Menaces informatiques et pratiques de sécurité en France

Édition 2018

- Les entreprises de plus de 100 salariés
- Les établissements de santé de plus de 100 lits
- Les particuliers Internautes

Club de la Sécurité de l'Information Français

Remerciements

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de cette étude, tout particulièrement :

Les responsables du groupe de travail

M. MOURER Lionel	ATEXIO	Responsable de l'étude et de la partie Entreprises
M. MONEGER Stéphane	CH BRIVE	Responsable de la partie Santé
M. NOTIN Jérôme	GIP ACYMA	Responsable de la partie Internautes

Les membres du Comité d'Experts

M. BAUDOT Christophe	SILPC
M. BEELMEON Richard	ALTRAN FRANCE
M. BEN AICHA Sofiene	HARMONIE TECHNOLOGIE
Mme BERARD Béatrice	CHU LYON
M. BLUM Patrick	ESSEC
M. BOCQUIER Olivier	ON-X
M. BODILIS Éric	HÔPITAUX DU TARN
M. CARRE Thibault	INQUEST
M. CASSOU-MOUNAT Bernard	ANSSI
M. FOUCAULT Jacques	CABINET CONSEIL J. FOUCAULT
M. GIORIA Sébastien	APPSECFR
M. HENNIART Thierry	RÉGION HAUTS-DE-FRANCE
M. JOUAS Jean-Philippe	CLUSIF
M. LABIDI Mehdi	ATEXIO
M. MAFILLE Hervé	UVU GROUP
M. MEYER Mathieu	GENWIN.TECH
M. MINASSIAN Vazrik	ADENIUM
M. MOISAN Noël	IT LINK
M. PETIT Adrien	INQUEST
M. STALTER Fabrice	CHRU STRASBOURG
M. WURSTHEISER Philippe	HUAWEI

Le CLUSIF remercie également vivement les représentants des entreprises, des établissements de santé 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

« *Ce qui compte ne peut pas toujours être compté, et ce qui peut être compté ne compte pas forcément.* ». C'est par cette citation d'Albert Einstein que je veux introduire cette nouvelle édition de MIPS. Parti du constat dans les années 90 que nous devions faire un inventaire de la sinistralité informatique, l'étude a petit à petit glissé vers la mesure des pratiques de sécurité. Percevons-nous toute la qualité des éléments remontés par notre étude ? Et quel sens les entreprises donnent-elles à ces résultats ?

Nous faisons le constat tous les deux ans d'une situation, celle de la plus ou moins prise en compte de la sécurité dans nos systèmes d'information, dans notre environnement numérique. Je me pose la question de l'usage que font nos lecteurs de cette étude, quelle conscience leur donne-t-elle ? Quelle perception ont-ils de la situation qu'est la leur, dans leur entreprise, leur établissement de santé ou leur collectivité territoriale ?

« *Ce qui compte ne peut pas toujours être compté…* ». Cette année encore, le RSSI manque de personnel et de budget, la fonction RSSI n'est pas encore clairement établie pour tous les secteurs et les entreprises de toutes tailles. MIPS tend à mettre en évidence une prise de conscience plus importante de la fonction de RSSI dans le monde de la santé. Quand verrons-nous une vraie progression des chiffres sur tous les fronts de la SSI et de la cybersécurité ? Certes les grandes organisations et les grands groupes disposent de moyens humains et financiers pour leur SSI. Mais les autres ? Comment leur faire comprendre les enjeux ?

« *… et ce qui peut être compté ne compte pas forcément.* ». Avons-nous loupé une métrique ? Un point de mesure dans notre étude ? Non, la pertinence de l'étude n'est plus à démontrer. Ce n'est pas de l'arrogance, c'est un constat. Ce que nous ne mesurons pas ici, ce n'est pas la sécurité telle qu'elle est perçue par ceux qui la font, les RSSI, les DSI et autres personnels de l'entreprise ou des organismes publics, mais bien la façon dont cette sécurité est assumée par les directions d'entreprise de toute taille. Il nous faudra passer par d'autres points de mesure pour expliquer la situation de nos entreprises. Poser la question aux seuls RSSI ne suffit plus.

Alors n'hésitez pas à vous servir de ces informations, de nombreuses institutions y font référence. Cette publication est faite pour être partagée, découpée, collée, citée et publiée. Il est urgent de faire savoir que nos entreprises ont grandement besoin d'un coup d'accélérateur pour leur SSI d'hier et leur cybersécurité d'aujourd'hui.

Le CLUSIF mène cette étude tous les deux ans car le travail est colossal. Il nous faut mobiliser les adhérents, des experts externes et un partenaire pour réaliser les statistiques. Je veux remercier ici, au nom du Conseil d'Administration, toutes celles et tous ceux qui s'investissent pour arriver à ce résultat. En particulier Luména DULUC et Lionel MOURER pour l'animation du Groupe de travail. Nous remercions aussi la collaboration avec la jeune plateforme « cybermalveillance.gouv.fr » pour son apport essentiel et pertinent sur la partie Internautes.

Jean-Marc GREMY

Président du CLUSIF

Synthèse de l'étude

Au travers de l'édition 2016 de son enquête sur les menaces informatiques et les pratiques de sécurité (MIPS), le CLUSIF réalise, comme tous les 2 ans, un bilan approfondi des usages en matière de sécurité de l'information en France.

Cette enquête se veut être une référence par la taille et la représentativité des échantillons d'entreprises (350 ont répondu) et des établissements de santé (200 ont répondu) interrogés. Par ailleurs, elle se veut relativement exhaustive, en prenant, cette année encore, l'ensemble des 14 thèmes de la norme ISO 27002:2013, relative à la sécurité des Systèmes d'Information.

Une modification majeure intervient cette année : l'enquête est structurée cette année de façon différente en termes de tranche d'effectifs, passant de 3 tranches (200-499, 500-999 et plus de 1 000 salariés) à 4 (100-249, 250-499, 500-1 999 et plus de 2 000 salariés). Ceci doit nous permettre dès 2018 et dans les années à venir d'identifier les pratiques des plus petites entreprises… Pour autant, des comparaisons (à isopérimètre) avec les années précédentes seront également effectuées.

Enfin, cette année comme depuis 2008, l'étude reprend le volet très complet consacré aux pratiques des particuliers utilisateurs d'Internet à domicile (1 000 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 : les attaques sont toujours bien présentes, mais… bis repetita, où est la gestion des incidents et le suivi de la sécurité ?

Point positif : le nombre d'acteurs de la SSI au travers de la mise en place d'organisations et de structures évolue toujours positivement… Pour autant, la « maturité SSI » stagne, principalement du fait 1] du manque de budget attribué à la SSI (36% des répondants), et 2] des contraintes organisationnelles (29%).

Côté budget, on constate une stagnation comparativement à 2016 (-1 point), pondérée par le fait que le poste ayant eu la plus grosse augmentation, cette année encore, est la mise en place de solution, avec 23% (27% des répondants ne savent pas…). On reste toujours dans la technique : ainsi pour beaucoup la sécurité reste une histoire de mise en place de solution technique…

Côté Politique de Sécurité de l'Information (PSSI), le nombre d'entreprises l'ayant formalisé continue sur la bonne pente à 75% (+ 6 points vs 2016 à isopérimètre) ; mais ce chiffre n'est que de 69% sur le nouveau périmètre, tiré vers le bas par les entreprises de 100 à 200 salariés. La DSI reste prépondérante dans la formalisation de la PSI (52%), alors que le RSSI est à 43%.

La fonction de Responsable de la Sécurité des Systèmes d'Information (RSSI ou RSI) est en recul entre 2016 et 2018 (67% vs 63%) et 85% des Banques-Assurances en ont un ! Les RSSI sont pour 49% d'entre eux rattachés à la Direction Générale améliorant grandement son « pouvoir d'arbitrage » et pour 30% à la DSI… L'importance du rôle de RSSI commencerait-elle à être comprise par les DG ?

Concernant les ressources humaines, les chartes sont maintenant bien déployées (84% en ont) et la sensibilisation s'établit à 50%, dont 15% qui la mesure.

L'inventaire des actifs est réalisé à 87% et 61% des entreprises ont classifié leurs actifs. Par ailleurs, si 80% des entreprises ont inventorié les risques auxquels elles sont exposées, seules 29% d'entre elles ont réalisé une évaluation formelle s'appuyant sur une méthode ou un référentiel (EBIOS à 24%, ISO 27005 à 21%, MEHARI à 11%, etc.).

La cryptographie est toujours peu utilisée (30% en font l'usage) et lorsqu'elle l'est, c'est la DSI qui en a largement le contrôle (72%).

La sécurisation physique passe par 3 dispositifs majeurs : détecteur incendie (73%), contrôle d'accès par badge (62%) et caméra (57%).

Du côté des technologies de protection, certains outils commencent à être un peu plus généralisés. Par exemple (chiffres 2016 vs 2018 à isopérimètre) : pare-feu sur PC portable passe de 80% à 88%, anti-virus/anti-malware sur smartphone et tablettes passent de 42% à 54%, pare-feu sur smartphone et tablettes passe 24% à 37%.

La formalisation des procédures de déploiement des correctifs de sécurité (patch management) est à 56% en 2018 et 75% des entreprises réalisent une veille permanente en vulnérabilités et en solutions de sécurité de l'information.

L'usage des équipements personnels (BYOD – Bring Your Own Device) est interdit pour 72% des entreprises…

La sécurité dans le cycle de développement régresse encore et de fait reste toujours trop insuffisante : prise en compte à 14%, - 3 points vs 2016 à isopérimètre ! Pourtant, un grand nombre d'attaques sont possibles du fait de failles applicatives liées au développement (injection, XSS, etc.).

L'infogérance représente toujours 44% de la gestion des SI des entreprises, dont 13% en totalité. Quand c'est le cas, 38% ne mettent toujours pas en place d'indicateurs de sécurité et 55% ne réalisent aucun audit sur cette infogérance. Ces chiffres sont encore plus flagrants sur les plus petites entreprises. Après une augmentation vertigineuse entre 2012 et 2016 (+28 points), l'utilisation du Cloud augmente toujours fortement cette année (+ 14 points) et près de la moitié (48%) des entreprises y font maintenant appel.

Côté « incidents de sécurité de l'information », le trio de tête est composé de (chiffre 2016 vs 2018 à isopérimètre) : pannes d'origine interne (31% vs 28%), infections par virus (44% vs 27%) et pertes de services essentiels 24% vs 22%). Malgré cela, seules 41% des entreprises disposent d'une cellule de collecte et de traitement des incidents de sécurité de l'information… De plus, au regard du Panorama de la Cybercriminalité du CLUSIF, 29% ont connu des attaques par Phishing (64% sans impact) et 17% via des fraudes aux présidents.

Pour la continuité d'activité, c'est l'indisponibilité des 'systèmes informatiques de gestion' qui représente le scénario le plus couvert (54%). Le BIA (Bilan d'Impact sur l'Activité), prenant en compte les attentes des « métiers » est réalisé 55% (dont 6 en cours) : comment les autres s'assurent-elles que leur PCA répond aux attentes de l'entreprise ? Enfin, pour ceux qui en dispose, 25% des plans « utilisateurs » et 20% des plans « IT » ne sont jamais testés : alors, sont-ils réellement efficients ?

Le RSSI n'intervient que pour 10% dans les déclarations « CNIL », en 4ème position après le DSI (34%), le Service RH (13%) et le CIL (11%). Le Règlement Général sur la Protection des Données (RGPD) a mobilisé de nombreuses ressources et 68% des entreprises se disent prêtes (dont 46% partiellement).

Sur une période de deux ans, 66% des entreprises interrogées ont réalisé au moins un audit ou contrôle de sécurité du Système d'Information (58% des audits d'architecture et 47% des tests d'intrusion). Ces audits sont motivés principalement par des exigences contractuelles ou règlementaires (33%), le respect de la PSSI (20%), des audits de tiers externes comme les assureurs ou les clients (16%).

Au secours : les tableaux de bord de la sécurité de l'information (TBSSI) baissent encore passant à 22% (vs 25% en 2016 à isopérimètre) ! 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…

Pour conclure ce résumé pour les Entreprises de plus de 100 salariés, on identifie clairement une meilleure maturité des plus grandes entreprises par rapport aux plus petites. Pour autant, les « attaques » sur l'information de désarment pas et chacun se doit de rester attentif dans la protection et prêt à réagir au moindre incident…

Établissement de santé : enfin une fonction RSSI au service de PSSI largement répandues !

L'enquête 2018 fait l'objet d'une modification significative de son périmètre, puisqu'il est étendu aux hôpitaux publics et structures d'hébergement médicalisé de plus de 100 lits. Les analyses développées dans ce document seront soit basées uniquement sur les données 2018, soit feront appel à des comparaisons avec les précédentes enquêtes avec des données 2018 « redressées périmètre 2014 ».

La sécurité des Systèmes d'Information de santé est soumise à un cadre réglementaire en constante évolution. Cette enquête va permettre de mesurer certains effets d'Hôpital numérique et autres exigences réglementaires (PGSSI-S, Certification des comptes, etc.). Elle traduit aussi les premiers impacts de la règlementation RGPD et des mises en œuvre des Groupements Hospitaliers de Territoire (GHT) : nouveaux métiers, stratégies de territoire, mutualisation…

Les résultats marquants de l'enquête MIPS 2018 du CLUSIF auprès des hôpitaux sont précisés ci-dessous.

Un des faits majeurs de l'étude est la Croissance spectaculaire du nombre d'établissements ayant formalisé leur PSSI (de 50% des établissements en 2014 à 92% en 2018). Le pilotage de la sécurité de l'information s'appuie majoritairement sur des normes ou des référentiels.

Beaucoup d'établissements ont effectué un inventaire au moins partiel de leurs risques, et en ont déduit un plan de réduction de ces risques. Le gestionnaire des risques est principalement le RSSI. Il est très positif de noter globalement une « croissante forte de la fonction RSSI » qui est attribuée dans 80% des établissements. Cela devient un « vrai métier » exercée à temps plein dans presque 1 établissement sur 2 (le chiffre a doublé en 4 ans). On parle maintenant d' « équipe » SSI dans 3/4 des établissements (+30%).

On constate par contre que les établissements sont incapables de bien évaluer les coûts liés à la sécurité de l'information (81% des répondants). De même, peu d'établissements (1/3) font une analyse de l'impact financier des incidents.

Cependant ces mêmes établissements affirment que budget sécurité de l'information est en augmentation pour 1/3 d'entre eux. C'est une tendance forte par rapport à la précédente enquête qui pointait majoritairement une stabilité des budgets pour 2 établissements sur 3. L'enquête pointe quand même le manque de budget (pour 52% des répondants) et le manque de personnel qualifié (43%) comme les principaux freins à la conduite des missions de sécurité de l'information. Et là, il n'y a malheureusement pas d'amélioration par rapport à l'étude de 2014.

Tous les établissements ou presque ont une charte d'utilisation du SI. D'autre part, de plus en plus d'établissements mettent en place des procédures de gestion des départs (de 60% à 80% des établissements). Enfin, 3 établissements sur 5 ont un programme de sensibilisation à la sécurité de l'information (en croissance de 50% sur 4 ans), avec un gros focus sur les VIP.

L'inventaire des actifs (informations et supports) est quasiment généralisé. L'inventaire, au moins partiel des risques devient une généralité (81% des répondants) cependant avec le bémol que seulement 1/3 des établissements utilise une méthode (EBIOS, ISO 27005, MEHARI).

On constate une très nette priorité à la protection des outils de mobilité qui prend ainsi en compte la transformation des usages en particulier le nomadisme. De même, Il y a une augmentation significative du nombre d'établissements de santé effectuant de la veille en vulnérabilité. Mais seulement 1 sur 2 formalise des procédures de déploiement de correctifs de sécurité. Enfin, ces vulnérabilités concernent un périmètre mal maîtrisé en particulier le biomédical.

Le fait notable dans les pratiques de sécurité est le filtrage des accès internet qui explose, puisqu'il passe de 14% en 2010 à 75% des établissements en 2018. Il y a Stabilité pour les interdictions qui frappent le BYOD (77%) et les RESEAUX SOCIAUX (44%).

Le recours à des spécialistes de l'hébergement de données de santé est relativement répandu puisque 42% des établissements ont externalisé tout ou partie de leur SI.

Les établissements semblent se donner les moyens de collecter les incidents de façon plus exhaustive, et d'être plus efficaces dans leur traitement (¾ des établissements ont une cellule contre moins de 50% en 2014). Parallèlement, l'enquête mesure un recul global de la sinistralité, mais les dépôts de plaintes et les signalements d'incidents graves restent faibles.

La gestion de la Continuité d'Activité continue à progresser dans le monde des hôpitaux à travers la mise en place de dispositifs de gestion de crise, ou la progression des tests de PCA/PRA.

Enfin, et concernant la conformité, plus de 8 établissements sur 10 déclarent être conformes aux exigences du Programme Hôpital Numérique. 56% des établissements seraient (partiellement) prêts pour le Règlement Général sur la Protection des Données (RGPD). Cette tendance, se matérialise en particulier à travers les audits puisque 7 établissements sur 10 déclarent mener en moyenne de 1 à 5 audits par an.

Internautes : de meilleures pratiques de sécurité, mais certaines sont encore difficiles d'adoption !

Cette année encore l'échantillon pour réaliser notre étude est représentatif, après redressement, de la population française. Cette population, pour la première année, utilise son téléphone mobile autant que son ordinateur portable pour se connecter à Internet.

Sur le plan de l'économie collaborative, les usages sont très différents entre l'Île-de-France (+5 points de 22% à 27%) et la province car ceux-ci restent stables au niveau national (16%). Concernant l'utilisation des équipements personnels utilisés dans un cadre personnel, la baisse identifiée en 2016 se poursuit au même rythme soit -4 points pour atteindre 36%. Le paiement des achats en ligne par les internautes se fait encore majoritairement sur un ordinateur plutôt que sur une tablette ou un téléphone mobile : 51% des sondés se refuse à utiliser des équipements mobiles pour finaliser un achat potentiel.

D'une manière générale, la perception des risques sur les données détenues par les internautes est relativement stable depuis 2014. Toutefois, la confiance continue de se dégrader pour les appareils mobiles. En parallèle, la perception des menaces liées à l'usage d'Internet sur la vie privée reste extrêmement forte, et stable depuis 2014 : 68% des sondés considère toujours en 2018 qu'Internet met leur vie privée en danger (16% fortement).

Malgré cette perception, seuls 58% déclarent vérifier et modifier régulièrement les paramètres de sécurité et confidentialité de leur profil sur les réseaux sociaux. En complément, l'étude ne montre pas d'évolution majeure dans l'utilisation des moyens de protection technique des équipements, et les équipements mobiles restent peu protégés : seulement un équipement sur deux dispose d'un moyen de protection.

Pour finir et concernant les Internautes, le niveau d'information liés au droit des internautes sur leurs données détenues par les fournisseurs de services numériques est encore très faible. L'entrée en application cette année du RGDP permettra, à n'en pas douter, une meilleure appréhension de ces droits et une meilleure protection des données personnelles que ces fournisseurs de services détiennent sur les internautes : l'étude 2020 permettra de le valider…

Pour conclure…

N'en doutons pas, la menace est encore bien présente et notre enquête montre de nouveau que les erreurs (et oui, personne n'est parfait), les malveillances (il paraît que c'est aussi un métier…) et les incidents de sécurité liés à l'information ne fléchissent pas !

La maturité des entreprises et des établissements de santé en matière de sécurité de l'information dépend encore pour beaucoup soit des « attaques » qu'ils ont vécu au sein de leur SI, soit des lois et règlements qui leur incombent. À quand une prise de conscience de la valeur de l'information sans obligation ? Le temps des politiques de sécurité « parapluie », que l'on formalise pour se donner bonne conscience, est globalement terminé ! les dirigeants doivent enfin le comprendre ! Il y va de la survie de leurs organisations, au regard des enjeux qu'elles portent et des données dont elles ont la responsabilité…

Alors, « au travail » et n'oublions pas « Un ordinateur en sécurité est un ordinateur éteint. Et encore…[1]. » !

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 de (liste non exhaustive) l'ANSSI[2], de la CPME[3], du GIP ACYMA[4] et bien entendu, du CLUSIF[5]…

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] Bill Gates (1955 -).

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

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

[4] www.cybermalveillance.gouv.fr

[5] https://clusif.fr/

Sommaire

Liste des figures

Méthodologie

L'enquête du CLUSIF sur les menaces informatiques et les pratiques de sécurité en France en 2018 a été réalisée de début janvier à mi-mars 2018, 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 2017.

Comme dans les études précédentes, trois cibles ont été retenues pour cette enquête en 2018 :

- les entreprises de plus de 100 salariés : 350 entreprises de cette catégorie ont répondu à cette enquête,
- les établissements de santé de 100 lits et plus : 151 d'entre eux ont accepté de répondre,
- les particuliers internautes (de 15 ans et plus) : 1 006 personnes, issues d'un panel d'internautes représentatifs, ont répondu à cette enquête 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 assez complète le niveau actuel d'implémentation des meilleures pratiques de ce domaine. Ces différents thèmes, numérotés dans la norme de 5 à 18, sont les suivants :

- 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 GMV Conseil en préservant un **total anonymat** 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 2018, 2016, 2014, etc. Les enquêtes ont été réalisées sur le premier trimestre de l'année de publication et les chiffres cités portent donc sur l'année précédente, respectivement 2017, 2015, 2013, etc.

Enfin, le groupe d'experts tient également 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 domaine spécifique de la sécurité du SI, de la personne répondant aux questions, de la « culture » et de la maturité de chaque entreprise, établissement de santé 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 du SI
- Thème 15 : Relations avec les fournisseurs
- Thème 16 : Incidents de sécurité
- 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 2018 de son enquête, le CLUSIF souhaitait interroger un échantillon d'entreprises légèrement différent que celui interrogé en 2014 et 2016. Le changement s'effectue dans la tranche d'effectifs des entreprises prises en compte, qui passent de 3 (200-499, 500-999 et plus de 1 000 salariés) à 4 (100-249, 250-499, 500-1 999 et plus de 2 000 salariés). Ce nouveau découpage permettra dans les années à venir de mieux comparer l'évolution de la maturité au sein des entreprises (en particulier les plus petites et les plus grandes).

Toutefois, les résultats de l'enquête ont également été analysés sur la base des effectifs 2016 (3 tailles d'entreprise) afin de pouvoir vérifier les écarts avec les années précédentes.

Les types d'entreprises ont été conservés tels quels afin de pouvoir comparer les progrès ou les éventuelles régressions. Ainsi, la cible est constituée des entreprises de plus de 100 salariés des secteurs d'activité suivants :

- Banque – Assurances,
- Commerce,
- Industrie - BTP,
- Services,
- Transport – Télécoms.

350 entreprises ont répondu à la sollicitation du CLUSIF (entretien de 27 minutes en moyenne), avec un taux d'acceptation d'environ 6% (8% en 2016) : sur 100 entreprises contactées, seulement 6 ont accepté de répondre à nos questions, ce qui a impliqué d'appeler environ 5 800 personnes !

L'échantillon est construit selon la méthode des quotas avec 2 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 INSEE.

Entreprise Taille / Secteur	100-249 salariés	250-499 salariés	500-1 999 salariés	2 000 et plus	Total	Total en %		Données INSEE
Banque - Assurance	12	3	4	5	**24**	**6,9%**	→	**5,1%**
Commerce	28	11	7	8	**54**	**15,4%**	→	**23,4%**
Industrie - BTP	83	49	15	11	**158**	**45,1%**	→	**37,1%**
Services	38	18	18	15	**89**	**25,4%**	→	**20,0%**
Transport – Télécoms	9	6	2	8	**25**	**7,1%**	→	**14,3%**
Total	**170**	**87**	**46**	**47**	**350**	**100,0%**		**100,0%**
Total en %	**48,6%**	**24,9%**	**13,1%**	**13,4%**	**100,0%**		↑ Redressement	
Redressement →	↓	↓	↓	↓				
Données INSEE	**62,9%**	**20,6%**	**13,4%**	**3,1%**	**100,0%**			

Au sein de chaque entreprise, nous avons cherché à interroger en priorité le Responsable de la Sécurité des Systèmes d'Information (RSSI). Celui-ci a répondu pour 25% (31% à iso périmètre pour 34% en 2016) des entreprises interrogées, mais plus de 40% dans les plus de 2 000 salariés.

Toutes tailles et secteurs confondus, les personnes sondées sont à plus de 73% des DSI (Directeur des Systèmes d'Information), des Directeurs ou Responsables informatiques ou des RSSI.

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. La question ne se pose plus.

Une légère reprise des budgets sécurité

Seules 20% des entreprises identifient les coûts (ce qui n'est pas forcément égal à un budget) liés à la sécurité de l'information.

Globalement, le pourcentage des budgets « constants » est de 35%, mais près de 33% des interviewés ne « savent pas » quelle est l'évolution du (de leur…) budget sécurité de l'information ! Reste que les budgets en augmentation (forte ou moyenne) se positionnent juste au-dessus des 30% et c'est dans l'Industrie-BTP que cette augmentation est la plus sensible (12%).

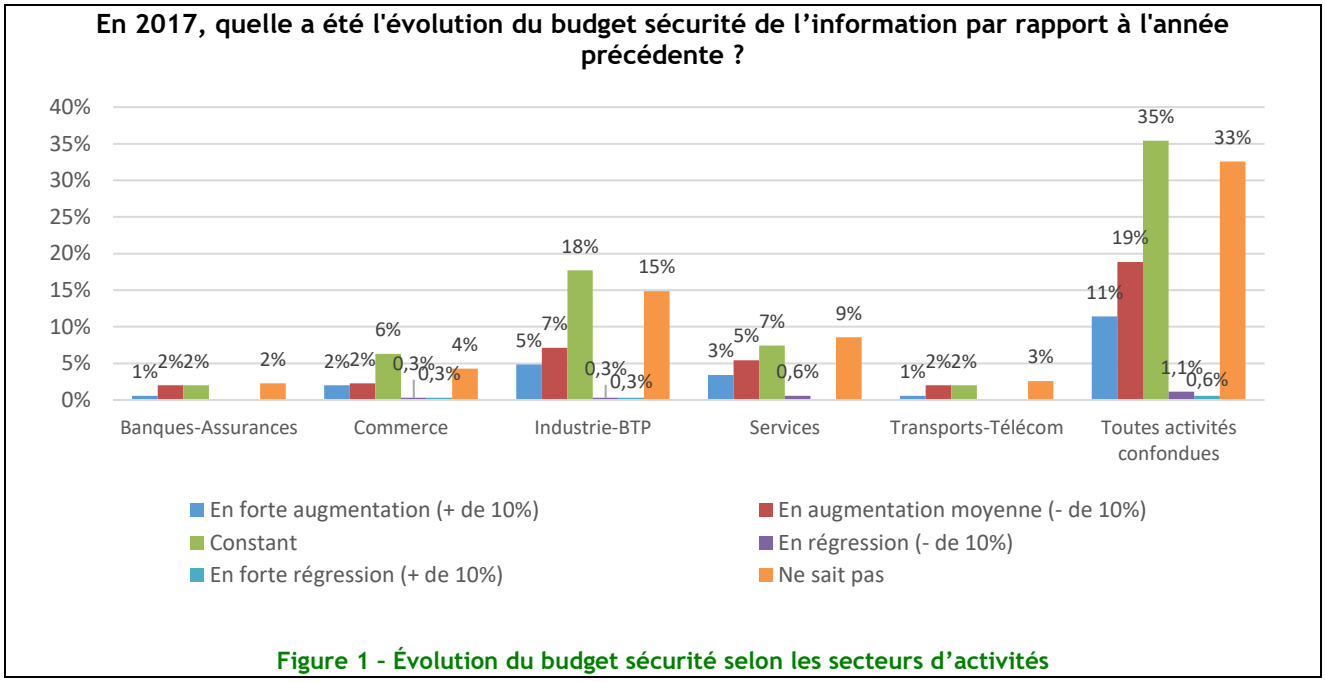


Figure 1 - Évolution du budget sécurité selon les secteurs d'activités

Par ailleurs, les postes prioritaires sont la « Mise en place de solutions » (23%), les « Contrôles & Audits » (17%) et la « Formation \ Sensibilisation » (12%) – à noter : la « Mise en place d'éléments organisationnels » sort du podium, montrant qu'une fois de plus et pour beaucoup d'entreprises, la sécurité est toujours une histoire de mise en place de solutions techniques.

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 à la figure ci-après.

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

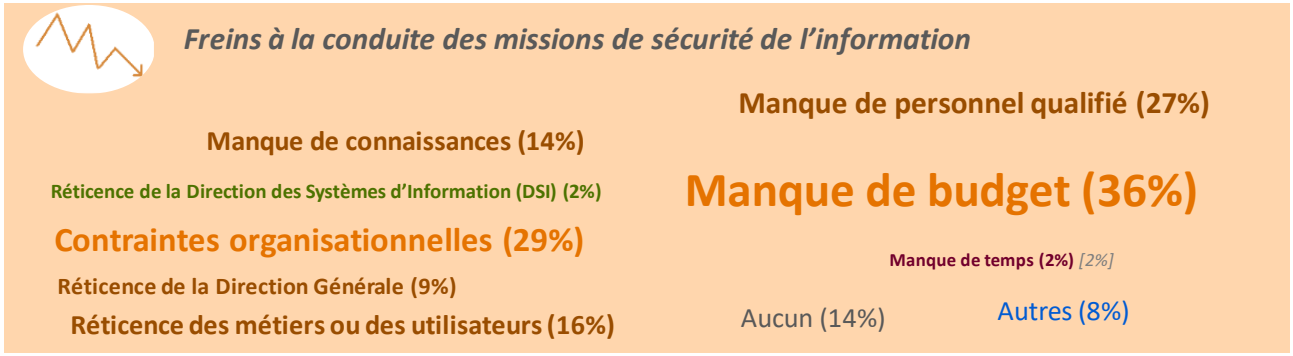


Figure 2 - Principaux freins à la conduite des missions de sécurité de l'information

La réticence de la Direction Générale est à 9%, en forte baisse tout comme celle de la DSI (2%). Il semble donc que dans un cadre législatif et réglementaire de plus en plus contraint, la SSI atteigne une certaine reconnaissance… qui ne se répercute pas dans les budgets. En effet, le premier frein principal reste, tout comme en 2014 et 2016, le manque de moyens budgétaires !

Arrivent ensuite les contraintes organisationnelles et le manque de personnel qualifié. Ce dernier reste (depuis de nombreuses années maintenant) le signe d'une continuelle difficulté à recruter dans le secteur de la SSI.

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 reste globalement stable, à 69%, malgré la prise en compte d'entreprises de moins de 200 salariés, ce qui marque en fait une progression à périmètre comparable (73% contre 69%). Ce pourcentage monte avec la taille des entreprises.

Votre entreprise a-t-elle formalisé sa Politique de Sécurité de l'Information (réponse = oui) ?

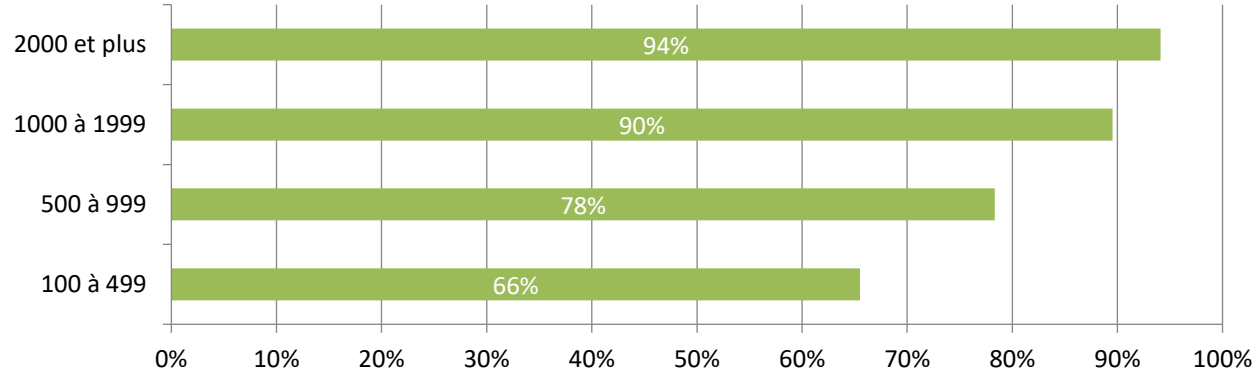


Figure 3 - Entreprises ayant formalisé leur Politique de sécurité

Cette politique est globalement à jour, surtout pour les entreprises ayant plus de 1 000 salariés.

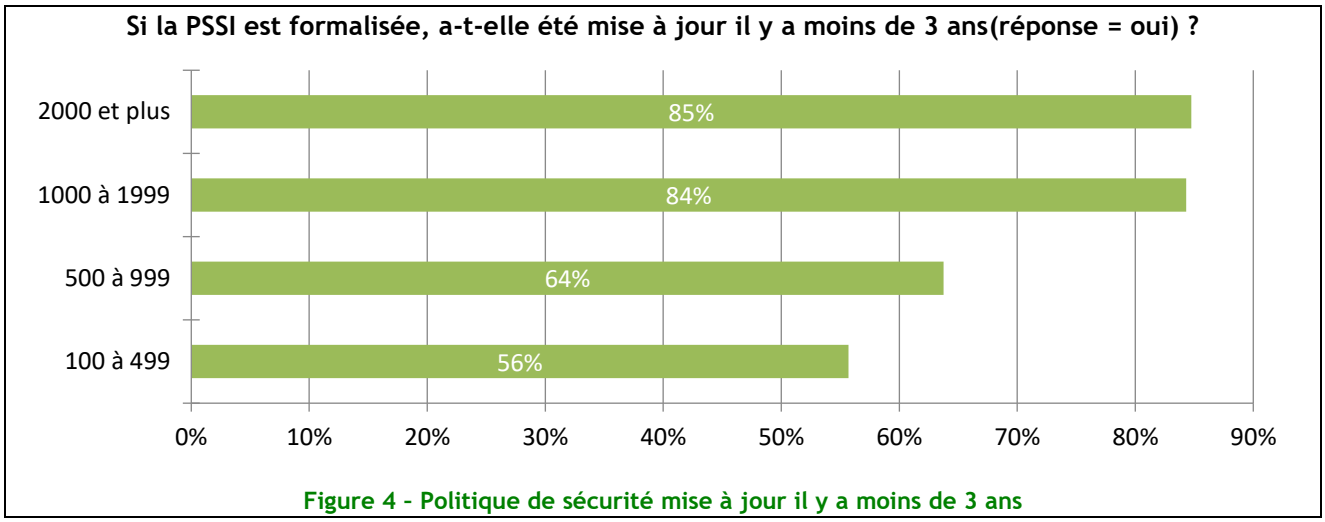


Figure 4 - Politique de sécurité mise à jour il y a moins de 3 ans

La PSSI des entreprises reste massivement soutenue par la Direction Générale pour près de 94% des entreprises répondantes (en très légère progression).

Communication de la Politique de sécurité

Cette Politique de sécurité est toujours largement diffusée à toutes les parties prenantes (77% dont 47% de manière proactive et explicite et 30% pour information, sans accompagnement spécifique). Ces chiffres restent stables.

La Direction Générale… très impliquée dans l'élaboration de la Politique de sécurité !

L'implication de la Direction Générale se confirme et est citée par un peu plus de 70% des entreprises.

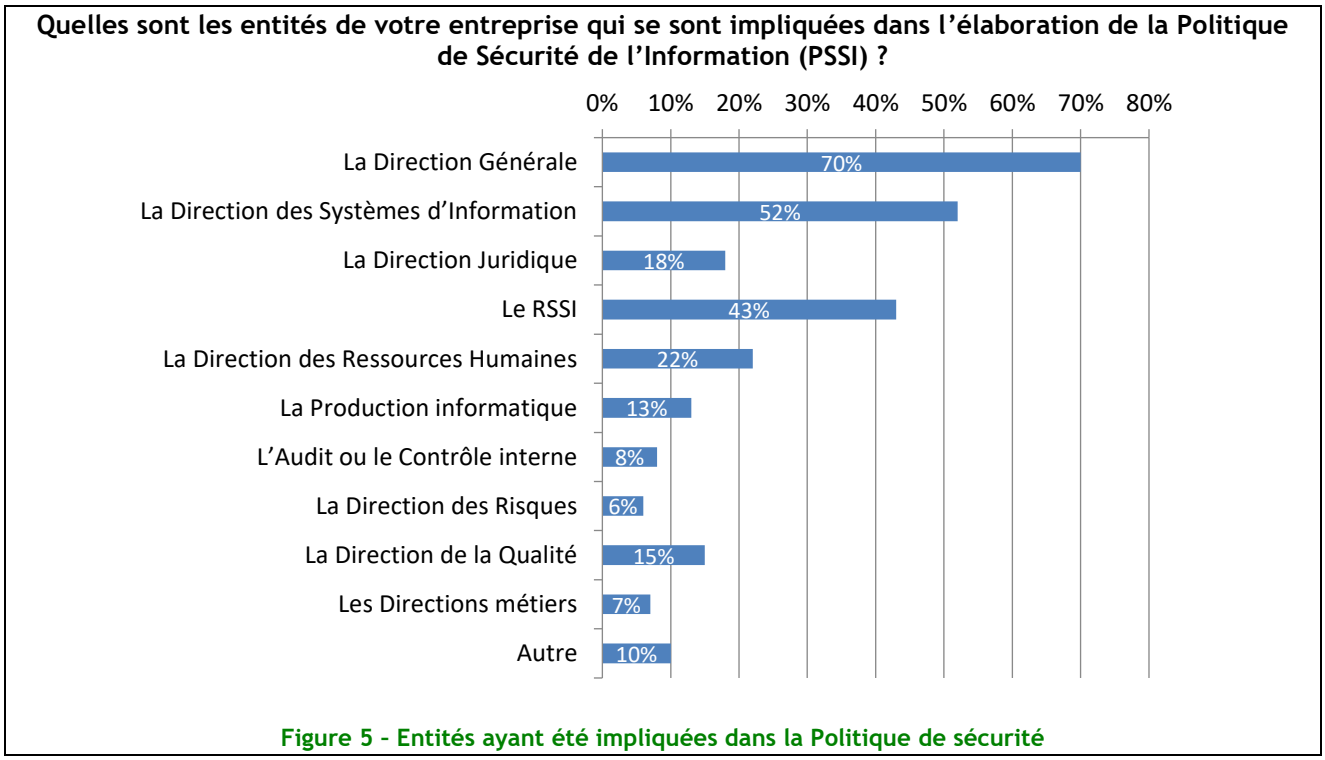


Figure 5 - Entités ayant été impliquées dans la Politique de sécurité

Pilotage de la sécurité de l'information

Cette nouvelle question fait apparaître clairement que le pilotage de la sécurité de l'information s'appuie très peu sur des outils méthodologiques ou des référentiels et, en particulier, que l'analyse des risques n'est utilisée que très marginalement, dans les entreprises, comme instrument de pilotage.

Bases sur lesquelles repose le pilotage de la sécurité de l'information	
■ Une ou plusieurs normes (ISO ou autre) et plus particulièrement : ISO 27001 et 27002 LPM PCI-DSS Autre	**29%** 23% 1% 2% 6%
■ La Politique de sécurité interne	**24%**
■ Le management des risques, et en s'appuyant sur un référentiel : ISO 27005 Méhari Ebios Autre	**7%** 1% 1% 2% 4%
■ Le management des incidents	**2%**
■ Bases de pilotage de la sécurité différentes ou non définies	**48%**

On notera cependant que parmi les 48% d'entreprises qui ne déclarent pas de base ou de référentiel sur lesquels s'appuierait le pilotage de la sécurité de l'information :

- 83% d'entre elles ont fait un inventaire au moins partiel des risques et en ont déduit, pour 41% un plan de réduction des risques, même si elles ne sont que 16% à avoir procédé à une analyse formelle des risques (voir thème 8),
- 15% déclarent utiliser un tableau de bord et 22% déclarent au moins un indicateur de pilotage (voir thème 18).

Ceci prouve, a priori, que ces entreprises ont entrepris nombre d'actions de sécurité, sans avoir défini de système de pilotage, que ces actions découlent de bonnes pratiques communément reconnues, de mesures évidentes à mettre en œuvre après avoir identifié certains risques, ou de toute autre cause.

Thème 6 : Organisation de la sécurité de l'Information

Légère régression de l'identification et de l'attribution de la fonction RSSI

Le nombre d'entreprises ayant identifié et attribué la fonction RSSI régresse légèrement et descend globalement, sur la population de l'échantillon 2018, à 58%. Elle serait de 63% à population comparable (sans les entreprises de moins de 200 personnes) alors qu'elle était de 67% en 2016.

Ce pourcentage varie notablement en fonction de la taille des entreprises et atteint 87% pour les entreprises de plus de 2 000 personnes.

La fonction de Responsable de la Sécurité des Systèmes d'Information (RSSI) ou de Responsable de la Sécurité de l'Information (RSI) est-elle clairement identifiée et attribuée (réponse = oui) ?

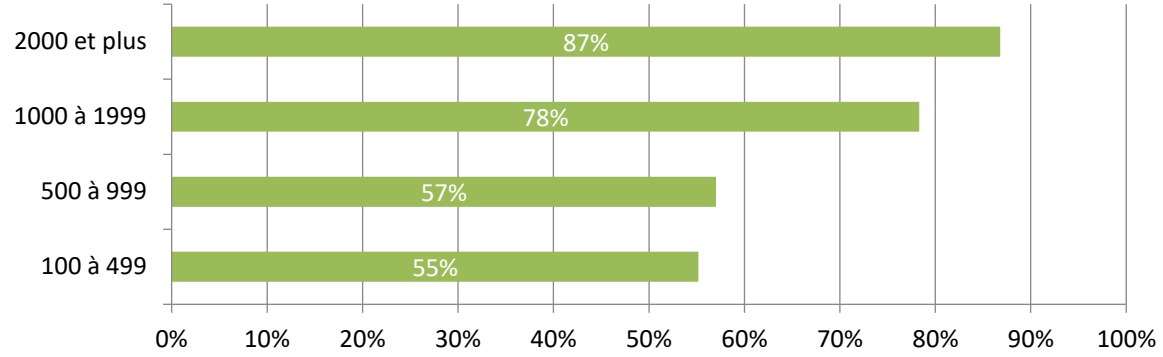


Figure 6 - Identification et attribution de la fonction RSSI

La fonction de RSSI, quand elle est attribuée, est occupée à plein temps pour 53% des entreprises, chiffre stable (52% en 2016) et quasiment indépendant de la taille des entreprises.

Quand la fonction de RSSI n'est pas attribuée, elle est en très grande majorité (les 2/3) assurée par le Directeur des Systèmes d'information ou le Responsable informatique.

Rattachement du RSSI

Le RSSI, quand la fonction est attribuée, est rattaché majoritairement soit à la Direction Générale soit à la DSI, avec une répartition différente selon la taille de l'entreprise.

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

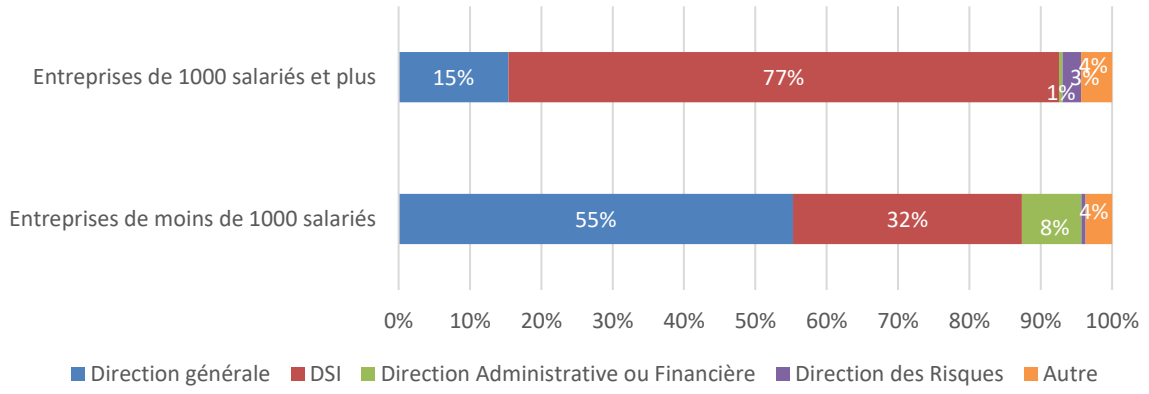


Figure 7 - Rattachement du RSSI (si la fonction est attribuée)

Temps consacré aux différents aspects de la fonction par le RSSI

Le temps consacré aux différents aspects de sa fonction, par le RSSI ressort ainsi :

- Aspects fonctionnels (Politique, analyse de risques, etc.) 25%
- Aspects techniques (architecture de sécurité, suivi de projets, etc.) 30%
- Aspects opérationnels (gestion des droits, administration, etc.) 25%
- Aspects juridiques (charte utilisateurs, recherche de preuve, etc.) 09%
- Aspects de communication (sensibilisation, etc.) 11%

Effectif total de l'équipe Sécurité (rattachée au RSSI)

Les effectifs rattachés directement au RSSI sont plutôt en baisse, par rapport à 2016.

Quel est l'effectif total (en équivalent temps plein – ETP) de l'équipe sécurité (sous la responsabilité directe du RSSI) de l'information permanente au sein de votre entreprise ?

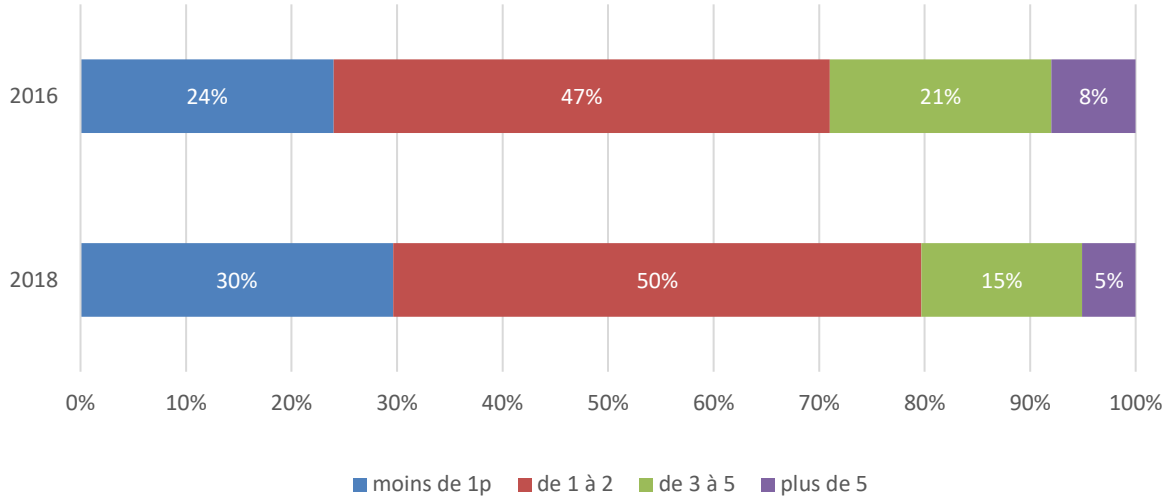


Figure 8 – Nombre de personnes rattachées au RSSI (en ETP)

Thème 7 – Sécurité des ressources humaines

Chartes d'usage ou d'utilisation du SI : un outil généralisé

84% des entreprises ont une charte d'usage ou d'utilisation du système d'information, dont 6% sont en cours d'élaboration. Les entreprises de services sont dans cette moyenne. Le secteur des banques-assurances ainsi que les transports et télécommunications pointent en tête (+10% par rapport à la moyenne). Sur le périmètre de l'étude de 2016, le taux d'adoption de la charte est de 86%, dont 6% en cours d'élaboration, soit une progression de 7,5% en 2 ans. Le déficit de 2 points entre le périmètre de l'étude 2016 et celui de 2018 révèle que les petites structures sont légèrement moins investies dans l'élaboration de cet outil.

Ces chartes sont assez largement communiquées. Dans 9 cas sur 10, les utilisateurs sont informés (communication simple ou signature) de l'existence de la charte. Il faut signaler que la charte est signée dans moins d'un cas sur 2 dans le secteur des transports-télécommunication mais pratiquement 8 fois sur 10 dans les autres secteurs. Les instances représentatives du personnel sont informées dans 85% des cas, chiffre au même niveau en 2016.

Comme en 2016, les chartes ciblent la globalité du personnel (99% dont 4% en cours).

Les entreprises adressent cette charte à leurs prestataires / fournisseurs dans 45% des cas en 2018 - 50% sur le périmètre de 2016 au même niveau qu'il y a 2 ans. Nous notons que les entreprises du secteur des transports-télécommunications sont en dessous de la moyenne (-30%).

Ces chartes constituent des outils de management et de sensibilisation à destination de l'ensemble des utilisateurs. Elles font parties de l'arsenal des mesures juridiques indispensables. Le recours aux services hébergés et l'ouverture des systèmes d'information impliqueraient que les entreprises accentuent leur diffusion auprès des prestataires et fournisseurs.

Un peu plus de trois quarts des entreprises s'assure (programme actif ou en cours) de la modification des droits d'accès des utilisateurs et de la restitution du matériel appartenant à l'établissement, en cas de départ ou de mutation du collaborateur. Si les chiffres sont similaires, à périmètre constant, à ceux de 2016, ils sont à la baisse sur le périmètre 2018.

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 de tout le matériel ?

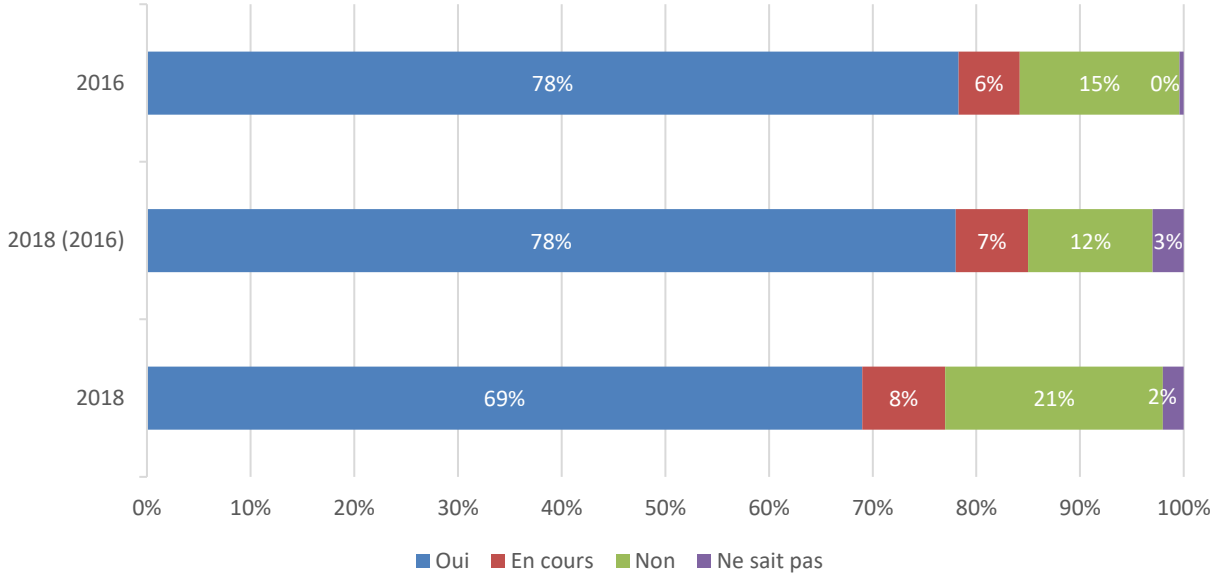


Figure 9 – Procédure de gestion de suppression des droits d'accès et de restitution du matériel

Des programmes de sensibilisation à la sécurité de l'information qui évoluent peu

Une entreprise sur 2 a un programme (ou en cours) de sensibilisation à la sécurité de l'information. À périmètre constant 2018/2016, le taux passe de 49% (dont 13 points en cours) à 57% (dont 10 points en cours). Le chiffre 2018 reflète une moindre propension des petites structures à travailler à la sensibilisation de leurs salariés.

Les moyens pour assurer la sensibilisation restent traditionnels. Le moyen principal est la publication de « news » dans l'intranet, l'envoi de mail ou la publication d'articles dans le journal interne.

Les acteurs décideurs sont des relais majeurs pour porter les messages à leurs équipes, et accessoirement dégager les budgets nécessaires à la sécurité des systèmes d'information. Les VIP sont désormais une cible des programmes de sensibilisation, même dans les petites structures.

La pédagogie restant une histoire de répétition, les actions périodiques et récurrentes progressent de 87% en 2 ans.

La mesure de l'impact de cette sensibilisation reste faible. Il est indispensable que les entreprises développent cette pratique dans les prochaines années pour défendre les moyens (financiers et humains) essentiels à une bonne sensibilisation.

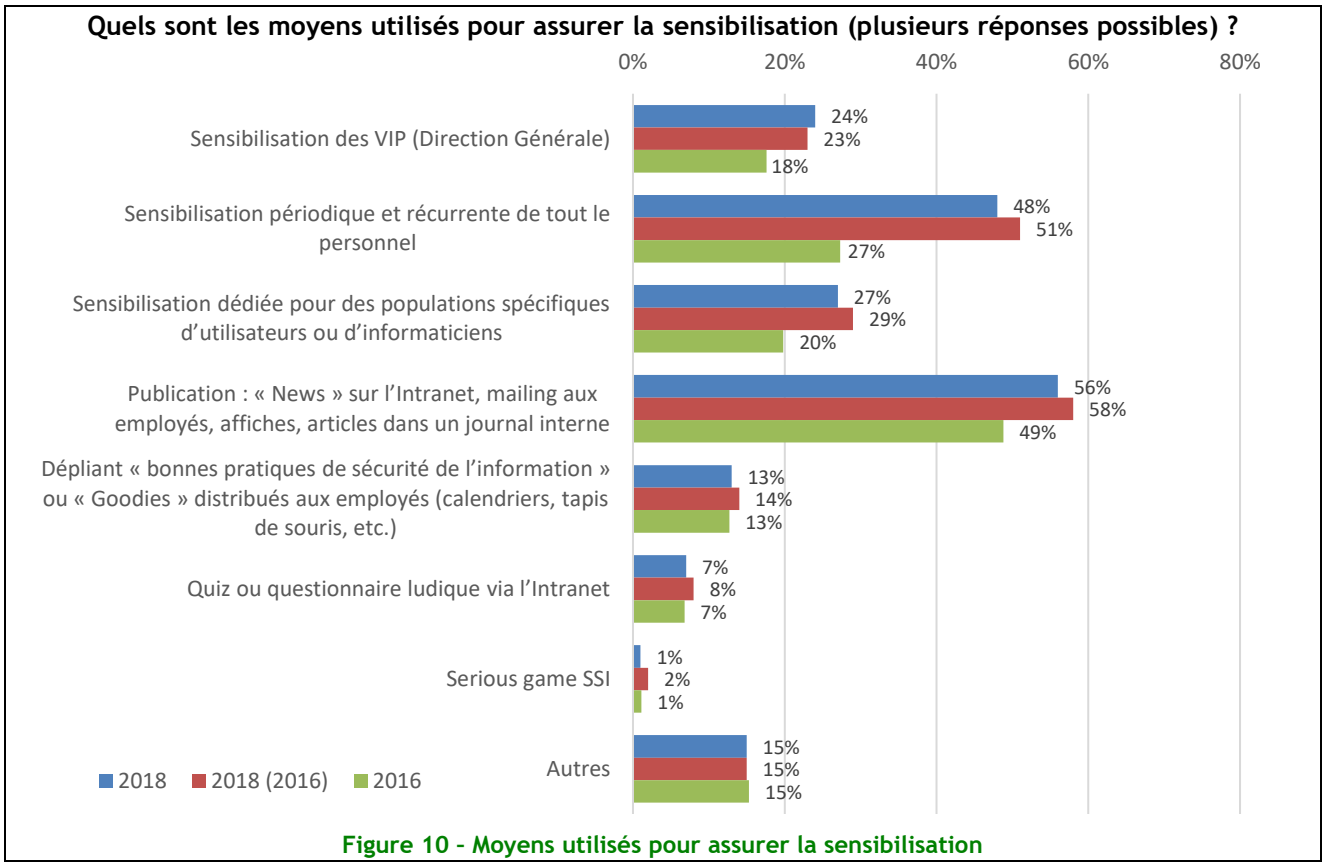


Figure 10 – Moyens utilisés pour assurer la sensibilisation

Thème 8 : Gestion des actifs

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

On ne protège bien que ce que l'on connait bien ! Cet adage a fait son chemin au sein des entreprises et notre enquête rapporte une croissance de plus de 10 points en 2 ans de l'inventaire des actifs[6], qui passe globalement de 74% à 85% pour les inventaires au moins partiels et de 33% à 56% pour les inventaires complets.

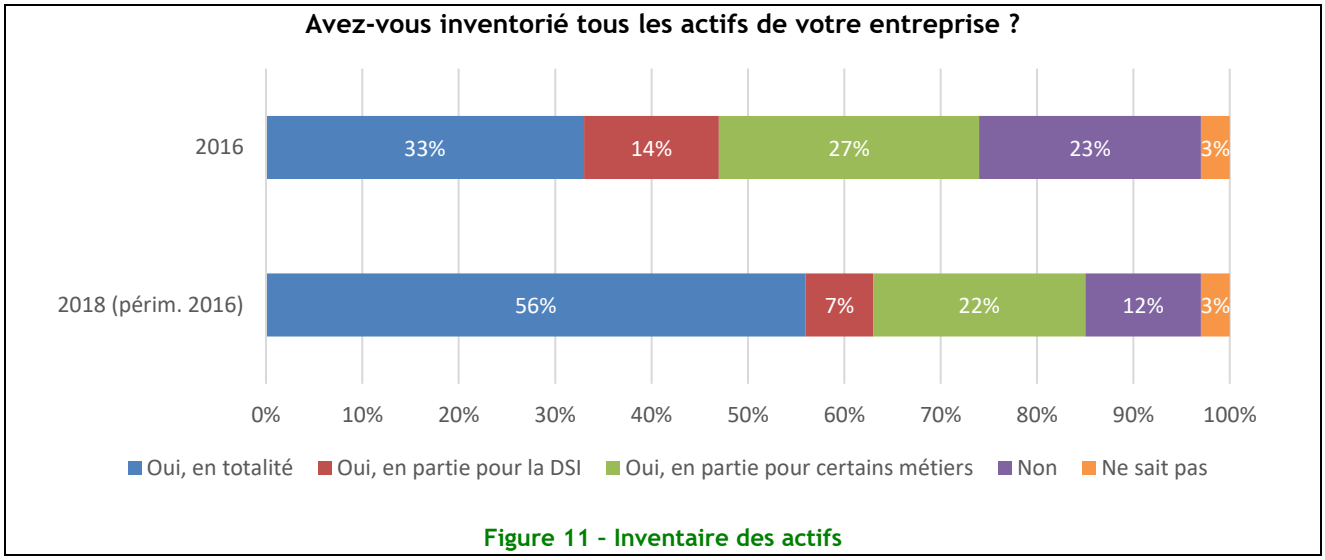


Figure 11 – Inventaire des actifs

[6] On notera que les questions sur les actifs précisaient « informations et leur supports », limitant ainsi la définition du terme.

Même croissance constatée pour la classification des actifs : +10 points sur deux ans, pour les entreprises ayant classifié, au moins partiellement, leurs actifs.

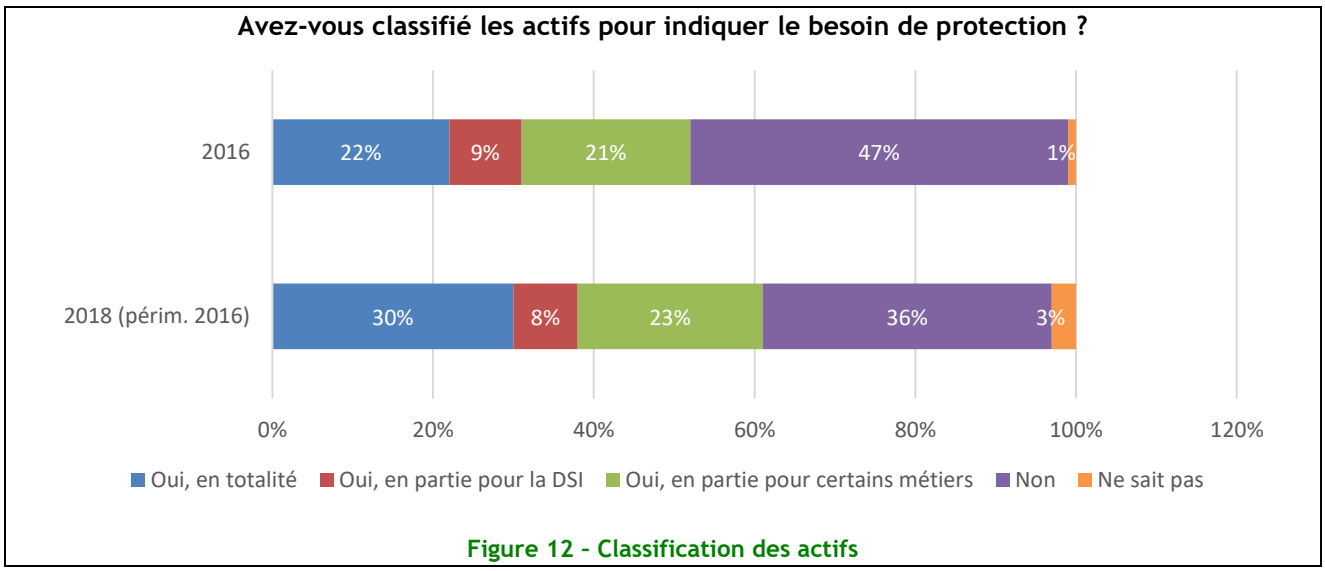


Figure 12 - Classification des actifs

Il reste que, même en progression de 8 points par rapport à il y a deux ans, le pourcentage d'entreprises ayant classifié totalement leurs actifs demeure faible et atteint à peine les 30%.

Quant au processus de classification en lui-même, très peu d'entreprises (13%) l'ont outillé ou industrialisé.

Le nombre de niveaux de sensibilité des informations le plus adopté est de 3[7].

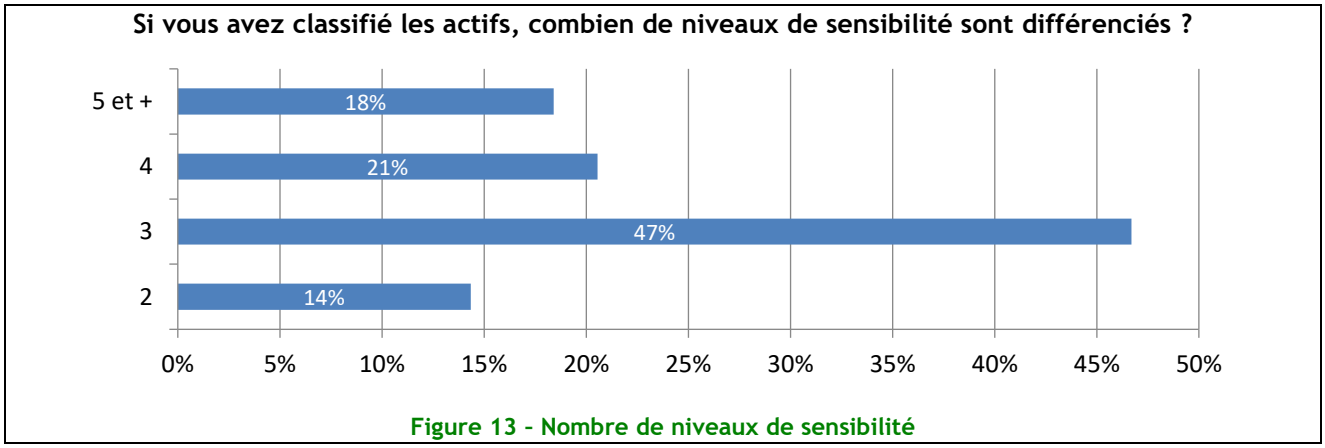


Figure 13 - Nombre de niveaux de sensibilité

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

Un peu plus de 80% des entreprises interrogées ont procédé à un inventaire au moins partiel des risques.

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

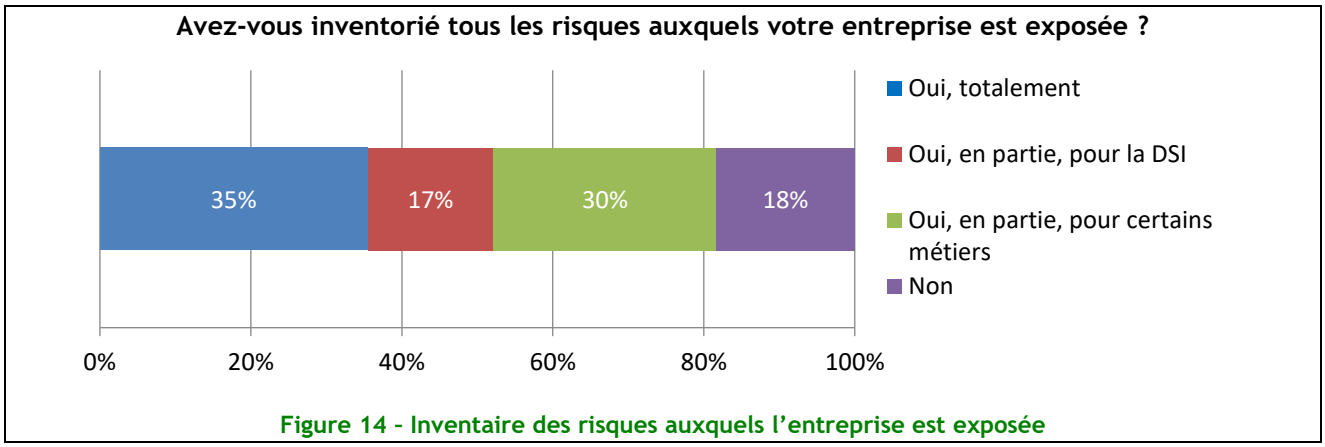


Figure 14 - Inventaire des risques auxquels l'entreprise est exposée

À la suite de cet inventaire des risques peu d'entreprises, en moyenne, en ont fait une analyse formelle (23%), mais ce chiffre global masque une nette différence selon que l'inventaire avait été fait totalement ou partiellement.

Type d'inventaire des risques effectué	Part d'entreprises ayant effectué, après leur inventaire, une analyse formelle des risques
Inventaire total	49%
Inventaire partiel, pour la DSI	12%
Inventaire partiel, pour certains métiers	15%

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

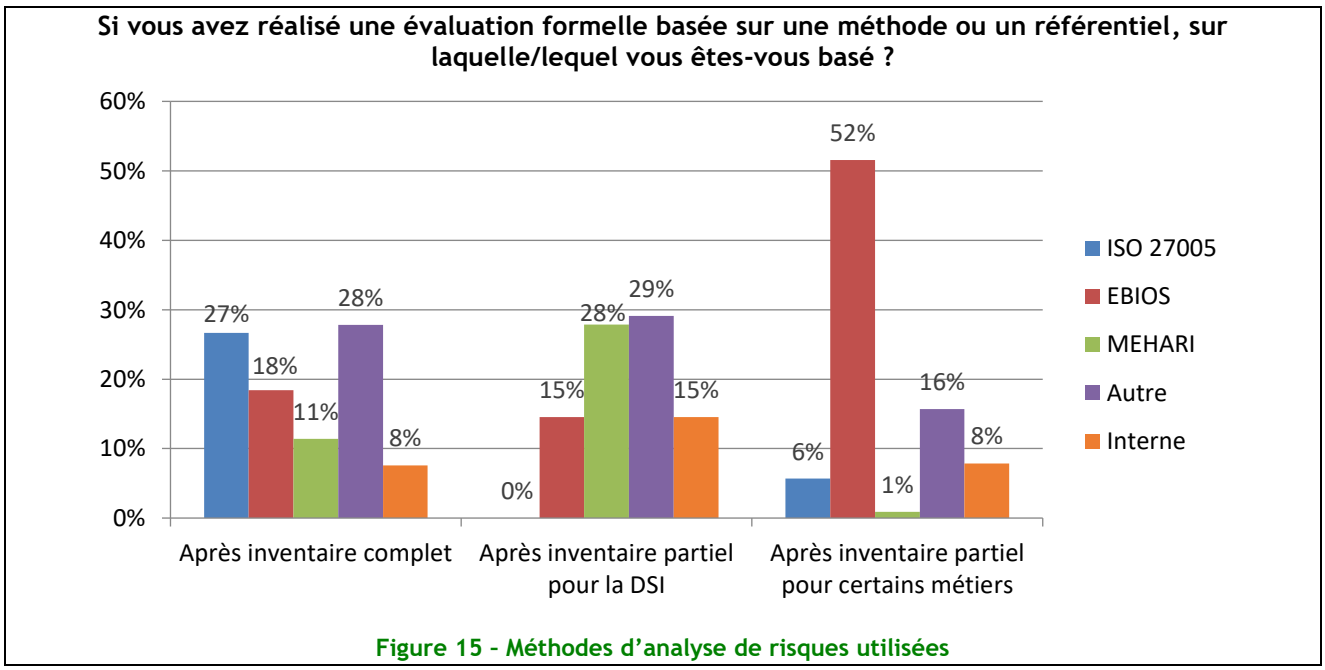


Figure 15 - Méthodes d'analyse de risques utilisées

Notons enfin que, lorsqu'elle est réalisée, l'analyse des risques l'est, dans près de 80% 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

Alors qu'en moyenne, seules 23% des entreprises ont fait une analyse formelle de leurs risques, 48% d'entre elles, c'est-à-dire plus du double, ont entrepris, après les avoir identifiés et inventoriés, un plan de réduction de leurs risques.

Pour celles qui avaient fait un inventaire complet de leurs risques, 80% en ont déduit un plan de réduction au moins partiel, alors que seules 49% en avaient fait une analyse formelle.

Si vous avez réalisé une évaluation des risques, avez-vous défini et argumenté le plan d'action d'amélioration de la sécurité de l'information de votre entreprise en fonction de cette analyse ?

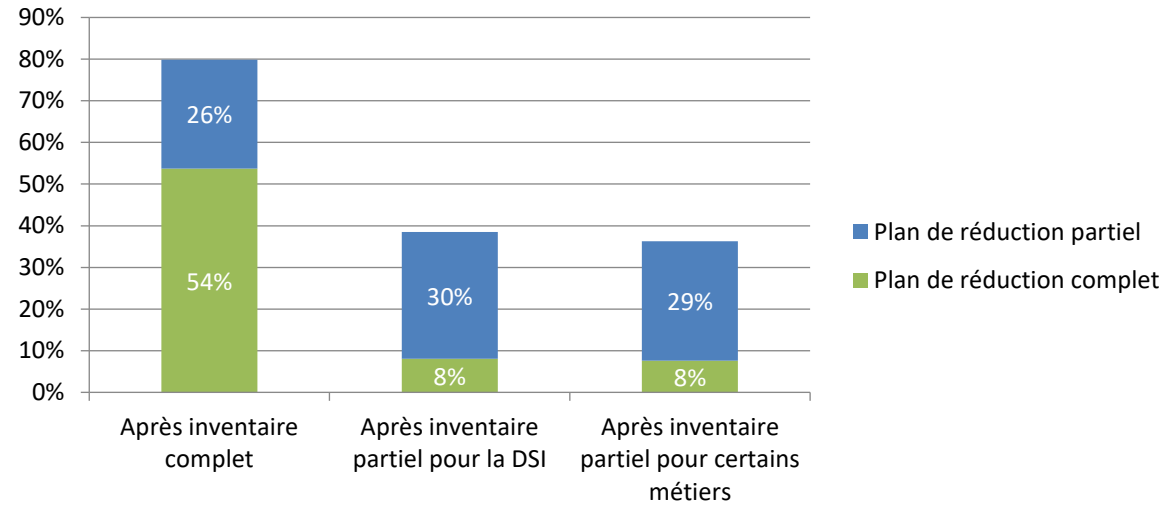


Figure 16 - Mise en place d'un plan de réduction des risques

On note par ailleurs que pour les entreprises ayant entrepris une analyse formelle, après inventaire même partiel, 75% ont établi un plan de réduction des risques.

Il n'y a donc pas déconnexion complète entre analyse des risques et plans de réduction des risques, ce qui est heureux, mais on constate néanmoins que nombre de plans de réduction de risques ont été faits sans méthodologie d'analyse sous-jacentes.

Dernier point : Les Directions générales ont accepté les risques résiduels et validés les plans d'action, au moins partiellement, pour une majorité d'entreprises et à hauteur de 80% pour celles qui avaient fait un inventaire complet de leurs risques.

Si vous avez réalisé une évaluation des risques, la Direction Générale a-t-elle accepté les risques résiduels et validé le plan d'action ?

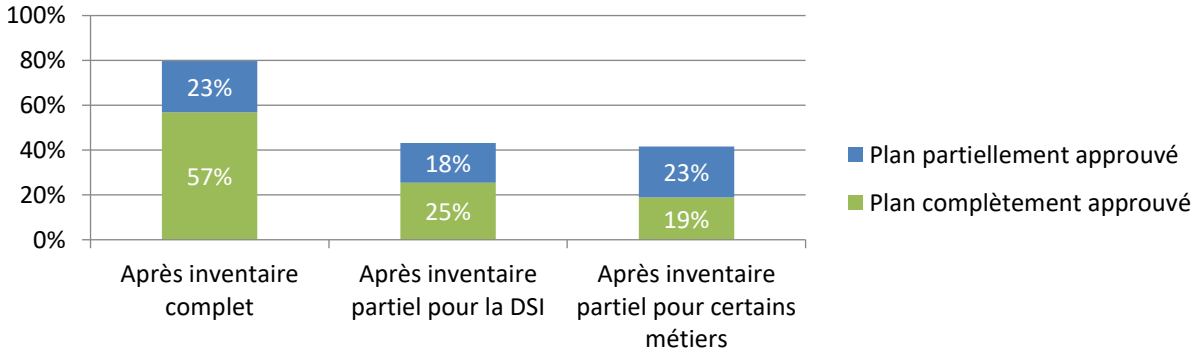


Figure 17 - Acceptation des risques résiduels et validation du plan d'action

Thème 9 : Contrôle d'accès

Une utilisation des technologies d'authentification en augmentation

On note une augmentation significative de l'emploi de « l'authentification par certificat électronique logiciel » qui passe de 52% en 2016 à 57% cette année (à isopérimètre). Cela s'explique par la tendance de généralisation de l'utilisation des smartphones d'entreprise et l'adoption des mécanismes d'authentification forte avec un deuxième facteur d'authentification porté par le smartphone, du fait notamment de la multiplication des cas d'usage, dans le domaine bancaire et du e-commerce notamment (achats en ligne, opérations bancaires digitalisées, etc.) qui ont été transposés sur des cas d'usage entreprise pour sécuriser les accès ou les opérations sensibles.

L'utilisation de la biométrie est également en augmentation (+4 points), et les solutions de Single Sign On de plus en plus répandues (+9 points). L'amélioration de l'expérience utilisateur tout en garantissant un niveau de sécurité adapté est le principal leitmotiv de cette progression.

Progression sur l'utilisation des Workflows d'approbation, recul de la gestion des habilitations par rôle

Dans le volet de la gestion des identités et des habilitations, on note une augmentation de l'utilisation de Workflows d'approbation (+ 4 points).

En revanche, on enregistre un recul sur les modèles d'habilitation par profil métier.

En analyse plus fine par secteur d'activité, ce recul est confirmé pour tous les secteurs, comme le montre le graphe ci-dessous.

Ce recul pourrait être expliqué par l'adoption des technologies d'IAG (Identity and Access Governance) permettant d'assurer plus facilement la conformité des comptes et la recertification. Ceci permet aux entreprises de revenir dans certains cas à des modèles d'habilitation basés sur les droits réels dans les applications sans forcément passer par les profils métier.

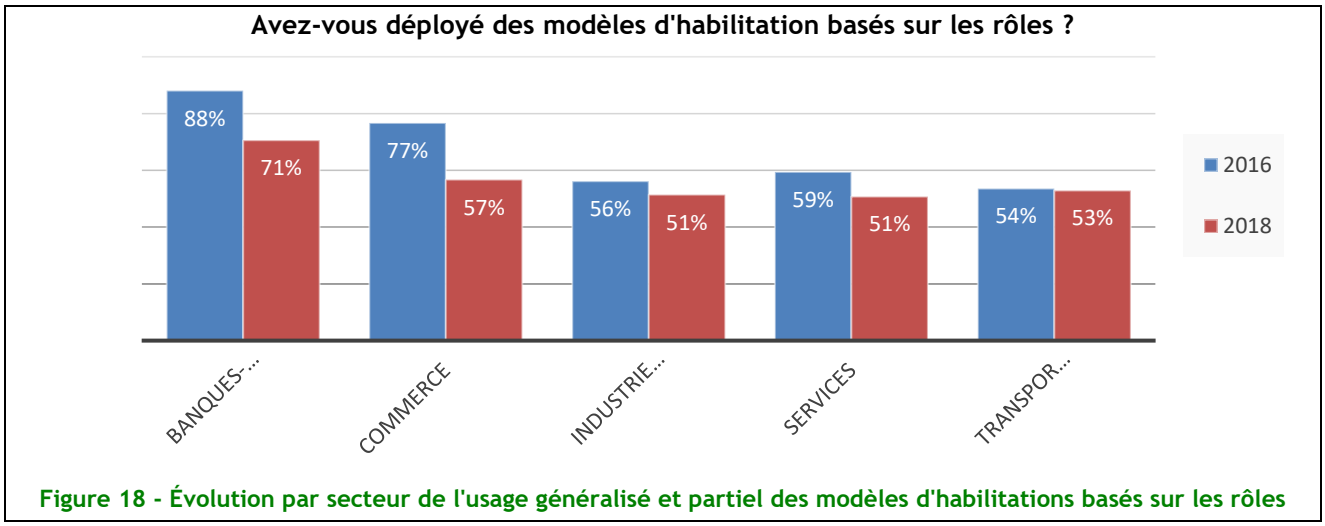


Figure 18 - Évolution par secteur de l'usage généralisé et partiel des modèles d'habilitations basés sur les rôles

Le provisionning automatique de comptes reste stable (un léger recul de 1 point par rapport à 2016). En analysant par secteur, on note que l'évolution n'est pas homogène.

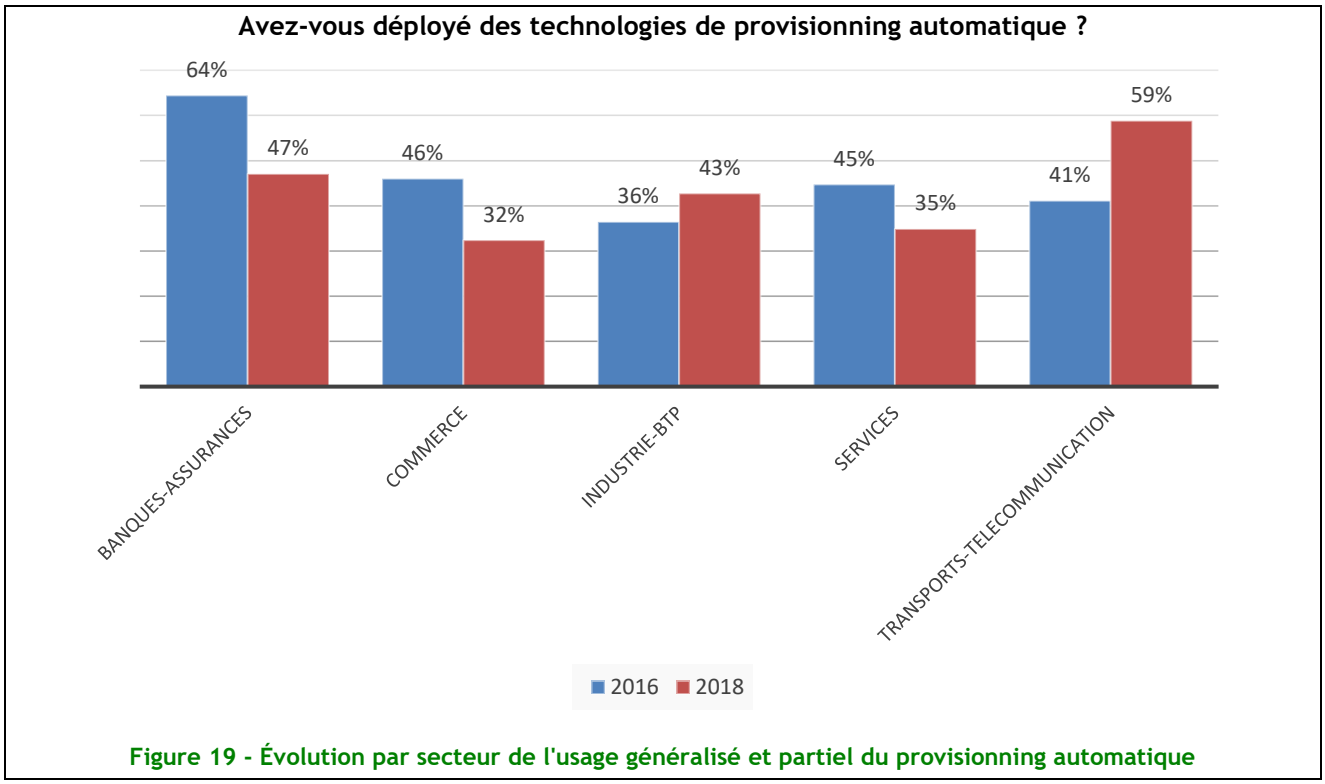


Figure 19 - Évolution par secteur de l'usage généralisé et partiel du provisionning automatique

Le radar ci-dessous reprend les évolutions pour l'ensemble des technologies / approches utilisées.

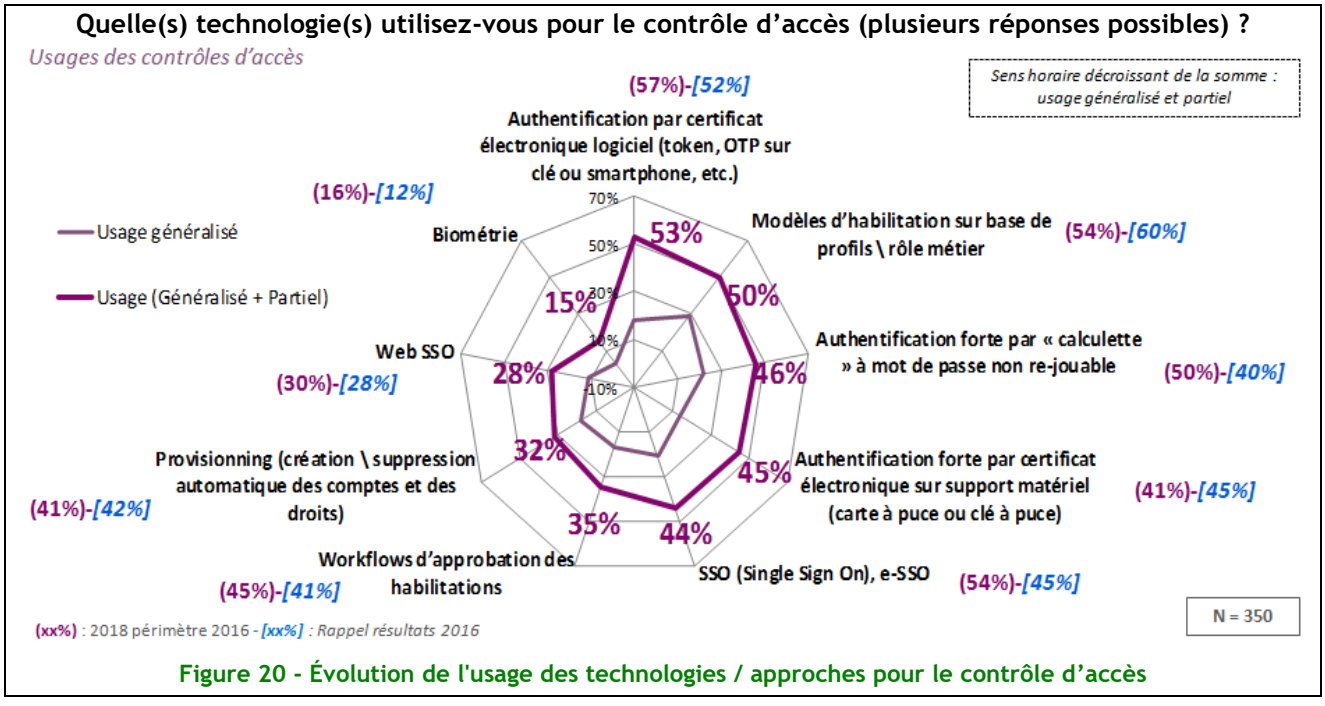


Figure 20 - Évolution de l'usage des technologies / approches pour le contrôle d'accès

La tendance pour l'adoption des procédures de gestion des accès logiques se confirme, notamment pour la gestion des comptes à privilèges

En comparant les chiffres 2018 par rapport au même périmètre de 2016, on note une légère augmentation de l'adoption de procédures formelles de gestion des comptes nominatifs.

Une augmentation plus significative (+11 points) est enregistrée pour les procédures de gestion des comptes administrateurs. Cela confirme la tendance de ces dernières années, au cours desquelles le sujet PAM (Priviledged Access Management) a pris de plus en plus d'importance dans le monde des entreprises.

L'adoption de règles de constitution de mots de passe est également en nette progression (+8 points à périmètres égaux)

L'adoption de ces procédures est moins marquée sur le nouveau périmètre des entreprises de 100 à 199 salariés.

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

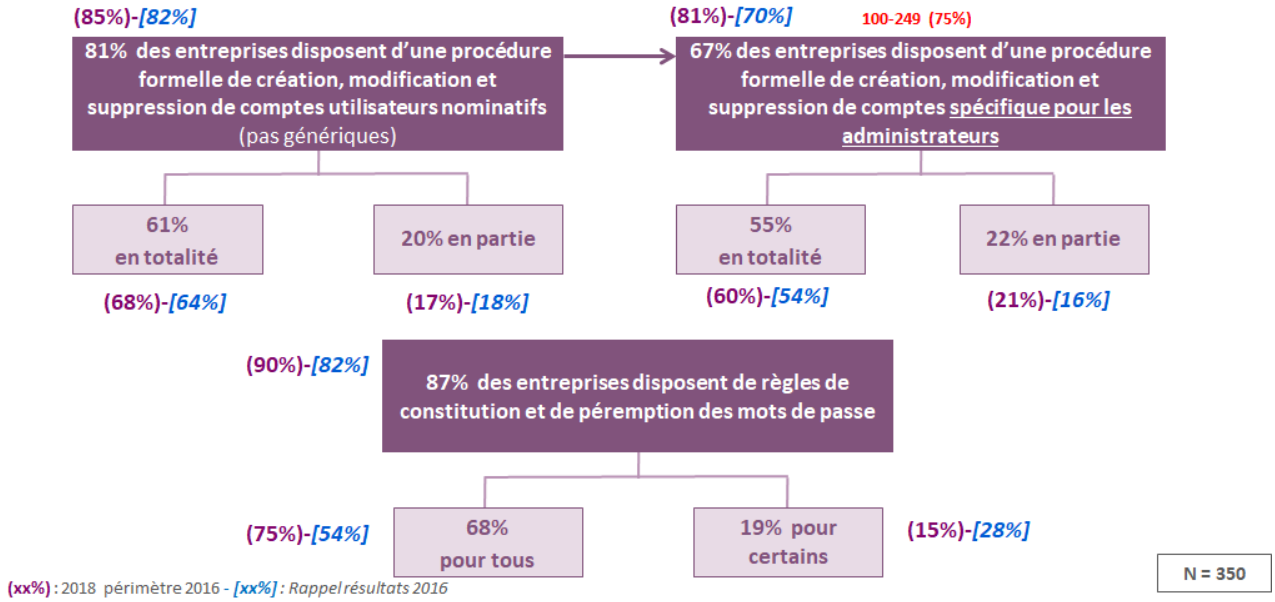


Figure 21 - Procédures de gestion des accès logiques

Si une procédure formelle de création, modification et suppression de comptes utilisateurs, prend-elle en compte spécifiquement les administrateurs (utilisateurs à « hauts privilèges ») ?

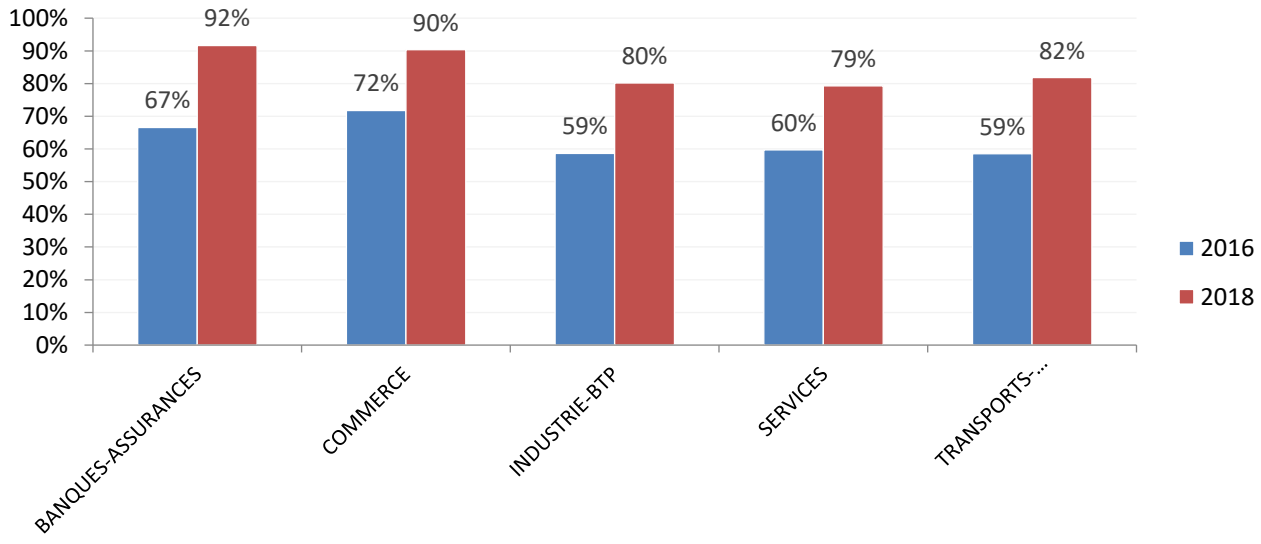


Figure 22 - Évolution par secteur de l'adoption de procédures formelles de gestion des utilisateurs à « haut privilèges »

Thème 10 - Cryptographie

La cryptographie est un moyen de sécurisation des données et de leur transport. Elle reste relativement peu utilisée, un tiers seulement des entreprises déclarent l'utiliser.

Utilisez-vous de la cryptographie ?

Figure 23 - Déploiement de la cryptographie

Son champ d'application principal reste toujours dans la banque/assurance, où elle dépasse les 51% d'usage.

La perception de la cryptographie comme une solution technique est certainement ce qui la positionne sous le contrôle de la DSI.

Si vous utilisez de la cryptographie, quel service interne porte la responsabilité de la gestion des moyens cryptographiques ?

La responsabilité de la gestion des moyens cryptographiques : le DSI dans 7 cas sur 10 avant le RSSI (RSI) dans 1 cas sur 10

Service responsable	%
DSI	72%
Juridique	1%
Direction métier	4%
Autre	23%

Figure 24 - Responsabilité des services de cryptographie

Cette technologie et les processus associés doivent manifestement gagner en maturité pour disposer d'un suivi formalisé, en particulier avec un cycle de vie des clés ou certificats décrit et encadré.

Les moyens de cryptographie mis en œuvre font-ils l'objet d'un suivi formalisé (cycle de vie des certificats, clés, etc.) ?

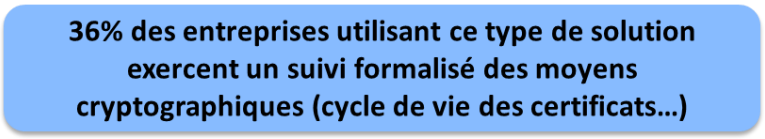


Figure 25 - Cycle de vie des moyens cryptographiques

Cette formalisation est ce qui permet de décrire les différentes phases que sont, pour ces clés ou certificats :

- Leur attribution à un utilisateur, à une application, ou à un terminal et leur format (longueur, hash, etc.),
- Leur renouvellement (ils ont une durée de vie généralement comprise entre 1 et 3 ans),
- Leur sécurisation (sauvegarde, archivage, clé racine, etc.),
- Leur révocation.
- Leur destruction.

Il faut d'ailleurs rappeler que si une solution de cryptographie est souvent nécessaire aux principales certifications, cette formalisation des processus liés à la gestion des clés ou certificats en est alors un élément obligatoire.

La présence des données de l'entreprise sur les terminaux utilisateurs, est une réalité, motivée par le fait que les utilisateurs demandent à travailler de manière nomade, déconnectée de l'infrastructure de l'entreprise.

Le chiffrement des données apparait donc comme une réponse appropriée au vol ou à la perte des terminaux (portable, smartphone, tablette).

On mesure aisément qu'il doit être pleinement maitrisé, puisqu'il pourrait constituer un élément de blocage si l'utilisateur ne pouvait accéder à ses données (les réponses indiquent d'ailleurs que le chiffrement des terminaux occupe une part significative des solutions en place : 40% des PC portables et 22% des smartphones et tablettes sont chiffrés).

Que dire de données chiffrées avec un certificat supprimé depuis le départ de l'utilisateur à qui il était affecté ?

La marche est donc encore significativement haute puisque ce n'est finalement que moins de 11% des entreprises interrogées qui disent disposer d'une solution avec tous les processus associés de manière formalisée.

On peut supposer que l'acquisition de cette maitrise sera un facteur clé pour le déploiement de ces moyens cryptographiques dans les entreprises.

Thème 11 : Sécurité physique et environnementale

Le pourcentage des entreprises qui veillent à la protection des supports physiques (bandes, CD, papiers, etc.) dans le cadre de leur PSSI est en 2018 de 68%. Sur le périmètre 2016, il passe de 70% en 2016 à 66% cette année. Cette baisse peut être justifiée par l'absence d'utilisation de plus en plus accentuée de ces supports physiques (avec toutefois une utilisation du papier qui reste encore significative).

Une disparité des pratiques est toujours constatée entre les différents secteurs d'entreprises, mais cette année, les Banques-Assurances se démarquent et gèrent de manière plus efficace la protection de leurs données sur supports physiques. Elles affichent un pourcentage de 71% contre une moyenne de 59%.

La sécurité de l'information englobe-t-elle la protection des données sur supports physiques amovibles (clés USB, bandes, CD, papiers, etc.) ?

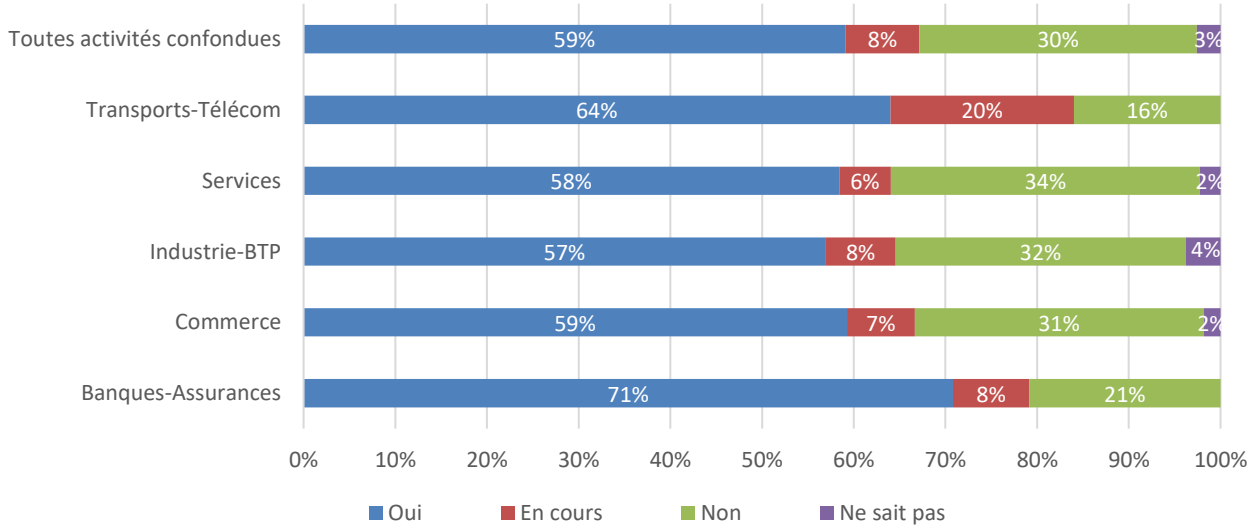


Figure 26 - Entreprises prenant en compte la protection des données sur supports physiques dans la PSSI

Par ailleurs, les dispositifs de sécurité physique implémentés ont continué d'augmenter par rapport aux années précédentes. On constate une prise de conscience et un souci de renforcer d'avantage cette sécurité

physique, ce qui est une bonne chose. La mise en place de ces dispositifs est plus accentuée chez les entreprises de 2 000 personnes et plus.

Trois entreprises sur quatre sont équipées de détecteurs d'incendie (73%) et deux sur trois de contrôle d'accès par badge (62%).

Des dispositifs de sécurité physique sont-ils implémentés pour sécuriser les salles machines dans votre entreprise ?

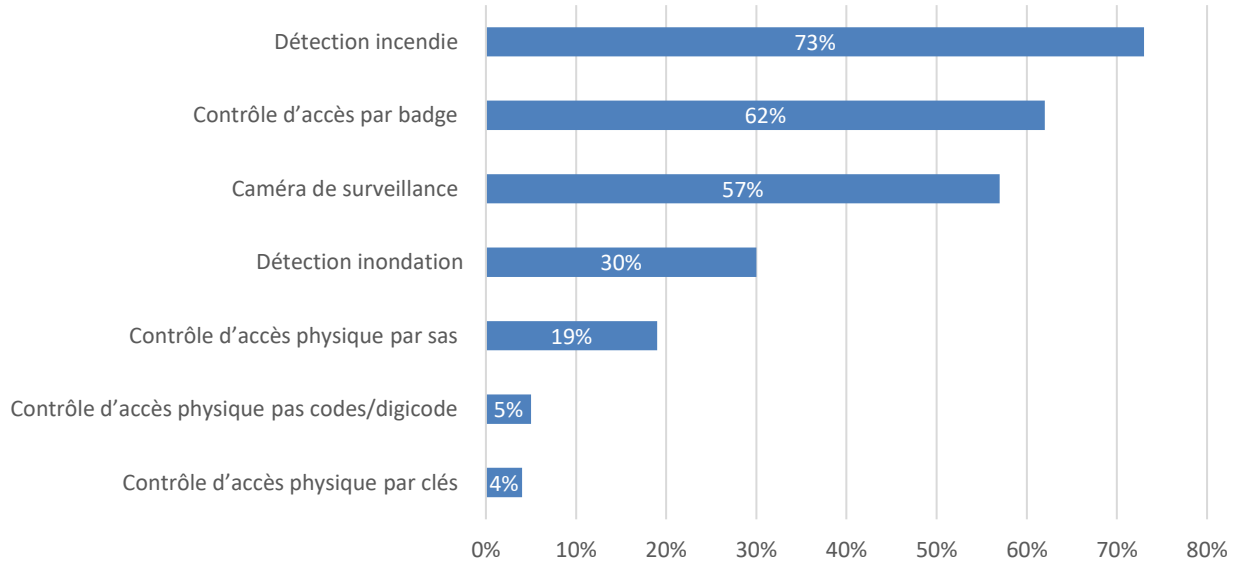


Figure 27 - Dispositifs de sécurité physique pour sécuriser les salles machines

Enfin, sous l'angle de la taille des entreprises, la sensibilité à la mise en œuvre de mesures de sécurité physique des entreprises est homogène : 59% en moyenne implémentent ce type de dispositifs, avec un minimum de 56% pour les entreprises de 250 à 499 salariés et un maximum de 63% pour les 2 000 et plus. Pour autant, 30% des entreprises (tous secteurs et tailles confondus) annoncent ne pas avoir déployé ce type de protection.

Thème 12 – Sécurité liée à l'exploitation

On peut fort heureusement se réjouir de la richesse des outils et sources d'information disponibles pour sécuriser l'exploitation. Nous allons aborder leur taux de pénétration dans l'entreprise, la croissance d'un sous-ensemble d'entre eux, l'hétérogénéité dans leur déploiement, sans oublier la multiplicité des sources d'information et la réactivité face aux menaces.

On pourrait résumer les solutions de sécurisation à deux grands ensembles :

1. La sécurisation de l'infrastructure (contrôle des accès, surveillance des différentes flux, sécurisation des échanges et données, etc.).
2. La protection des terminaux utilisateurs.

Quel usage avez-vous pour les solutions de sécurisation ?

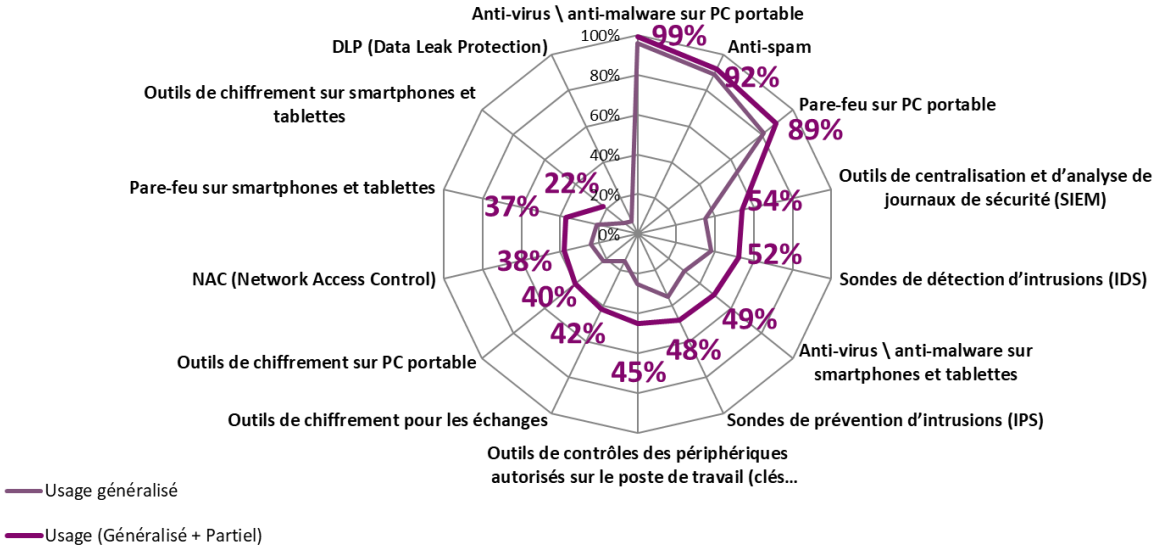


Figure 28 – Solutions de sécurité déployées

Les réponses montrent que c'est cette deuxième composante qui continue d'augmenter, alors que la première stagne voire régresse suivant la typologie de la solution de sécurité déployée.

C'est donc au plus près de l'utilisateur que les solutions s'étendent. On le constate avec leur croissance notable entre 2016 et 2018 :

- + 13 points : pare-feu sur smartphones et tablettes,
- + 12 points : anti-virus/antimalware sur les smartphones et tablettes,
- + 8 points : pare-feu sur PC.

La gestion des terminaux non propriétés de l'entreprise (BYOD) traduit d'ailleurs cette évolution : si leur usage est majoritairement proscrit, quand il est autorisé, 14% des entreprises y étendent leur sécurisation.

Les protections contre les menaces « logiques » sont-elles étendues au BYOD ?

Pas de BYOD	52%
Oui	8%
Partiellement	6%
Non	27%
Autre	7%

Figure 29 – Solutions de sécurité étendues au BYOD

Comment expliquer ce centrage des solutions autour de l'utilisateur ? Les raisons sont diverses mais on peut retenir :

- La part croissante du nomadisme avec comme corollaire la nécessité de sécuriser le poste de l'utilisateur en dehors de l'entreprise (90% 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,
- Le constat d'une utilisation importante du matériel de l'entreprise pour accéder à des sites et messageries non professionnelles.

L'offre est donc pléthorique et il apparait nettement que l'implémentation de ces solutions est très inégale, tant dans le choix que dans le niveau de déploiement.

Quelles solutions de sécurisation sont déployées ?

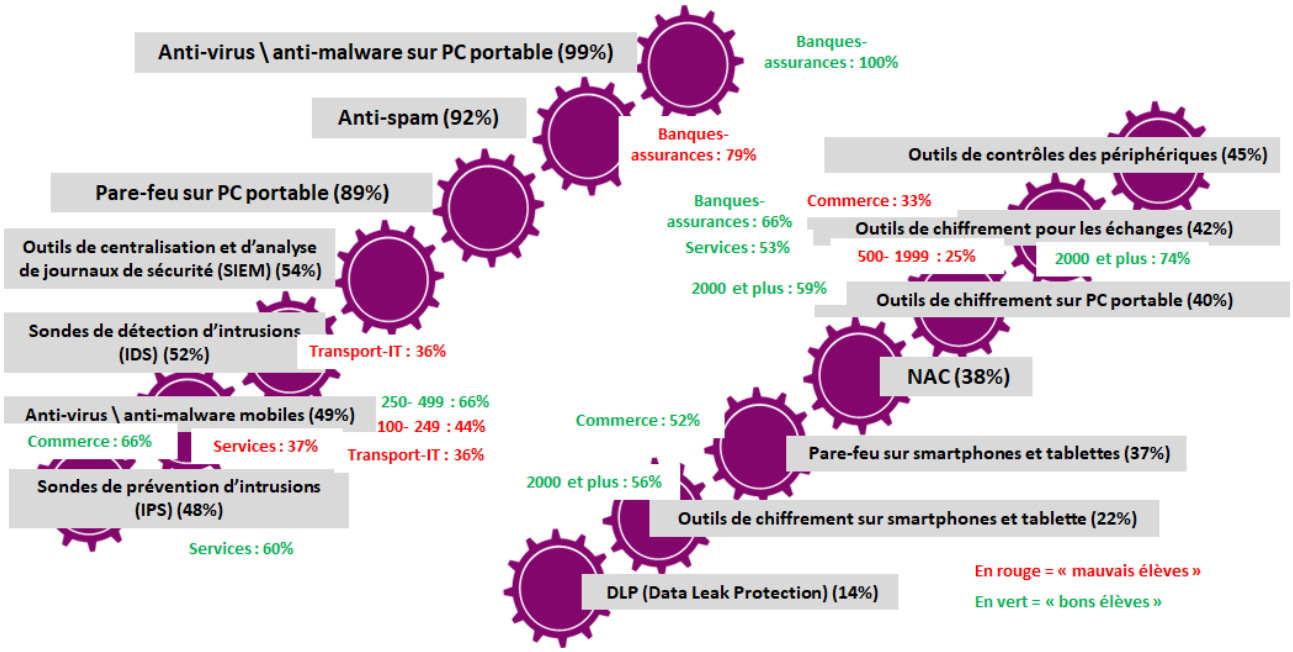


Figure 30 – Solutions de sécurisation déployées

Il est difficile d'établir des éléments de justification d'un type de solution à un secteur d'activité ou une taille d'entreprise. Cependant on peut prendre en considération des critères comme :

- Le règlementaire qui impose des solutions : le chiffrement des échanges est majeur pour le secteur de la banque-assurance,
- L'adaptation aux besoins du terrain (anti-virus/ anti-malware sur les mobiles significativement déployés dans le secteur du commerce (66%),
- La complexité / coût des solutions (le chiffrement sur PC portable est fortement déployé (59%) sur les structures de plus de 2 000 personnes).

Mais ce qui est rassurant c'est que chacun devrait pouvoir trouver une solution appropriée à ses besoins.

Sécuriser l'exploitation, c'est prendre en compte le caractère dynamique des attaques, et la nécessité de s'y adapter. C'est ce que couvre la veille en vulnérabilités, en effet, celles-ci font l'objet d'une grande attention de la part des entreprises.

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

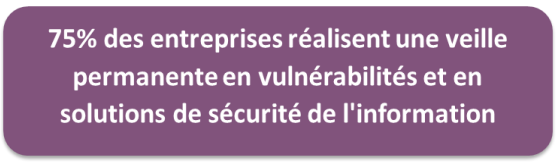


Figure 31 – Veille permanente en vulnérabilités

Ce qui représente une augmentation non surprenante de plus de 20% sur 2 ans !

Non qu'elles soient forcément plus nombreuses, mais elles sont certainement plus médiatisées, et leur impact plus significatif (chacun se rappellera l'exploitation de la vulnérabilité du composant « *Server Message Block v1* » avec *Wannacry* ou autre r rançongiciel qui s'en sont emparés).

Si la veille se systématise, elle s'articule autour de plusieurs médias et on peut noter que :

- Peu d'entreprises se tournent vers un fournisseur de services payant pour disposer de ces informations,
- Pour chaque entreprise, ce sont plusieurs sources qui sont consultées.

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

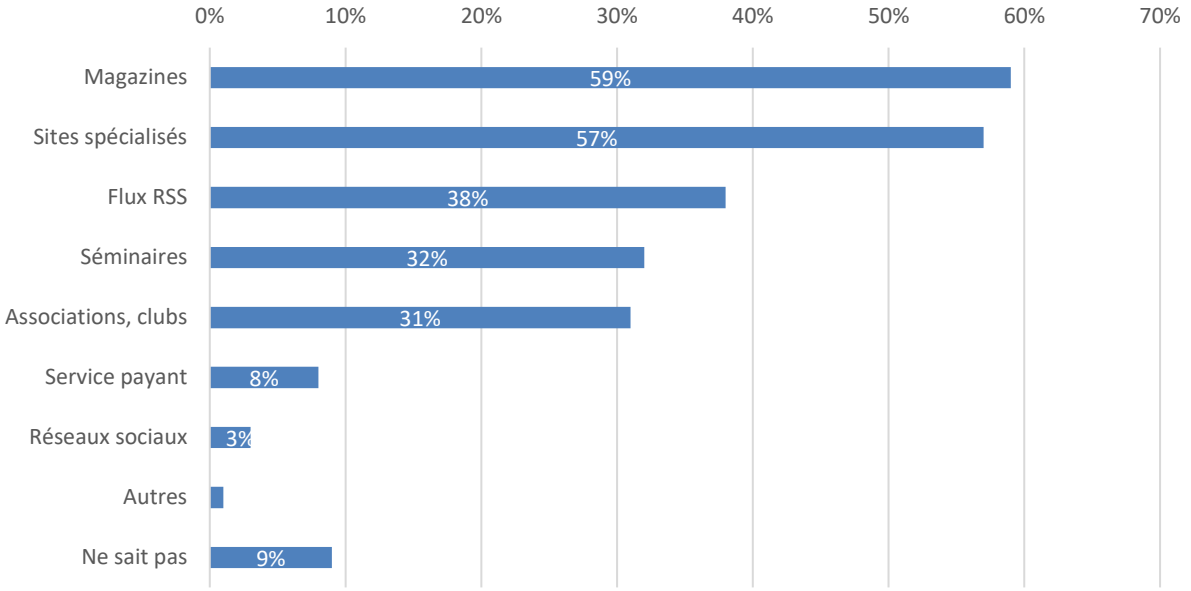


Figure 32 - Sources consultées pour la veille en vulnérabilités et solutions

Cette hétérogénéité peut s'expliquer par le besoin de disposer du maximum d'informations dans les meilleurs délais, avec en même temps une prise d'avis sur les solutions à appliquer et l'urgence de le faire.

L'actualité autour des failles des processeurs Intel, par exemple, a démontré la divergence d'avis des différents acteurs (constructeurs, éditeurs, etc.).

Ce mode réactif semble d'ailleurs se constater dans l'application des correctifs de vulnérabilité par les entreprises : 56% d'entre elles ont formalisé des procédures de correctifs de sécurité.

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

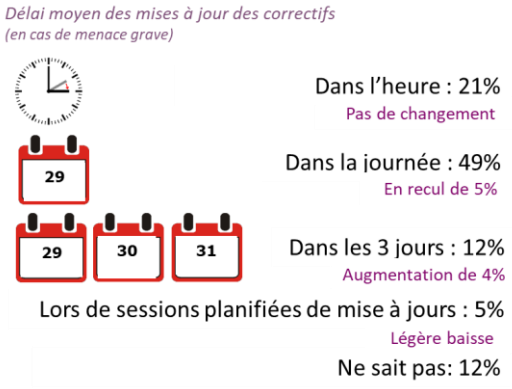


Figure 33 - Délais de mise en œuvre des correctifs

La veille en vulnérabilités augmente donc fortement, mais sans entrainer une formalisation plus importante dans la gestion des correctifs.

On note même un glissement dans la réactivité en cas de vulnérabilité identifiée (davantage dans les 3 jours plutôt que dans la journée). Il ne faut pas forcément y voir une baisse de vigilance. Ce report peut s'expliquer par :

- La difficulté de maintenir opérationnelle l'infrastructure de production avec ses services, avec une gestion des changements urgents,
- Le constat sur ces derniers mois de devoir désinstaller les correctifs des vulnérabilités : certains constructeurs/opérateurs ayant livré « un peu trop rapidement » (failles Intel), d'autres ayant généré des interruptions de service (failles SMB).

L'exploitation dispose aujourd'hui d'un bel arsenal de solutions de sécurisation. La principale difficulté est donc de choisir celles qui répondent le mieux aux besoins de l'entreprises puis d'en faire l'appropriation pour les adapter à son organisation et à ses méthodes. Le paysage risque donc de bouger encore.

Thème 13 : Sécurité des communications

À périmètre constant (2016), l'évolution est peu sensible…

Avec un nouveau périmètre cette année, les tendances restent à peu près les mêmes. On remarque tout de même que les entreprises restent encore réticentes à utiliser des smartphones et tablettes fournis en interne pour accéder au SI. En effet, 34% des entreprises interdisent en 2018 l'utilisation des smartphones et tablettes pour accéder au SI, mais c'est 72% lorsqu'il s'agit de smartphones et tablettes personnels (BYOD).

L'accès depuis l'extérieur à partir de poste de travail non maîtrisés (cyber café, poste de travail personnel) est interdit en 2018 à hauteur de 69%.

Quelle est la position de votre Politique de Sécurité de l'Information vis-à-vis des sujets suivants ?

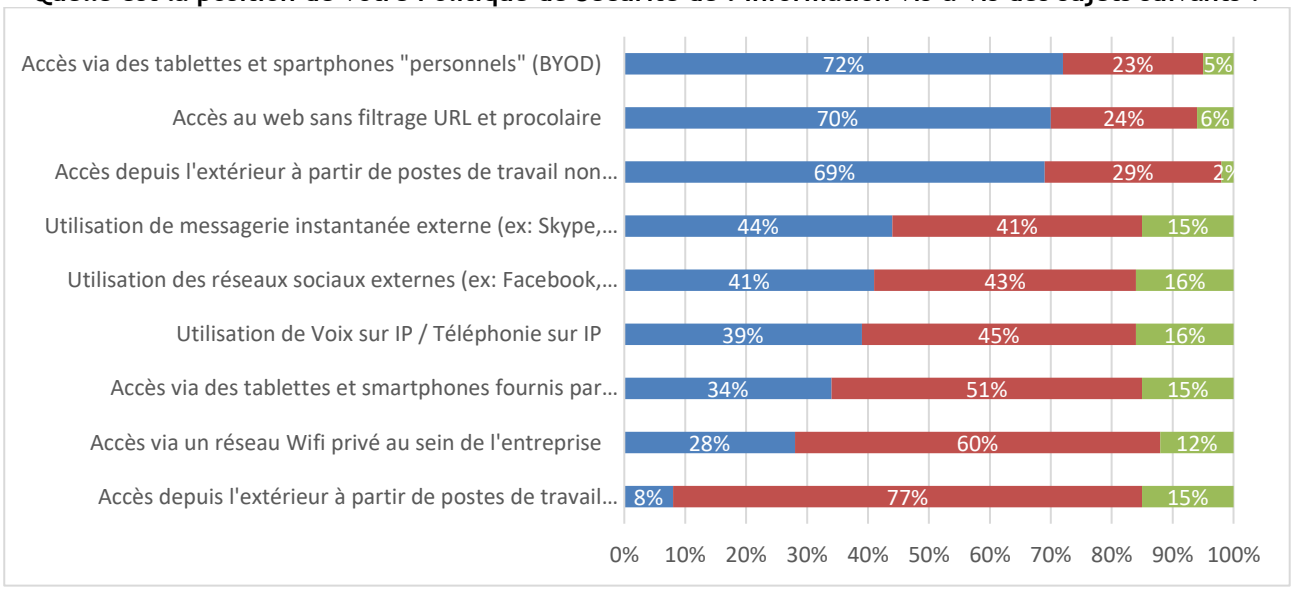


Figure 34 - Position de la PSSI concernant la sécurité des communications

Les messageries instantanées externes gagnent encore du terrain avec une interdiction qui passe de 49% en 2016 à 43% en 2018 (périmètre 2016). Ce qui confirme la tendance vue entre 2014 et 2016 avec une baisse de l'interdiction de 7 points.

Si sur l'année 2016 l'interdiction d'accès au Web sans filtrage a très légèrement augmenté par rapport à 2014, l'année 2018 (périmètre 2016) présente une baisse de l'interdiction passant de 73% à 68%.

On note une évolution en faveur de l'accès via un réseau Wi-Fi privé au sein des entreprises, avec une baisse de l'interdiction d'accès en 2018 (périmètre 2016), situé à 21% contre 28% en 2016. Ce qui confirme la tendance vue entre 2014 et 2016 avec une baisse de l'interdiction de 13 points.

Quelle est la position de votre PSSI vis-à-vis de l'accès via un réseau Wi-Fi privé au sein de l'entreprise ?

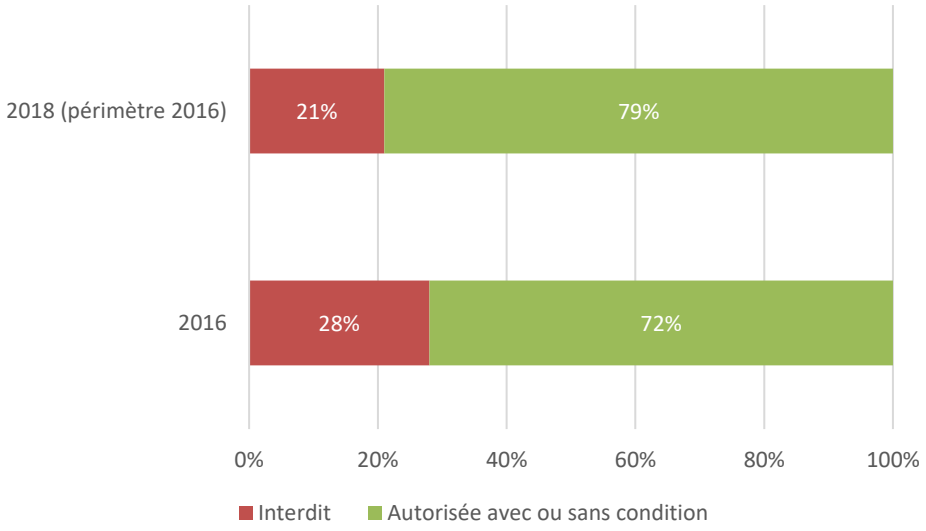


Figure 35 - Accès via un réseau Wi-Fi privé au sein de l'entreprise

Thème 14 : Acquisition, développement et maintenance du SI

L'ensemble des règlements actuels impliquent une augmentation de la sécurité dans le développement (ex PCI-DSS, RGPD avec le Security by Design), qu'il soit effectué en interne via des prestataires voire acquis (progiciels).

Un cycle de développement sécurisé doit comporter divers éléments comme :

- Sécurité du design de l'architecture du logiciel,
- Secure Coding,
- Tests de sécurité (Revue de code, Tests d'intrusions, Tests unitaires sécurité),
- Suivi en production des vulnérabilités,
- Etc.

Nous pouvons noter peu d'évolution sur ce sujet depuis 2010. Peu d'entreprises ont mis en place de réels cycles de développement sécurisé.

Il semble que les entreprises n'aient pas encore pris conscience totalement de l'impact des vulnérabilités applicatives au sein de leur métier.

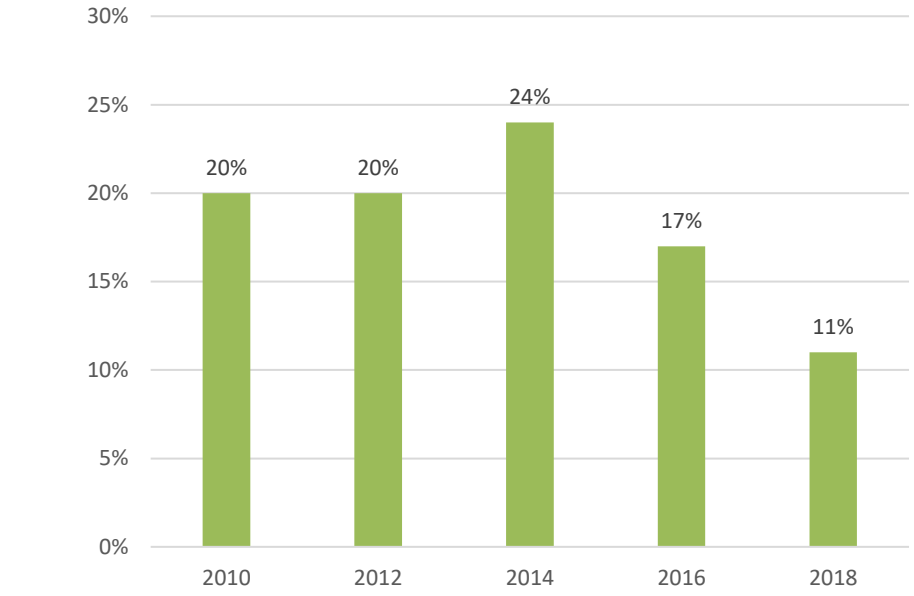


Figure 36 - Mise en place de cycles de développement sécurisé

Il y aurait même une tendance à la baisse sur cette mise en place, que nous pouvons peut-être expliquer par la transformation numérique de nombreuses entreprise et la mise en place des cycles de développement de type DevOps. **Néanmoins il convient de garder en tête que dans un cycle de type DevOps la sécurité du développement doit encore plus qu'être présent.**

Parmi ces entreprises ayant mis en place un cycle sécurisé, la majorité ne colle pas à une méthode « commerciale », mais applique plutôt des bonnes pratiques pragmatiques.

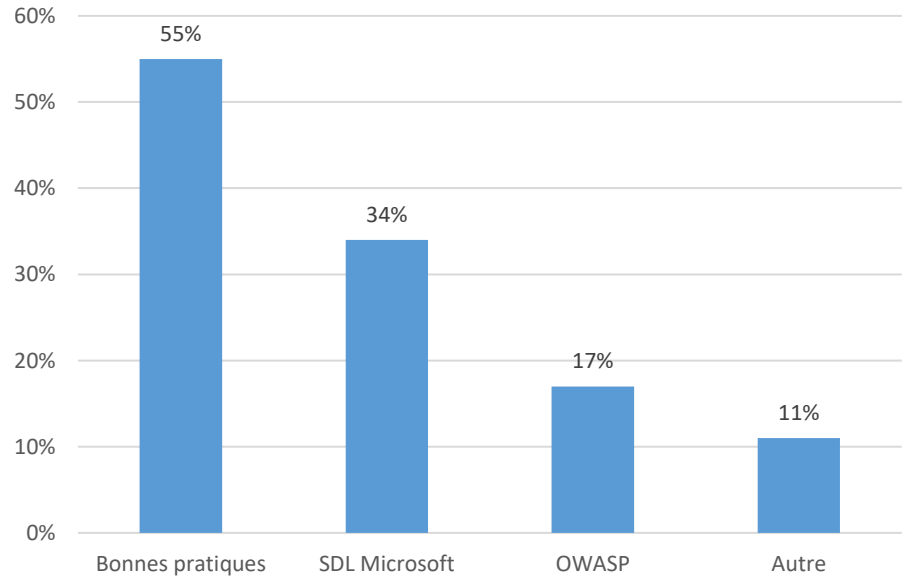


Figure 37 - Méthodes de développement sécurisé

Thème 15 : Relations avec les fournisseurs

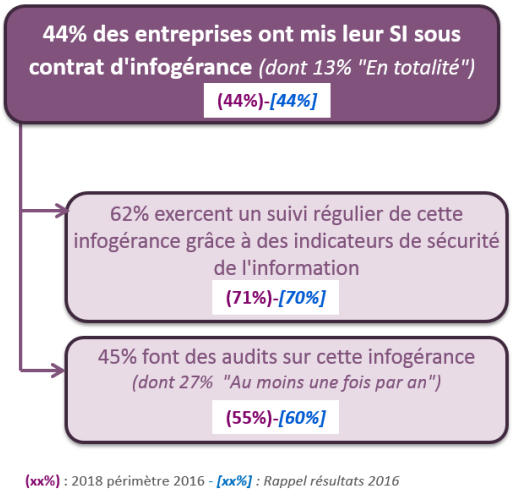
Une infogérance en stagnation mais un recours aux solutions en cloud en forte progression

La part du recours à l'infogérance reste stable depuis 2016, un peu moins de la moitié des entreprises ayant recours à ces prestations (44% en 2016 et 2018). On note même 13% d'entreprises qui ont une infogérance totale de leur SI.

On note qu'une bonne partie de ces prestations font l'objet d'un suivi régulier (62% sur le périmètre 2018). Il faut préciser que le chiffre 2018 sur le périmètre 2016 augmente de 9 points. Les entreprises de 100 à 200 salariés, moins mature sur les problématiques de sécurité de manière générale n'entrent pas dans le périmètre pris en compte.

Dans cette même tendance, seulement 45% précisent pratiquer des audits – 55% sur le périmètre de 2016, en baisse de 5 points.

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

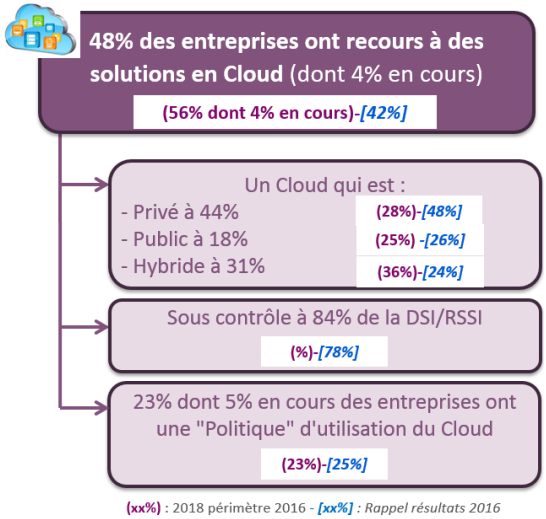


(xx%) : 2018 périmètre 2016 - [xx%] : Rappel résultats 2016

Figure 38 – Mise en infogérance (totale ou partielle) du SI

La tendance montre bien l'utilisation plus importante de prestations d'infogérance et le marché est assez tendu aujourd'hui. Pour se démarquer, les prestataires n'hésitent pas à mettre les moyens dans les certifications de sécurité (ISO27001 par exemple).

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



(xx%) : 2018 périmètre 2016 - [xx%] : Rappel résultats 2016

Figure 39 – Utilisation des services en cloud

Parmi ces prestations d'externalisation, le cas spécifique du cloud est mis en avant et on note une augmentation de 14 points depuis 2016. Sur le périmètre de 2018, l'utilisation du cloud représente presque une entreprise sur deux (48%).

Par rapport à l'utilisation des différents types de cloud, le cloud privé est majoritairement privilégié, mais on note une baisse notable sur le périmètre 2016 (baisse de 20 points). Cette baisse pourrait s'expliquer par le prix de ce genre de solution pour les structures plus importantes, car on note en effet une utilisation du cloud privé plus importante sur le périmètre 2018 (44%). L'utilisation des cloud publics est constante (autour d'une entreprise sur 4). Les entreprises semblent se tourner vers les solutions Hybride avec une augmentation de 12 points.

Les exigences de sécurité liées à l'utilisation de ces prestations expliquent un pourcentage élevé de ces cloud qui sont sous contrôle de la DSI/RSSI (84%). En revanche, malgré ce contrôle, seules 23% de entreprises consommatrices de ces prestations disposent à ce jour d'une Politique d'utilisation, qui pourrait s'expliquer en partie par l'explosion rapide de l'utilisation de ces solutions qui n'a pas permis aux entreprises de mettre à disposition la documentation adéquate.

Les changement brusques sur les types de cloud utilisés aujourd'hui par les entreprises en 2018 peut s'expliquer d'une part par le coût des solutions et leur complexité et d'autre part, par les exigences de sécurité plus importantes qui obligent les entreprises à se poser des questions sur la sécurité de leurs infrastructures. On suppose que la maitrise de ces solutions n'est à ce jour pas encore mature et qu'il faudra encore quelques années pour stabiliser les chiffres.

Thème 16 : Incidents de sécurité

Une collecte élargie et un traitement plus réactif malgré des moyens plus réduits

La préoccupation des entreprises à collecter les incidents de sécurité va croissante, en élargissant les périmètres surveillés. Si les principales sources de collectes restent liées à l'informatique de gestion (85%), l'informatique des services généraux (67%) et l'informatique industrielle (51%), les plus fortes progressions concernent plutôt les autres formes d'informations ou les processus de l'entreprise (respectivement 32% et 16%).

Cette couverture plus large s'accompagne parallèlement d'une nette diminution du temps de résolution des incidents auxquels les entreprises ont dû faire face. Ainsi, pour 70% d'entre elles (58% en 2016), l'incident le plus sévère en termes de disponibilité de service a été traité en moins de 24h, et 86% l'ont traité en moins de 72h (sur ce délai, à périmètre constant, le taux de résolution s'est amélioré de 27 points). Le traitement technique n'est pas la seule réaction adoptée : il se double de plus en plus d'actions juridiques, comme le dépôt de plainte à la suite des incidents sur le SI (17%).

Cependant, il est à noter que, paradoxalement, les cellules de collecte et traitement des incidents de sécurité se font plus rares (41%, -3 points vs 2016), soient-elles dédiées ou partagées avec d'autres fonctions. Pour autant, il existe une importante disparité entre la taille des entreprises et les secteurs d'activité quant à la mise en place de groupe de gestion des incidents de sécurité. En effet, les entreprises de plus de 2 000 salariés (62%) et celles du secteur Banque-Assurance (58%) semblent les mieux dotées. Parmi ces dernières, 33% d'entre elles ont mis en place une cellule dédiée au traitement des incidents de sécurité.

Une fréquence d'incidents à la baisse dans un contexte de menaces assez stable

En 2018, les entreprises ont une nouvelle fois été confrontées à des incidents dont les causes sont variées et d'origine autant interne qu'externe. Les incidents les plus fréquemment signalés ont eu pour cause :

- Les infections virales, provenant d'attaques non ciblées, qui ont touché près d'un tiers des entreprises (30%),
- Les pannes d'origine interne affectant le matériel et/ou le logiciel (23%),
- La perte de services essentiels tels que l'électricité, l'eau, le système de climatisation ou les liens télécoms (22%),
- Les erreurs d'utilisation du SI (16%),
- Le vol ou la disparition de matériel informatique ou télécom (10%),

- Les erreurs de conception dans la réalisation ou la mise en œuvre des logiciels ou procédures (8%),
- Les attaques logiques ciblées (8%),
- Les fraudes informatiques ou télécoms, notamment les détournements de fonds ou de biens (7%),
- Les actes de chantage ou d'extorsion informatique (7%).

Les autres causes, auxquelles moins de 5% des entreprises ont été confrontées en 2018, concernent des risques liés à la sécurité physique ou environnementale (accidents physiques, sinistres naturels) ou des actes de malveillance volontaires (intrusion logique/physique, vandalisme, sabotage ou divulgation d'informations par exemple).

Si cette hiérarchie, basée sur la « popularité » du vecteur d'incident, est relativement similaire aux années passées, elle ne doit pas masquer une tendance générale à la baisse de la fréquence et du nombre d'occurrence des incidents.

En effet, à panel identique (pour rappel, le panel d'étude 2018 est plus large), les entreprises indiquent connaître une fréquence d'incidents moindre en comparaison à 2016 concernant quasiment l'ensemble des causes identifiées.

Au cours de l'année 2017, votre organisme a-t-il subi des incidents de sécurité de l'information consécutifs à… ?

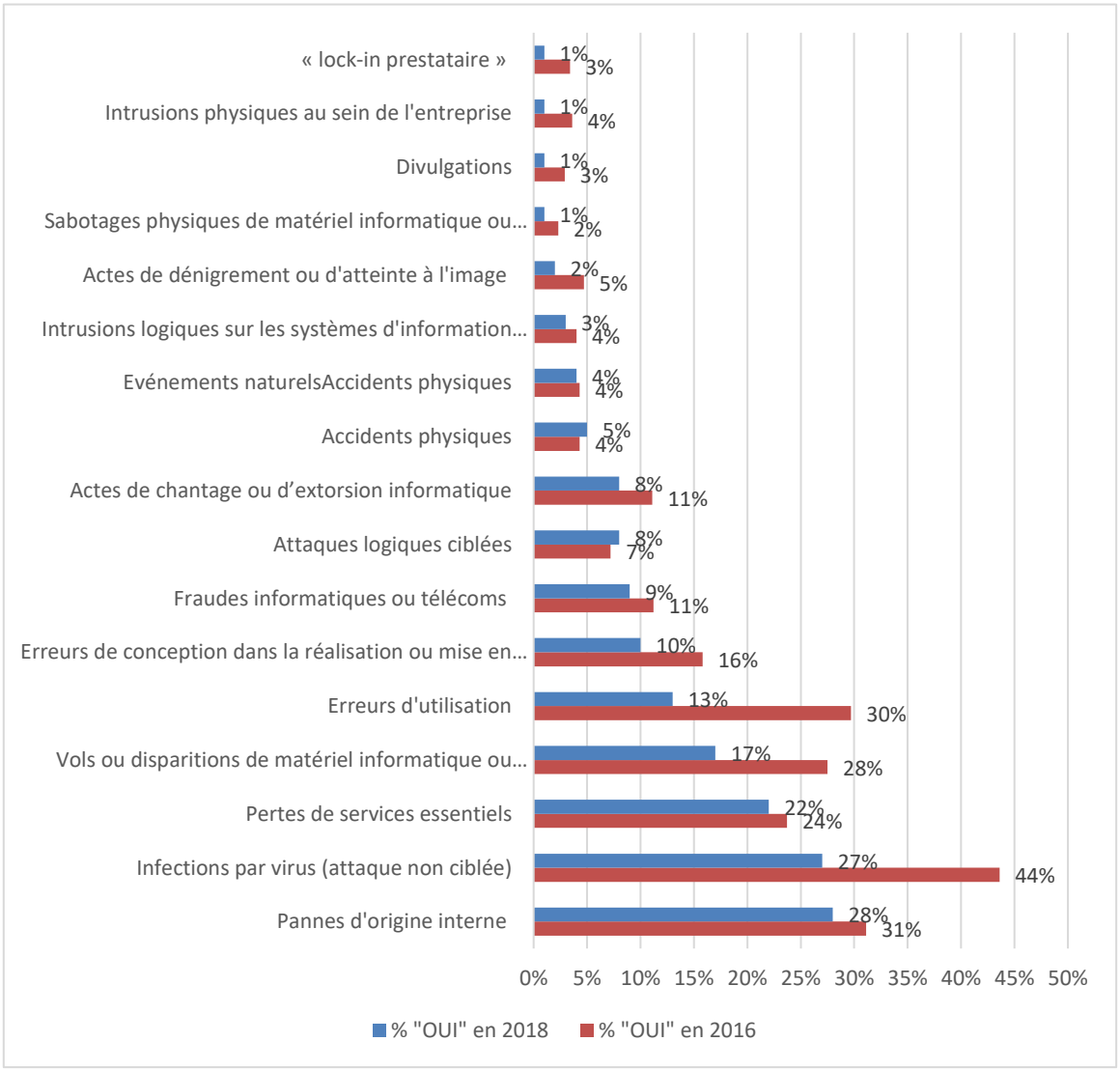


Figure 40 - Comparaison des fréquences d'incidents entre 2016 et 2018 (périmètre 2016)

Les types d'incidents connaissant les régressions les plus significatives sont :

- Les infections virales issues d'attaques non ciblées (-17% vs 2016),
- Le vol ou la disparition de matériel informatique ou télécom (-17% vs 2016),
- Les erreurs d'utilisation du SI (-11% vs 2016).

La baisse observée de la variété d'incidents rencontrés s'accompagne d'un autre signe encourageant : la diminution du nombre lui-même d'incidents. Ainsi, ces derniers se font plus rares et se répètent moins lorsqu'ils surviennent.

Cette corrélation est particulièrement vraie concernant les causes d'incidents les plus fréquentes :

- Les infections virales issues d'attaques non ciblées (en moyenne 3,7 vs 12,31 en 2016),
- Les erreurs d'utilisation du SI (en moyenne 6,7 vs 9,78 en 2016),
- Les vols ou disparitions de matériel informatique ou télécom (en moyenne 3,2 vs 6,16 2016),
- La perte de services essentiels (en moyenne 4,0 vs 6,85 en 2016),
- Les pannes d'origine interne affectant le matériel et/ou le logiciel (en moyenne 3,4 vs 5,97 en 2016).

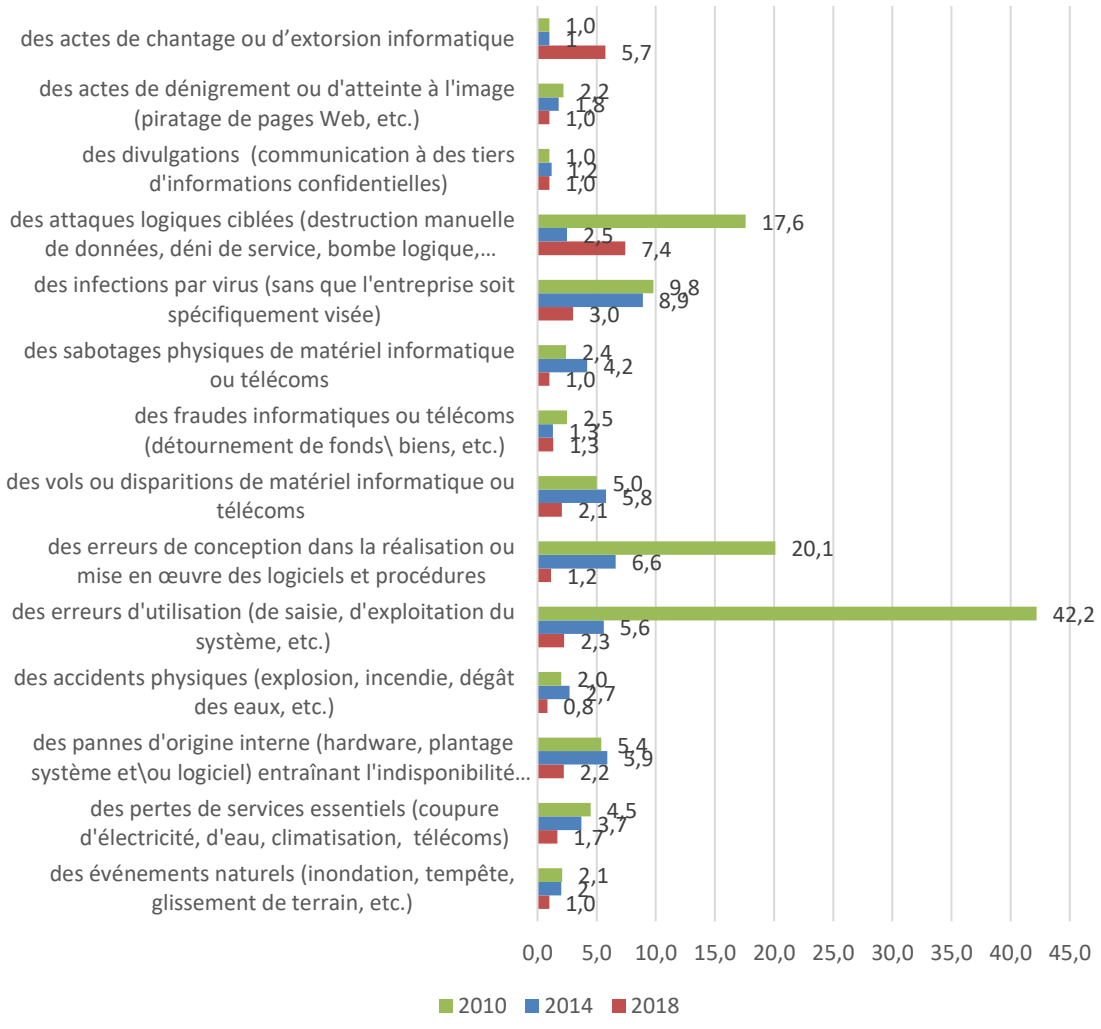


Figure 41- Nombre moyen d'incidents

A l'inverse, certaines causes moins fréquemment rencontrées voient le nombre d'incidents qu'elles engendrent rester stables, voire prendre de l'ampleur, comme :

- Les attaques logiques ciblées (en moyenne 7,4 vs 2,19 en 2016),
- Les actes de chantage et d'extorsion informatique (en moyenne 6,0 vs 4,5 en 2016),
- Des accidents physiques (en moyenne 3,9 vs 2,1 en 2016).

La propagation des attaques de type rançongiciel et la sophistication des attaques ciblées (type APT) ces dernières années confirment cette observation.

La cybercriminalité voit les attaques plus simples se répandre

Parmi les sujets de préoccupation en matière de cybercriminalité, les entreprises restent confrontées aux classiques du domaine.

Les actes de cybermalveillance basés sur l'exploitation du facteur humain (e.g. via ingénierie sociale) sont prépondérants et largement représentés par :

- Les tentatives d'hameçonnage (phishing),
- Les rançons et fraudes au président,
- Les fraudes aux moyens de paiement.

En comparaison, les sujets nécessitant notamment des moyens de mise en œuvre plus considérables (e.g. cyber-espionnage) ou dépassant les intérêts propres des entreprises (e.g. cyber-conflit ou hacktivisme) ont été moins virulents pour celles-ci.

Bien que peu répandue actuellement, la cybercriminalité exploitant les monnaies virtuelles pourrait bien voir son essor se confirmer à court terme (e.g. minage via navigateur web).

Les sujets suivants ont été abordés lors du Panorama de la Cybercriminalité du CLUSIF au cours des dernières années. Avez-vous été confrontés à un ou plusieurs de ces sujets en 2017 ?

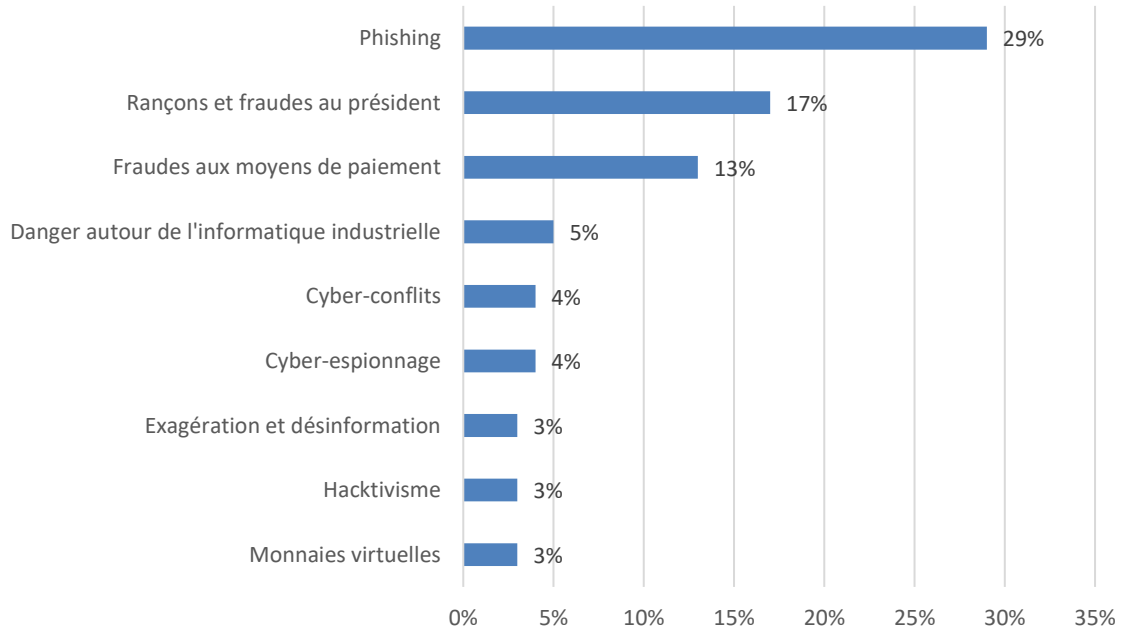


Figure 42 - Sujets de cybercriminalité auxquels les entreprises ont eu à faire face en 2017

Le phishing, populaire mais efficacité limitée

La tentative d'hameçonnage (phishing) est la principale menace cybercriminelle évoquée par les entreprises. Ce danger est loin d'être récent ; pour autant, il préoccupe largement les entreprises – 57% d'entre elles jugeant « forte » son importance contre 13% la jugeant « faible ».

Par ailleurs, le phishing touche globalement tous les secteurs d'activité et les structures de toute taille, près de la moitié d'entre elles affirmant y être confrontées. Cet acte cybercriminel affecte cependant encore davantage le secteur des Transports-Télécoms (44%) et les entreprises de plus de 2 000 salariés (47%).

Ce vecteur d'attaque, bien que commun, dispose d'une efficacité limitée en matière de réussite à infecter les organisations ciblées. 64% des entreprises affirment n'avoir connu aucun impact lié au phishing cette année, contre 5% reconnaissant le vol de données et 3% la prise de contrôle à distance de postes.

En réaction, deux types de mesures sont principalement mises en œuvre :

- Une réponse technique, avec le renforcement des mesures de sécurité (5%),
- Une réponse comportementale, qui vise à mieux sensibiliser les utilisateurs (9%).

Rançons et fraudes, les autres vecteurs de cybercriminalité

La « fraude au président » et les autres formes de rançonnement, ainsi que la fraude aux moyens de paiement, font aussi partie des types des tentatives, voire actes de cybercriminalité les plus courantes auxquelles les entreprises ont eu affaire cette année (respectivement 17% et 13%).

La perception de l'importance de l'impact de ces actes est, quant à elle, plus faible que pour la tentative d'hameçonnage. En effet, si 55% des entreprises les considèrent bien d'importance « forte », 25% d'entre elles perçoivent les « fraudes au président » d'importance « faible » et cette perception monte à 31% pour les fraudes aux moyens de paiement.

Par ailleurs, si, en général, moins de 20% des entreprises affirment devoir faire face à ce type d'action, les organisations de plus de 2 000 salariés sont les principales cibles des cybercriminels (30% ont été touchées par des rançons et « fraudes au président » et 23% par des fraudes aux moyens de paiement).

L'évaluation et la couverture des préjudices financiers ne sont pas encore la norme

En cas d'acte cybercriminel réussi, les impacts pour les entreprises peuvent potentiellement représenter un préjudice certain, selon la nature de l'action et sa capacité de nuisance. Lorsque l'incident est détecté, des mesures de traitement sont quasiment systématiquement engagées pour assurer un retour à la normale dans les meilleurs délais.

Cependant, en phase post-traitement, si un retour d'expérience peut avoir lieu, l'évaluation des impacts financiers dus à l'incident est réalisée par moins de la moitié des entreprises (43%). Cette démarche est la plus répandue dans les secteurs de la Banque-Assurance (63%) et, non seulement auprès des entreprises de plus de 2 000 salariés (53%) mais aussi auprès de celles de plus de 500 salariés (46%).

Cette représentativité est d'ailleurs très similaire à celle observée en matière d'assurance. En effet, les entreprises évaluant les préjudices liés aux incidents de sécurité sont principalement celles ayant complété la logique par la souscription à des polices d'assurance (25%).

Notons que, si certaines entreprises veillent bien à couvrir leur patrimoine informationnel au sein de l'entreprise, peu d'entre elles (17%) y inclut la valeur de l'information contenue sur les appareils mobiles (e.g. smartphones, tablettes).

Logiquement, à la suite d'un sinistre avéré, son financement repose essentiellement sur les capacités de trésorerie de l'entreprise victime (42%), qui peut éventuellement avoir provisionné le risque en amont via un poste budgétaire prévisionnel. Compte-tenu du faible taux de pénétration de la logique d'assurance, seules 5% d'entre elles ont su réduire l'impact par activation de leur police – ce qui, d'ailleurs, est plus régulier auprès des entreprises du secteur Transports-Télécoms (8%).

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

L'indisponibilité d'un fournisseur essentiel : le parent pauvre de la gestion de la continuité d'activité

Comme l'indique la figure ci-dessous, seules 15% des entreprises prennent en compte l'indisponibilité d'un fournisseur essentiel. Pourtant la gestion de la continuité d'activité implique de prendre en compte ce scénario de défaillance dans la poursuite des activités en cas de crise. En effet, la continuité de service des opérateurs télécoms, des fournisseurs d'énergie (ou autres utilités) est essentielle à la continuité d'activité et une attention particulière doit être portée à ces partenaires.

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

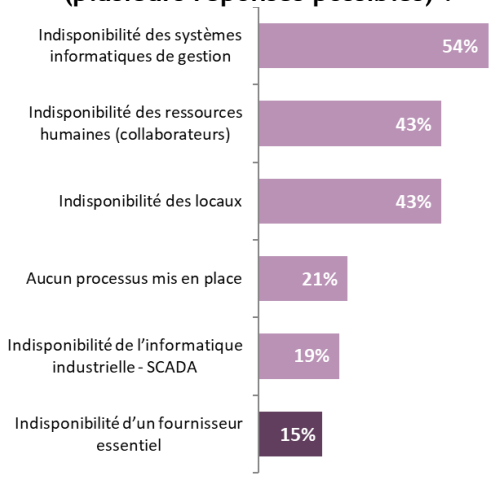


Figure 43 - Scénarios de sinistres couverts

Un net développement de la mise en place de dispositifs de gestion de crise !

Pour rappel, dans le cadre de l'étude de 2016, près de la moitié des entreprises interrogées n'avait pas de processus de gestion de crise formalisée. En 2018, cette proportion tombe à un taux faible de 15%, ce qui marque un net progrès en matière de préparation à la gestion de crise.

La gestion de crise dans votre entreprise comprend-elle (plusieurs réponses possibles) ?

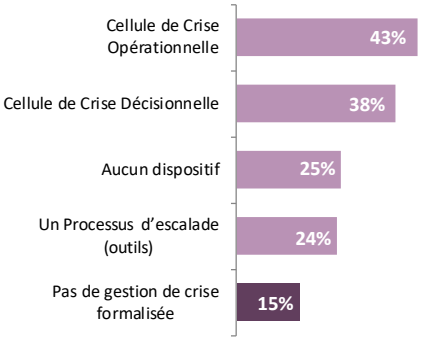


Figure 44 - Moyens mis en œuvre dans le cadre de la gestion de crise

Thème 18 : Conformité

Ce thème aborde les éléments liés à la conformité sous trois aspects :

- La conformité avec la Loi Informatique et Libertés,
- Les audits de sécurité,
- L'utilisation de tableaux de bord.

Conformité avec la Loi Informatique et Libertés

La déclaration des traitements à la CNIL est toujours assurée en majorité par la DSI (34%), puis de manière presque équivalente, à 13% par le Correspondant Informatique et Libertés (CIL) ou le Délégué à la Protection des données/Data Protection Officer (DPO/DPD), par le service RH (13%) et dans une moindre mesure, par le service juridique (10%). De manière surprenante, le rôle du CIL n'augmente pas par rapport à 2016, alors même que l'application du Règlement Général sur la Protection des Données (RGPD) devrait rendre sa présence plus fréquente dans les entreprises.

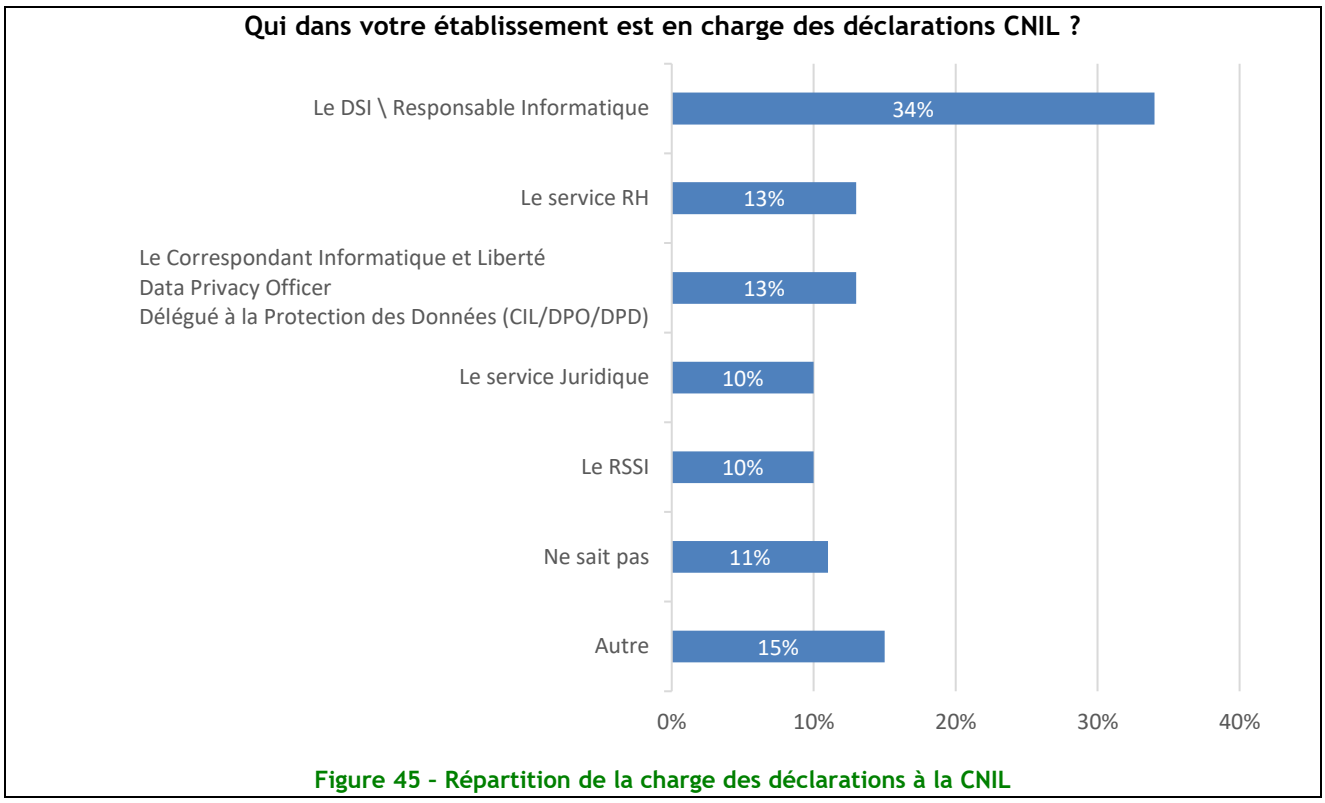


Figure 45 – Répartition de la charge des déclarations à la CNIL

On note que le CIL est beaucoup plus impliqué dans le secteur Banque-Assurances (29%) et qu'au contraire, il l'est très peu dans secteur Transports-Télécom où les déclarations sont bien plus souvent réalisées par le DSI (44%) comme dans les services (41%).

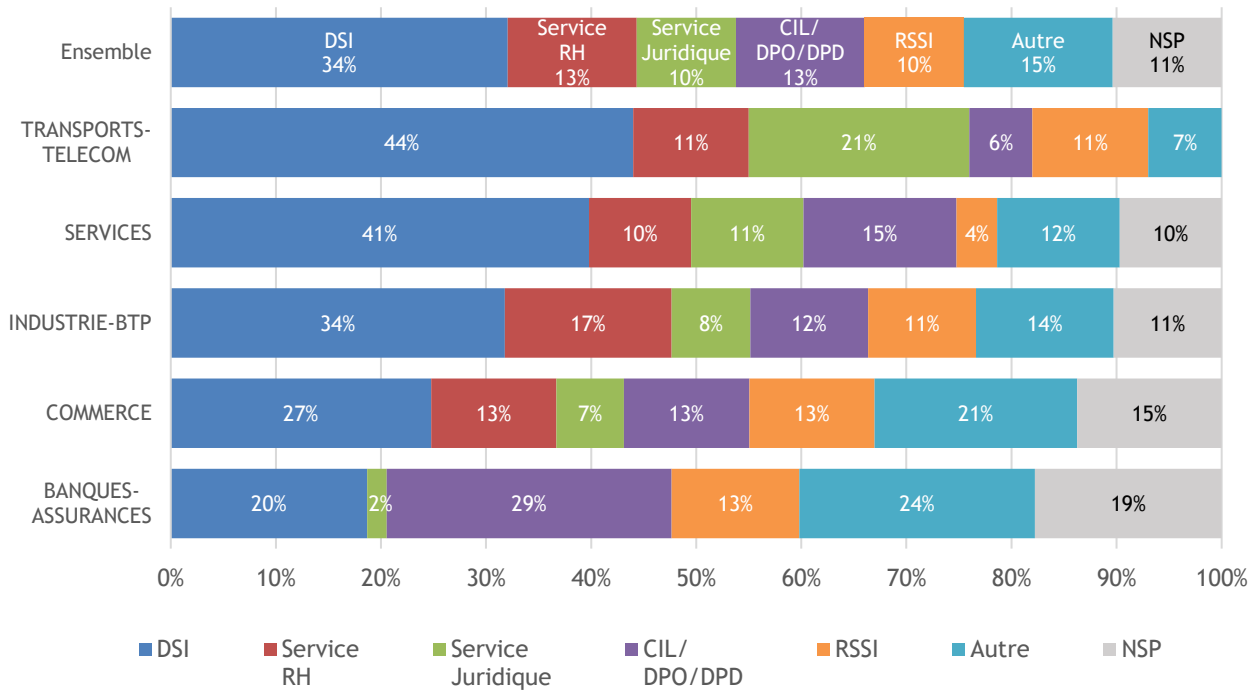


Figure 46 - Répartition de la charge des déclarations à la CNIL selon le secteur d'activité

La différence reste surtout liée à la taille des entreprises. Dans les grandes entreprises (plus de 2 000 personnes), c'est le service juridique qui est le plus souvent en charge des déclarations CNIL (26%), contre 19% entre 500 et 2000 personnes, et seulement 5% en dessous de 250. Le CIL est également cité largement dans les grandes entreprises (24%).

Dans les petites structures où il n'y a souvent pas de CIL ni de service juridique, c'est le DSI qui se charge des déclarations (40%).

Il reste surprenant que le CIL ne soit pas cité plus souvent, au moins dans les grandes entreprises, dans la mesure où le Règlement Européen sur la protection des données personnelles rend la fonction quasiment obligatoire à partir du 25 mai 2018.

La conformité au RGPD

Deux ans après l'entrée en vigueur du Règlement Européen sur la Protection des Données (RGPD) et à quelques mois de son entrée en application, les entreprises semblent être majoritairement prêtes à affronter l'échéance.

Ainsi 68% d'entre elles indiquent être prêtes pour le RGPD, dont 46% partiellement.

On note également que seules 8% « ne savent pas », ce qui confirme que le sujet est maintenant bien intégré dans les réflexions.

C'est dans le secteur de Banque-Assurance que l'on note le taux de préparation (totale ou partielle) le plus élevé (77%).

Votre entreprise est-t-elle prête pour le Règlement Général sur la Protection des Données (RGPD) ?

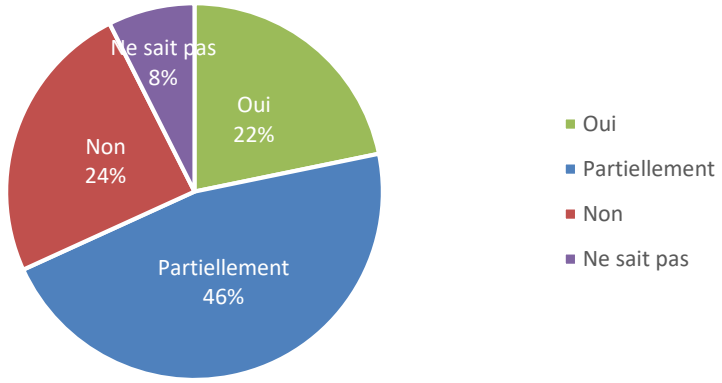


Figure 47 – Répartition du degré de préparation au RGPD

Les audits de sécurité

Comme lors de la précédente enquête, 24% des entreprises indiquent qu'elles sont soumises à des lois ou règlementations spécifiques en matière de sécurité de l'information.

La proportion de répondants indiquant ne pas savoir si leur entreprise est concernée par des règlementations spécifiques reste élevée et même en hausse à 16%.

On note par ailleurs des différences importantes selon les secteurs : les plus concernées par des règlementations spécifiques étant de très loin les banques et assurances (40%), suivies les services (30%) et par les transports (23%).

De la même façon, les grandes entreprises (plus de 2 000 salariés) semblent plus conscientes de leur règlementation spécifique (35%) que la moyenne (18%).

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

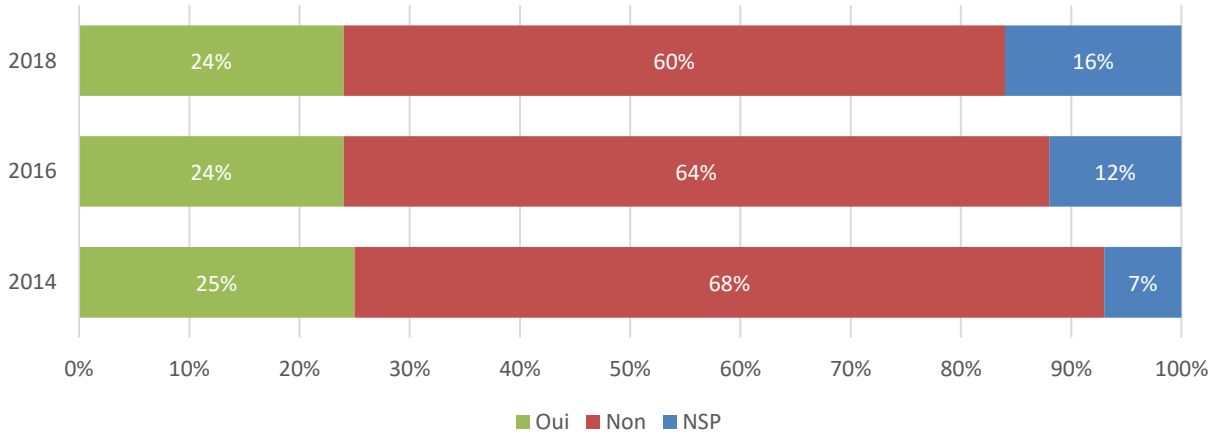


Figure 48 – Entreprises soumises à des lois/règlementations spécifiques pour la sécurité des SI

Dans ce contexte, ce sont toujours près des deux-tiers des entreprises qui ont réalisé un audit de sécurité au cours de deux dernières années, reflétant une relative stabilité dans le temps. On note d'ailleurs que celles qui ne pratiquent aucun audit, sont en diminution régulière (19%, contre 25 puis 22% lors des précédentes enquêtes).

Combien d'audits ou de contrôles de sécurité du Système d'Information sont menés en moyenne au sein de votre entreprise sur une période de 2 ans ?

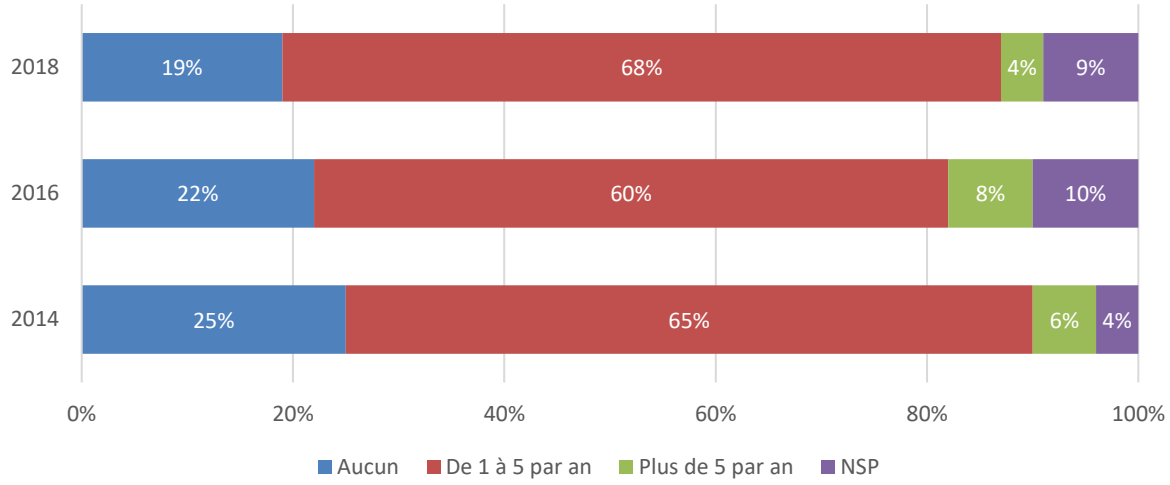


Figure 49 - Nombre d'audits de sécurité du SI réalisés sur une période de 2 ans

Les grandes entreprises pratiquent les audits de façon quasi systématique (91% contre 68% en moyenne). Le secteur Banques-Assurances est également le plus consommateur de ce type de prestation (76%) contre seulement 55% dans le secteur Transports-Télécom.

Les audits réalisés portent essentiellement sur les tests d'architecture (58%) et les tests d'intrusion (47%). Viennent ensuite les audits de configuration (45%), les audits organisationnels (39%) et les revues de droits d'accès logiques (34%), puis les audits de continuité d'activité (32%) et les audits physiques (30%).

En ce qui concerne les motivations de ces audits, l'existence d'une exigence contractuelle ou règlementaire est la première citée (33%). Viennent ensuite le respect de la PSSI (20%) puis à égalité l'audit de tiers externe et les suites d'un incident (16%).

Toutefois, 24% des répondant indiquent que les audits sont réalisés sans motivation particulière.

Quelles sont les motivations principales qui déclenchent ces audits ?

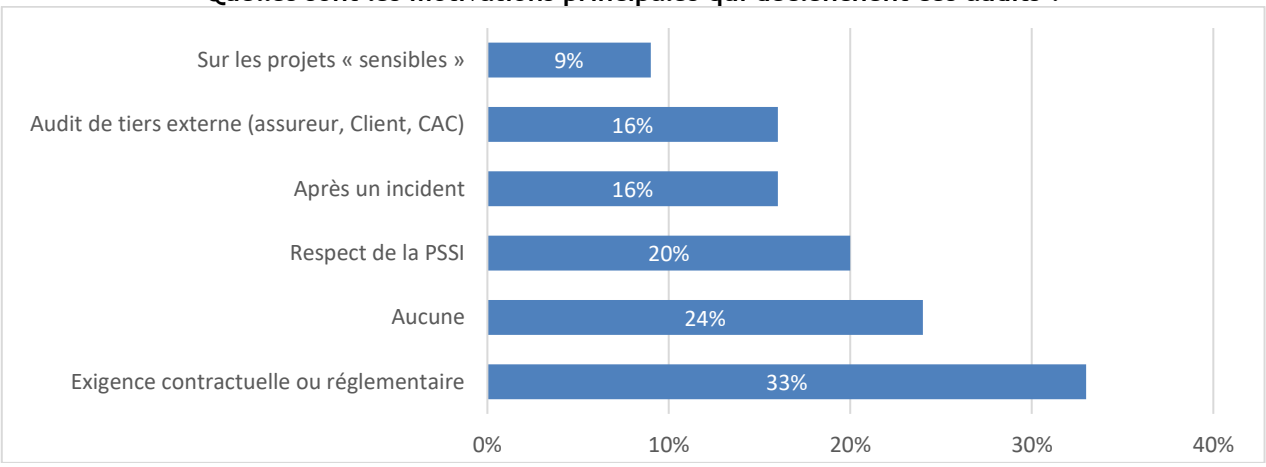


Figure 50 - Motivations déclenchant les audits de sécurité

Utilisation de tableaux de bord de sécurité

L'utilisation de tableaux de bord reste très largement absente, une majorité d'entreprises (71%) indiquant ne pas en avoir mis en place. On observe cette année une diminution sensible du nombre d'entreprises qui disent disposer de tableaux de bord (22% contre 25% en 2016).

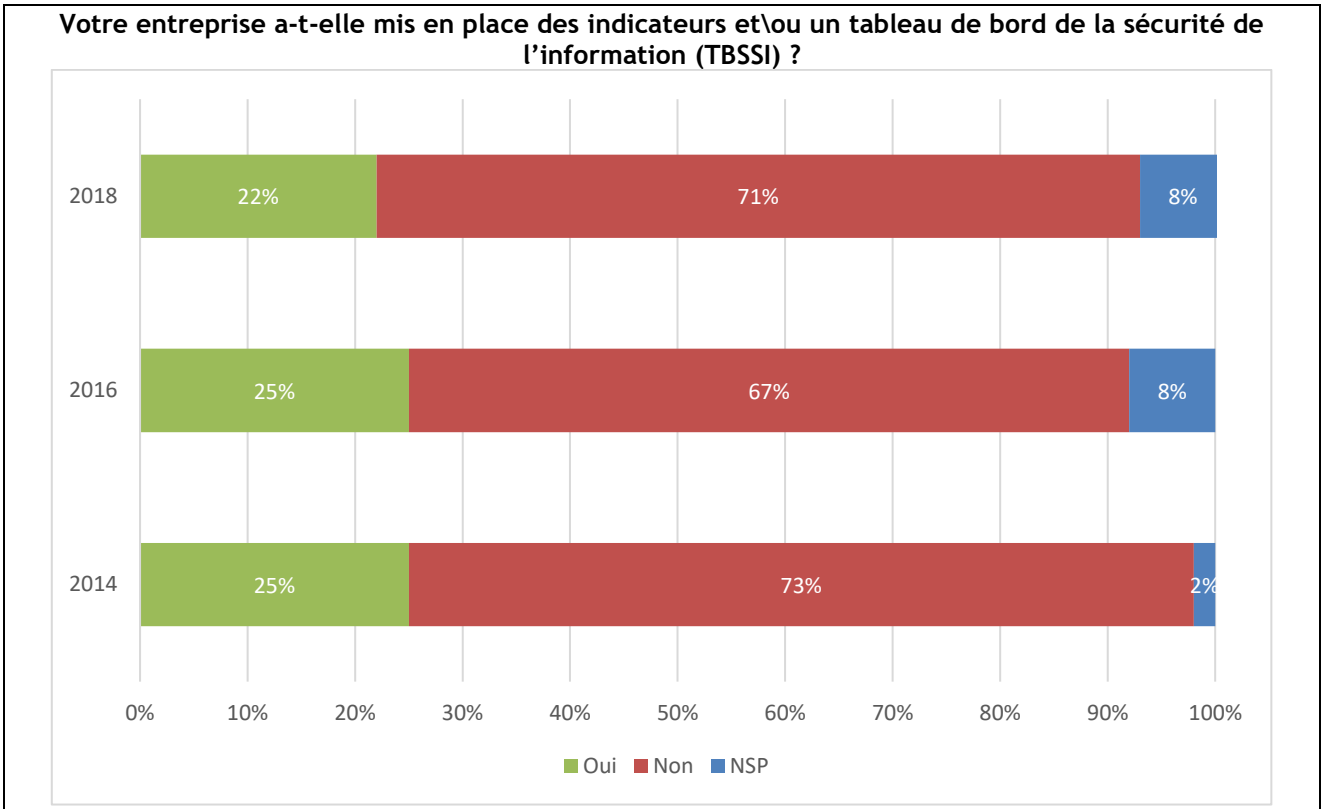


Figure 51 – Mise en place de tableaux de bord de la sécurité de l'information

On note au cours des dernières enquêtes, une connaissance encore incertaine des indicateurs (17% ne savent pas répondre). Cette année marque une augmentation sensible des indicateurs stratégiques, synonyme d'un intérêt grandissant de la part des Directions générale (32%) et une certaine stabilité pour la SSI (42%) tandis que la vocation opérationnelle des indicateurs reste la motivation principale (74%).

Santé

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

Les établissements de santé de plus de 100 lits

Présentation de l'échantillon

Présentation de l'échantillon

L'enquête a été réalisée par téléphone début 2018 auprès des hôpitaux publics et structures d'hébergement médicalisé de plus de 100 lits :

- 127 hôpitaux et 24 structures d'hébergement médicalisé y ont répondu (soit 151 répondants), 67% des établissements appartiennent à un groupement,
- La personne ciblée était le Responsable de la Sécurité des Systèmes d'Information, ou à défaut le responsable informatique ou toute personne ayant cette question en charge. La durée moyenne de l'entretien téléphonique est de 24 minutes.

Il est important de noter que le périmètre d'étude a été modifié par rapport à la précédente enquête qui date de 2014 :

- En 2014, seuls les établissements de 200 lits et plus étaient interrogés. En 2018, l'étude porte sur les établissements de 100 lits et plus,
- En 2014, seules les Activités hospitalières étaient concernées. En 2018, l'enquête est étendue aux établissements d'Hébergement médicalisé.

Profil des établissements interrogés et redressement effectué

Un redressement a été effectué afin que l'enquête soit représentative des types d'établissements (Activités hospitalières / Hébergement médicalisé) et des tranches en nombre de lits.

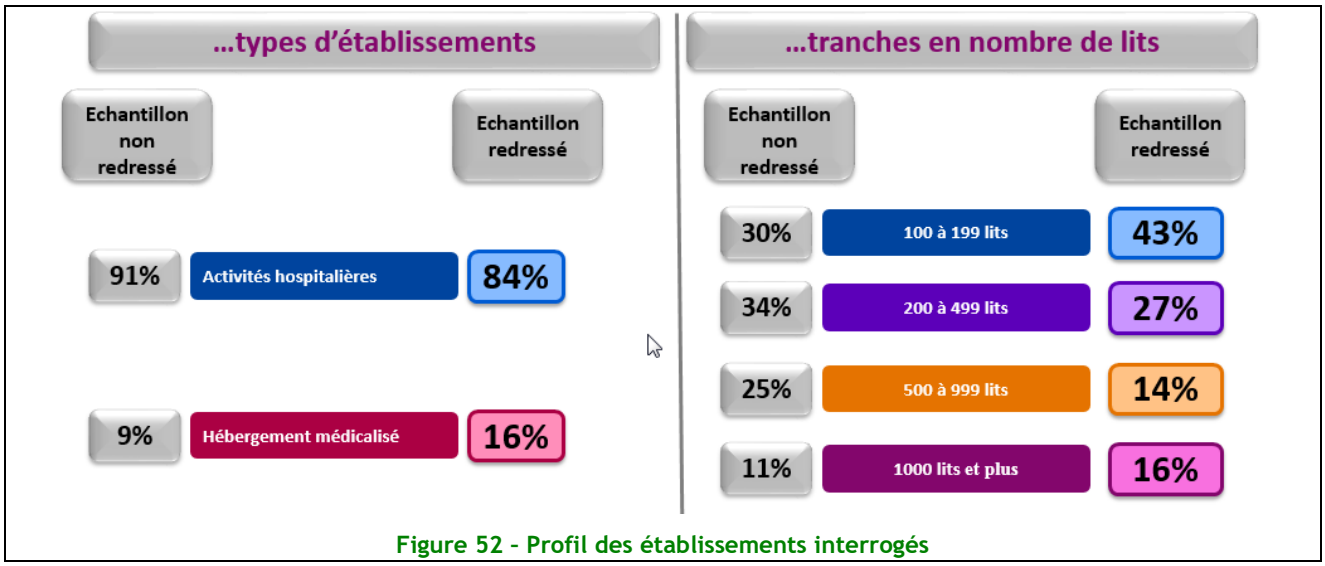


Figure 52 - Profil des établissements interrogés

Profil des personnes interrogées

Les répondants dépendent à 86% des fonctions SI. Pour le reste, 11% dépendent des fonctions de management et de gestion, 3% des fonctions techniques et de sécurité.

Une évolution majeure est à constater par rapport aux précédentes études puisque ce sont les RSSI qui ont majoritairement répondu à l'enquête, alors qu'en 2014 et 2010 les sondés étaient principalement des directeurs ou responsables SI/informatique. Ceci permet de penser qu'il y a une vraie professionnalisation de la fonction de gestion de la sécurité du SI avec plus d'expertise, plus de moyens et plus d'autonomie.

Une double analyse des résultats

Du fait de la modification du périmètre d'étude, et afin de pouvoir comparer avec les enquêtes de 2010 et 2014 (lorsque les questions sont identiques), une double analyse des résultats est présentée :

- Analyse 2018, basée sur 151 établissements,
- Analyse 2018 sur périmètre 2014, basée sur 109 établissements.

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

Progression de la formalisation et confirmation de son importance

Le nombre d'établissements ayant formalisé leur PSI fait un bond spectaculaire, passant de 50% en moyenne à près de 90%. Ceci peut s'expliquer au moins en partie par le levier réglementaire de plus en plus insistant dans la sphère santé (PSSI ministérielle, PGSSI-S Asip, référentiel de certification des établissements de santé HAS, Certification des comptes…).

Votre établissement a-t-il formalisé sa Politique de Sécurité de l'Information (réponse = oui) ?

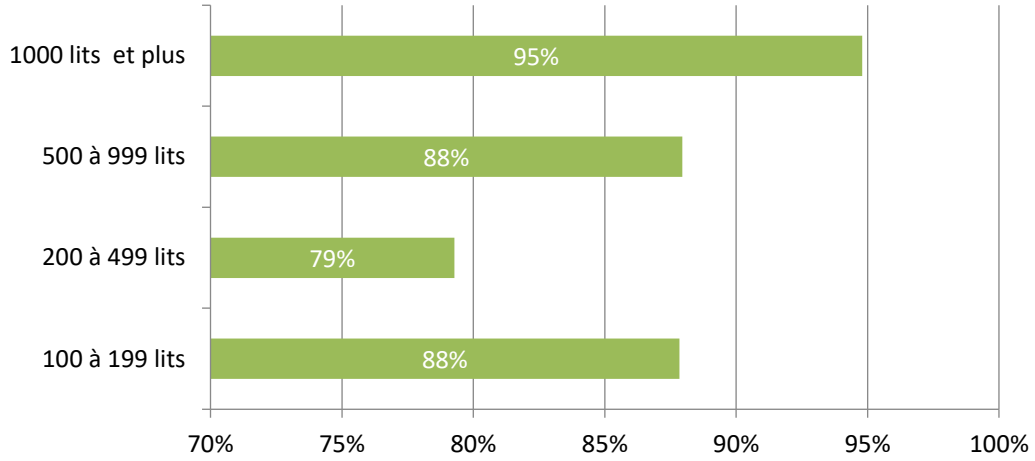


Figure 53 - Établissements ayant formalisé leur Politique de sécurité

De plus, cette politique est globalement à jour, surtout pour les petits établissements.

Si la PSSI est formalisée, a-t-elle été mise à jour il y a moins de 3 ans (réponse = oui) ?

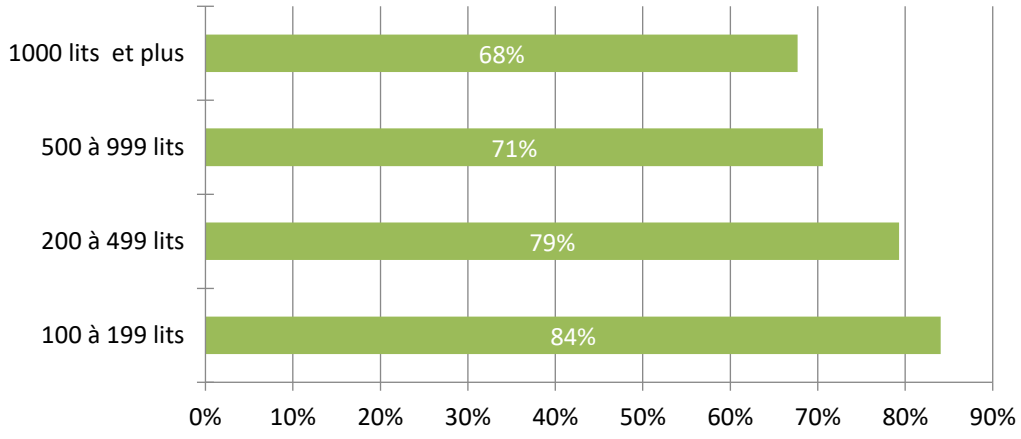


Figure 54 - Établissements ayant mis à jour leur Politique de sécurité il y a moins de 3 ans

La PSI des établissements de santé reste massivement soutenue par la Direction Générale pour près de 95% des établissements).

Communication de la Politique de sécurité

Cette Politique de sécurité est largement diffusée à toutes les parties prenantes (81% dont 37% de manière proactive et explicite et 44% « pour information », sans accompagnement spécifique). Ces chiffres sont en nette progression par rapport à la dernière enquête (68% dont 31% de manière proactive et explicite) et 37% pour information.

La Direction Générale…très impliquée dans l'élaboration de la Politique de sécurité !

L'implication de la Direction Générale se confirme et est citée par un peu plus de 75% des établissements, les DSI étant à peu près également citées.

Les principaux acteurs de la formulation de la PSSI sont la DG, la DSI, et le RSSI.

Quelles sont les entités de votre établissement qui se sont impliquées dans l'élaboration de la Politique de Sécurité de l'Information (PSSI) ?

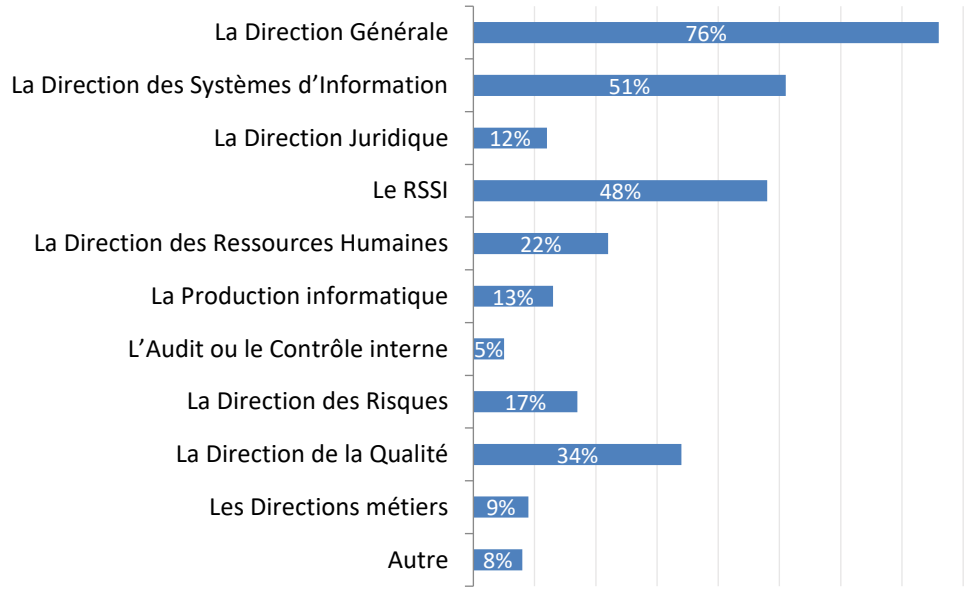


Figure 55 - Entités ayant été impliquées dans la Politique de sécurité

Pilotage de la sécurité de l'information

Cette nouvelle question fait apparaître clairement que le pilotage de la sécurité de l'information s'appuie majoritairement sur des normes ou des référentiels, mais que l'analyse des risques n'est utilisée que très marginalement, dans les entreprises, comme instrument de pilotage.

On notera cependant que, bien que le management des risques soit très peu cité comme instrument de pilotage, 94% des établissements ont effectué un inventaire au moins partiel de leurs risques, que 74% en ont déduit un plan de réduction des risques (voir thème 8) et que 25% utilisent, comme indicateur de tableau de bord, une cartographie des risques.

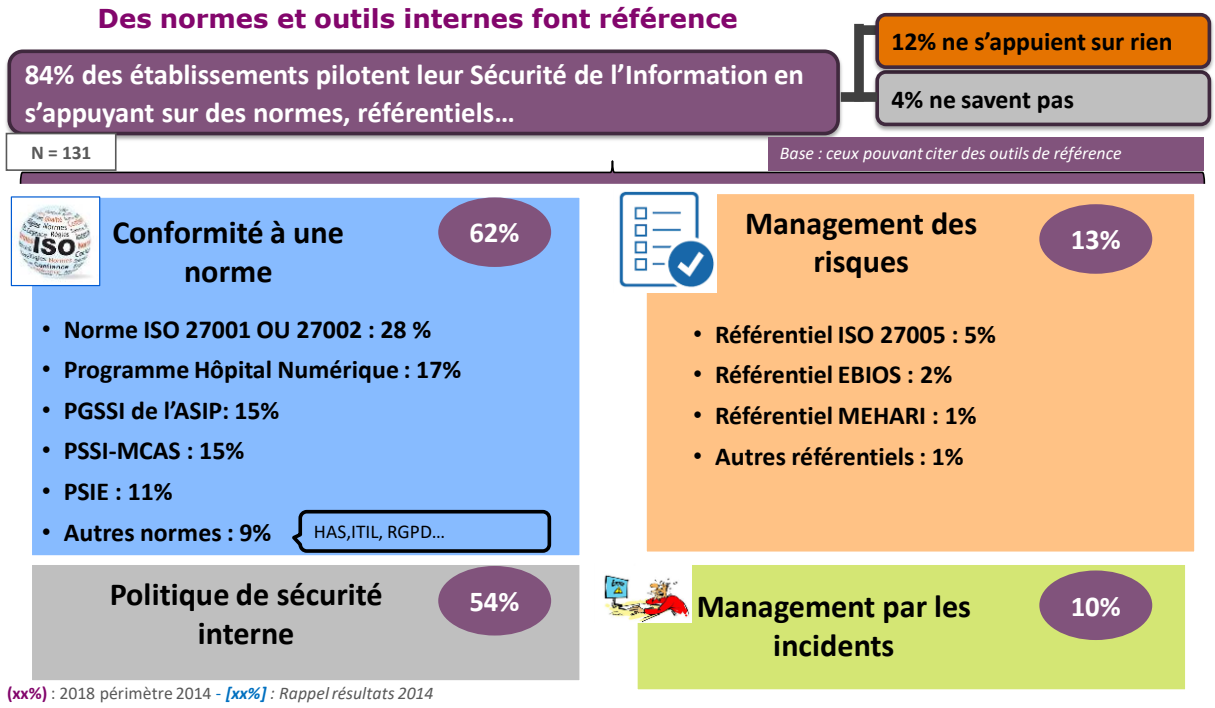


Figure 56 - Outils de référence de la PSI

Thème 6 : Organisation de la sécurité de l'Information

Nette progression de l'identification et de l'attribution de la fonction RSSI

Le nombre d'établissements ayant identifié et attribué la fonction RSSI progresse nettement et atteint globalement, sur la population de l'échantillon 2018, 80%. Elle est même de 90% à population comparable (mêmes types et mêmes tailles d'établissement) alors qu'elle était de 60% en 2014.

La fonction de Responsable de la Sécurité des Systèmes d'Information (RSSI) ou de Responsable de la Sécurité de l'Information (RSI) est-elle clairement identifiée et attribuée (réponse = oui) ?

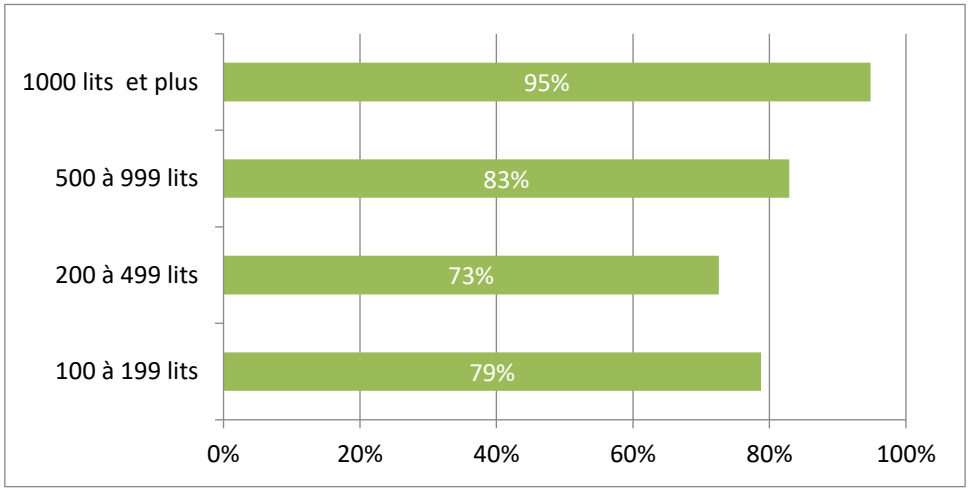


Figure 57 - Établissements ayant clairement identifié et attribué la fonction RSSI

Ce pourcentage varie notablement en fonction de la taille des établissements et atteint 95% pour les établissements de plus de 1000 lits.

La fonction de RSSI, quand elle est attribuée, est occupée à plein temps pour 47% des établissements, chiffre en progression également (à isopérimètre, 58% en 2018 contre 26% en 2014) et atteint 78% pour les établissements de plus de 1000 lits (31% pour ceux de moins de 1000 lits). Le RSSI assure cette fonction pour plusieurs établissements dans 44% des cas.

Quand la fonction de RSSI n'est pas attribuée, elle est en très grande majorité (les 2/3) assurée par le Directeur des Systèmes d'information ou le Responsable informatique.

Le Règlement Général sur la Protection des Données (RGPD) installe un rôle de Délégué à la protection des données ou Data Protection Officier (DPO) pour chaque organisation à partir du 25 mai 2018.

Le DPO est tourné vers la personne, comme par exemple pour s'assurer de la protection des données à caractère personnel dans le cadre d'un traitement informatisé de la paie, alors que le RSSI est tourné vers l'activité de l'entreprise, comme par exemple pour la disponibilité du Dossier Patient Informatisé (DPI) dans le cadre de la prise en charge des patients pour un établissement de santé.

Le DPO doit dans la cadre de la protection des données à caractère personnel traiter des aspects de sensibilisation, fonctionnels de type politique, juridiques, d'analyses d'impact sur la vie privée, etc.

Les méthodologies étant similaires, plusieurs RSSI occupant cette fonction à plein temps risquent, à la mise en application du RGPD, d'avoir à la partager avec la fonction de DPO. À suivre dans la prochaine enquête MIPS !

Rattachement du RSSI

Le RSSI, quand la fonction est attribuée, est rattaché majoritairement soit à la Direction Générale soit à la DSI, avec une répartition différente selon le type et la taille de l'établissement.

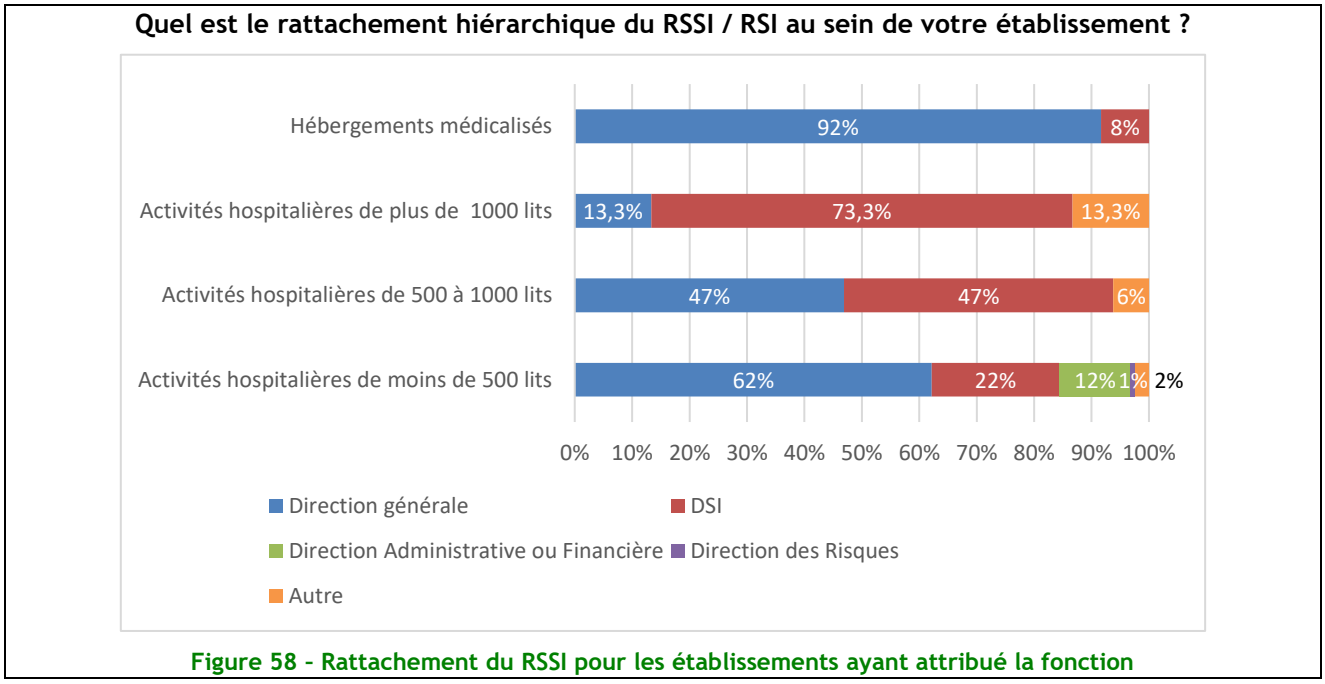


Figure 58 – Rattachement du RSSI pour les établissements ayant attribué la fonction

Temps consacré aux différents aspects de la fonction par le RSSI

Le temps consacré aux différents aspects de sa fonction, par le RSSI ressort ainsi :

- Aspects fonctionnels (Politique, analyse de risques, etc.) 25%
- Aspects techniques (architecture de sécurité, suivi de projets, etc.) 25%
- Aspects opérationnels (gestion des droits, administration, etc.) 24%
- Aspects juridiques (charte utilisateurs, recherche de preuve, etc.) 12%
- Aspects de communication (sensibilisation, etc.) 14%

Effectif total de l'équipe Sécurité (rattachée au RSSI)

Les effectifs rattachés directement au RSSI sont en nette augmentation, avec près de 70% des établissements ayant une équipe rattachée au RSSI comportant plus d'une personne – tant sur le périmètre 2018 que 2014, (contre 45% il y a quatre ans) :

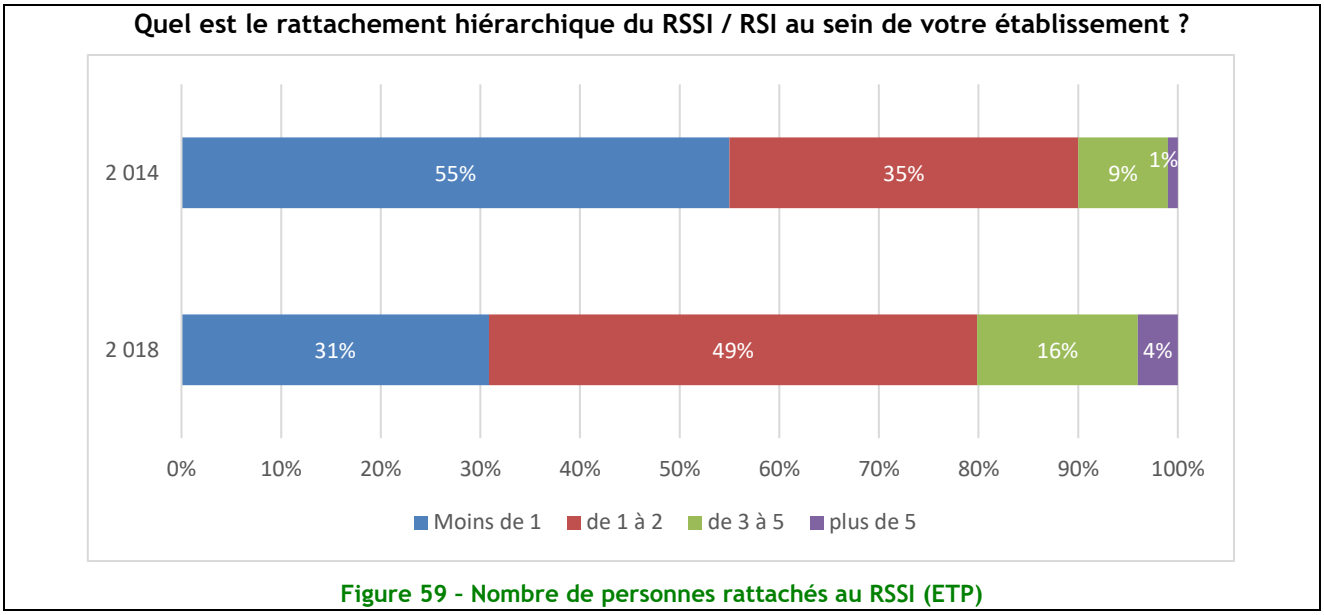


Figure 59 – Nombre de personnes rattachés au RSSI (ETP)

Une mauvaise identification des coûts de la sécurité de l'information

Plus de 81% des établissements ne sont pas en capacité d'identifier les coûts liés à la sécurité de l'information. De plus, l'étude 2018 ne permet pas de déterminer de façon fiable le budget moyen consacré à la sécurité (en montant ou en part du CA).

Évolution du budget sécurité de l'information par rapport à l'année précédente

Le budget sécurité de l'information est en augmentation pour plus d'un établissement sur 3 (et même 2/3 pour les hôpitaux de plus de 1000 lits). C'est une tendance forte par rapport à la précédente enquête qui pointait majoritairement une stabilité des budgets pour 2 établissements sur 3.

Cette évolution des coûts est cependant mal connue pour 38% des établissements contre 11% en 2014 (à isopérimètre), ce qui confirme la mauvaise identification des coûts liés à la sécurité de l'information.

Augmentation du budget dédié aux solutions techniques (année n/n-1)

La plus grosse augmentation de budget réside dans la mise en place de solutions techniques (25% des établissements ont augmenté leur budget sur ce poste par rapport à l'année précédente). Ce chiffre important (bien qu'en baisse par rapport à 2014) traduit le besoin croissant de renouvellement, d'extension et de sécurisation des infrastructures.

Les établissements (16% des répondants) continuent aussi à apporter une attention spécifique aux solutions métier qui contribuent à l'informatisation du parcours de soins et donc à la sécurisation des prises en charge.

L'augmentation des budgets consacrés aux contrôles/audits (pour 14% des établissements), aux actions de formation/sensibilisation des personnels (11%) et à la mise en place d'éléments organisationnels (8%) permet de penser que de vraies politiques de sécurité des systèmes d'information commencent à se mettre en place.

Cependant, dans la continuité de 2014, un quart des établissements « ne savent pas » quelles sont les évolutions budgétaires : c'est un indicateur de l'absence d'un plan d'actions sécurité formalisé, valorisé et suivi. Les marges de progression sont donc encore importantes.

Manque de budget et absence de personnel qualifié sont les principaux freins

Le manque de budget (pour 52% des répondants) et le manque de personnel qualifié (43%) sont les principaux freins identifiés à la conduite des missions de sécurité de l'information. Il n'y a malheureusement pas d'amélioration par rapport à l'étude de 2014.

Coté personnel qualifié, il y a cependant des évolutions positives :

- On peut raisonnablement espérer la mise en place de compétences sécurité mutualisées à travers les GHT afin de répondre aux impératifs du RGPD,
- La fonction RSSI est de plus en plus présente avec une croissance des effectifs.

Il reste cependant, dans beaucoup d'établissements, à identifier un vrai budget sécurité du système d'information qui serait la déclinaison d'une politique et d'un projet sécurité de l'information.

Thème 7 – Sécurité des ressources humaines

Chartes d'usage ou d'utilisation du SI généralisées

96% des établissements ont une charte d'usage ou d'utilisation du système d'information, dont 5% sont en cours d'élaboration. Sur le périmètre de l'étude de 2014, le taux d'adoption de la charte est de 100%, dont 4% en cours d'élaboration.

Ces chartes sont très largement communiquées. Le processus règlementaire d'opposabilité est en progression. Les utilisateurs la signent dans 73% des cas - 65% sur le périmètre 2014, soit +14 points en 4 ans. Plus l'établissement est grand, moins il a tendance à faire signer le document (écart de 12 points entre les extrêmes). Les instances représentatives du personnel sont informées dans 92% des cas (périmètre 2014), en progression de 9 points en 4 ans. Sur le périmètre 2018, la charte est soumise aux IRP dans un peu moins de 9 cas sur 10.

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 de tout le matériel ?

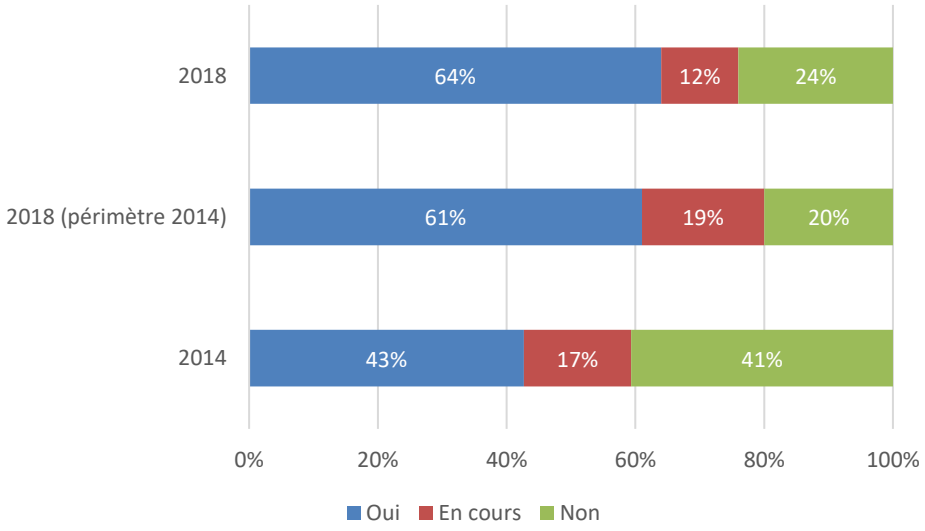


Figure 60 – Procédure de suppression des accès et restitution du matériel

Les chartes ciblent la globalité du personnel (99%, +4 points en 4 ans). Les établissements adressent cette charte à leurs prestataires / fournisseurs pour 66% d'entre eux en 2018 (77% sur le périmètre de 2014, soit +30 points en 4 ans). Les petits établissements sont largement moins enclins à cette pratique (12 points en dessous de la moyenne).

Ces chartes constituent toujours des outils de management et de sensibilisation à destination de l'ensemble des utilisateurs. Elles font partie de l'arsenal des mesures juridiques indispensables. Le recours aux services hébergés et l'ouverture des systèmes d'information des établissements impliquent une généralisation à l'ensemble des acteurs accédant au système d'information.

Trois quarts des établissements s'assurent (programme actif ou en cours) de la modification des droits d'accès des utilisateurs et de la restitution du matériel appartenant à l'établissement, en cas de départ ou de mutation du collaborateur. Cette tendance est en forte progression depuis 4 ans.

Des programmes de sensibilisation à la sécurité de l'information en forte progression

3 établissements sur 5 ont un programme de sensibilisation à la sécurité de l'information, c'est 40% de plus que lors de la dernière étude. Faut-il y voir le résultat du programme Hôpital Numérique évoqué il y a 4 ans ?

Les moyens pour assurer la sensibilisation restent traditionnels. Le moyen principal est la publication de « news » dans l'intranet, l'envoi d'email ou la publication d'articles dans le journal interne.

Quels sont les moyens utilisés pour assurer la sensibilisation ? (plusieurs réponses possibles)

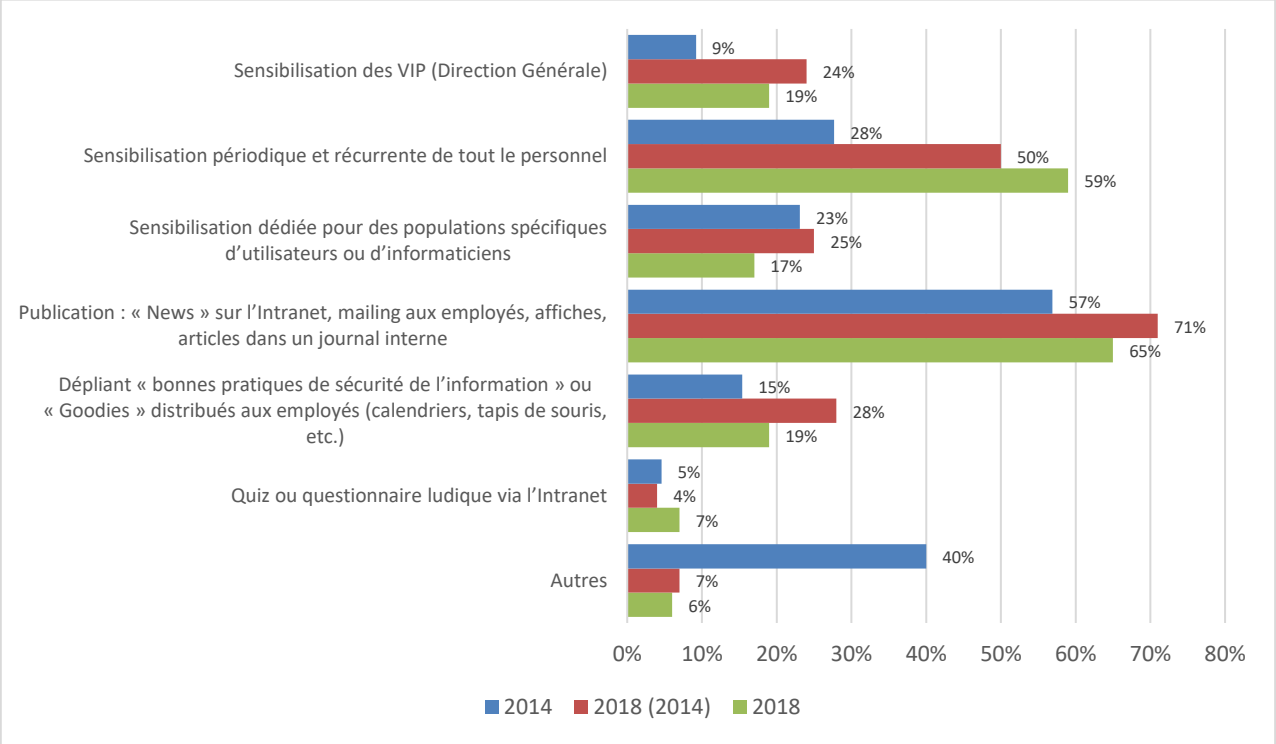


Figure 61 - Moyens utilisés pour la sensibilisation

Les acteurs décideurs sont des relais majeurs pour porter les messages à leurs équipes, et accessoirement dégager les budgets nécessaires à la sécurité des systèmes d'information. Aussi, les VIP sont désormais une cible privilégiée des programmes de sensibilisation (+166% en 4 ans).

De même, la pédagogie restant une histoire de répétition, les actions périodiques et récurrentes sont deux fois plus nombreuses qu'il y a 4 ans.

La mesure de l'impact de cette sensibilisation reste faible et stagne autour de 30% et devra être développée dans les prochaines années pour défendre les moyens (financiers et humains) indispensables à une bonne sensibilisation.

Nous notons un effondrement des solutions propres qui n'ont pas réussi à convaincre (autres, -33 points depuis la dernière étude). Sans doute que l'efficacité de ces solutions n'était pas à la hauteur des coûts élevés associés à leurs spécificités.

Thème 8 : Gestion des actifs

Très forte progression de l'inventaire des actifs : l'inventaire au moins partiel devient une généralité

En 4 ans les établissements déclarant avoir inventorié tous leurs actifs passent de 17 à 65% et, pour les inventaires partiels de 72 à 90%.

En 4 ans les établissements déclarant avoir inventorié leurs actifs passent de 71% à 88% :

- de 17 à 58% pour les inventaires complets,
- de 54 à 30% pour les inventaires partiels.

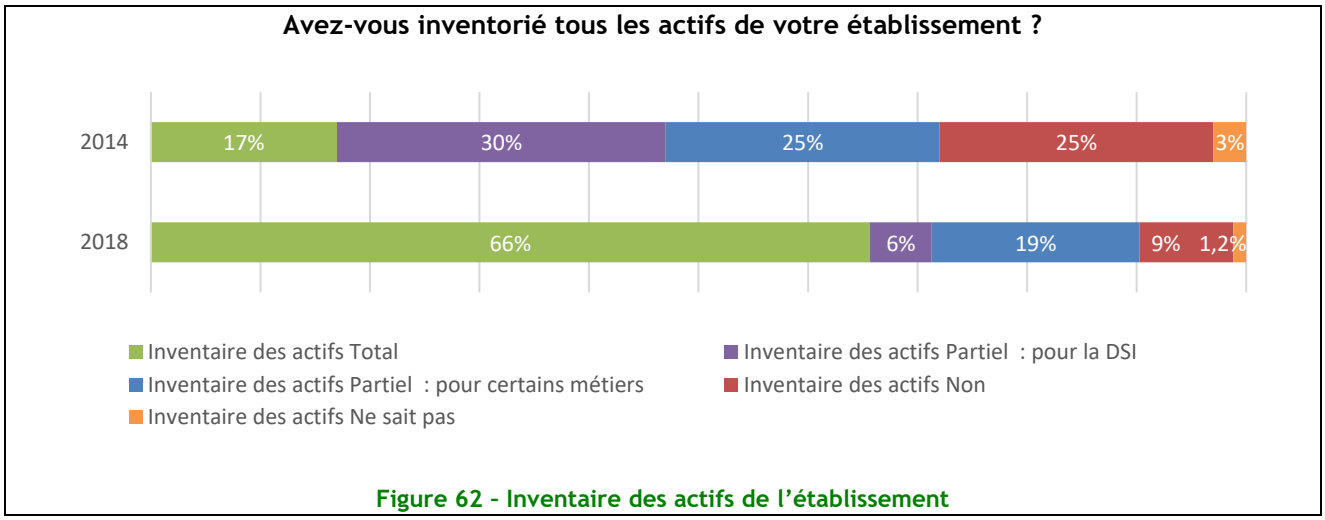


Figure 62 - Inventaire des actifs de l'établissement

À noter que ces chiffres sont peu sensibles à un tri selon la taille ou la nature des établissements.

La classification des actifs se généralise

La classification au moins partielle des actifs progresse, pour atteindre en moyenne 71%. Les établissements médicalisés (qui ne figuraient pas dans les statistiques de 2014) atteignent, pour leur part 96% de classification au moins partielle et 43% de classification de tous les actifs.

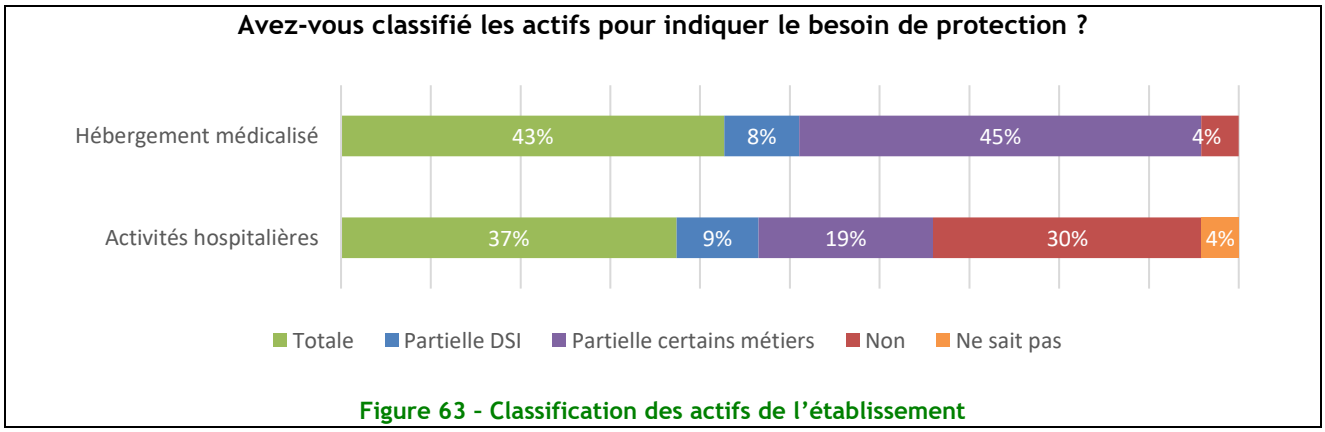


Figure 63 - Classification des actifs de l'établissement

Le nombre de niveaux de classification marque une tendance à l'augmentation, le nombre d'établissements déclarant uniquement 2 niveaux étant en nette diminution (8% contre 20% il y a 4 ans).

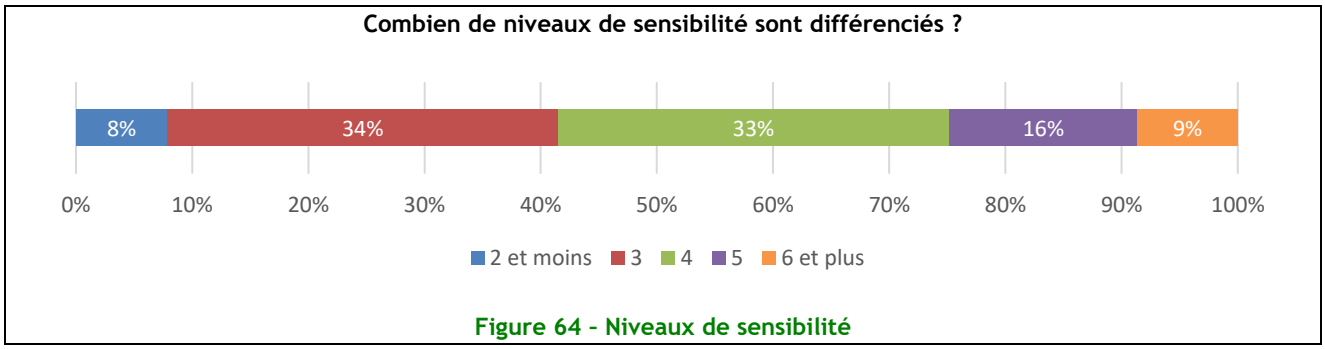


Figure 64 - Niveaux de sensibilité

Pour cette classification, 27% des établissements déclarent avoir « outillé » ou industrialisé la démarche, avec divers outils dont Excel pour 20% d'entre eux.

L'inventaire des risques devient une généralité

L'inventaire, au moins partiel des risques devient une généralité pour plus de 80% des établissements, en notant cependant qu'il est plus partiel dans les établissements médicalisés.

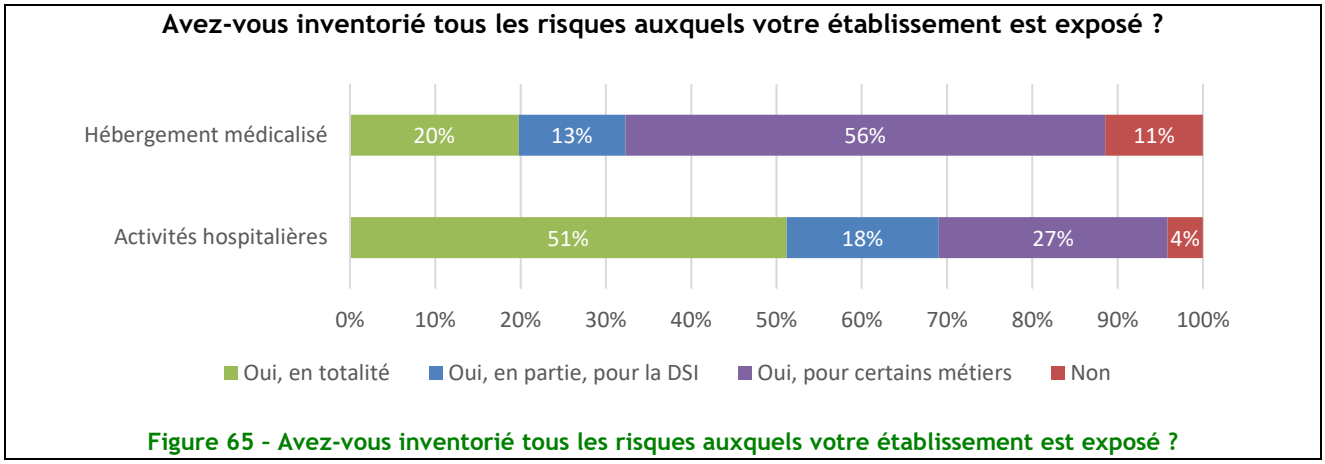


Figure 65 - Avez-vous inventorié tous les risques auxquels votre établissement est exposé ?

L'analyse formelle des risques identifiés n'est pas généralisée

L'analyse formelle des risques identifiés n'est réalisée que par 41% des établissements ayant effectué un inventaire au moins partiel de leurs risques, avec une plus forte proportion pour ceux ayant effectué un inventaire complet.

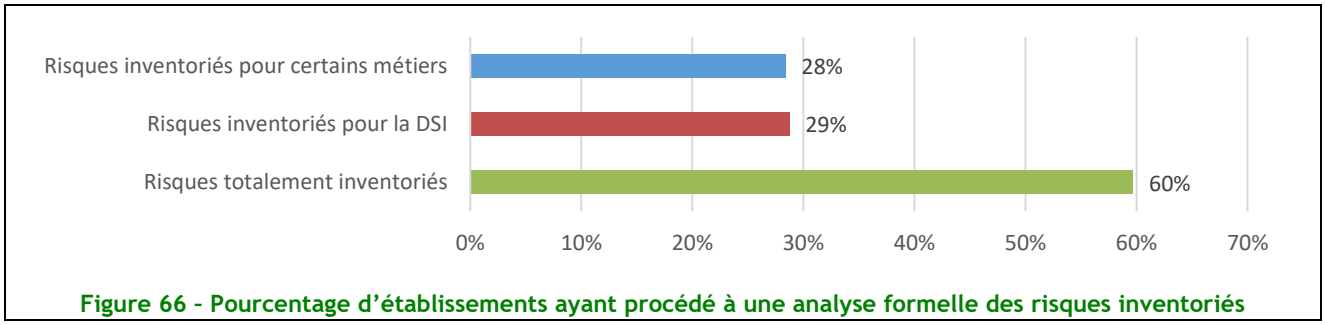


Figure 66 - Pourcentage d'établissements ayant procédé à une analyse formelle des risques inventoriés

Pour les établissements ayant effectué une analyse formelle de leurs risques, Ebios est la méthode la plus utilisée.

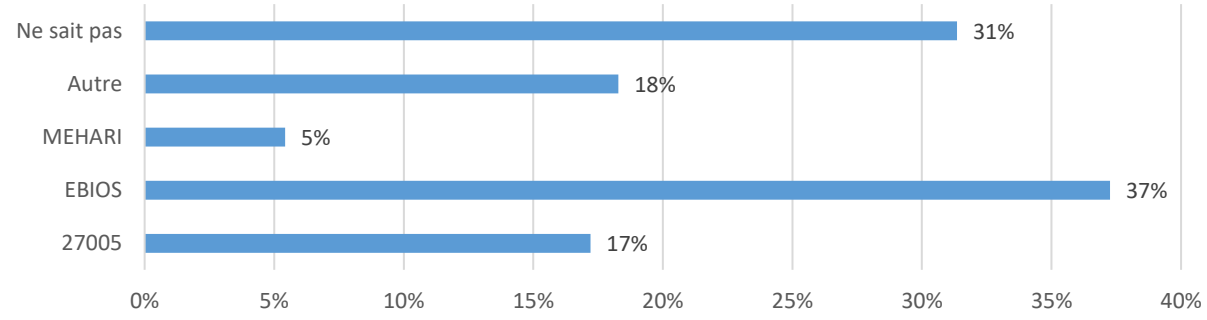


Figure 67 – Méthodes d'analyse des risques utilisées

À noter que certains établissements utilisant plusieurs méthodes, la somme des pourcentages dépasse 100%.

Cette analyse est menée principalement par le RSSI (dans la moitié des cas) et les résultats en sont validés par la Direction de l'établissement, au moins partiellement, dans 76% des cas

Cependant, même si l'analyse formelle des risques n'est pas généralisée, la grande majorité des établissements, en moyenne 74%, a établi un plan de réduction de leurs risques.

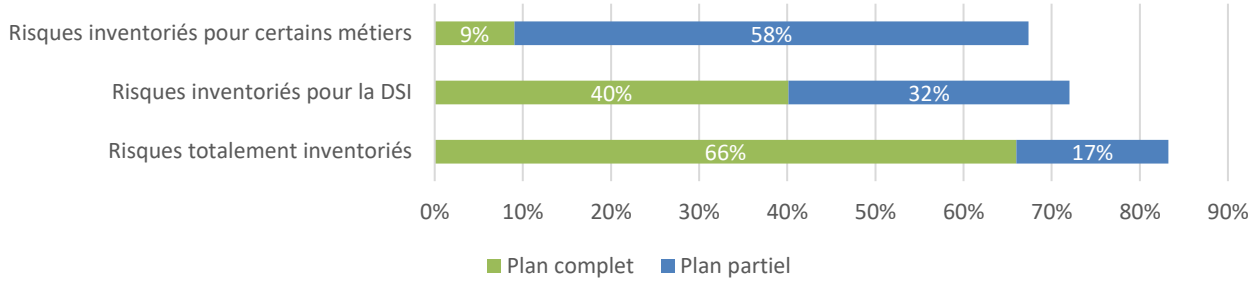


Figure 68 – Pourcentage d'établissements ayant établi un plan de réduction des risques

On notera enfin, que pour les établissements ayant effectué une analyse formelle de leurs risques, 90% d'entre eux ont établi un plan de réduction des risques.

Thème 9 : Contrôle d'accès

Il est constaté une nette augmentation de la mise en œuvre de modèles d'habilitation basés sur des rôles et profils, d'authentification forte par « calculette » à mot de passe non-rejouable, de SSO, de workflows d'approbation des habilitations et de provisionning. D'autres technologies comme les certificats électroniques logiciels et les Web SSO sont stables. A contrario, les certificats électroniques sur support matériel et la biométrie sont en baisse.

Ces résultats sont le témoin d'une volonté affirmée des structures de santé de suivre les exigences de sécurité (Hôpital Numérique, Certification des Comptes, PSSI-S, …) mais également d'adapter toujours plus finement les droits de chaque utilisateur à leurs missions. La diversité des technologies expérimentées, retenues ou rejetées, traduit également une volonté d'adapter les technologies aux usages des métiers, à la maturité des technologies et aux coûts budgétaires induits.

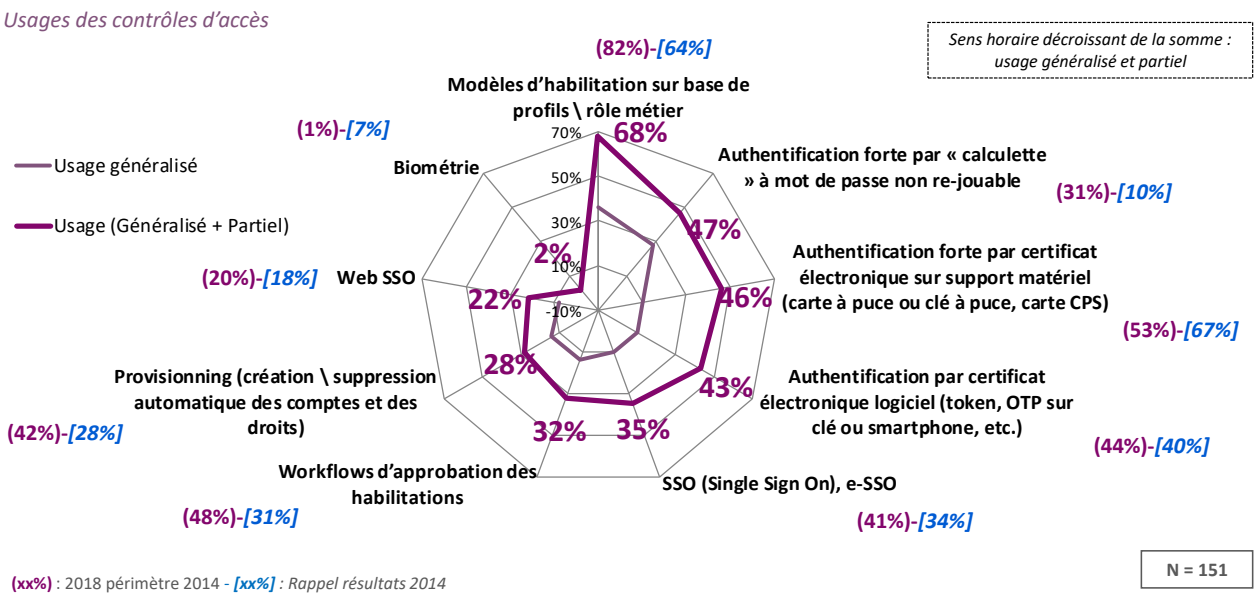


Figure 69 – Technologies / approches de sécurisation en matière de contrôle d'accès logique

L'utilisation de différentes technologies n'est pas homogène et varie selon la taille des structures de santé.

Il y a globalement une progression des procédures de gestion des comptes ce qui semble montrer une certaine cohérence avec le déploiement des technologies. En effet, le déploiement d'une politique de contrôle d'accès inclus à la Politique de Sécurité du SI ne se limite pas au déploiement des technologies mais nécessite la mise en œuvre de procédures formelles.

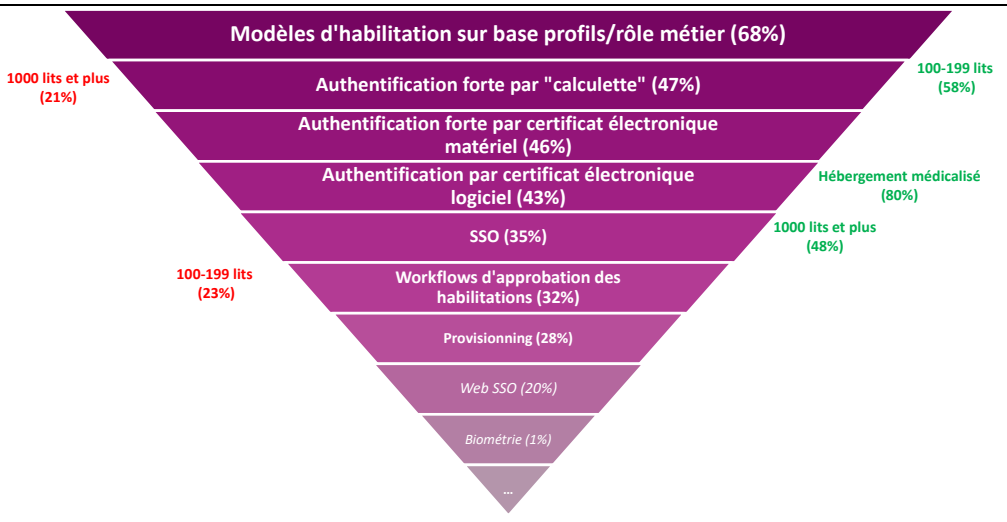


Figure 70 – Technologies / approches de sécurisation en matière de contrôle d'accès logique (détail par taille de structure)

Ainsi, 70% des structures de santé disposent d'une procédure formelle de gestion de comptes utilisateurs nominatifs et 79% d'entre elles disposent de procédures spécifiques pour les administrateurs. Enfin, 87% des structures de santé disposent de règles de constitution des mots de passe.

On peut supposer que cette évolution positive depuis 2014 (+10 points sur les règles de constitution des mots de passe et +12 points sur les procédures formelles des comptes administrateurs) soit liée à la mise en œuvre des bonnes pratiques largement préconisées par l'ANSSI, la CNIL, la CCI, le CLUSIF, etc. A contrario, on note une perte de 7 points pour les procédures formelles sur les comptes génériques ce qui pourrait être le reflet d'un travail avant tout porté sur les comptes à risque.

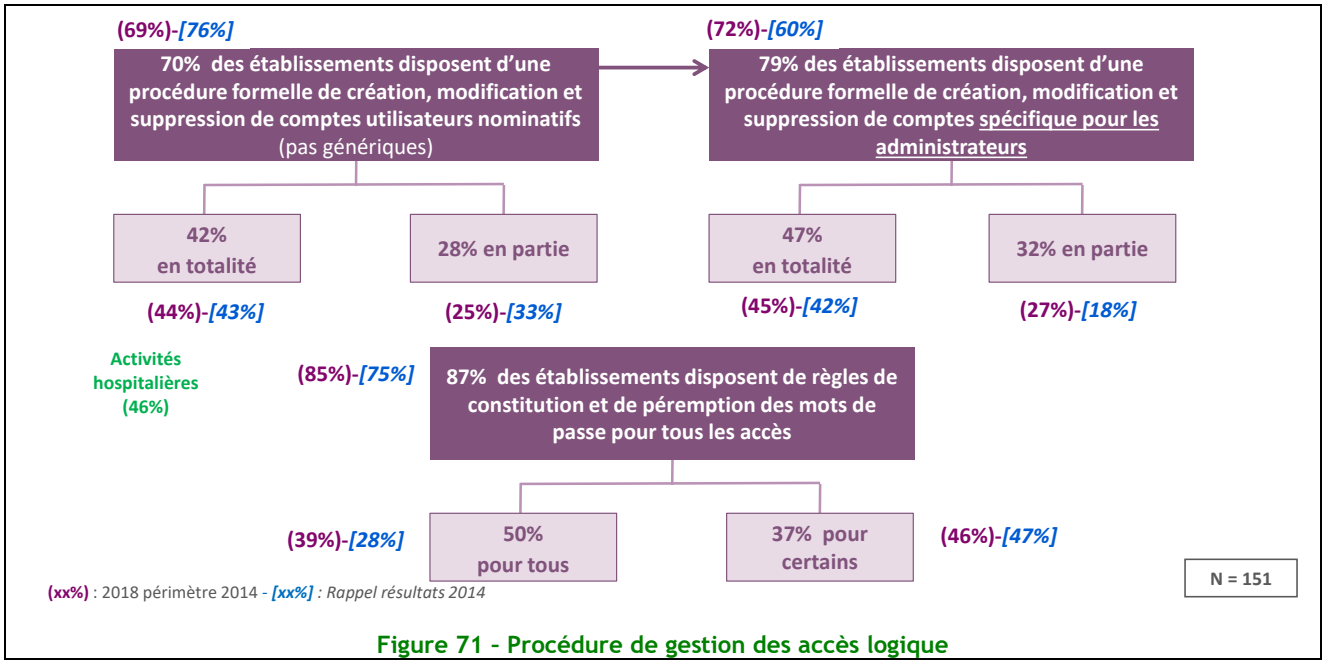


Figure 71 - Procédure de gestion des accès logique

Thème 10 – Cryptographie

Des outils cryptographiques très largement sous-exploités

La cryptographie est encore sous utilisée -40% en moyenne tous établissements confondus. Si ce chiffre est faible, il faut noter que le secteur de la santé a un taux d'appropriation de la cryptographie supérieur de 10 points à celui des entreprises.

Lorsqu'elle est utilisée, c'est très largement (à 71%) la DSI qui porte la responsabilité de la gestion des moyens cryptographiques (attribution, révocation, destruction des clés).

Les moyens de cryptographie mis en œuvre font l'objet d'un suivi formalisé (cycle de vie des certificats, clés, etc.) dans un peu moins d'une utilisation sur 2.

Avec l'arrivée du RGPD, le chiffrement des données et la gestion des clés associées (attribution, révocation, archivage et destruction) seront amenés à se développer.

Le chiffrement est en effet une des mesures qui sera fréquemment préconisée lors des études d'impacts sur la vie privée.

Thème 11 : Sécurité physique et environnementale

Les dossiers des patients sous format papier de plus en plus sous la responsabilité du corps médical

Bien que la transition numérique porte ses fruits avec des productions directes de documents dématérialisés, il n'empêche que le dossier papier est toujours présent : radios, analyses, comptes rendus pour ne citer qu'eux. Le dossier patient sur papier connaît au moins deux lieux de stockage : le service des soins et les archives, avec un va et vient souvent très important. Ceci explique sans doute les réponses à notre question. Ainsi, le dossier papier serait sous la responsabilité du corps médical lorsque le patient est présent et du management lorsque le dossier est archivé ou en transit. Nous notons une nette progression de la

responsabilité portée par le corps médical qui passe de 53% en 2014 à 78% en 2018. Quant au service informatique et pour 13% des établissements, il porterait probablement la responsabilité de sécuriser la disponibilité des outils qui permettent de retrouver facilement l'archive de ce dossier au format papier.

Qui est responsable de la sécurité physique du dossier patient sur papier ?

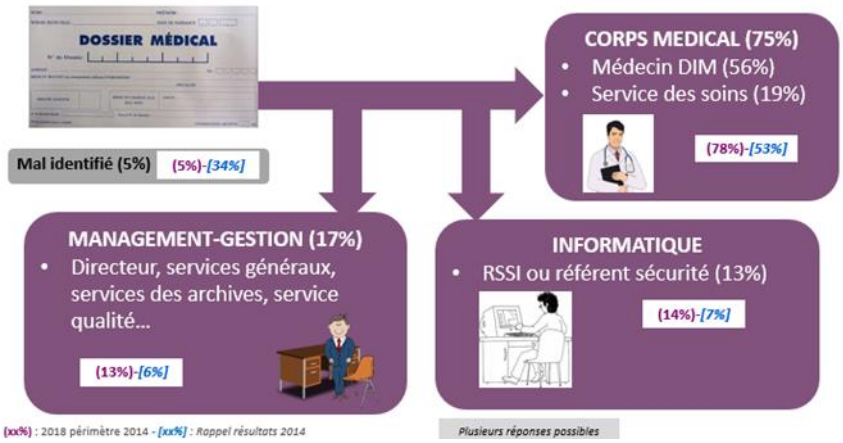


Figure 72 – Responsabilité de la sécurité physique du dossier patient

3 dispositifs majeurs de sécurisation physique des salles machine : caméra, détecteur incendie et contrôle d'accès par badge

Pour l'édition 2018, nous avons introduit une nouvelle question qui porte sur les dispositifs de sécurité physique. Pour 66% des établissements interrogés, la détection incendie arrive en tête probablement pour protéger les personnes, à moins que cette détection active un système d'extinction automatique pour éviter la destruction de la salle machine. Ce Chiffre devrait cependant s'approcher des 100% dans la mesure ou la détection incendie est une obligation.

29% des établissements possèdent quant à eux une détection inondation ; probablement ceux dont les salles machines se trouvent en sous-sol de l'établissement.

Dans ces environnements où beaucoup de visiteurs circulent librement dans les locaux, l'accès physique aux salles serait contrôlé dans 50% des cas par un badge d'accès et/ou une caméra de surveillance. Ainsi en cas de violation des locaux, des premiers éléments de preuve pourraient être exploités à la condition que les systèmes d'enregistrement soient correctement gérés.

Plus globalement, il y a beaucoup de passage dans les hôpitaux, avec des personnels souvent isolés ou en sous-effectif, avec des patients et accompagnants de plus en plus agressifs. La vidéosurveillance est une des réponses à ces situations à risque.

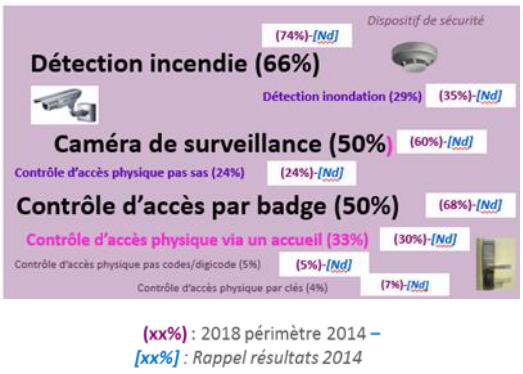


Figure 73 – Zones sécurisées et matériels

Thème 12 : Sécurité liée à l'exploitation

Sécurité liée à l'exploitation / logiciels malveillants

Un effort significatif a été réalisé entre 2014 et 2018 pour mettre en œuvre des sondes de détection. Si cette composante critique de la sécurisation du système d'information parait devoir être mieux prise en compte passant de 47% (2014) à 65% (2018) pour un IDS[8] et de 34% (2014) à 61% (2018) pour un IPS[9], l'enquête ne permet pas d'appréhender le type d'outils utilisés et de faire un bilan qualitatif d'implémentation. Le système de détection d'intrusion est en voie de devenir un composant critique d'une architecture de sécurité informatique, l'utilisation de produits ayant obtenu un visa de sécurité s'avère primordial.

Au vu des résultats de l'enquête, la prise en compte de la protection des mobiles devient une priorité des établissements de santé, prenant ainsi en compte la transformation des usages. De fait, le développement des outils de chiffrement sur ces supports de 4% (2014) à 12% (2018), le développement des pare-feux sur ce type d'outils de 11% (2014) à 31% (2018) et le développement d'antivirus sur ce type d'outil dans des proportions identiques sont à noter. Pour autant, en l'absence d'information à ce jour sur la mise en œuvre des bonnes pratiques de sécurité, notamment sur la gestion des pare-feux, de telles évolutions positives sont sans doute à nuancer.

Les outils de chiffrement sur les portables sont en progression de 18% (2014) à 36% (2018). Ce bon score peut laisser penser que les établissements ayant répondu à l'enquête sont soucieux des questions touchant à la protection des informations sensibles particulièrement du fait du nomadisme. Ceci est particulièrement important dans le domaine de la recherche médicale qui devrait être particulièrement concernée par cette mesure.

Par ailleurs, on constate un fort développement d'outils de plateforme extrahospitaliers, centrés sur le parcours patient, avec multiplicité d'acteurs en mobilité. Ces nouveaux usages nécessitent une sécurisation accrue des supports d'accès (smartphones, tablettes) à ces plateformes.

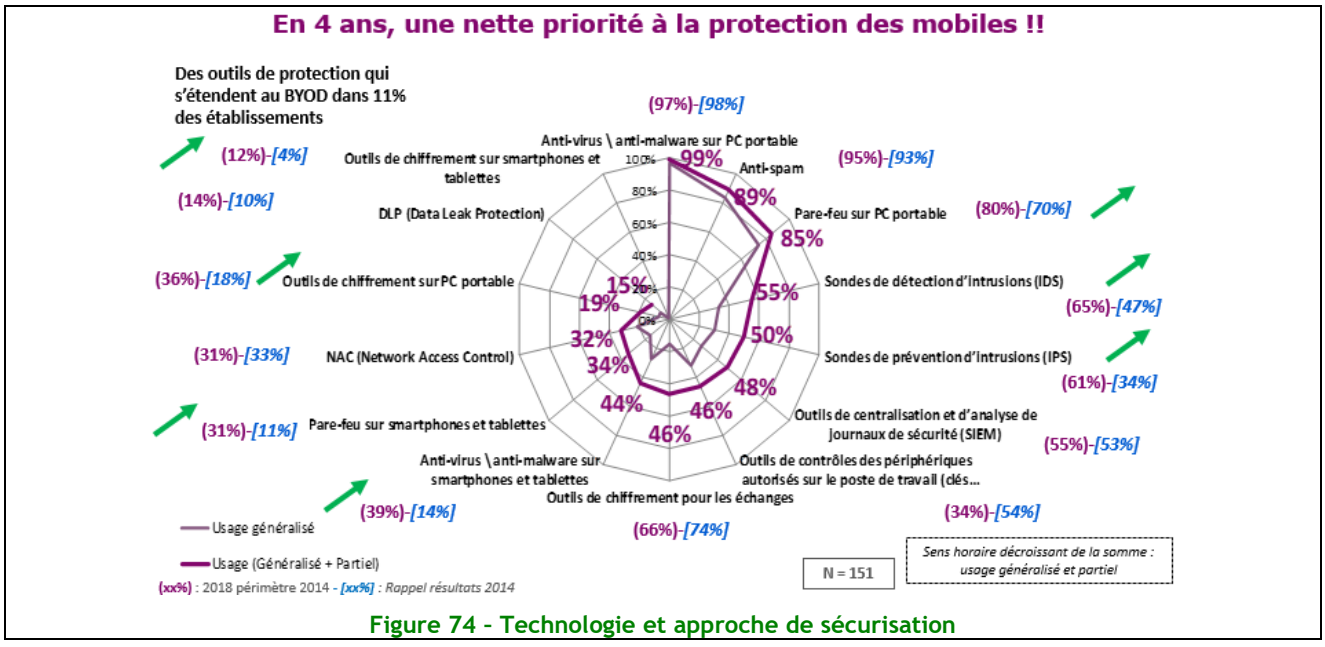


Figure 74 – Technologie et approche de sécurisation

L'inconnu reste deux questions non appréhendées à ce jour dans l'enquête quant à la mise en œuvre du patch management à l'échelle de l'ensemble de l'établissement (biomédical, technique, recherche) et intégrant le périmètre serveurs.

[8] IDS : Intrusion Detection System, mécanisme permettant de détecter un trafic malicieux et de lever une alarme.

[9] IPS : Intrusion Prevention System, mécanisme permettant de détecter un trafic malicieux et de le bloquer.

Sécurité liée à l'exploitation / vulnérabilités techniques

L'augmentation du nombre d'établissements de santé effectuant de la veille permanente en vulnérabilité est un point significatif qui montre la prise en compte des équipes techniques du risque lié au numérique et à la sensibilisation de ces mêmes équipes à la cybermenace. Cette évolution positive est à mettre en rapport avec le développement de sites spécialisés comme la cyber veille[10] et la meilleure connaissance des outils de veille mis en ligne par le CERT-FR[11].

Deux points méritent néanmoins d'être soulignés :

- La faiblesse de déploiement de correctifs de sécurité, même si le nombre d'établissement déclarant avoir une procédure formalisée passe de 43% en 2014 à 59% en 2018,
- L'absence de connaissance du périmètre concerné, notamment en ce qui concerne le biomédical et les services de maintenance et de travaux. À ce titre, il convient d'être particulièrement vigilant sur les vulnérabilités de ces composants numériques.

Plus largement, il faut relever l'importance de la mise en œuvre des mesures contenues dans des guides de bonnes pratiques (cf. Introduction) permettant de garantir la cohérence du parc, l'éventuelle qualification de correctif, l'isolement de composants obsolètes, etc.

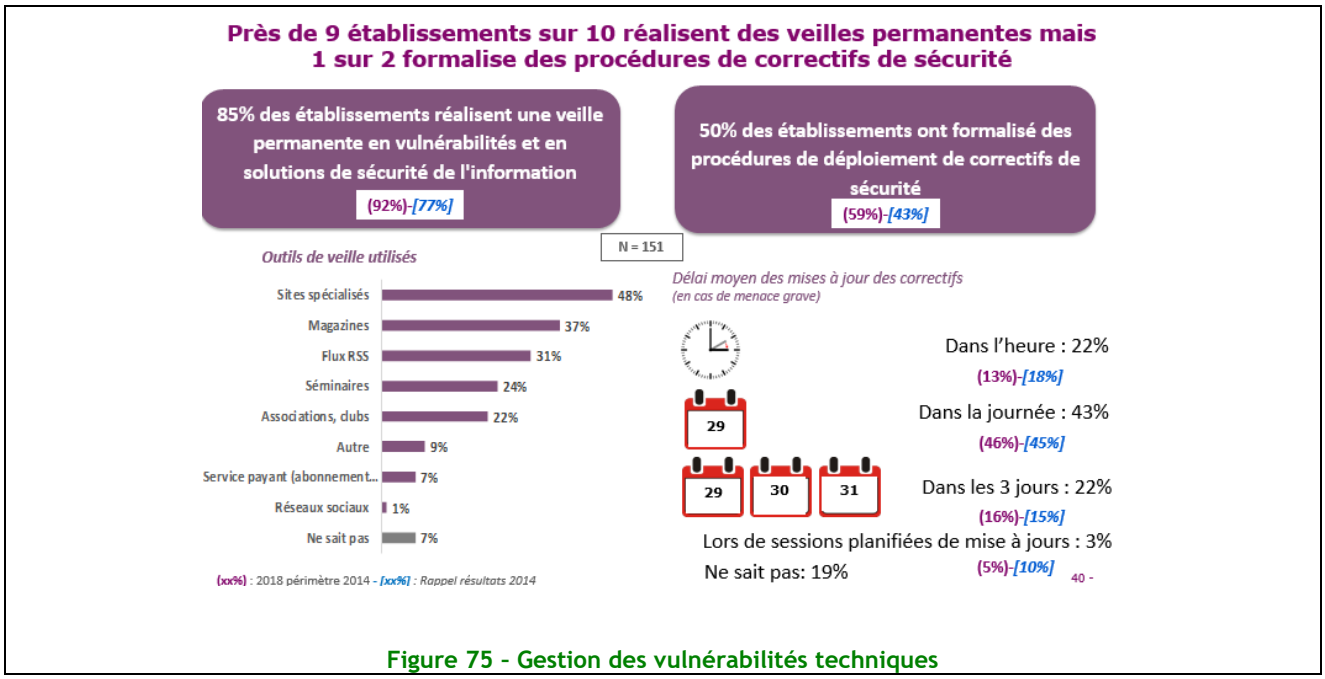


Figure 75 - Gestion des vulnérabilités techniques

[10] https://www.cyberveille-sante.gouv.fr/

[11] https://www.cert.ssi.gouv.fr/

Thème 13 : Sécurité des communications

Les évolutions à périmètre constant (2014)

Situation stable sur le BYOD et l'utilisation des réseaux sociaux

L'accès au SI via des terminaux personnels (BYOD) comme des smartphones ou des tablettes reste soumis à interdiction dans 77% des établissements.

L'utilisation des réseaux sociaux est également une constante, elle reste stable avec 41% d'interdiction en 2014 comme en 2018.

Légères variations

L'interdiction d'accès au SI via un réseau Wi-Fi privé au sein de l'établissement est en recul de 2 points (34% à 32%), l'interdiction de l'usage de tablettes et smartphones fournis par l'établissement en recul de 5 points (51% à 46%) et l'accès depuis l'extérieur à partir de PC non maîtrisés en recul de 6 points (59% à 53%).

Par ailleurs, on note une évolution dans l'utilisation des messageries externes, car l'interdiction de leur utilisation est en recul significatif de 14 points (70% à 56%) ce qui confirme une tendance déjà amorcée en 2010 (80% d'interdiction à l'époque).

Sur la VoIP, son interdiction est en augmentation de 8 points (34% à 42%).

Filtrage des accès web : le vrai durcissement

Comme l'indiquent les chiffres, la seule amélioration significative des pratiques de la sécurité au sein des établissements de santé est le filtrage des accès web. En effet, en 2014, 14% seulement des établissements de santé indiquaient mettre en place un filtrage systématique des accès internet. En 2018, sur le même périmètre, il y en a 75%.

Différences notables entre le périmètre 2014 et 2018

Il est également intéressant de comparer les résultats 2018 en fonction du périmètre étudié.

Pour rappel, le périmètre 2018 inclut, en plus du périmètre 2014, les établissements de 100 à 199 lits, et également des établissements d'hébergement médicalisé.

Ce que l'on peut remarquer, c'est que les restrictions sécurité sont majoritairement mieux implémentées sur le périmètre global que sur celui de 2014.

On constate ce phénomène sur les interdictions d'accès depuis l'extérieur à partir d'un poste de travail nomade fourni par l'établissement (23% contre 14%), l'interdiction de l'utilisation des réseaux sociaux (57% contre 41%) et l'interdiction d'accès depuis l'extérieur depuis un poste de travail non maîtrisé (68% contre 53%).

Seule exception significative : l'interdiction d'accès web sans filtrage est moins importante sur le périmètre global (66% contre 75%).

Ci-après les résultats compilés pour l'étude de 2018 sur les sujets abordés :

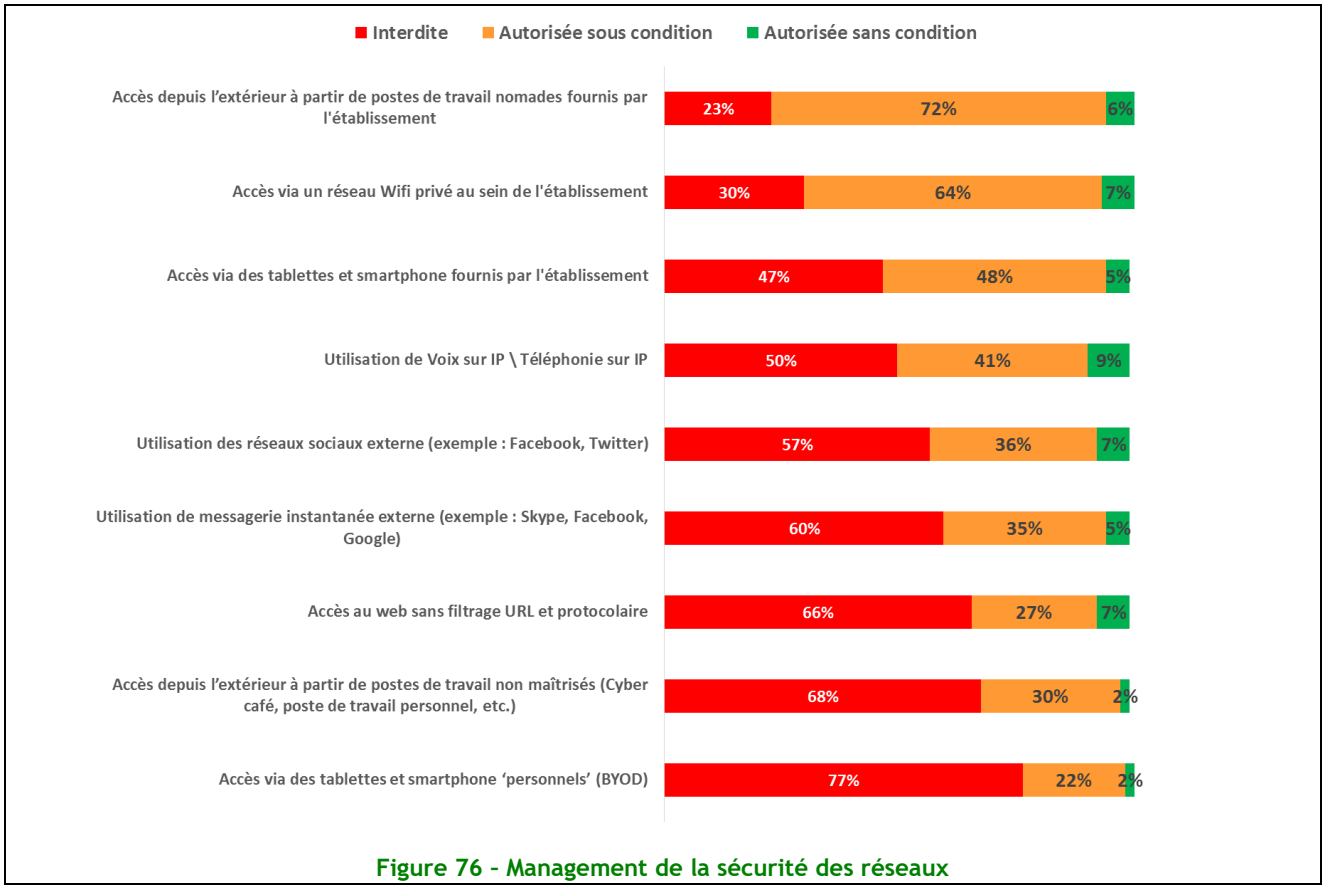


Figure 76 – Management de la sécurité des réseaux

Thème 14 : Acquisition, développement et maintenance du SI

Le développement sécurisé quasi-inexistant : moins de 2% des établissements ayant des pratiques de sécurité du développement en place

Nous pouvons nous demander si cela est dû à la forte place des progiciels ou matériels spécifiques ou si cela est parce que les métiers et directions privilégient la mise en œuvre très attendue des aspects fonctionnels et techniques dans leurs solutions, en oubliant la sécurité.

Nous ne pouvons que noter une faible évolution depuis une décennie sur ce sujet au sein des établissements de santé.

Parmi ces entreprises ayant mis en place un cycle sécurisé, la majorité ne colle pas à une méthode « commerciale » mais applique plutôt des bonnes pratiques pragmatiques.

Thème 15 : Relations avec les fournisseurs

Un recours significatif à l'externalisation auprès d'un hébergeur de données de santé

La question du recours à des spécialistes de l'hébergement de données de santé n'avait pas été encore directement adressée lors des études précédentes.

L'étude 2018 révèle que 42% des établissements interrogés ont aujourd'hui recours à un hébergeur de données de santé. Ce taux reste identique (41%) que l'on intègre ou non les établissements de 100 à 200 lits.

Il est à noter que 6% des établissements interrogés ont même fait le **choix de confier la totalité de leur Système d'Information à un hébergeur de données de santé**.

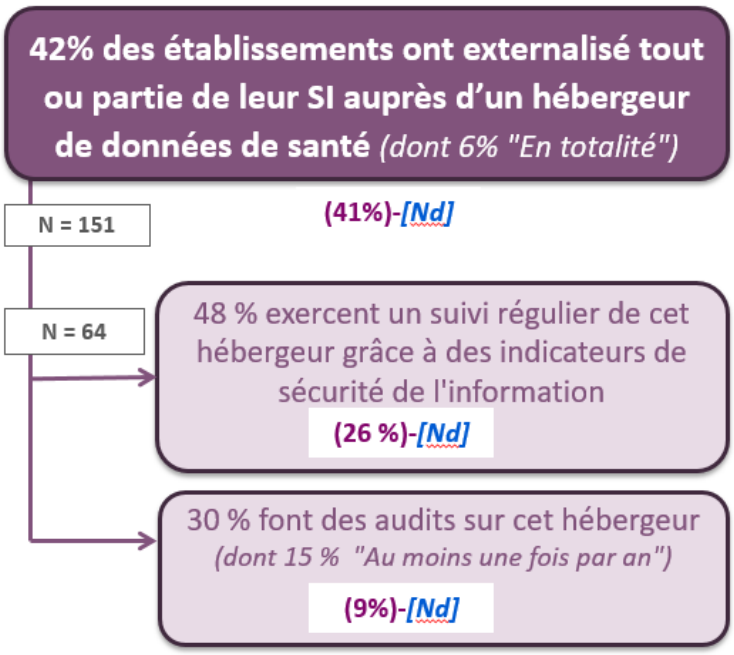


Figure 77 – Externalisation auprès d'un hébergeur de données de santé

Il apparaît que parmi les établissements qui ont franchi le pas de l'externalisation pour tout ou partie de leur système d'information, environ la moitié (48%) a le souci d'assurer un suivi régulier de leur hébergeur par des indicateurs de sécurité de l'information.

Au-delà de ce suivi « qualité », 30% des établissements ayant recours à l'externalisation assurent effectuer ou faire effectuer des audits de leur hébergeur de données de santé ponctuellement ou à intervalle régulier, et 15% au moins une fois par an, témoignant ainsi d'une vigilance des établissements sur les services externalisés et les conditions de mise en œuvre.

Précisons que l'activité d'hébergement de données de santé est soumise à agrément ou certification (Article L.1111-8 du Code de la Santé Publique). La procédure d'agrément précisée par le décret du 4 janvier 2006 a vu les premiers hébergeurs de données de santé agréés à partir de 2009. 120 hébergeurs sont agréés à ce jour (Liste consultable sur le site de l'ASIP Santé). En 2018, la procédure d'agrément évolue en procédure de certification, réalisée par un organisme certificateur accrédité, sur un référentiel de certification comportant notamment les exigences et contrôle de l'ISO 27001:2013.

On peut s'attendre à une progression de l'externalisation, avec la mise en œuvre des Schéma Directeur des Systèmes d'Information (SDSI) convergents de GHT (Groupement Hospitalier de Territoire). À confirmer lors de la prochaine étude MIPS.

Émergence des services en Cloud

L'utilisation du Cloud est présente dans 25% des établissements interrogés (dont 2% en cours). Considérant le périmètre d'établissements 2014, ce taux passe à 35% des établissements (dont 7% en cours), ce qui pourrait laisser entendre que l'usage de services cloud dans les établissements est plus développé dans les établissements de plus de 200 lits (à isopérimètre).

Quels sont les services en Cloud ? Quels usages (partage/échanges de documents, mails, prise de main à distance, IoT ? Comment les classifie-t-on ? Quels niveaux de maîtrise peut-on assurer ?

Toujours est-il que les établissements interrogés et ayant recours à des services en Cloud ont tous pu se prononcer sur le type de Cloud, avec une majorité en cloud dédié (Privé = 49%). Ces services en Cloud sont pour 74% des établissements réputés sous contrôle de la DSI /RSSI.

Toutefois, une part relativement faible des établissements a pu s'intéresser à la formalisation de ses règles internes « Cloud » expliquant ce qui est autorisé ou non : 10% a formalisé ou est en cours de formalisation d'une politique d'utilisation du Cloud ».

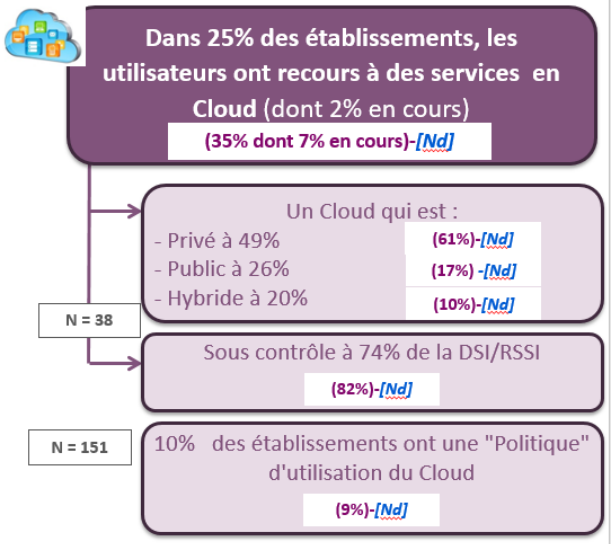


Figure 78 - Utilisation des services en Cloud

Thème 16 : Gestion des incidents

Existence d'une cellule de collecte et de traitement des incidents de sécurité

57% des établissements ont une cellule de collecte et de traitement des incidents (dédiée dans 17% des établissements, partagée avec d'autres fonctions dans 40% des établissements). Ce chiffre est en croissance régulière depuis 2010. On constate que la taille de l'établissement joue favorablement sur la mise en place de ce type de structure.

Les établissements semblent se donner les moyens de collecter les incidents de façon plus exhaustive, et d'être plus efficaces dans leur traitement.

	Analyse suivant périmètre 2014		
	2010	2014	2018
% des établissements dotés d'une cellule de gestion des incidents	33%	56%	76%

Types d'incidents de sécurité collectés par la cellule

La cellule collecte avant tout les incidents de sécurité liés à l'informatique de gestion (78% des répondants) et des services généraux (71%).

Cette cellule ne relève les incidents liés à l'informatique des dispositifs biomédicaux que chez un sondé sur 2. Il n'y a donc pas d'amélioration par rapport à 2010 ce qui doit être une **source de préoccupation et de vigilance forte** :

- Vu la difficulté à sécuriser ces dispositifs,
- Vu les difficultés « relationnelles », voire les incompatibilités, entre les services biomédicaux et les services informatiques.

La « convergence » Informatique et Biomédical devrait être une préoccupation majeure dans les SI hospitaliers. Ce pourrait être un sujet de travail pour les GHT.

Il n'y a pas d'évolution quant aux principales sources d'incidents, les chiffres variant peu de 2014 à 2018. Seuls les incidents liés aux processus sont en baisse significative. Ceci s'explique certainement par une meilleure analyse des incidents et une catégorisation plus précise.

Durée maximale des incidents (nouvelle question)

75% des incidents sont résolus en moins de 24h, et 16% entre 24h et 3 jours.

Dépôt de plaintes à la suite d'incidents liés à la sécurité de l'information

Alors que les incidents de sécurité du SI sont en croissance dans les hôpitaux, le nombre de dépôts de plainte, bien que multiplié par 3 depuis 2014 (de 4% en 2010 à 11% en 2018), reste faible en valeur absolue.

Le dépôt de plainte est une démarche indispensable si l'établissement estime être victime d'une infraction. Cette démarche est alors importante en cas de responsabilité potentielle de l'établissement, selon les conséquences de l'infraction. Également, par rapport à une couverture assurantielle, sur le périmètre du Système d'Information, la plainte est indispensable pour l'instruction de l'affaire.

Le faible taux des dépôts de plainte traduit certainement un manque de sensibilisation des établissements, voire une méconnaissance de la législation. **C'est un axe important de progrès pour les acteurs de la sécurité des SI.**

Déclaration des incidents sur la plateforme « Portail de signalement des évènements sanitaires indésirables » (nouvelle question)

Le décret du 12-09-2016 prévoit le signalement sans délai des incidents graves de sécurité des systèmes d'information. Peuvent être considérés comme graves :

- Les incidents ayant des conséquences potentielles ou avérées sur la sécurité des soins,
- Les incidents ayant des conséquences sur la confidentialité ou l'intégrité des données de santé,
- Les incidents portant atteinte au fonctionnement normal de l'établissement, de l'organisme ou du service.

Moins d'un incident sur cinq (18%) est déclaré sur cette plateforme. Cependant ce chiffre grimpe à 30% sur le périmètre 2014 (hôpitaux de plus de 200 lits) : 1 incident sur 3 dans ce type de structure est donc un incident grave, ce qui peut paraitre important.

Les gros établissements déclarent beaucoup plus que les petits. Il n'est cependant pas possible de pousser plus loin notre analyse :

- Les petits établissements ont-ils moins d'incidents graves ?,
- Les petits établissements déclarent-ils moins car méconnaissent-ils cette nouvelle législation ?,
- Y a-t-il une crainte de communiquer sur « ses problèmes » ?

Hiérarchie des incidents recensés

L'analyse 2018 tous types d'établissements confondus fait ressortir 2 types d'incidents principaux :

- 33% des établissements ont été confrontés à une « infection par virus »,
- 29% des établissements déclarent des « pannes d'origine interne ».

Afin de pouvoir comparer l'évolution des incidents recensés, l'analyse qui suit est réalisée sur le périmètre 2014.
Tout comme en 2014, nous pouvons observer un recul global de la sinistralité. Les différentes mesures prises par les DSI ont un impact concret sur la survenue des incidents ou tout du moins sur leur connaissance et leur traitement.

Les problèmes d'indisponibilité à la suite de pannes d'origine interne se maintiennent en première position depuis 2010. Ce chiffre est assez étonnant étant donné la fiabilité des architectures virtualisées, et du développement de PCA. Peut-être faut-il investiguer du côté des indisponibilités induites par une mauvaise gestion des changements (matériels, logiciels ou organisationnels) : processus de Gestion des changements.

Après une baisse en 2014, plus de 42% des établissements déclarent des infections par virus.

Les différentes autres « attaques informatiques » (fraude informatique, sabotage physique, attaque logique ciblée, divulgations, actes de chantage ou d'extorsion) ont été repérées dans moins d'un établissement sur 10.

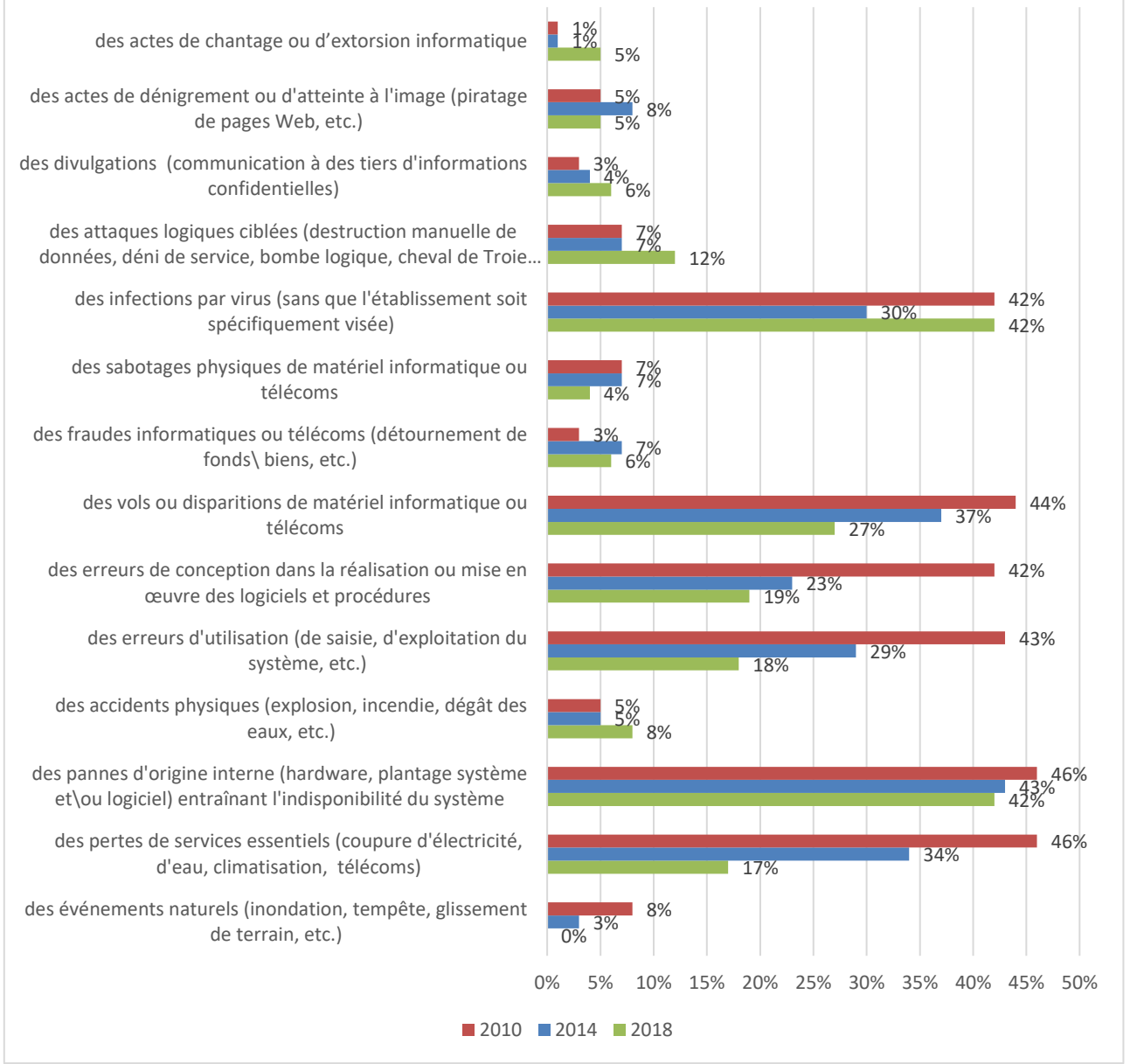


Figure 79 - Comparatif des incidents (2010 - 2014 - 2018)

Les politiques de sécurisation des accès aux locaux et aux équipements, se traduisent par une forte diminution des vols avec 27% d'établissements concernés en 2018 contre 37% en 2014 et 44% en 2010.

Les « Erreurs de conception dans la réalisation ou mise en œuvre des logiciels et procédures » tout comme « les erreurs d'utilisation » sont en diminution régulière, ce qui traduit une meilleure maitrise des outils et des processus SI.

Il est aussi positif de noter que la « perte de services essentiels » est en diminution forte à 17% (34% en 2014 et 46% en 2010). Ceci traduit un effort continu de fiabilisation de ces services.

Le recul global de la sinistralité constaté ci-dessus se constate aussi à travers le nombre moyen des incidents par catégorie qui est en forte de baisse de l'ordre de 2 à 3 fois moins d'incidents qu'en 2014.

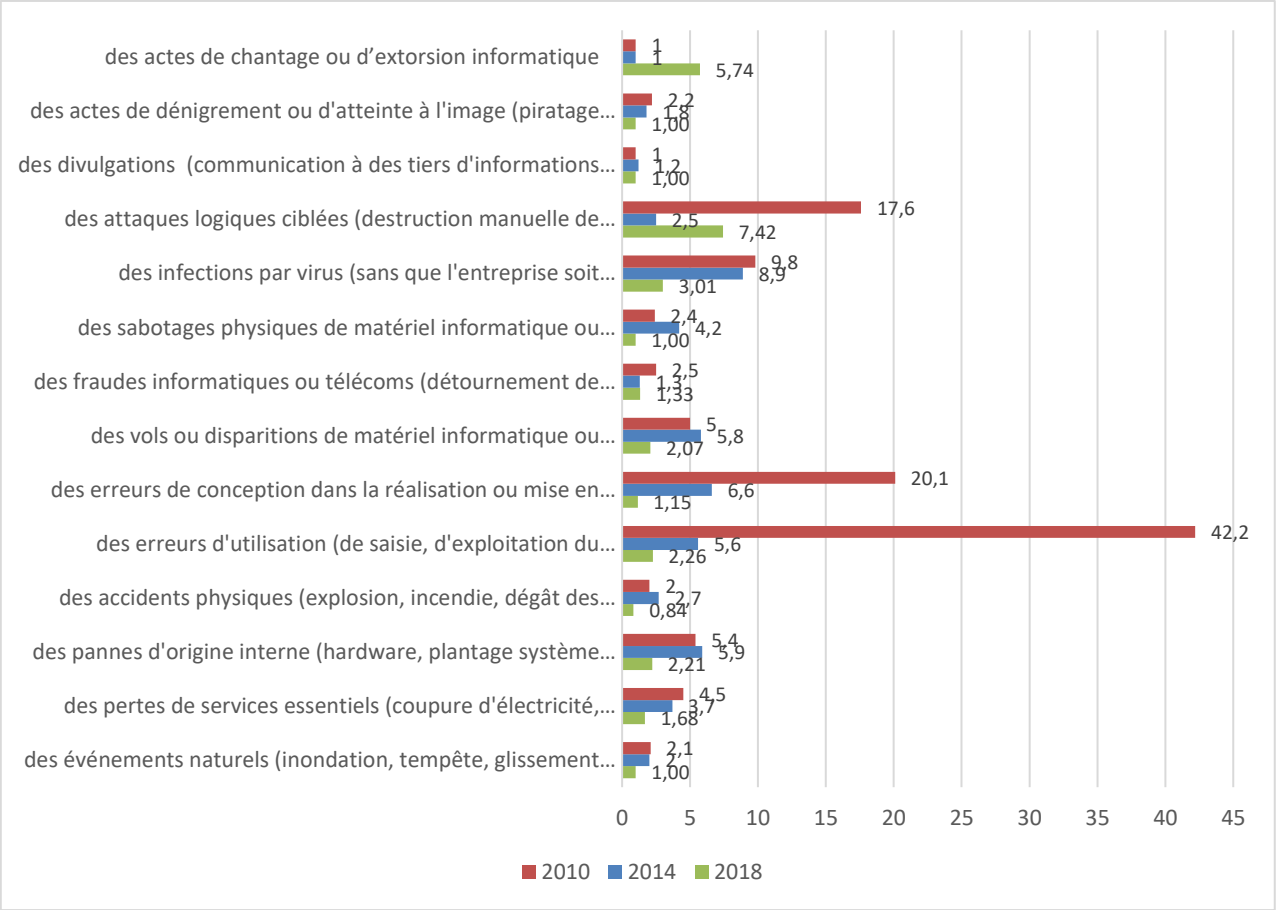


Figure 80 - Nombre moyen d'incidents

Confrontation avec les sujets du Panorama de la Cybercriminalité du CLUSIF

Pour 23% des établissements, le Phishing est le sujet majeur auxquels ils sont confrontés. Si l'on revient sur le périmètre de l'enquête 2014, ce chiffre est encore plus significatif puisque 40% des établissements en font alors leur sujet majeur.

Cependant, les impacts constatés sont très faibles.

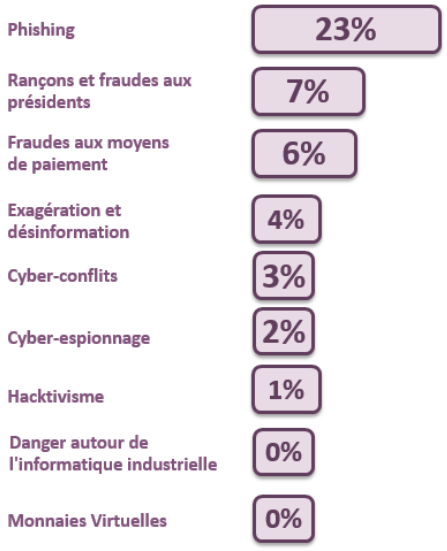


Figure 81 - Confrontation aux sujets du #Panocrim

Impact financier des incidents

Dans la lignée de 2014, peu d'établissements (un peu plus d'un tiers) font une analyse de l'impact financier des incidents survenus sur le Système d'Information.
Il est aussi remarquable de constater, qu'il n'y a pas encore une véritable prise en compte de la valeur des données, puisque moins d'un quart des établissements ont conduit une démarche d'analyse de la valeur des informations potentiellement perdues, altérées ou volées à travers la souscription d'une police d'assurance.
D'autre part, dans 57% des cas, les interlocuteurs ne savent pas comment l'impact des incidents a été financé.

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

L'indisponibilité d'un fournisseur essentiel : le parent pauvre de la gestion de la continuité d'activité

Comme l'indique la figure ci-dessous, seules 19% des établissements de santé prennent en compte l'indisponibilité d'un fournisseur essentiel. Pourtant la gestion de la continuité d'activité implique de prendre en compte ce scénario de défaillance dans la poursuite des activités en cas de crise. En effet, la continuité de service des opérateurs télécoms, des fournisseurs d'énergie (ou autres utilités) est essentielle à la continuité d'activité et une attention particulière doit être portée à ces partenaires.

Il faut aussi noter que prêt d'un établissement sur cinq n'a mis en place aucun processus.

Figure 82 - Couverture de la gestion de la continuité d'activité

L'équipement des salles de crise : Peut mieux faire !

Même si plus de la moitié des établissements de santé ont mis en œuvre une cellule de crise, seuls 27% ont équipé leur salle de gestion de crise. Or, la possibilité de connecter des équipements informatiques au réseau interne et externe tout comme la gestion de la téléphonie fixe sont les dispositifs essentiels au bon fonctionnement d'une cellule de crise.

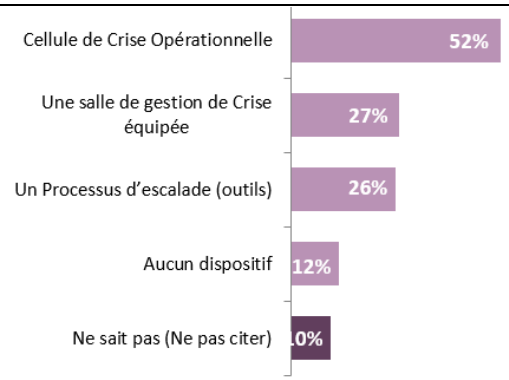


Figure 83 - Composition de la gestion de crise

Thème 18 - Conformité

Une conformité à consolider : les exigences du PHN, un vrai moteur du changement

67% des établissements sont soumis à des lois et/ou des règlements spécifiques en matière de sécurité de l'information. La politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales (PSSI-MCAS) est très majoritairement mise en avant.

Un peu plus de 8 établissements sur 10 affirment être, ou en cours, de conformité aux prérequis sécurités du Programme Hôpital Numérique instauré à partir de 2012. C'est 3 fois plus qu'il y a 4 ans. Plus l'établissement est grand, moins il est enclin à affirmer sa conformité (+/- 5 points autour de la moyenne).

À moins de 6 mois de l'échéance (les établissements ont été sondés début 2018), moins d'un établissement sur 5 se dit totalement prêt pour le Règlement Général sur la Protection des Données. Pour deux établissements sur 5, le travail de conformité est toutefois engagé. Ce chiffre cache une forte disparité entre les petites unités (de 100 à 200 lits) qui ne sont que 46% à être totalement ou partiellement conformes lorsque ce chiffre est de 68% pour les établissements de 1000 lits et plus.

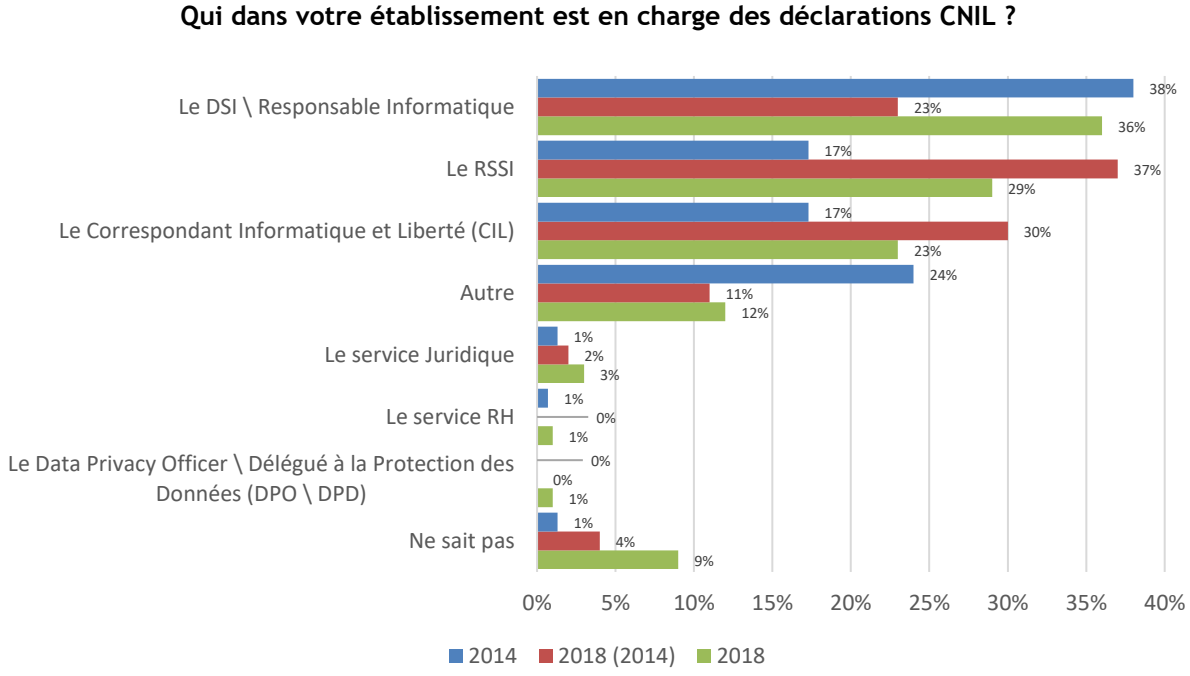


Figure 84 - Répartition de la charge des déclarations à la CNIL

La marche à franchir reste haute. À peine un établissement sur 4 a désigné un Correspondant Informatique et Libertés. Le sujet de la conformité Informatique et libertés, quand il est pris en compte, est plutôt considéré comme un sujet technique du système d'information. Les pratiques devront évoluer. Il sera délicat pour le DSI, ou le RSSI sous l'autorité de ce dernier, d'assurer le rôle de Délégué à la protection des données, dont la désignation est rendue indispensable par le RGPD dans une grande majorité des cas. Ce dernier doit pouvoir travailler sans recevoir aucune instruction en ce qui concerne l'exercice de ses missions. De même, le responsable de traitement doit veiller à ce que, le cas échéant, les autres missions et tâches du DPO n'entrainent pas de conflit d'intérêt.

Tableaux de bord : Une maturité qui progresse. Les efforts SSI peinent à être mesurés

Si oui, quels sont les types d'indicateurs que vous suivez dans ce tableau de bord ? (plusieurs réponses possibles)

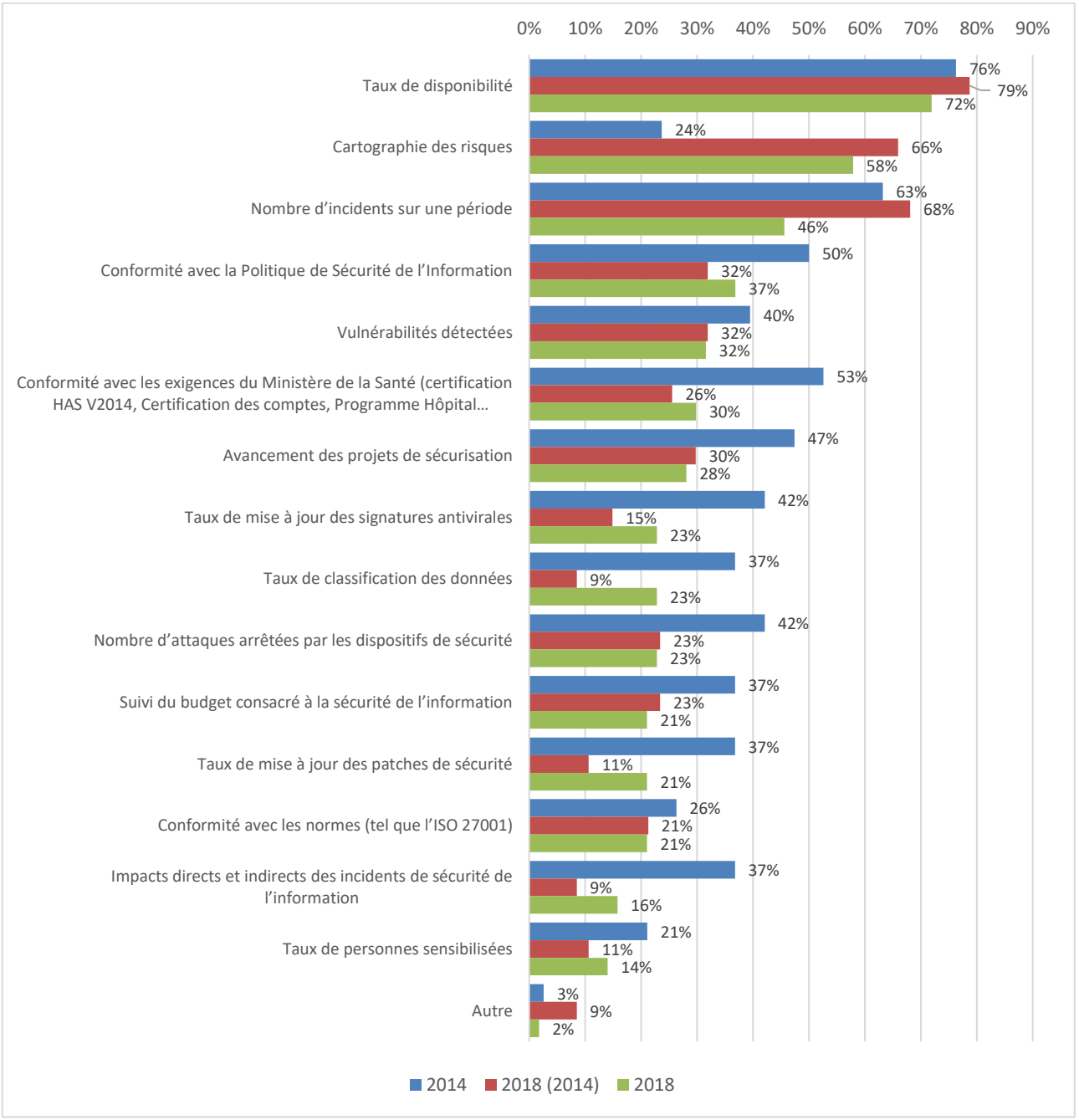


Figure 85 - Types d'indicateurs de tableaux de bord de la sécurité de l'information

À périmètre constant, la mise en œuvre de tableaux de bord SSI progresse fortement passant de 25% à 43% des répondants. Sur le périmètre 2018, un peu moins de 40% des établissements déclare avoir mis en place des indicateurs et/ou un tableau de bord de la sécurité de l'information. Les établissements de plus de 1000 lits sont notablement bien au-dessus de cette moyenne (+20 points).

Pour les établissements les ayant mis en place, les cibles de ces tableaux de bord restent stables dans le temps. Ils sont avant tout un outil de suivi opérationnel de la SSI pour 73% des établissements. Les tableaux de bord ou indicateurs sont exploités pour piloter la fonction SSI dans 38% des établissements. Ils ont du mal à atteindre les directions générales et les comités de direction. Les tableaux de bord ou indicateurs stratégique sont annoncés par 17% des établissements, en recul de 6 points en 4 ans.

Les indicateurs sont d'ordre technique (taux de disponibilité, etc.). Bien que seulement 11% des établissements déclarent s'appuyer sur le management des risques pour piloter la sécurité de l'information (cf. thème 5), la cartographie des risques pointe en deuxième position des indicateurs les plus cités. Ainsi, tel monsieur Jourdain, les RSSI managent les risques sans le savoir, poussés en cela par les règlements et les normes. Signe supplémentaire que le programme Hôpital Numérique est un facteur clé de la SSI dans le secteur.

Une démarche d'amélioration continue qui se renforce d'année en année

Près de 7 établissements sur 10 déclarent mener en moyenne de 1 à 5 audits par an. C'est 30% de plus que lors de la dernière étude. Le taux passe à 9 établissements sur 10 dans la catégorie 1000 lits et plus.

Ces audits sont principalement techniques. Les audits techniques intrusifs sont deux fois plus nombreux qu'en 2014, preuve que l'ouverture des systèmes d'information est une préoccupation des établissements de santé. Les audits de code ne sont cités que par 13% des établissements, en corrélation avec les très faibles résultats du thème 14.

Quels types d'audit ou de contrôles de sécurité du système d'information sont menés au sein de votre établissement ?

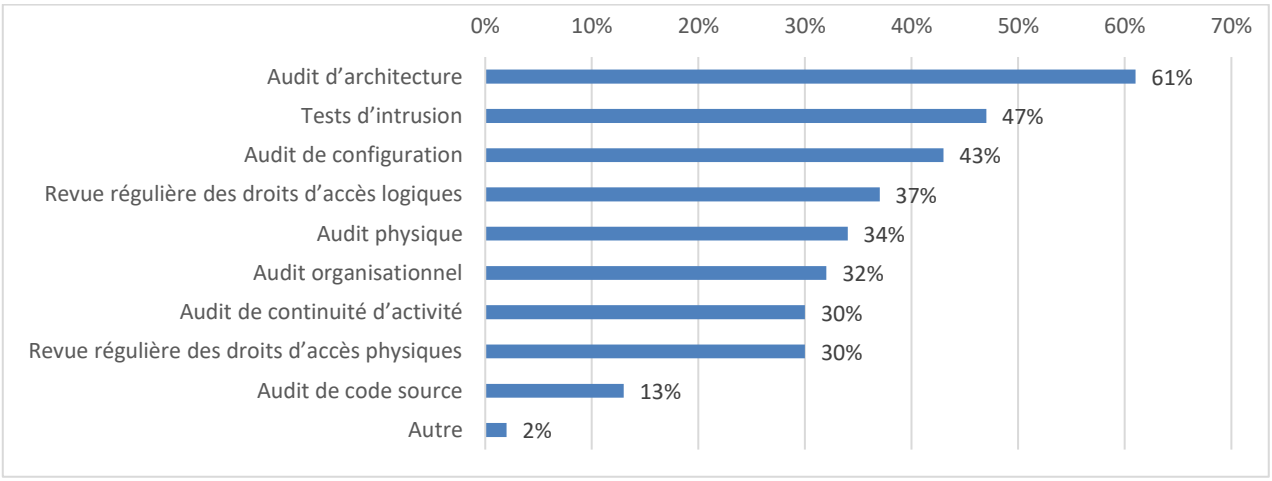


Figure 86 - Typologie d'audit ou de contrôles de sécurité du système d'information

La motivation à lancer un audit se positionne sur les objectifs de conformité aux exigences contractuelles ou réglementaire externes et au respect de la PSSI interne. Il s'agit donc bien d'une démarche proactive. Les audits déclenchés à la suite d'incident restent secondaires. Les tiers externes apparaissent moins intrusifs qu'en 2014. Ces derniers considèrent que les démarches de conformité, volontaires ou contraintes, sont gages de bonnes pratiques.

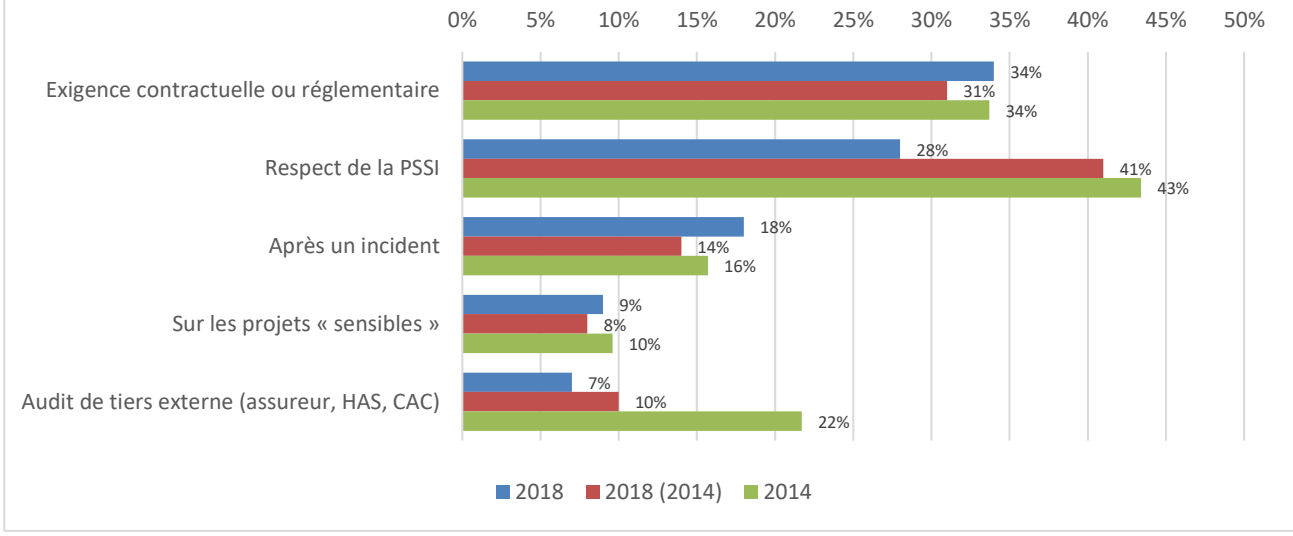


Figure 87 - Motivations déclenchant les audits de sécurité

Les particuliers Internautes

- Présentation de l'échantillon
- Partie I : Identification et inventaire ordinateur et smartphone
- Partie II : Usages des internautes
- Partie III : Perception de la menace et sensibilité de l'utilisateur aux risques et à la sécurité de l'information
- Moyens et comportements de sécurité

Les particuliers internautes

Présentation de l'échantillon

L'objectif, cette année encore, a été de pouvoir suivre les évolutions des usages des internautes ainsi que leur perception et sensibilité aux menaces et leurs comportements de sécurité depuis les précédentes études. L'échantillon de cette nouvelle étude est donc très proche des éditions passées, avec un panel de 1006 internautes de plus de 15 ans interrogés.

On retrouve ainsi :

- 52% de femmes et 48% d'hommes,
- 45% ont moins de 45 ans et 31% ont plus de 60 ans,
- 51% d'actifs et 49% d'inactifs (étudiants, sans emploi et retraités),
- 35% ont des enfants à la maison (en couple ou parents isolés).

Cet échantillon a fait l'objet, comme il est d'usage, d'un redressement sur les données statistiques nationales comme par exemple : le sexe, l'âge, le lieu d'habitation, …

Partie I – Identification et inventaire ordinateur et smartphone

Une égalité parfaite entre les smartphones/ordinateurs portables d'un côté et les tablettes/ordinateurs fixes de l'autre

En 2018, le smartphone confirme encore sa progression pour la consultation d'Internet puisque pour la première année il arrive au niveau de l'ordinateur portable, pour certainement le dépasser dans les années à venir. Les internautes français augmentent également leur nombre d'équipements de ce type de terminaux qui passe à une moyenne de 1,19 par foyer (1,04 en 2016).

Un taux d'usage des équipements connectés qui progresse … sauf pour les ordinateurs fixes

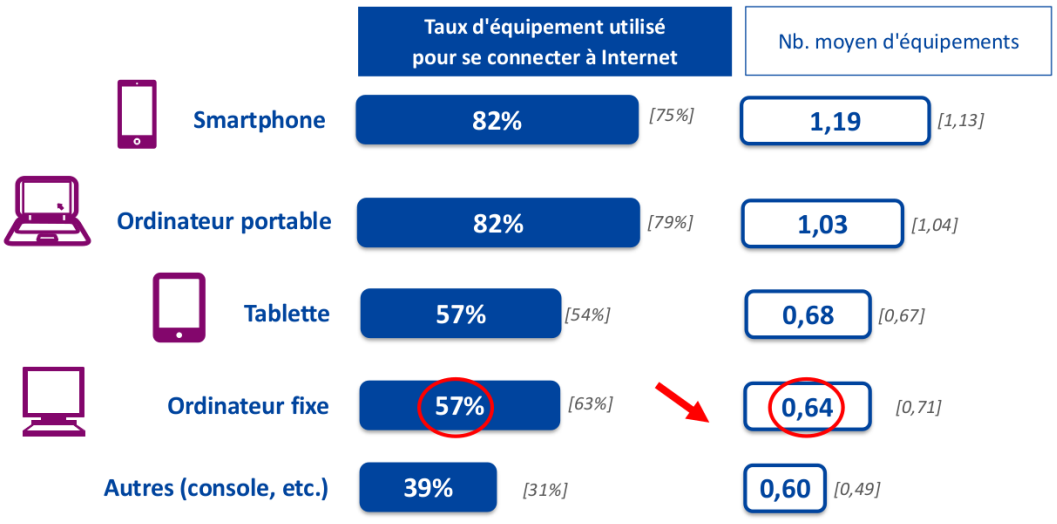


Figure 88 - Équipements des internautes

De la même manière, la tablette arrive pour la première année exactement au même niveau que l'ordinateur portable par une légère augmentation de son usage (57% des internautes en utilisent en 2018, contre 54% en 2016) mais surtout par une baisse significative de l'utilisation des ordinateurs fixes : -6 points.

Les ordinateurs sont d'ailleurs le seul type d'équipement qui voit une baisse d'utilisation pour se connecter à Internet.

Des internautes toujours plus connectés en mobilité

Dans la continuité des années précédentes, les internautes utilisent de plus en plus hors de leur domicile leurs équipements mobiles afin de se connecter à Internet. Il y avait 13% d'utilisateurs toujours connectés en 2012, et le double en 2018, soit 26%. À l'opposé, 33% des Français en mobilité coupaient les connexions données en 2012. Ils ne sont plus que 16%.

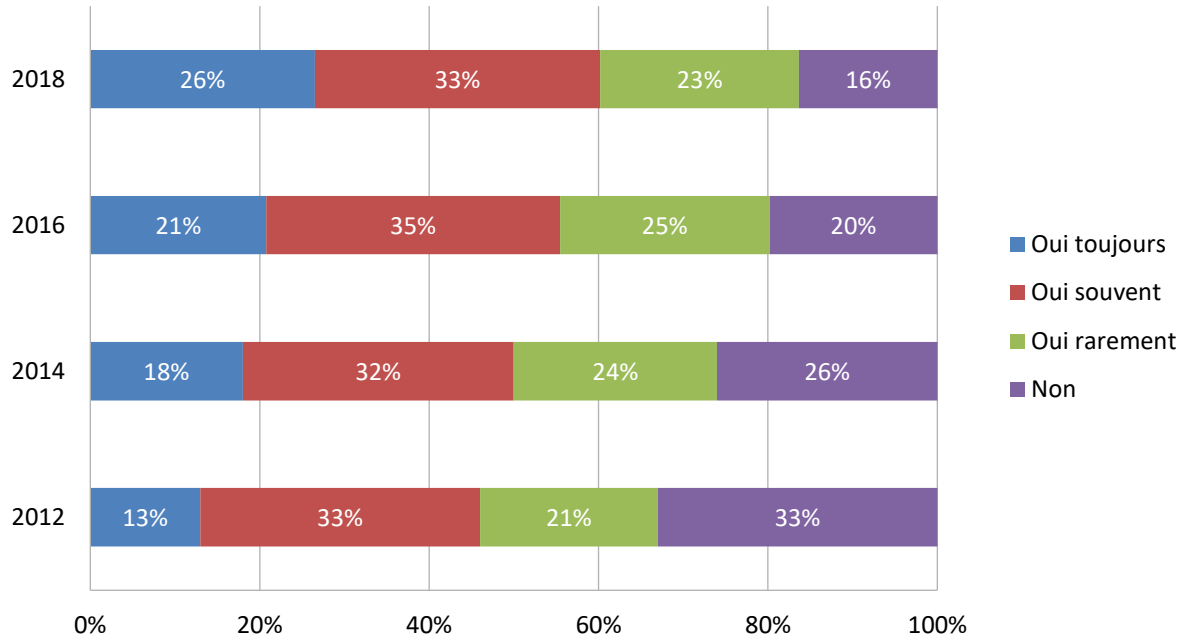


Figure 89 - Taux de connexion permanente à Internet sur les terminaux mobiles

L'étude démontre par ailleurs que 51% des 15-29 ans et 35% des 30-44 ans sont toujours connectés en mobilité, permettant de confirmer que la tendance devrait se poursuivre dans les prochaines années.

Des montres et des consoles de jeux plus connectés

Si la part des objets de la vie courante réellement connectés augmente peu (2,1 objets connectés par foyer en moyenne en 2018 contre 2,0 en 2016), les internautes s'équipent de plus en plus de montres connectées (16% des internautes disposent d'une montre connectée en 2018 contre 10% en 2016) et permettent à leurs consoles de jeux d'accéder à Internet (35% des consoles de jeux sont connectées en 2018 contre 32% en 2016). Au-delà de ces évolutions, aucun objet connecté n'est concerné par la révolution annoncée.

Partie II - Usages de l'internaute

Le Wi-Fi à domicile continue à avoir un réel succès

En 2018 les internautes sont 89% à opter pour la connexion à l'Internet via Wi-Fi depuis leur domicile.

Cette nouvelle progression de 4 points par rapport à 2016 et récurrente depuis 2012 peut s'expliquer par la démocratisation de ce mode d'accès embarqué dans les équipements connectés, notamment pour ceux dont le seul moyen d'accès au réseau est le Wi-Fi et qui sont en constante progression voire également de la suppression progressive des ports réseaux physiques pour cause de miniaturisation sur les équipements connectés plus historiques ou encore du fait des évolutions de la technologie autorisant des débits toujours plus élevés rendant son usage confortable.

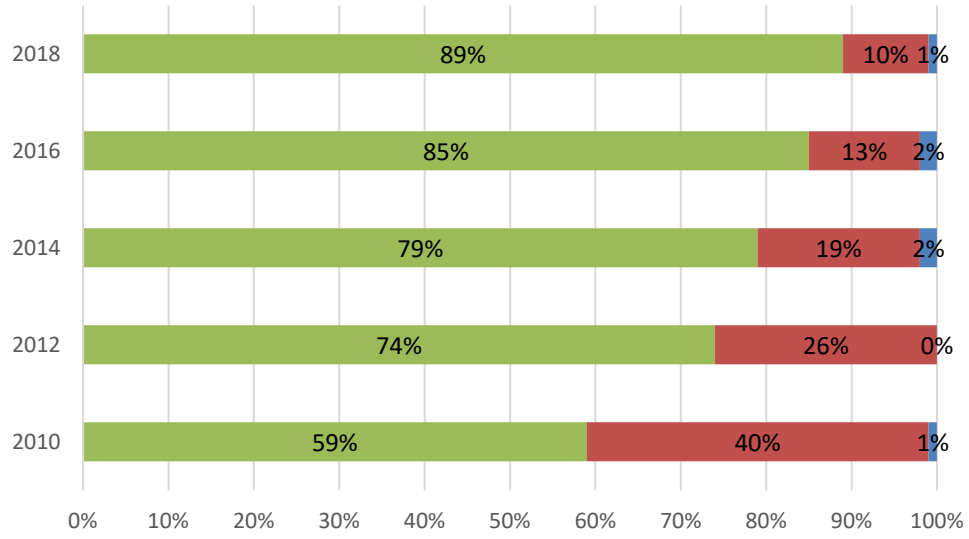


Figure 90 - Connexion Wi-Fi (sans fil)

Pour les réfractaires à ce mode de connexion, la raison avancée de craintes pour la sécurité de l'information fait un bon de 7 points par rapport à 2016.

Cloisonnement des sphères personnelles et professionnelles, des comportements variés…

La baisse entamée en 2016 de l'utilisation d'équipements personnels pour des activités professionnelles se poursuit en 2018 au même rythme de -4 points pour atteindre 36% en moyenne. Un CSP+ sur deux continue cependant à adopter ce comportement comme en 2016. Les jeunes de 15 à 29 ans et les franciliens stagnent également à des valeurs bien au-dessus de la moyenne de 55% et 47% respectivement.

Cependant, les personnes indiquant se connecter « Très Souvent » et « Souvent » à distance au réseau de leur entreprise depuis leur domicile avec leur accès Internet personnel reste élevé et à peu près constant (+1 point par rapport à 2016 pour arriver à 41%) et augmente même de 3 points si on inclut les personnes ayant répondu « parfois » passant ainsi de 62 à 65% en moyenne. Les franciliens sont les plus nombreux à faire appel à ce type de service, 71% d'entre eux indiquant se connecter Très Souvent, Souvent ou Parfois au réseau de leur entreprise. Ceci peut s'expliquer car l'Ile de France est le bassin d'emploi où se concentre une grosse proportion d'activités tertiaires.

L'utilisation d'équipements professionnels pour une activité personnelle reste par contre constante entre 2018 et 2016, que ce soit en moyenne (36%) ou chez les CSP+ (47%), les 15/29 ans (48%) et les franciliens (48%) qui sont au-dessus de la moyenne.

Des Usages d'Internet matures, même pour les plus récents d'entre eux

En 2018 les usages faits de l'Internet ne connaissent pas de profonds bouleversements comparativement à 2016 ou aux années précédentes.

Il est à noter que les utilisations à caractères purement récréatifs (navigation web, visionnage de vidéos et écoute de musique en ligne, téléchargement, …) connaissent un certain recul (de 96% en 2016 à 84% en 2018) quand les usages relevant d'un côté pratique (démarches administratives, opérations bancaires, stockage en ligne et services en lignes communautaires) passent de 61% à 63%. Ceci démontre une certaine évolution de la société française qui utilise de manière croissante de vrais services en ligne pour les démarches de la vie du quotidien, au-delà des simples aspects de divertissement.

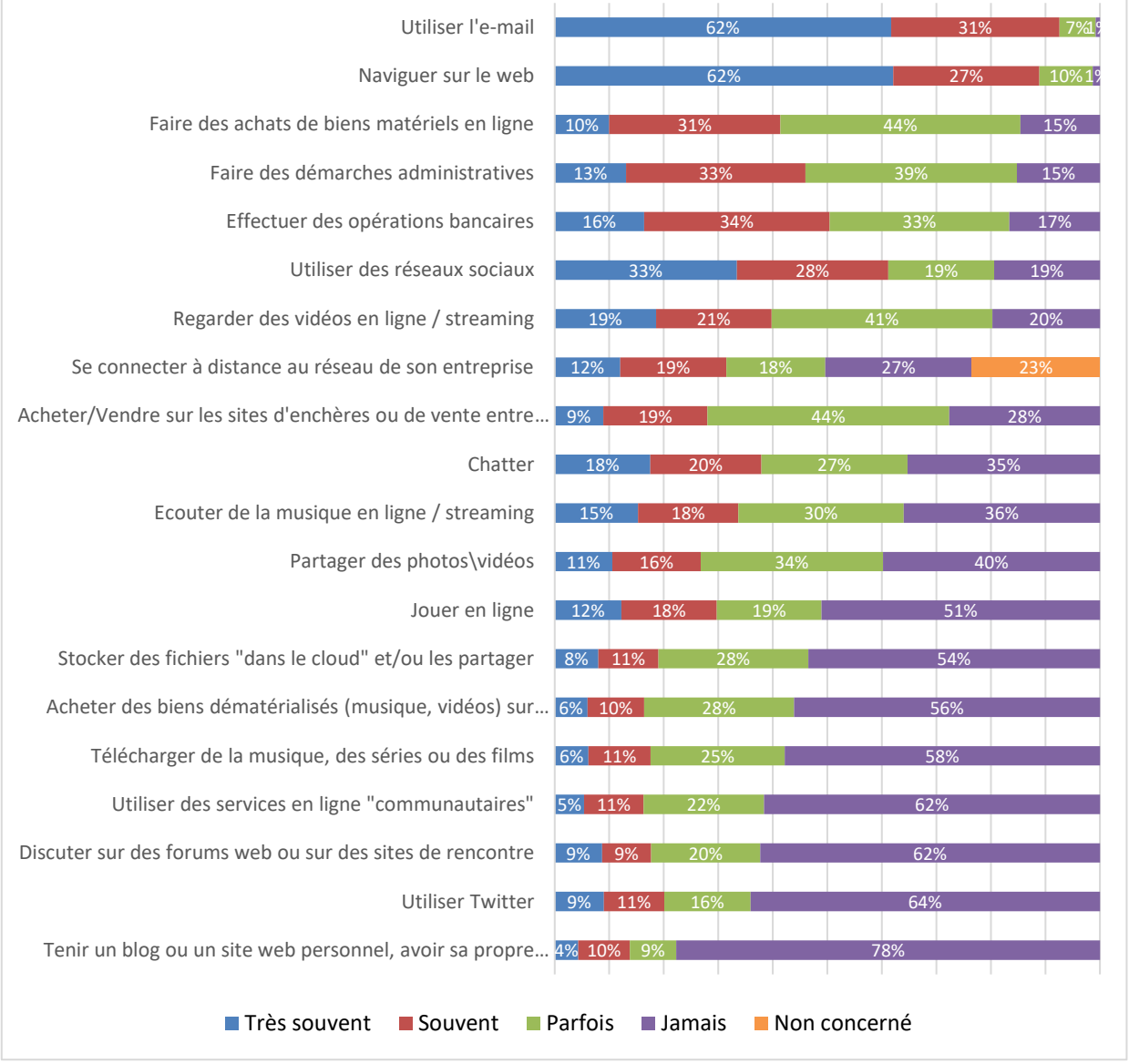


Figure 91 - Nature de l'usage de l'Internet

Adoption des services d'économie collaborative : grosses variations entre les régions et les générations

Si la moyenne nationale d'utilisation des services d'économie **collaborative** n'a pas augmenté par rapport à 2016 (stable à 16%), un focus sur l'Île de France nous révèle toutefois une assez nette croissance des usages « Très souvent » + « Souvent » (+5 points de 22% à 27%) avec un transfert de 3 points des « Parfois » vers les « Souvent » indiquant une évolution vers un usage plus régulier de ces services.

L'usage de tels services par la catégorie d'âge des 15/29 ans est toujours bien supérieur à la moyenne (36% au lieu de 16% le font « Très Souvent » et « Souvent ») et progresse de 3 points par rapport à 2016. Ce sont les 30/44 ans utilisant « Parfois » ce service qui connaissent la plus forte croissance (+6 points) et sont dorénavant un peu plus d'un sur quatre à se laisser tenter. La même catégorie d'âge utilisant ces services « Souvent » progresse également de 3 points.

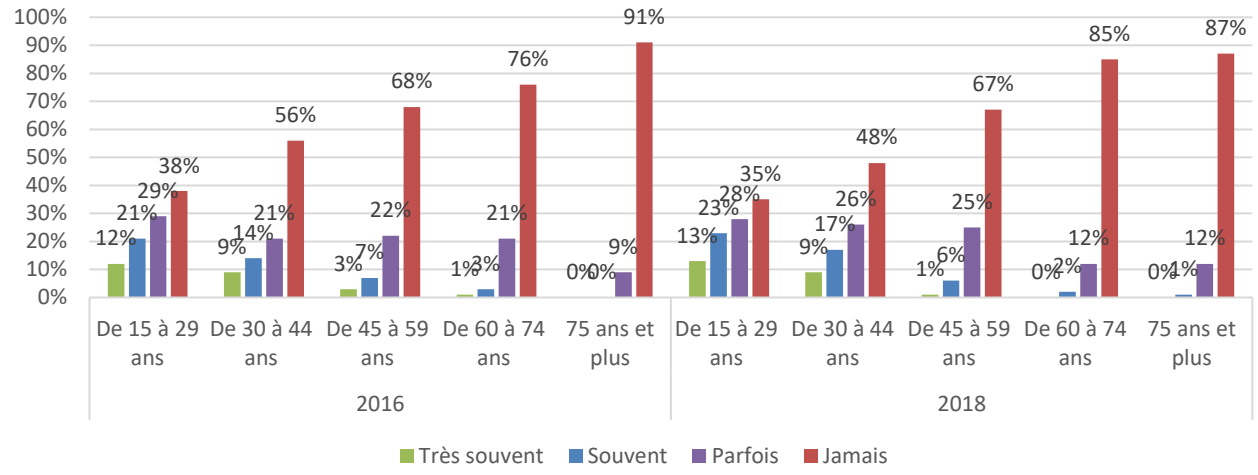


Figure 92 - Évolution de l'utilisation des services de l'économie collaborative selon les tranches d'âge

Les services de stockage dans le nuage pour ses données personnelles décollent enfin avec +6 points en moyenne par rapport à 2016. Encore une fois, on retrouve les catégories CSP+, les 15/29 ans et 30/34 ans ainsi que les franciliens comme usagers fréquents et au-dessus de la moyenne (44%, 42%, 45% et 43% respectivement). Ils progressent aussi tous comparativement à 2016, le record revenant aux 30/44 ans avec +13 points.

Paiement en ligne, les réticences baissent mais doucement

L'acte d'achat en ligne (67% des sondés en moyenne) ne recule pas par rapport à 2016 sauf très légèrement pour les biens matériels dont c'est surtout leur fréquence qui diminue.

Le paiement de ses achats se fait majoritairement sur ordinateur plutôt que sur tablette et mobile où une personne sur deux est réticente à effectuer un paiement en moyenne (les plus seniors sont même trois sur quatre à ne jamais payer en ligne depuis un mobile ou une tablette).

De plus, même si la tendance est à la baisse, le paiement en ligne ne s'envisage toujours pas sans que certaines conditions soient remplies.

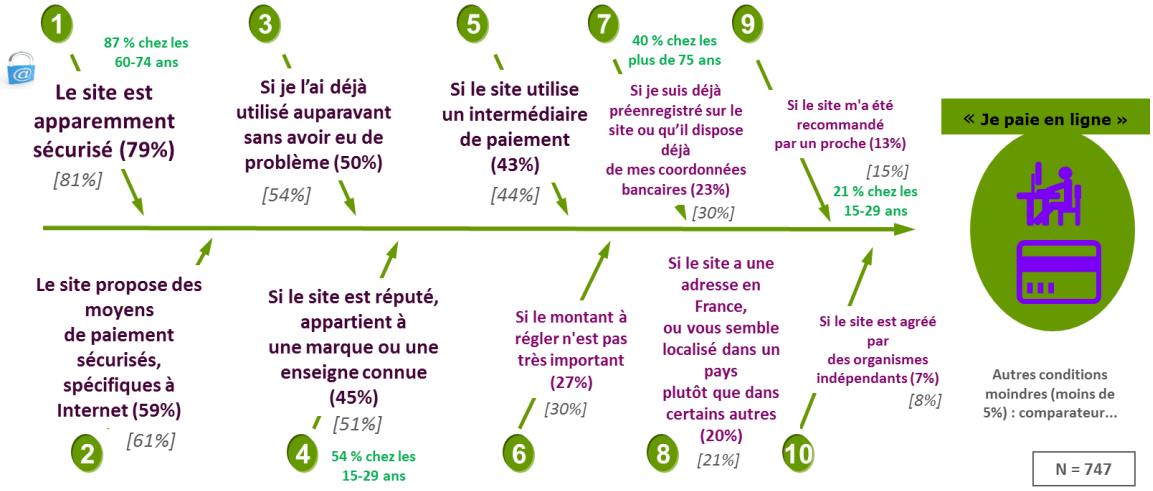


Figure 93 - Conditions requises par les internautes pour réaliser un paiement sur Internet

Les conditions qui arrivent en tête sont essentiellement celles liées à la sécurité du site (4 personnes sur 5 en moyenne) ainsi que des moyens de paiement associés ou encore à sa réputation.

Petite spécificité des personnes de plus de 75 ans pour qui il est plus important que la moyenne (40% contre 23%) d'être préenregistré notamment avec leurs informations bancaires.

Données personnelles, le RGPD n'a pas encore porté ses fruits

En moyenne, comparativement à 2016, le comportement des internautes vis-à-vis de la divulgation de données personnelles au travers de formulaires reste identique. Deux sur trois consentent à remplir des formulaires s'ils ont un sentiment de confiance et 13% remplissent toujours des formulaires sans aucune condition préalable. Ce chiffre grimpe même à 25% pour les 15/29 ans, en forte progression par rapport à 2016 où ils n'étaient que 17% dans cette classe d'âge à adopter ce comportement.

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

Les menaces d'Internet : une perception en hausse

La perception des risques sur les données détenues par les internautes (documents, photos, vidéos, etc.) stockées sur les ordinateurs fixes ou portables est **relativement stable depuis 2014**.

Pour les smartphones et tablettes, après une dégradation entre 2014 et 2016, **la confiance remonte en 2018** : si les internautes qui ne perçoivent aucun ou peu de risques pour leurs données sont aujourd'hui 31% contre 27% en 2016, on note en parallèle que l'intérêt pour la question a sensiblement progressé. En effet, les personnes qui ne savent pas répondre, ou qui ne sont pas concernées, sont passées de 28% à 24% puis 19% entre 2014 et 2018. Cette évolution se fait essentiellement au profit d'un sentiment de risque important ou très important (42%, 49% puis 50% sur les trois dernières enquêtes).

Quels risques pensez-vous qu'Internet fait courir à vos données (documents, photos, vidéos, etc.) ?

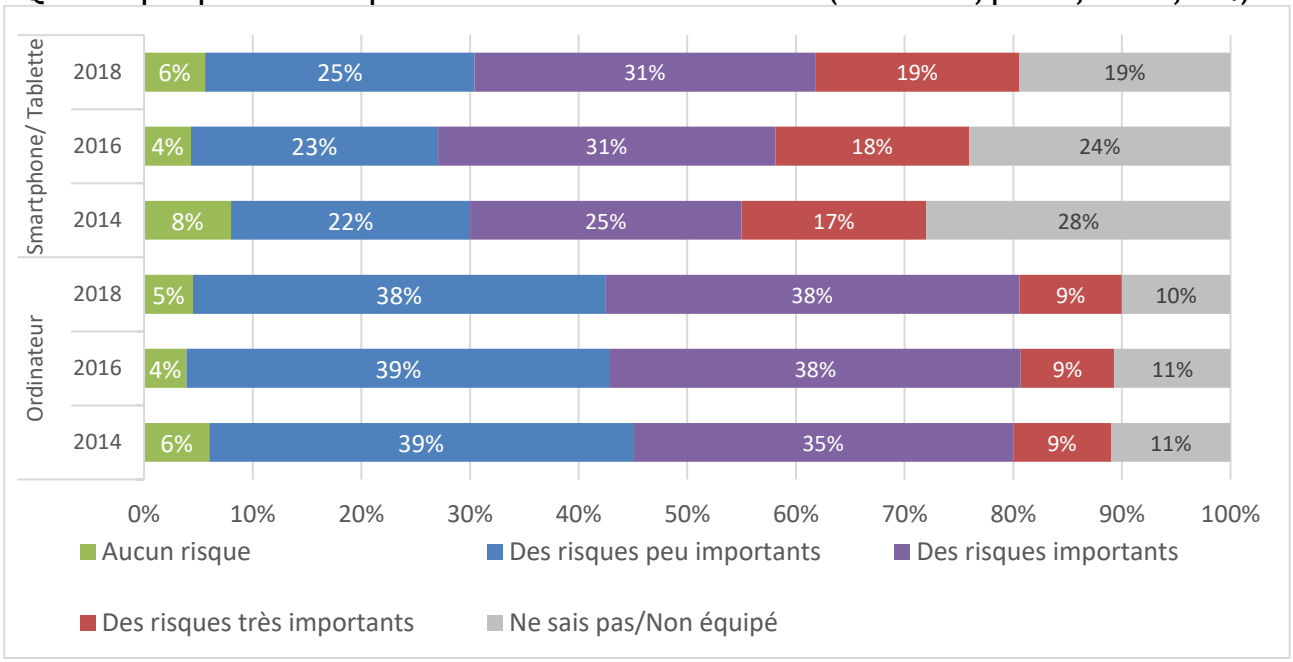


Figure 94 – Perception du risque concernant les données stockées sur les équipements connectés

Les internautes utilisateurs de tablettes et de smartphones semblent deux fois plus nombreux à ne pas savoir répondre que les utilisateurs d'un ordinateur. Cet écart est toutefois à considérer avec précaution. En effet, si l'option « non équipé » a bien été proposée pour les matériels mobiles, elle ne figure pas dans les réponses concernant les ordinateurs fixes.

Des menaces sur la vie privée très largement perçues

Globalement, 87% des personnes interrogées estiment qu'il est important de protéger sa vie privée, voire très important pour 48% d'entre elles.

La perception des menaces d'Internet sur la vie privée reste stable et extrêmement forte. 68% des personnes interrogées estiment qu'Internet met leur vie privée en danger, dont 16% « fortement », et cette perception reste inchangée depuis 2014.

On note en revanche une différence sensible en fonction de l'âge des internautes. Les plus jeunes ont une plus grande perception du danger d'Internet que leurs ainés : 70% chez les moins de 30 ans et chez les 30 à 44 ans. Cependant, chez les 45 à 59 ans, la perception n'est que de 64%.

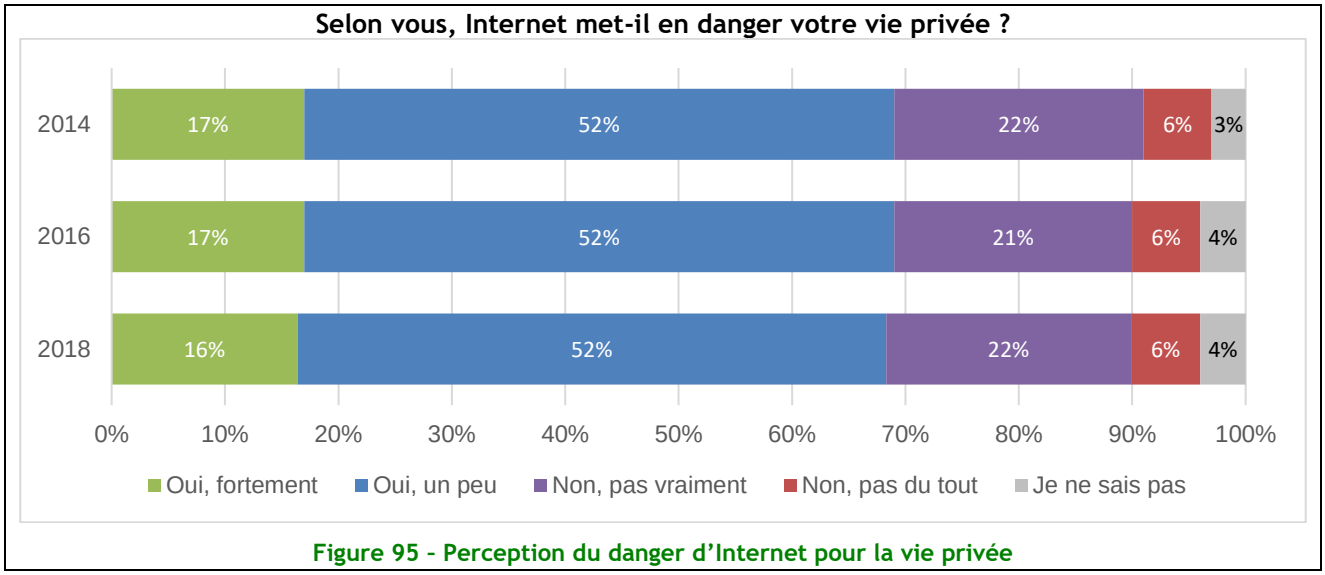


Figure 95 - Perception du danger d'Internet pour la vie privée

En ce qui concerne la protection de la vie privée, on observe une lente diminution de son importance aux yeux des internautes. Ils sont maintenant 13% à considérer qu'elle n'a que peu ou pas d'importance. Cette évolution est peut-être liée aux habitudes de transparence prises avec les réseaux sociaux.

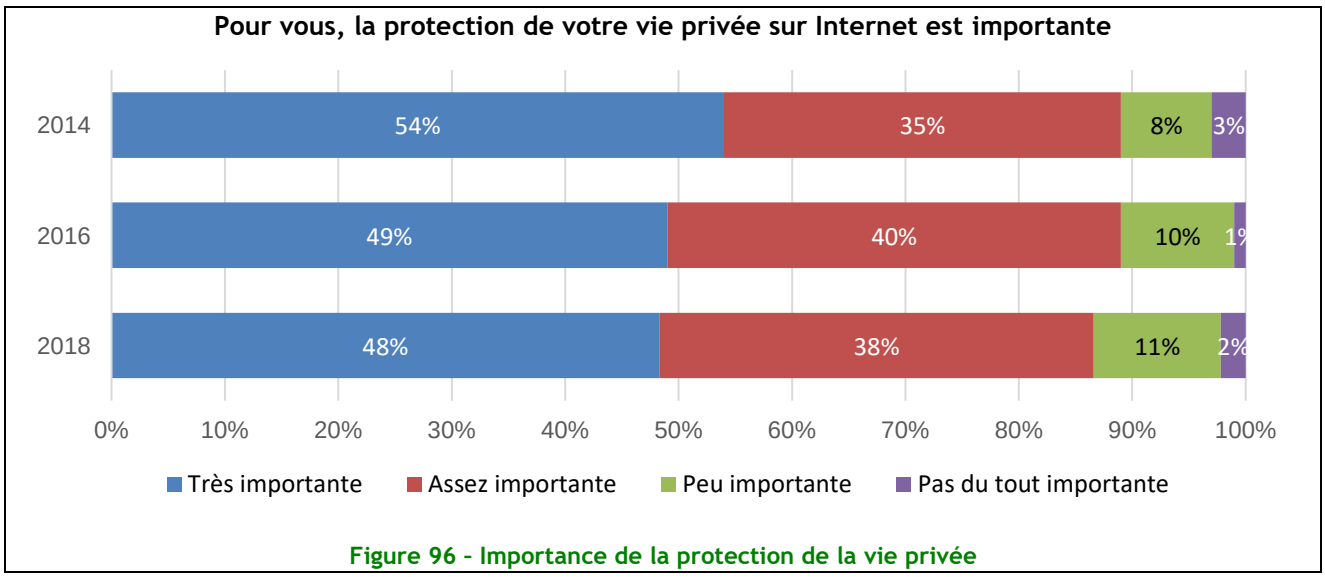


Figure 96 - Importance de la protection de la vie privée

Précautions de base : la moitié des internautes y pensent

Malgré cette perception du danger, les internautes ne semblent pas majoritairement savoir comment s'en protéger.

Ainsi, parmi ceux qui utilisent les réseaux sociaux, seuls 58% disent vérifier et modifier régulièrement les réglages des paramètres de sécurité et de confidentialité de leur profil sur les réseaux sociaux.

On constate également que si la prudence est globalement importante (de l'ordre de 60%), le taux de réglage des paramètres diminue chez les personnes les plus âgées (39%).

Vérifiez-vous et modifiez-vous régulièrement les paramètres de sécurité et de confidentialité de votre profil sur : les réseaux sociaux/les OS

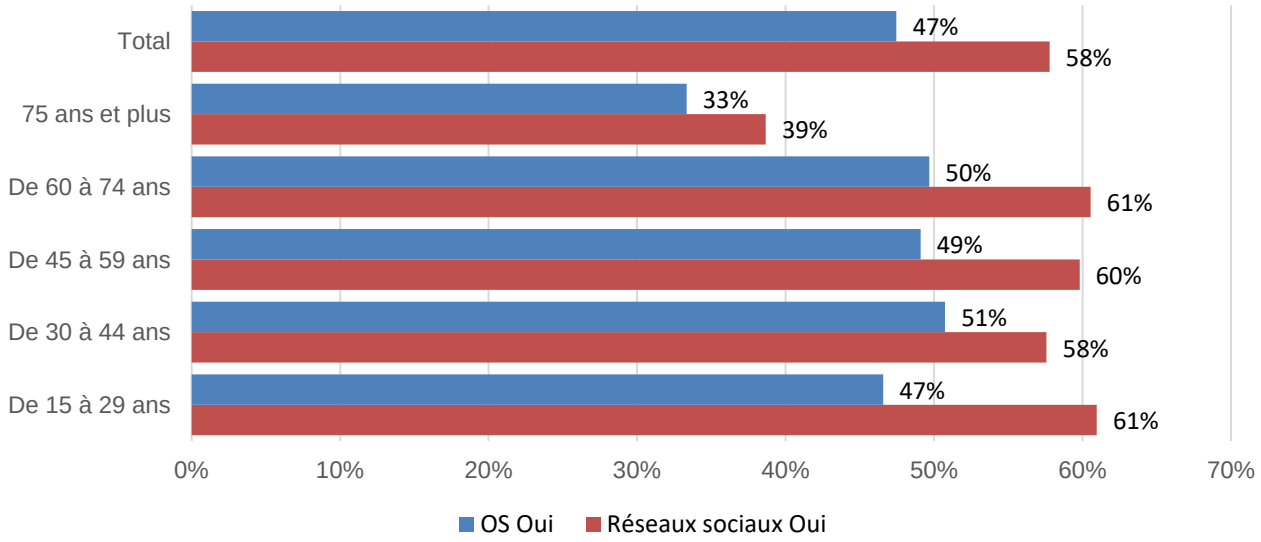


Figure 97 – Taux de surveillance des paramètres de profil selon l'âge

Le constat est assez similaire pour ce qui concerne la protection de leur profil sur leur ordinateur. En moyenne, parmi ceux qui se disent concernés, seuls 47% des internautes disent modifier régulièrement les paramètres de sécurité et de confidentialité des systèmes d'exploitation de ce type d'équipement.

Utilisation du « cloud » : une grande incertitude

Interrogés sur la perception des risques du stockage dans le « cloud » vis-à-vis de la perte et de la destruction des données, ou de leur confidentialité, plus de 40% des internautes (42%, 44%) avouent de pas savoir arbitrer sur le niveau de risque entre le « cloud » et le stockage local.

Pour ceux qui se prononcent, le stockage local parait légèrement plus sûr en ce qui concerne la confidentialité (30%) mais plus risqué (32%) pour la perte/destruction de données.

Selon-vous, le stockage de vos informations dans le « cloud » augmente ou diminue-t-il les risques comparé au stockage local en ce qui concerne : la perte ou la destruction de données / la confidentialité ?

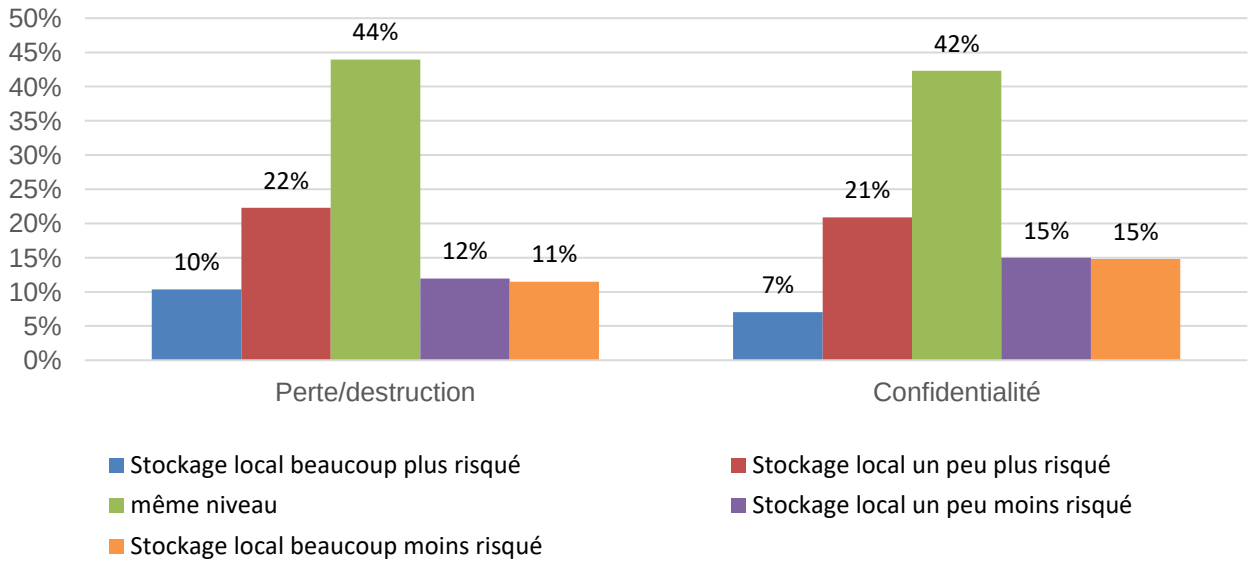


Figure 98 - Perception du risque du « cloud » par rapport au stockage local

Perte ou vol de données : baisse sensible sur les PC

Le nombre de personnes qui déclarent avoir subi la perte ou le vol de données sur un ordinateur au cours des deux dernières années est en diminution sensible (18% contre 24% en 2016), poursuivant la tendance observée depuis 2014 (35%).

Sur les équipements mobiles, la perte de données est également en légère baisse (13%). Elle est aussi moins fréquente que sur les postes de travail, ce qui s'explique sans doute par un usage plus encadré sur ce type de matériels où l'utilisateur ne dispose que de peu d'accès au système.

En ce qui concerne l'environnement « cloud », les internautes formulent un taux de perte de données très inférieur à celui des équipements personnels (10%). Cela s'explique certainement par un accès plus difficile à l'environnement système, et par les moyens de protection intrinsèques de ce type d'environnement.

Dans le 24 derniers mois, avez-vous subi une perte ou un vol de données qui étaient stockées : sur votre ordinateur, sur votre smartphone ou votre tablette, dans le cloud ?

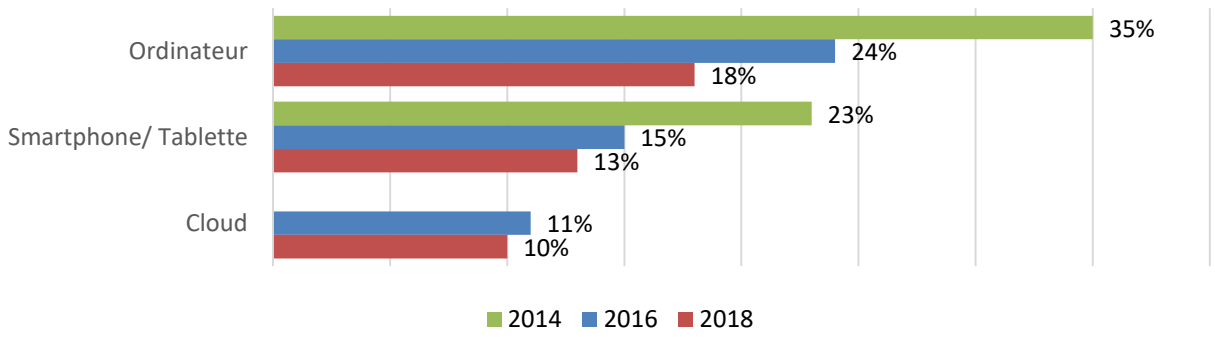


Figure 99 - Perte de données subie sur un ordinateur, un équipement mobile ou dans le cloud

Comme on l'observait déjà en 2016, sur PC, la panne et l'erreur de manipulation ne sont plus les causes majeures (5% et 4%), ce qui pourrait s'expliquer par une maturité croissante des internautes. Parmi les causes identifiées, le virus ou le piratage restent les plus cités, aussi bien sur ordinateur (8%) que sur smartphone et tablette (5%).

Dans l'environnement cloud, la détermination de la cause semble plus difficile (9% des personnes ne connaissant pas la cause de la perte de données). Les premières causes citées sont, à part égale, le virus ou le piratage, et l'erreur de manipulation (3%).

Pour quelle(s) raison(s) avez-vous perdu ces données ? (plusieurs réponses possibles)

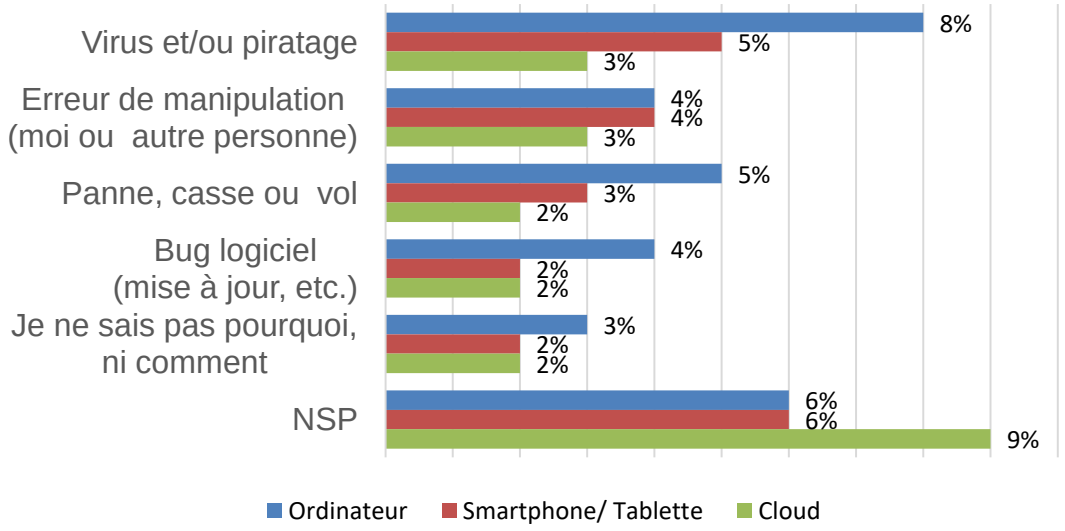


Figure 100 - Raisons des pertes de données sur un ordinateur, un équipement mobile ou dans le cloud

Évolution de la menace sur les équipements informatiques

La perception de l'évolution de la menace est particulièrement stable par rapport à 2016. Les internautes estiment toujours très largement (44%) que les dangers pesant sur leurs ordinateurs, comme sur les équipements mobiles, augmentent par rapport aux années précédentes.

Par rapport aux années précédentes, estimez-vous que les dangers et les risques auxquels votre ordinateur, vos smartphone ou tablettes, sont exposés sont…

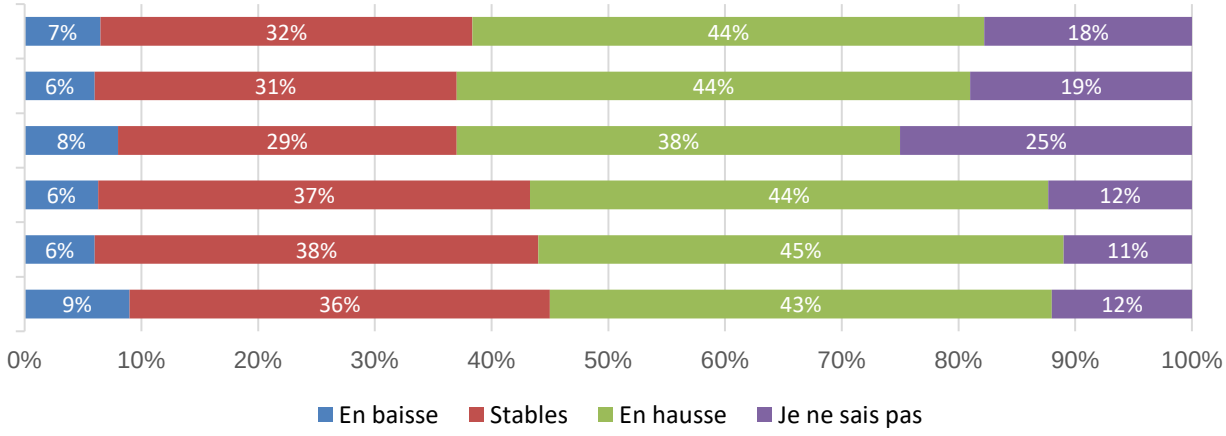


Figure 101 - Évolution de la perception du risque sur les équipements connectés

Une perception des menaces en léger recul

L'enquête de 2016 avait introduit une nouvelle façon de présenter la perception des menaces, qui permet une vue plus synthétique et un classement de menaces par ordre d'importance.

Un score moyen a été calculé en pondérant les réponses, sur l'échelle suivante : risque nul (1), peu important (2), important (4), très important (7), sans tenir compte des réponses « Je ne sais pas ».

Chaque menace est ainsi notée selon la répartition des réponses, un score de 4 ou plus dénotant un risque important, tandis qu'un score inférieur à 4 indique un risque modéré.

Sur les 21 menaces proposées aux internautes, 16 sont considérées comme représentant un risque important, mais pour la plupart, cette perception est en diminution sensible par rapport à 2016 et 2014 :

- L'infection par un virus : elle reste la menace la plus importante,
- L'installation de logiciels malveillants (cheval de Troie, rançongiciel, Cryptolocker) vient en deuxième et troisième places,
- Les escroqueries à la carte bancaire ou le phishing qui étaient en deuxième place en 2016, ont été moins souvent cités cette année.

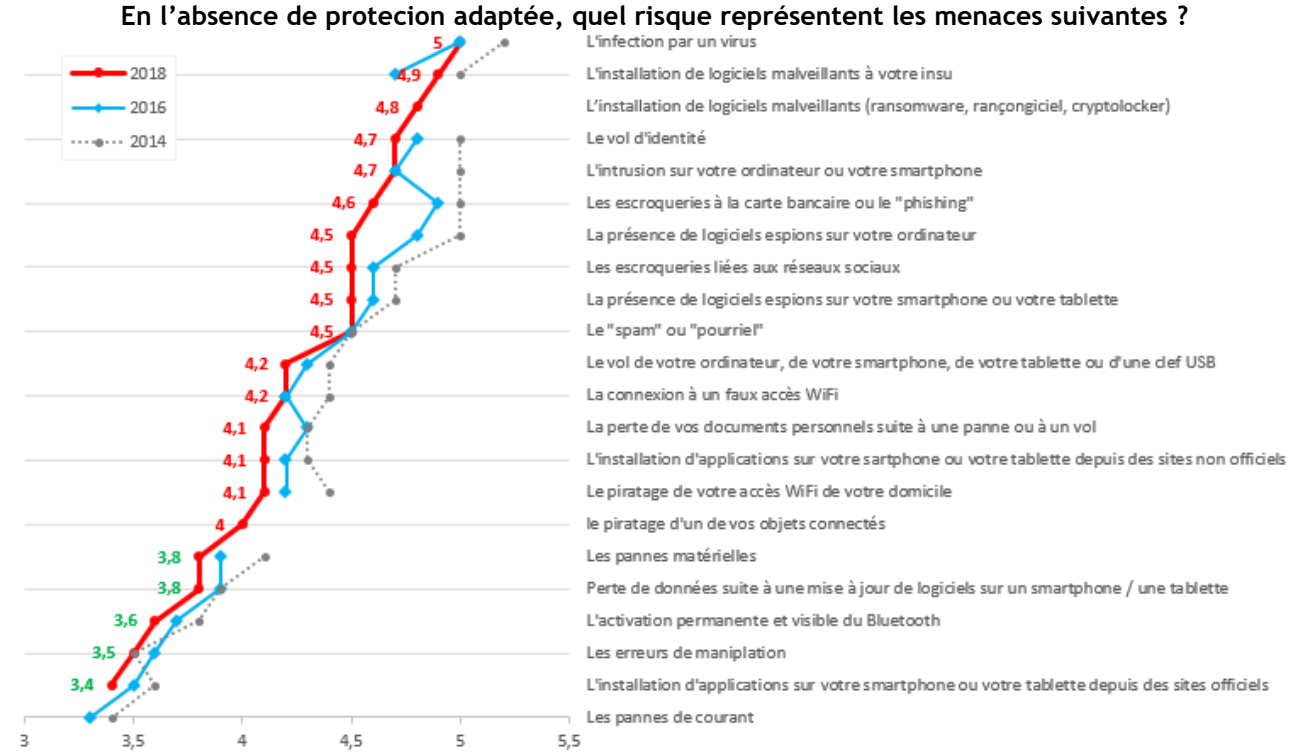


Figure 102 - Perception de la gravité de la menace en l'absence de protection adaptée

Globalement, Internet reste perçu comme la principale source de menaces (virus, logiciels espions ou malveillants, vol d'identité, escroqueries), devançant les menaces locales (piratage du Wi-Fi, vol de l'ordinateur, pannes matérielles).

Paiement sécurisé à partir de quel dispositif ?

Les tendances constatées en 2016 se confirment en 2018 : le paiement en ligne sur un ordinateur est perçu par les internautes comme plus sécurisé (39% en 2018 et 40% en 2016) que sur un smartphone ou une tablette (3% en 2018 et 2016).

En parallèle, un internaute sur trois estime que le paiement en ligne est autant sécurisé sur un ordinateur que sur un smartphone ou une tablette.

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

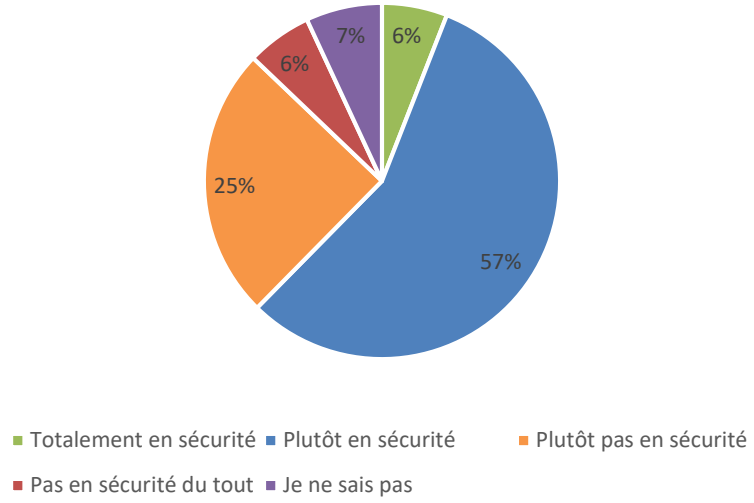


Figure 103 -Perception de la sécurité du paiement en ligne sur un ordinateur vs sur un smartphone

Les facteurs d'influence sur les risques

Quels sont les éléments influençant les risques ?

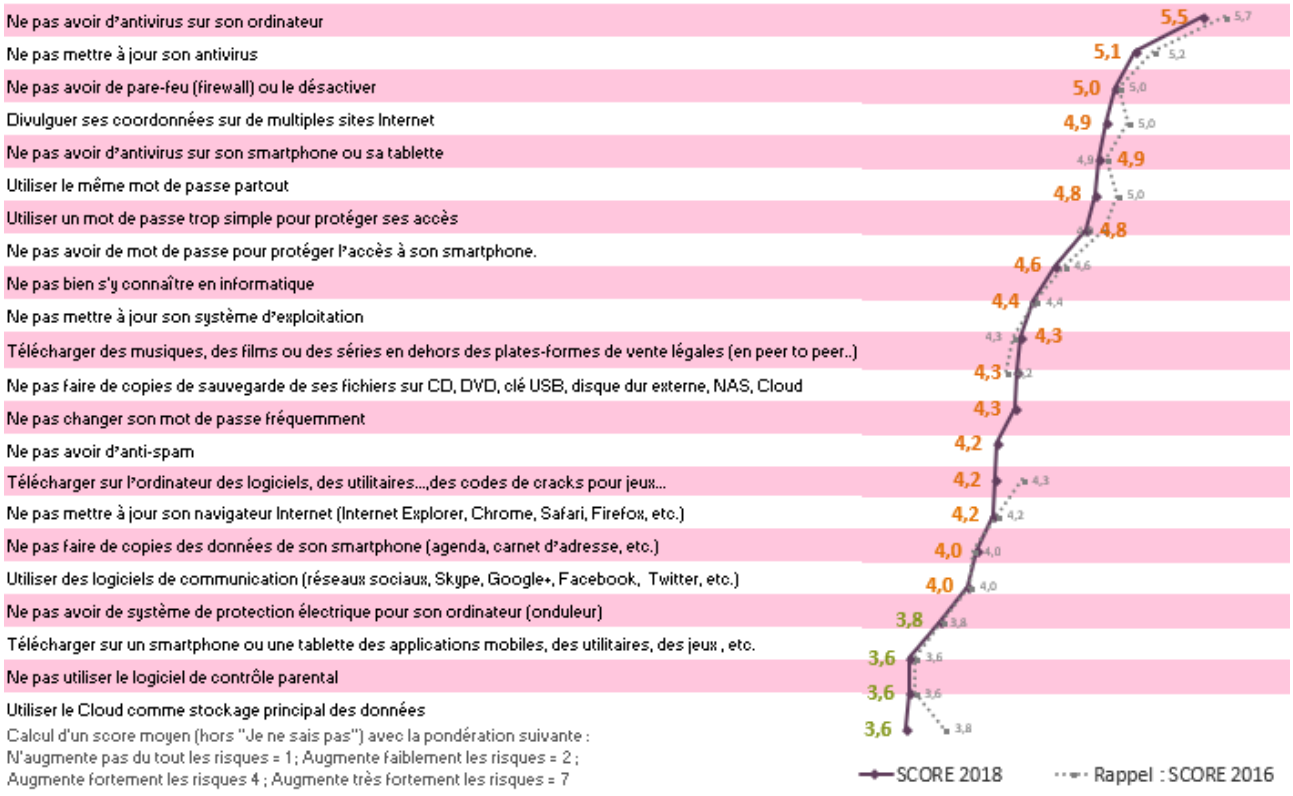


Figure 104 -Perception de la sécurité du paiement en ligne sur un ordinateur vs sur un smartphone

De manière générale, les internautes ont conscience que leur comportement sur internet peut être facteur d'augmentation des risques qu'ils encourent. Le constat établi entre 2016 et 2018 n'a pas changé, les comportements liés aux antivirus (absence ou non mise à jour de la solution), pare-feu et mots de passe (absence, simplicité ou réutilisation d'une plateforme à une autre) sont les facteurs les plus susceptibles d'aggraver les risques. Ces situations et pratiques à risque sont complétées par la divulgation des coordonnées sur de multiples sites Internet.

Partie IV - Moyens et comportements de sécurité

Un recours aux moyens de protection traditionnels

Depuis 2016, les internautes ont **renouvelé leur confiance dans les moyens de protection traditionnels**. Pas de nouveauté majeure, les ordinateurs, tablettes et smartphones sont toujours sécurisés par les solutions classiques anti-virus, pare-feu ou encore anti-spam.

Quels moyens de protection utilisez-vous pour garantir la sécurité de votre ordinateur / de votre smartphone ou de votre tablette ? (1/2)

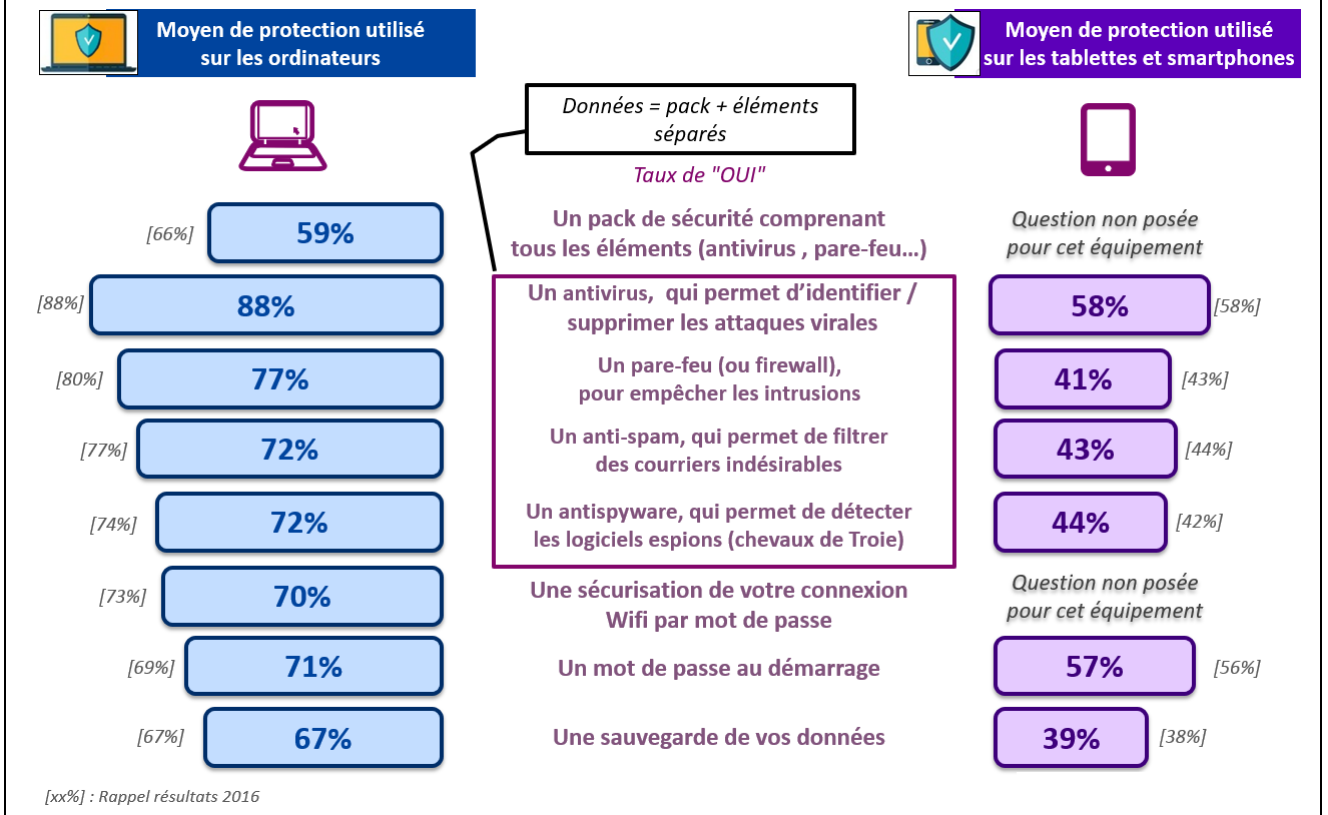


Figure 105 - Moyens de protection utilisés sur un ordinateur et sur une tablette/smartphone (1/2)

Si l'anti-virus (88%) est toujours autant déployé sur les ordinateurs des internautes, ce n'est pas le cas des **autres moyens de protection traditionnels qui rencontrent une légère diminution** : baisse de 3 points pour le pare-feu, 5 points pour l'anti-spam et 2 points pour l'anti-spyware. Par ailleurs, la régression la plus importante concerne le déploiement du « **pack de sécurité** » (le quatuor anti-virus, pare-feu, anti-spam et anti-spyware) n'équipe que **59% des ordinateurs en 2018 contre 66% en 2016**.

Les tablettes et les smartphones ne connaissent pas le même niveau de protection que les ordinateurs : **seulement un équipement sur deux dispose d'un moyen de protection**. L'anti-virus est la solution la plus déployée (58%), ainsi que le mot de passe au démarrage (57%).

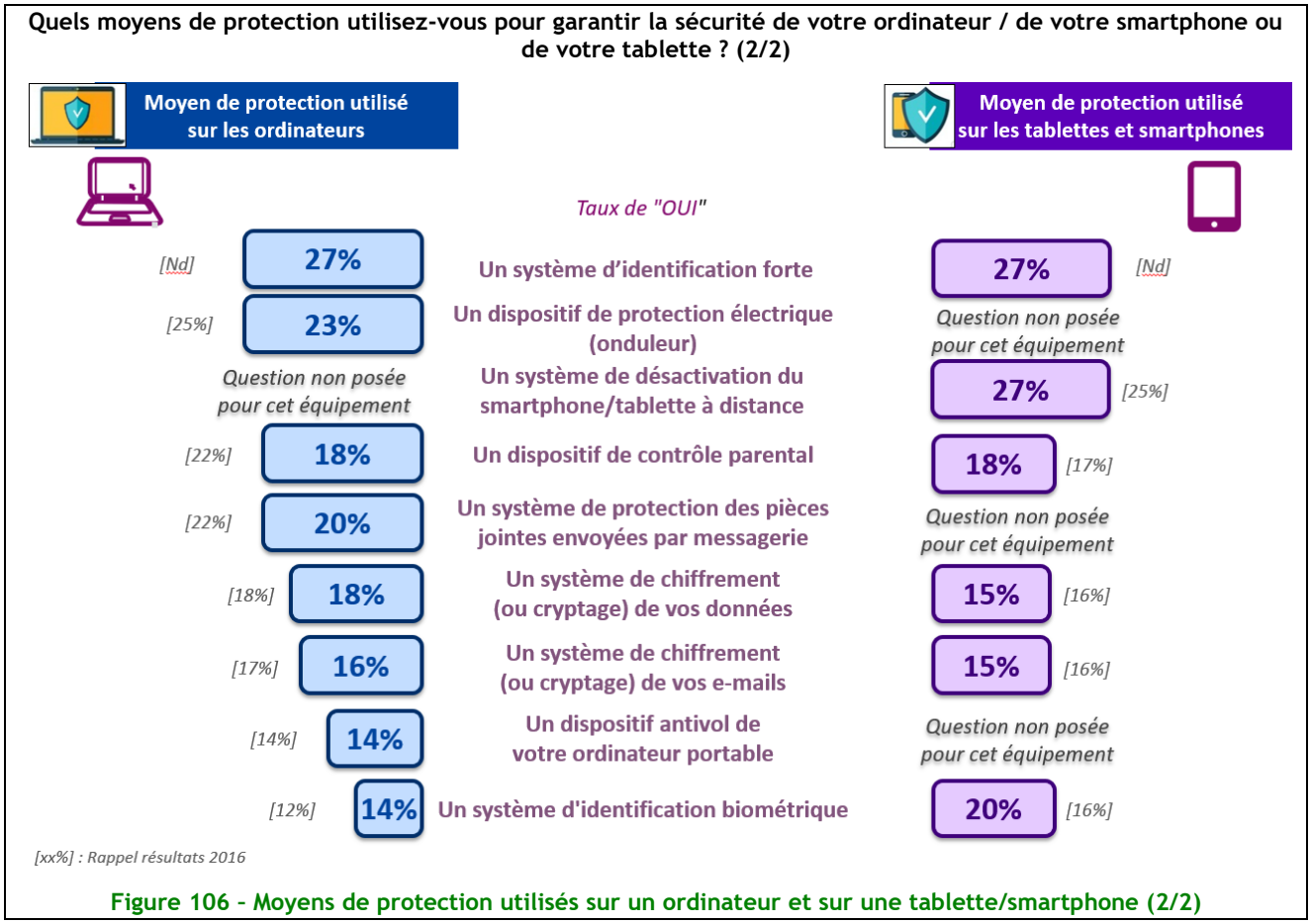


Figure 106 – Moyens de protection utilisés sur un ordinateur et sur une tablette/smartphone (2/2)

Concernant les moyens de protection utilisés de manière plus marginale, **le système d'identification biométrique** est le seul ayant rencontré une réelle augmentation de son utilisation sur l'ensemble des typologies d'équipement : taux de couverture est de 14% en 2018 (contre 12% en 2016) pour les ordinateurs et de 20% en 2018 (contre 16% en 2016) pour les tablettes et smartphones.

Une population toujours prudente mais peu technophile

Le niveau de sensibilité face à la nécessité de disposer d'une mise à jour automatique de l'ordinateur est **toujours aussi important** : 82% des internautes ont cette fonctionnalité activée (faible baisse de 2 points par rapport à 2016). Même si cette dernière n'est pas autant déployée sur les smartphones, **les utilisateurs sont de plus en plus nombreux à y avoir recours** : 57% en 2018 contre 53% en 2016.

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

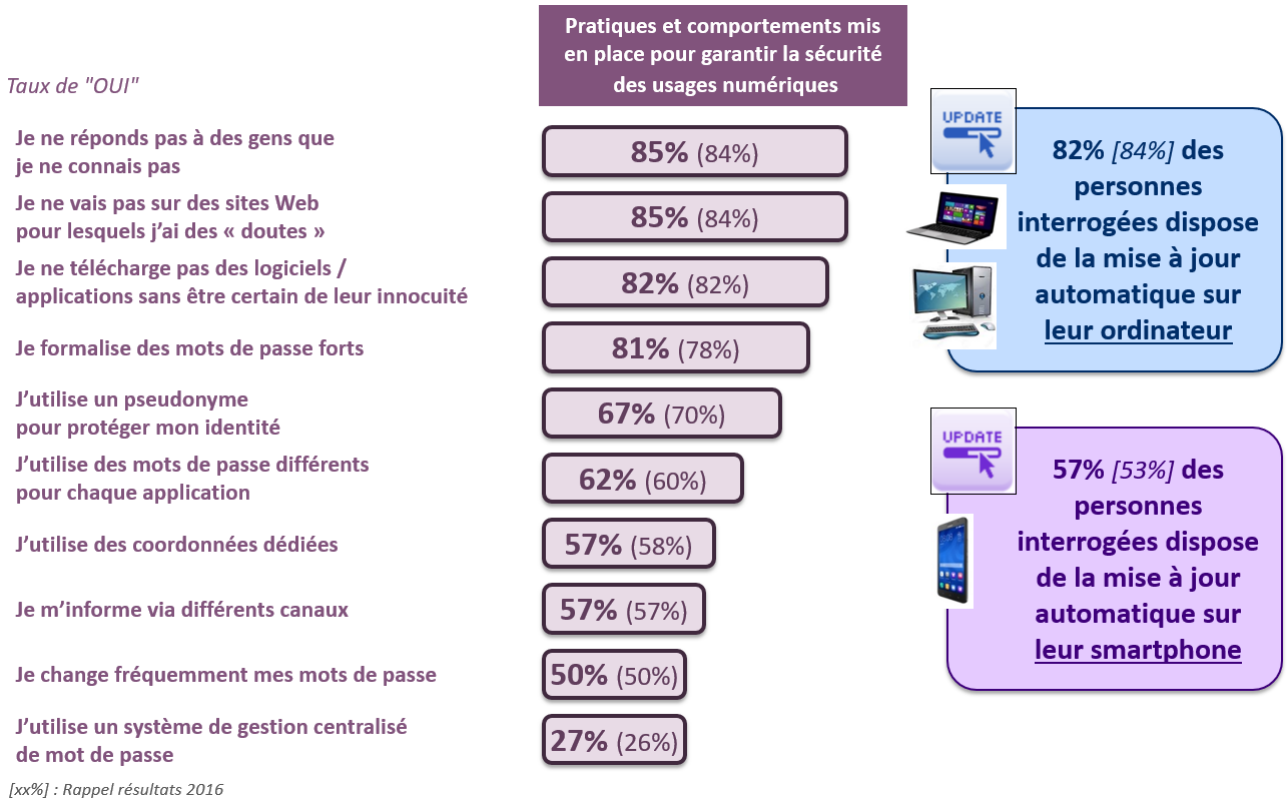


Figure 107 - Comportements de sécurité des internautes

La tendance constatée en 2016 était la suivante : face à une situation où il existe un risque potentiel lié à un contenu suspicieux (message provenant d'un expéditeur inconnu, lien vers un site web douteux, téléchargement d'application légitime), **les internautes choisissaient de pas donner suite à la sollicitation**. Cette tendance est confirmée puisqu'en 2018, **plus de 80% des internautes adoptent un comportement préventif face à ce type de situation**.

Par ailleurs, plus d'un internaute sur deux n'hésite pas à **se renseigner via différents canaux lorsqu'il est confronté à une situation à risque.**

Sur Internet, vous sentez-vous ?

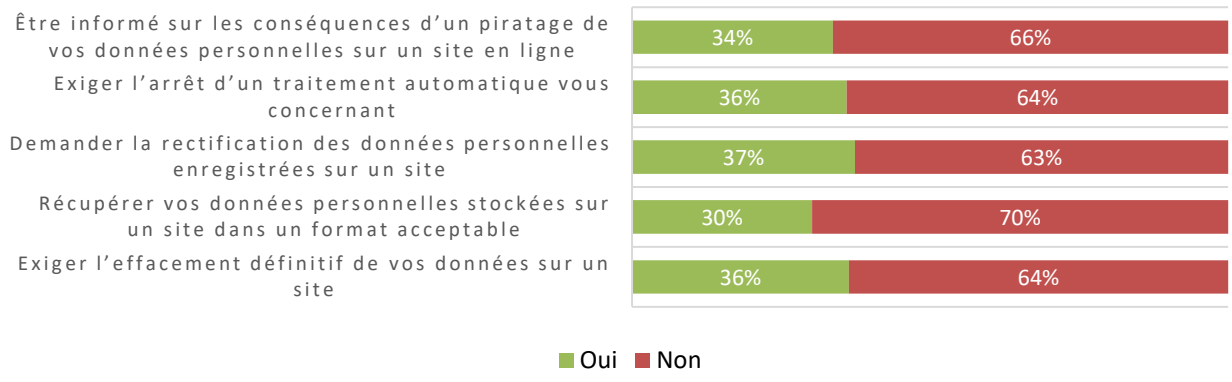


Figure 108 - Sentiment de sécurité sur Internet

En matière d'usages liés aux mots de passe, les comportements des internautes sont toujours sensiblement les mêmes en 2018 : 50% d'entre eux modifient leurs mots de passe fréquemment et 27% ont un recours à une solution de gestion centralisée (26% en 2016). Ce dernier point peut s'expliquer par une sensibilisation encore faible liée à l'usage de ce type de solution mais également la complexité de sa mise en œuvre.

Si cette population reste relativement prudente, près de deux internautes sur trois éprouvent un sentiment de sécurité sur Internet.

Une population pas suffisamment informée sur l'exercice de ses droits sur Internet

Les internautes disposent de certains droits sur Internet liés au Règlement Général sur la Protection des Données comme l'effacement définitif de leurs données sur une site ou la rectification des données personnelles enregistrée sur un site. **Le niveau de sensibilisation lié à ces droits reste faible**, en effet, seulement un internaute sur trois s'estime être suffisamment informé par rapport aux droits dont il dispose. Il est probable que ce taux relativement bas s'explique par l'entrée en application très récente du RGPD et sera amené à évoluer positivement au cours des mois à venir.

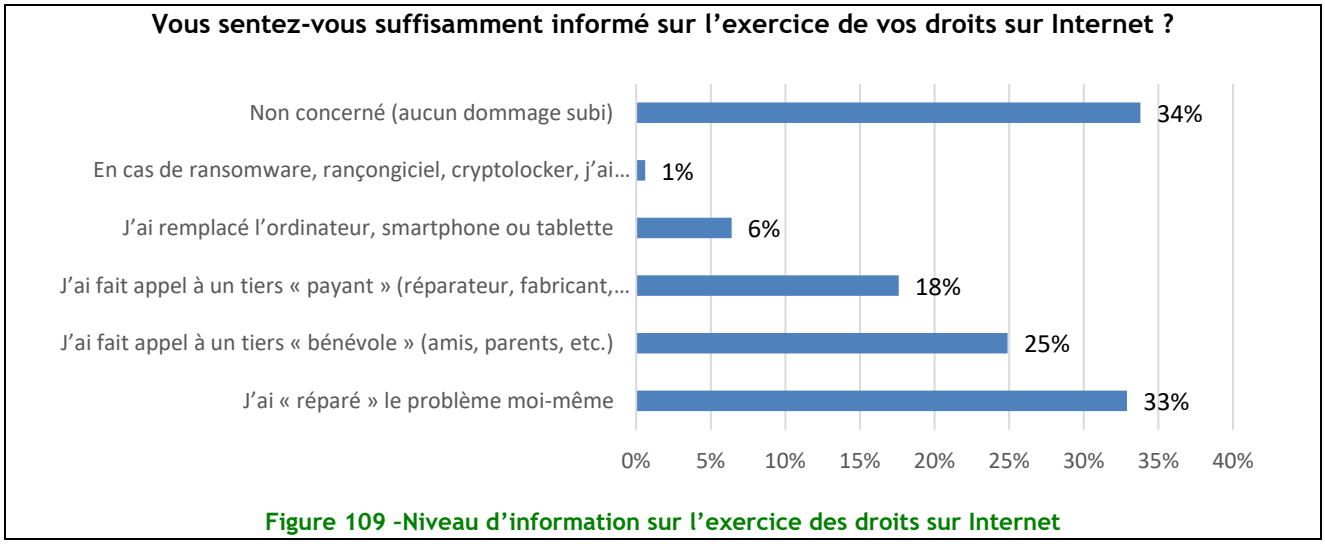


Figure 109 -Niveau d'information sur l'exercice des droits sur Internet

Des prestataires spécialisés peu sollicités en cas de dommage

Lors d'un dommage sur leur machine, les internautes ont avant tout le réflexe **de gérer l'incident par leurs propres moyens soit en le « réparant » eux-mêmes, soit en faisant appel à leur entourage qui agit de manière bénévole**. Seulement 18% d'entre eux sollicitent les services d'un prestataire spécialisé. Ce dernier point peut s'expliquer par une non volonté de la part des internautes d'engager des frais non prévus.

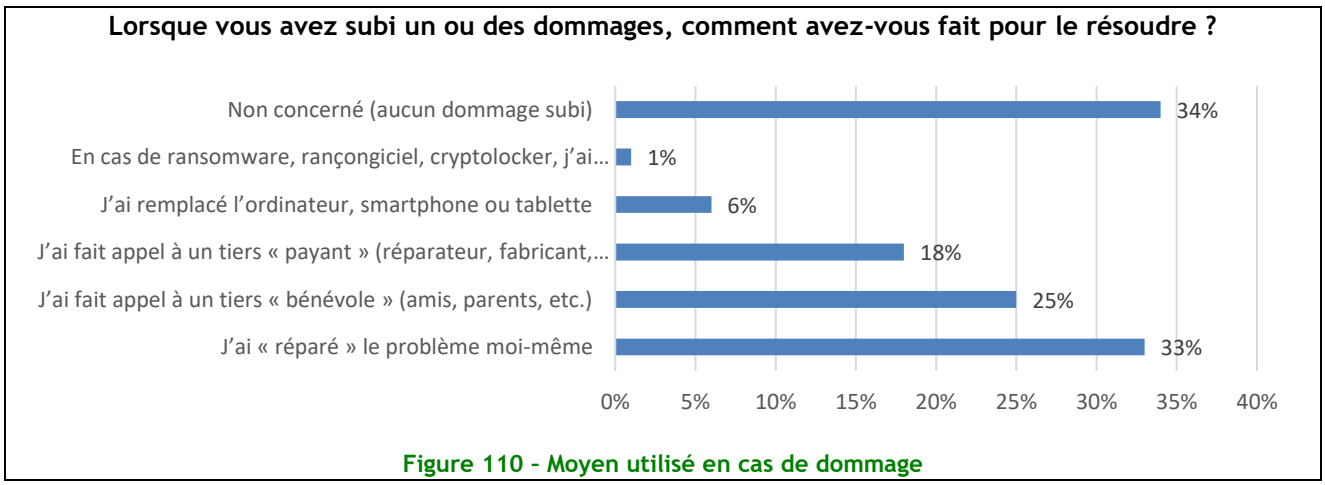


Figure 110 - Moyen utilisé en cas de dommage

L'ESPRIT DE L'ÉCHANGE

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

11, rue de Mogador
75009 Paris
✆ 01 53 25 08 80
clusif@clusif.fr

Téléchargez les publications du CLUSIF sur

www.clusif.fr