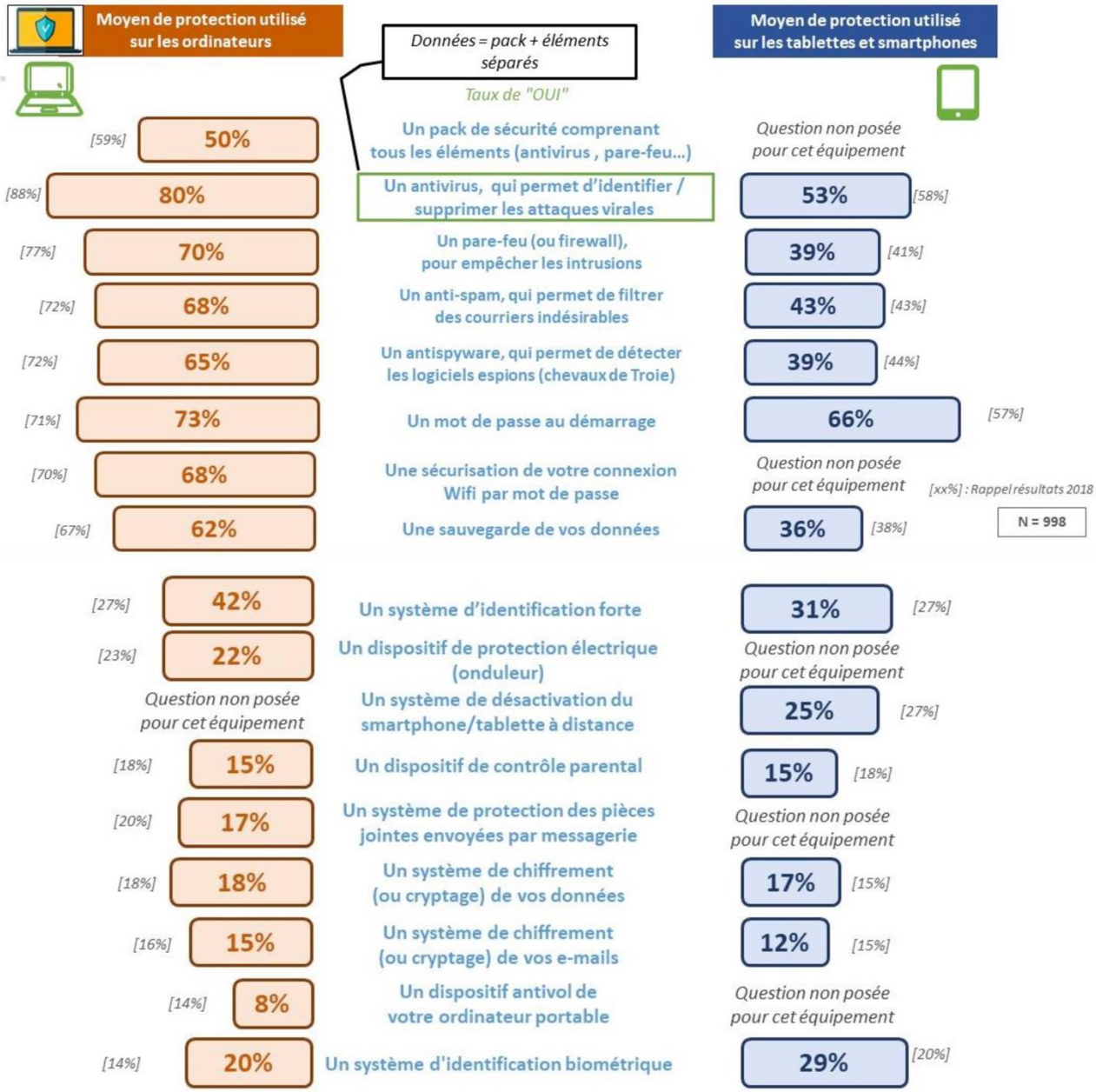


Figure 127 – Moyen de protection

Pratiques pour sécuriser les équipements

Si la part des internautes qui ont activé les mises à jour automatiques continue de baisser légèrement sur les ordinateurs (84 % en 2016, 82 % en 2018 et 79 % en 2020), sa progression s'accélère sur les équipements mobiles puisqu'elle passe de 53 % en 2016 à 57 % en 2018 et 65 % en 2020.

Concernant les autres bonnes pratiques pour sécuriser leurs équipements et leurs usages, les internautes évoluent progressivement vers un meilleur respect.

À noter toutefois que l'usage des pseudonymes pour protéger son identité est en baisse depuis plusieurs années, passant successivement de 70 % en 2016 à 67 % en 2018 et 65 % en 2020. De même, la proportion des internautes qui multiplient les sources d'information diminue pour passer de 57 % en 2018 à 51 % en 2020.

Quels comportements et bonnes pratiques adoptez-vous pour garantir et améliorer la sécurité de vos usages numériques ?

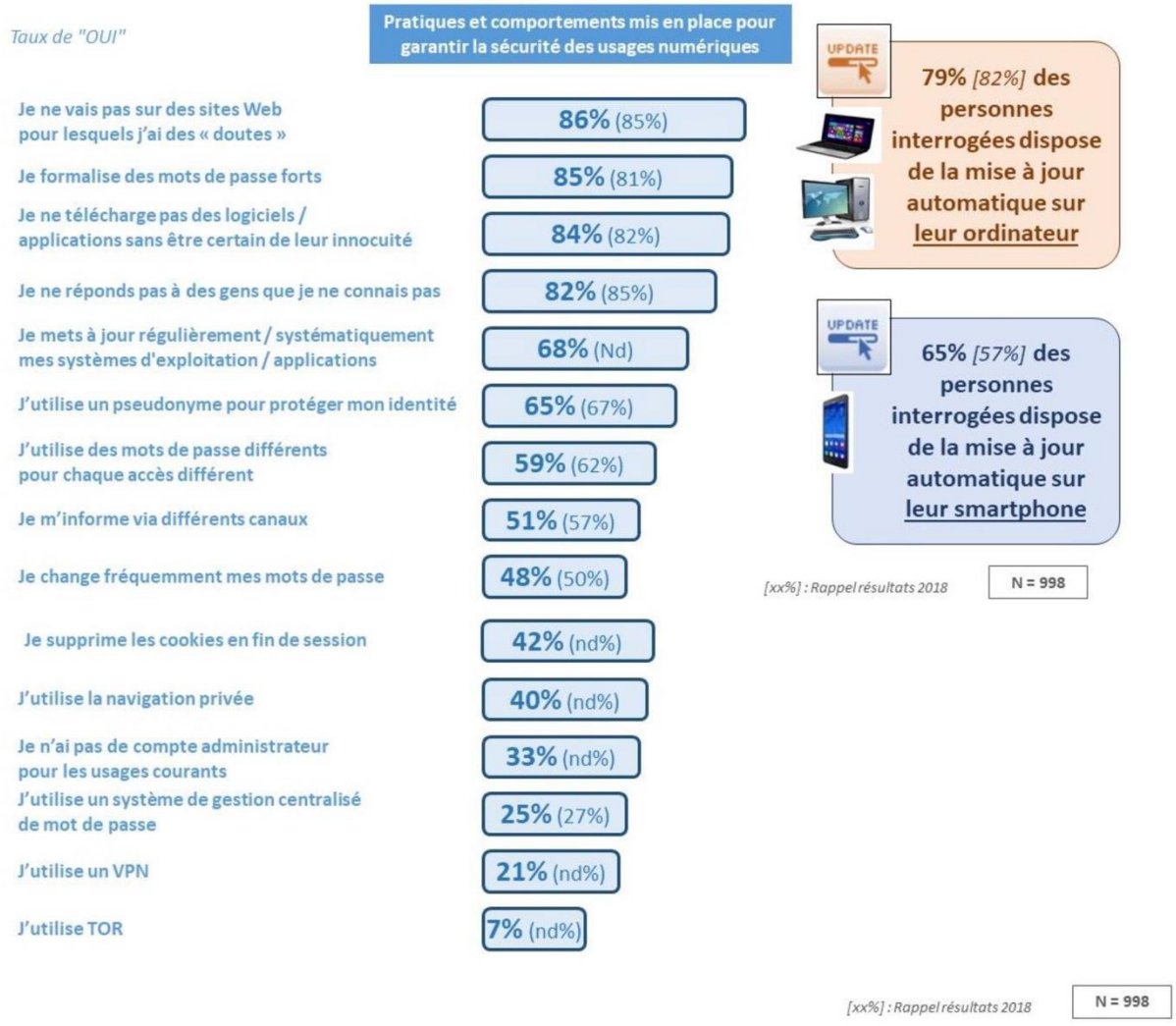


Figure 128 – Comportement et pratiques pour sécuriser les équipements et usages

On observe par ailleurs des taux de réponse positive assez importants sur l'utilisation de nouvelles bonnes pratiques pour lesquelles les internautes n'étaient pas interrogés les années précédentes.

Les bénéfices du RGPD non encore perçus

Le règlement général sur la protection des données (RGPD) s'applique depuis le 25 mai 2018 à toute organisation, publique et privée, quelle que soit sa taille (entreprise, ministère, administration, collectivité, association, etc.), mais il semble que les internautes ne soient pas encore à l'aise avec ce dispositif en qualité de consommateur. En effet, la part des sondés qui se sentent informés de leurs droits – renforcés par le nouveau cadre réglementaire – n'évolue que très peu entre 2018 et aujourd'hui, voire baisse pour certains.

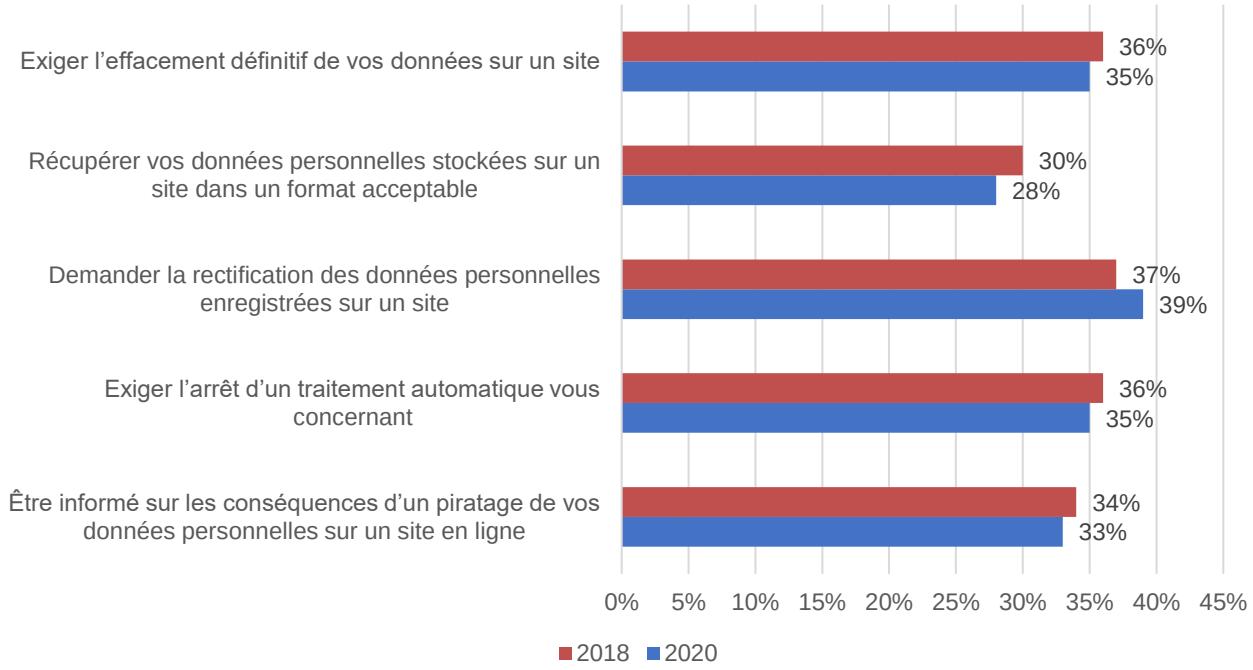


Figure 129 – Exercice de leurs droits par les internautes

Des prestataires spécialisés de plus en plus sollicités en cas de perte ou vol de données

Face aux incidents, les internautes réparent de moins en moins par eux-mêmes leurs équipements endommagés et font moins appel à leur entourage.

Si la majorité des internautes continue de se débrouiller seule, la part de ceux qui réparent eux-mêmes leur(s) ordinateur(s) passe de 43 % en 2018 à 38 % en 2020 ; ce taux suit une évolution globalement similaire pour les mobiles et les tablettes (38 % *vs* 46 % en 2018) et encore plus marquée pour le cloud, où il passe de 47 % à 31 %. De plus, la proportion de sondés qui font appel à des tiers bénévoles baisse très fortement, seuls 23 % des victimes ayant fait ce choix pour les ordinateurs en 2020 contre 40 % en 2018. On note que la baisse est encore plus brutale pour les mobiles et tablettes (44 % en 2018 *vs* 20 % en 2020) et, dans une moindre mesure, également pour le cloud (39 % en 2018 *vs* 17 % en 2020).

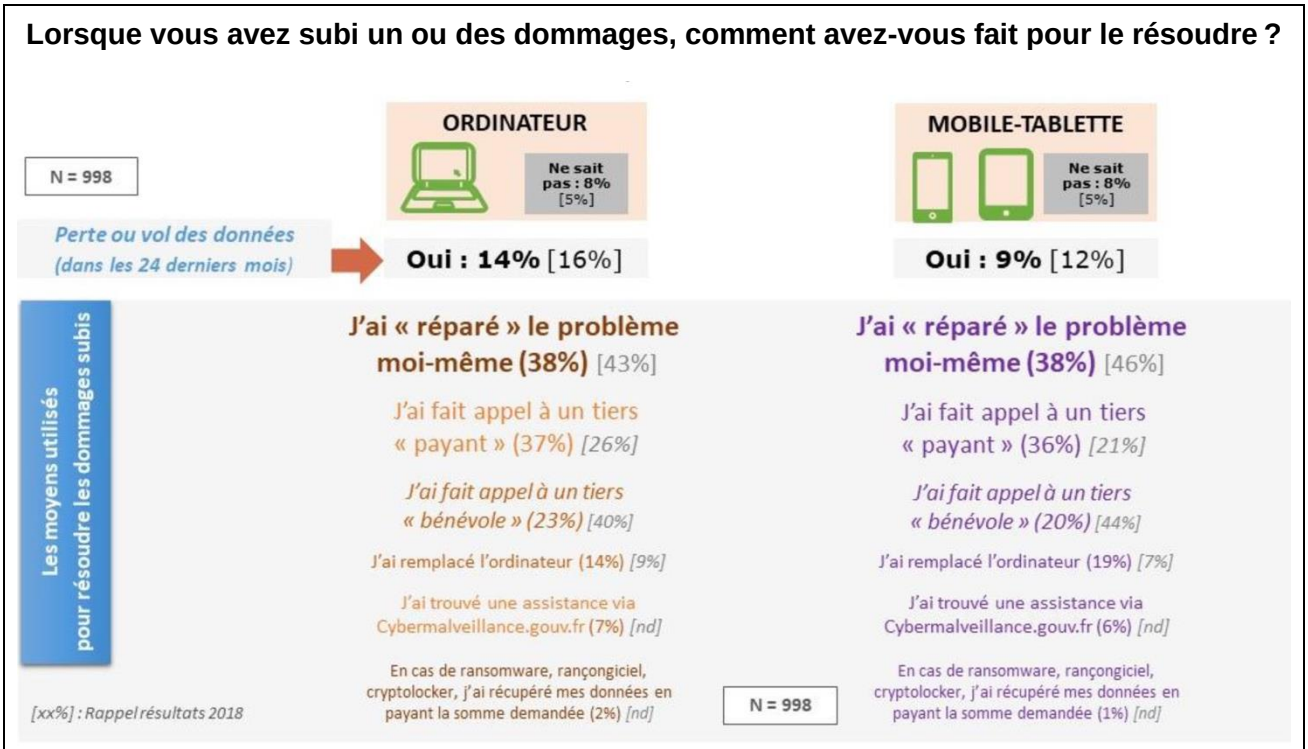


Figure 130 – Moyen de résolution des dommages pour les ordinateurs et mobiles/tablettes

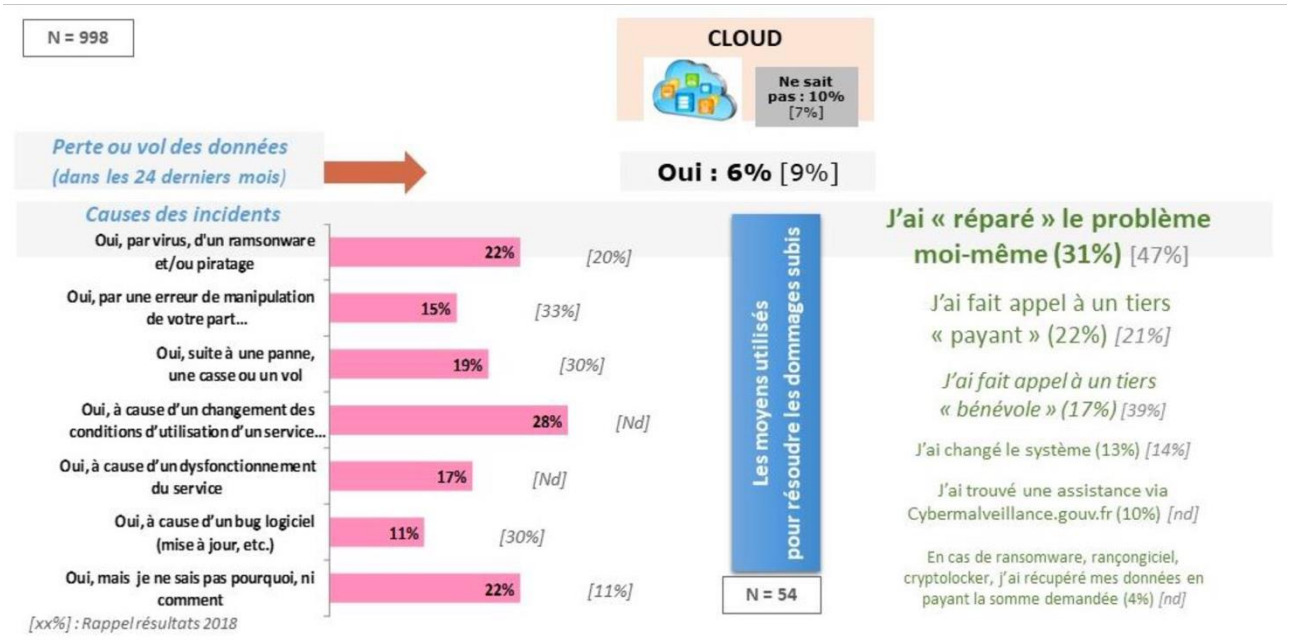


Figure 131 – Moyen de résolution des dommages dans le cloud

De manière générale, lorsque la résolution des dommages est déléguée à un tiers, elle se fait au bénéfice de prestataires non bénévoles, ces derniers arrivant aujourd'hui en premier choix pour assister les victimes : 37 % pour les ordinateurs (26 % en 2018), 36 % pour les mobiles/tablettes (21 % en 2018) et 22 % pour le cloud (21 % en 2018).

À noter l'arrivée dans ce classement, parmi les moyens d'assistance, du dispositif cybermalveillance.gouv.fr, lancé fin 2017 et qui n'apparaissait donc pas lors de l'étude de 2018 : 7 % des victimes y ont trouvé de l'assistance pour leur ordinateur, 6 % pour les tablettes et 10 % pour les données stockées dans un cloud.

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