Menaces informatiques et pratiques de sécurité en France

Édition 2014

- Les entreprises de plus de 200 salariés
- Les hôpitaux publics
- 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
Mme COURTECUISSE Hélène	LISIS CONSEIL	Responsable Hôpitaux
M. PRISO Serge	DEVOTEAM	Responsable Internautes

Les membres du Comité d'Experts

M. BAUDOT Christophe	SYNDICAT INTERHOSPITALIER DU LIMOUSIN
Mme BERARD Béatrice	CHU NANCY
M. BLUM Patrick	ESSEC
M. BÔLE Thierry	IFP ÉNERGIES NOUVELLES
Mme BUTEL Annie	BNP PARIBAS
M. CORDIER Cédric	HOSPICES CIVILS DE BEAUNE
Mme COUWEZ Marie-Agnès	PEA CONSULTING
M. CRUMBACH Albert	CHR METZ-THIONVILLE
Mme DE CADEVILLE Anne	AGENCE RÉGIONALE DE SANTÉ DE HAUTE NORMANDIE
M. DELALLEAU Hervé	INPI
M. DEPAUL Jonathan	IMPRIMERIE NATIONALE
M. DRAPEAU Romain	CH NIORT
M. DUCHESNE Stéphane	CHU BORDEAUX
M. FOUCAULT Jacques	TIBCO SERVICES
M. GIORIA Sébastien	ADVENS
M. GREMY Jean-Marc	CABESTAN CONSULTANTS
M. GUÉRIN Olivier	CLUSIF
Mme GUIGNARD Martine	IMPRIMERIE NATIONALE
M. HAMON Bruno	MIRCA
Mme LANG Astrid	AP-HP
M. MAUJEAN Xavier	ORANGE
M. MINASSIAN Vazrik	ADENIUM
M. NORMAND Yves	SYNDICAT INTERHOSPITALIER DE BRETAGNE
M. TAVEAU Pierre	CHU POITIERS

Le CLUSIF remercie également vivement les représentants des entreprises et hôpitaux publics ainsi que les internautes qui ont bien voulu participer à cette enquête.

Enquête statistique réalisée pour le CLUSIF par le cabinet GMV Conseil et Survey Sampling International.

Avant-propos

Une nouvelle fois, j'ai l'honneur de préfacer l'édition 2014 de notre étude MIPS, en espérant que celle-ci réveille votre intérêt mais surtout qu'elle alimente vos réflexions quotidiennes. Que vous soyez professionnel de la Sécurité du Système d'Information, que vous ayez des responsabilités dans l'entreprise ou même, que vous soyez un citoyen conscient des enjeux de ce « cybermonde » et, en particulier, de sa sécurité, ce rapport vous apportera une vision éclairée par l'analyse de nos experts du contexte actuel de la SSI.

Depuis toujours, alimenter la réflexion des professionnels de la Sécurité du Système d'Information est l'objectif majeur du CLUSIF. Ce rapport est une de ses sources clé, il représente un complément à notre Panorama de la Cybercriminalité. Ce qui est une tendance dans le Panorama, devient, à court ou moyen terme, un constat dans MIPS.

J'en veux pour preuve les sinistres par attaques logiques ciblées, dont nous suivons l'évolution depuis quelques années, qui font cette année un bond en avant impressionnant (+8%).
Par rapport à ceci, je ne peux que me réjouir de l'augmentation du nombre de plaintes déposées suite aux incidents. C'est bien la preuve d'une prise de conscience des entreprises et des individus que les instruments de lutte contre la délinquance informatique sont multiples et que le juridique en fait bien partie.

A contrario, nous sommes nombreux à être préoccupés du retour en force des erreurs d'utilisation et des erreurs de conception, les deux ayant augmenté de manière importante entre 2010 et 2014. Le suivi des incidents permet sans nul doute d'avoir une visibilité sur ces erreurs ; avant l'entreprise les soupçonnait, maintenant elle les mesure et les gère. Et ceci pourra nous permettre de les combattre vraiment.

Ce constat doit inciter les offreurs et utilisateurs à travailler ensemble, main dans la main. Le salut de la sécurité, de la cybersécurité si on étend la SSI à l'ensemble de ses acteurs y compris les cybercitoyens, passera par une amélioration de la qualité de tous les produits des technologies de l'information. Mais l'utilisateur doit aussi prendre conscience de l'usage qu'il fait de la technologie. Se former, respecter les règles, ne pas se mettre en danger et prévenir de tout événement anormal. La SSI, à elle seule, ne peut pas tout !

Finalement, je crois que ces mots, de Pascal LOINTIER, écrits pour l'édition 2010, sont la meilleure description du bon usage de ce rapport et ils devraient être dans le préface de toutes les éditons :

« L'étude MIPS :

- *pour le Responsable ou Fonctionnaire de la Sécurité des Systèmes d'Information ou pour un chef d'entreprise, c'est le moyen de mettre en perspective sa propre politique de sécurité ou d'identifier les freins rencontrés par des entreprises tierces,*
- *pour un Offreur de biens ou un Prestataire de services en Sécurité des Systèmes d'Information, c'est mieux apprécier la nature du marché, le déploiement des offres et/ou les attentes et besoins à combler,*
- *pour nos services institutionnels et ceux en charge d'une mission de veille, quelle soit technique, réglementaire ou sociétale, c'est l'opportunité de détecter des phénomènes émergents ou représentatifs d'une volumétrie, voire sa contraposée si on considère par exemple la réticence toujours forte à évoquer les fraudes financières et les malveillances internes. »*

Je ne peux que souhaiter que vous puissiez vous saisir de ce rapport comme vous l'avez fait les années précédentes.

Lazaro Pejsachowicz
Président du CLUSIF

Synthèse de l'étude

Au travers de l'édition 2014 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 de par la taille et la représentativité des échantillons d'entreprises (350 ont répondu) et des hôpitaux publics (150 ont répondu) interrogés. Par ailleurs, elle se veut relativement exhaustive, en reprenant, cette année encore, l'ensemble des 11 thèmes de la norme ISO 27002:2005[1], relative à la sécurité des Systèmes d'Information.

Enfin, cette année comme en 2008, 2010 et 2012, elle reprend le volet très complet consacré aux pratiques des particuliers utilisateurs d'Internet à domicile (1 000 répondants).

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

Entreprises : une évolution « tranquille... » qui continue dans un contexte financier et organisationnel toujours contraint

Le nombre d'acteurs de la SSI, au travers de la mise en place d'organisations et de structures (RSSI, Correspondant Informatique et Libertés (CIL), PSSI, charte interne et externes, etc.) continue à évoluer positivement. Pour autant, la « maturité SSI » elle stagne, voire régresse dans certains domaines… Toutefois, ceci est principalement dû 1] au manque de budget attribué à la SSI, et 2] à un manque de connaissances des nouveaux RSSI, principalement issus du domaine « technique ».

Côté budget, on constate une légère reprise, pondérée par le fait que le poste ayant eu la plus grosse augmentation, cette année encore, est la mise en place de solution, avec 26%. On reste toujours dans la technique : ainsi pour beaucoup la sécurité reste une histoire de mise en place de solution technique…

Le nombre d'entreprises ayant formalisé leur PSI est demeuré quasi-inchangé depuis 2010 (64% en 2014, 63% en 2010 et 2012). Ce point reste étonnant au vu de la forte progression du nombre de RSSI… Les normes de sécurité poursuivent leur influence grandissante sur la Politique de Sécurité de l'Information (PSI) des entreprises, passant de 75% en 2012 à 79% en 2014.

La fonction de Responsable de la Sécurité des Systèmes d'Information (RSSI ou RSI) est de plus en plus clairement identifiée et attribuée au sein des entreprises (62% vs 37% en 2008), ce qui va dans le sens de l'histoire. En grande majorité, les RSSI sont rattachés à la DSI (46%), ce qui pose encore la question de son « pouvoir » d'arbitrage… Mais ne vaut mieux-t-il pas un RSSI mal rattaché que pas de RSSI du tout ? : la question reste ouverte…

Point négatif : après une forte progression des analyses de risques entre 2012 et 2012 (54% totale ou partielle vs 38%), celles-ci stagnent, voire régresse légèrement !

Concernant la sensibilisation, pas de grand mouvement, en dehors de celle des VIP qui passe de 18% en 2012 à 31% en 2014…

L'accès nomade aux ressources de l'entreprise continue de se généraliser. La maturité des solutions technologiques de connexions, de contrôle des postes nomades et des informations qui transitent, permet un meilleur contrôle des risques associés.

Les PDA, tablettes et smartphones fournis par l'entreprise connaissent toujours une augmentation importante de leur usage : aujourd'hui, l'accès au SI avec ces équipements est autorisé dans plus de la moitié des entreprises interrogées. Mais gare aux équipements personnels (BYOD – *Bring Your Own Device*) : ces derniers ont vu leur taux d'interdiction passer de 38% à 66% !…

[1] Aux esprits chagrins qui se demanderaient : « mais pourquoi ne pas être parti sur la version 2013 », je répondrai tout simplement 1] « par manque de temps » et 2] « ce sera le cas pour l'étude 2016 : encore un peu de patience… ».

L'utilisation de la messagerie instantanée (non fournie par l'entreprise) et des réseaux sociaux, bien qu'en augmentation, est encore majoritairement interdite par les politiques de sécurité dans les entreprises (interdite à 70% en 2012 vs 56% en 2014).

Du côté des technologies de protection, globalement, rien ne bouge entre 2012 et 2014… Par exemple, les outils de chiffrement sur PC portables ne sont utilisés que par un tiers des entreprises. Idem pour les dispositifs de contrôle d'accès mis en œuvre qui stagnent voire régressent, à l'exception du SSO et du web SSO.

44% des entreprises ont placé leur SI en tout ou partie sous infogérance (9% en totalité et 35% partiellement) et quand c'est le cas, 32% ne mettent pas en place d'indicateurs de sécurité et 44% ne réalisent aucun audit sur cette infogérance (+11 points vs 2012) !… L'utilisation du Cloud augmente de façon importante (38%, + 24 points vs 2012) même s'il représente moins de 50% des entreprises.

De même, après plusieurs années d'augmentation régulière (jusqu'en 2010), suivi d'une régression en 2012, la formalisation des procédures opérationnelles de mise à jour des correctifs de sécurité (patch management) est, en 2014, en stagnation (60% vs 60% en 2012).

La Sécurité dans le cycle de développement progresse, mais reste toujours trop insuffisante (prise en compte à 24%, + 4 points vs 2012) !… Pourtant, il n'est plus à démontrer que nombreux sont les piratages qui utilisent des failles applicatives liées au développement (injection, XSS, etc.).

Ces deux dernières années marquent une régression dans la gestion des incidents de sécurité par les entreprises. En 2012, 45% (vs 53% en 2012) d'entre elles ont une cellule (dédiée ou partagée) à la gestion des incidents de sécurité.

Les types d'incidents rencontrés par les entreprises repartent fortement à la hausse par rapport à l'étude 2012, avec comme trio de tête :

- les pertes de services essentiels qui passent de 26% (2012) à 39%,
- les vols qui passent de 19% (2012) à 37%,
- les pannes d'origine interne qui passent de 25% (2012) à 35%.

Du côté du nombre d'incidents par an d'origine malveillante dans les entreprises, les « infections par virus » restent en pole position (14,4 incidents de sécurité dus à des virus dans l'année), suivi par les « attaques logiques ciblées » (10,5) et les « vols » (7,1).

Un peu plus du quart (27%) des entreprises ne prennent pas en compte la continuité d'activité. Ceci est en légère régression au regard des résultats de l'étude réalisée en 2012. Sans surprise, l'indisponibilité des 'systèmes informatiques de gestion' représente le scénario le plus couvert (60%). Le BIA (Bilan d'Impact sur l'Activité), prenant en compte les attentes des « métiers » se démocratise (55%, +12 points vs 2012). Reste que 25% des plans de continuité existants ne sont jamais testés par les utilisateurs : alors, à quoi servent-ils ?…

Le CIL, relativement présent dans les entreprises, n'intervient que pour 14% dans les déclarations CNIL.

Sur une période de deux ans, 71% (- 3 point vs 2012) des entreprises interrogées ont réalisé au moins un audit ou contrôle de sécurité du Système d'Information par an. Ces audits sont motivés principalement par le respect de la PSSI (43%), des exigences contractuelles ou règlementaires (33%) ou des exigences externes, comme les assurances ou les clients (32%).

Enfin, si les tableaux de bord de la sécurité de l'information (TBSSI) progressent, passant de 15% en 2012 à 25% en 2014, le chemin reste encore long. En effet, 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 des organisations.

Au final, les entreprises avancent, encore et toujours, et tranquillement, encore et toujours…

Hôpitaux publics : et si les exigences règlementaires étaient le moteur de l'évolution des pratiques de sécurité ?…

La sécurité des Systèmes d'Information de santé est soumise à un cadre réglementaire renforcé, dont la particularité a longtemps été la protection de la confidentialité de l'information médicale personnelle. Avec le développement de l'informatisation de la production des soins, les exigences d'intégrité, de continuité et d'auditabilité/preuve vont croissant.

Aussi, l'État et les acteurs de la santé et du médico-social sont-ils en train d'élaborer avec le soutien de l'ASIP Santé une Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S), à laquelle participent fortement les acteurs de la Santé et les RSSI des hôpitaux pour sa déclinaison opérationnelle.

En parallèle, le programme « Hôpital Numérique », qui constitue un cadre directeur de la modernisation du Système d'Information des établissements sanitaires à 5 ans (lancé par la direction générale de l'offre de soins, DGOS, Ministère de la Santé, en novembre 2011), comprend une obligation d'atteindre des prérequis en matière de sécurité de l'information :

- Identité / Mouvement,
- Fiabilité / Disponibilité,
- Confidentialité.

Les indicateurs permettant de mesurer l'atteinte du niveau indispensable dans ces domaines sont également utilisés par la Haute Autorité de Santé pour la certification des établissements sanitaires.

Ces nouveaux chantiers, à l'aune de la maturité nécessaire pour atteindre un niveau de maîtrise de la sécurité, constituent un levier puissant de mobilisation des directions générales des établissements, d'autant plus que l'établissement ne peut candidater pour émarger au volet financier du programme s'il n'a pas rempli certains prérequis, parmi lesquels celui de disposer d'un référent sécurité SI de l'établissement…

À l'action directe de l'État s'ajoutent d'autres initiatives. Parmi elles, citons (liste non exhaustive) :

- la CNIL, qui a publié son Guide des Professionnels de santé, afin d'aider les responsables des traitements métiers et les référents sécurité SI à protéger les informations nominatives,
- l'ASIP Santé qui met au point, depuis 2012, un espace de confiance pour messageries sécurisées de santé, réservé à l'ensemble des professionnels de santé (médecins, pharmaciens, chirurgiens-dentistes, sages-femmes, masseurs-kinésithérapeutes, pédicures-podologues, infirmiers),
- l'Association pour la Promotion de la Sécurité des Systèmes d'Information (créée le 9 août 2010 – Journal Officiel N34 du samedi 21 août 2010), ayant comme objectif de promouvoir la sécurité des SIH français et de ses connexions européennes, par le regroupement et la réflexion d'experts.

Les résultats marquants de l'enquête MIPS 2014 du CLUSIF auprès des hôpitaux sont précisés ci-dessous.

La moitié des hôpitaux n'ont toujours pas formalisé leur PSI… Lorsqu'elle existe, l'ISO 2700x (31%) et le guide de l'ANSSI (23%) sont utilisés en priorité comme source d'inspiration.

60% des hôpitaux ont nommé un RSSI ou Référent Sécurité (PHN), or, seulement 17% des répondants à l'enquête ont cette fonction…

Les établissements ont réalisé une analyse de risque dans 60% des cas, en utilisant principalement EBIOS (26%), suivi de l'ISO 27005 (20%) puis MEHARI (15%). Les chartes de sécurité continuent d'augmenter fortement (89%, vs 63% en 2010 et 42% vs 2006). À peine un tiers des établissements ont un programme de sensibilisation à la sécurité de l'information.

L'accès aux outils de messagerie instantanée et aux réseaux sociaux reste globalement interdit (70%).

Les ordinateurs (fixes et portables) maintiennent un niveau de protection très élevé vis-à-vis des risques « classiques » (anti-virus, pare-feu, anti-spam). De leur côté, les équipements mobiles (smartphones et tablettes) ne semble pas être particulièrement pris en compte…

Le recours à l'infogérance stagne (28% partiellement et 3% en totalité, vs respectivement 25% et 1% en 2010), avec un manque de suivi par des audits (70%) ou des indicateurs (66%) !

On observe une forte progression des procédures de création / modification / suppression des comptes utilisateurs nominatifs (43%, + 19 points vs 2010).

Bien qu'elle progresse depuis 2010 (77% 'systématiquement' + 'en partie', vs 59% en 2010), la veille en vulnérabilités n'est pas encore arrivée à un niveau de maturité suffisant pour être systématisée au sein des hôpitaux. Les procédures de gestion des correctifs de sécurité sont en léger recul (43%, vs 47% en 2010) et le développement sécurisé quasi-inexistant (7% ont mis en place des cycles de développement sécurisés).

Seul 10% des hôpitaux dispose d'une cellule de collecte et de traitement des incidents de sécurité dédiée et 44% n'en n'ont toujours pas !

Globalement, les types d'incidents rencontrés par les hôpitaux sont en léger recul par rapport à l'étude 2010, avec comme trio de tête :

- les pannes d'origine interne qui passent de 46% (2010) à 43%,
- les vols qui passent de 44% (2010) à 37%,
- les pertes de services essentiels qui passent de 46% (2010) à 34%.

Du côté du nombre d'incidents d'origine malveillante par an, les « infections par virus » restent en pole position (8,9 incidents de sécurité dus à des virus dans l'année), suivi par les « vols » (5,8) puis les « sabotages physiques ciblées » (4,2).

La gestion de la Continuité d'Activité progresse dans le monde des hôpitaux. Ces derniers traitent en majeur partie l'indisponibilité du SI (65%) et plus d'un hôpital sur deux a pris en compte l'indisponibilité de leurs locaux. La prise en compte des enjeux métier (au travers du BIA) est réalisée dans 41% des cas. Enfin, par rapport à 2010, on constate une très forte baisse en termes de fréquence des exercices et particulièrement pour ceux situés dans la tranche « Jamais » (51% vs 11% en 2010).

Enfin et concernant la conformité, près de 9 établissements sur 10 affirment être conforme (ou en cours de l'être) aux prérequis sécurité d'Hôpital Numérique (fiabilité, disponibilité, confidentialité). Toutefois, à peine la moitié des établissements réalisent au moins un audit par an. Côté tableaux de bord (TBSSI), même si on constate une nette progression (25% vs 7% en 2010), la formalisation de ces derniers reste faible !

Internautes : la menace sur les données personnelles et la vie privée plus que jamais présente avec les nouveaux usages

L'échantillon d'internautes français consultés est constitué de façon à être représentatif de la population française.

En 2014, le taux d'équipement en informatique continue à augmenter dans les foyers (4,6 en moyenne) et l'ordinateur fixe ou portable constitue toujours l'équipement le plus utilisé pour la connexion à Internet au sein des familles françaises avec une préférence pour les ordinateurs portables.

Le wifi continue sa progression (79% vs 74 en 2012) comme mode d'accès au réseau local. À noter toutefois, si 40% des internautes ne se connectent pas en wifi parce qu'ils n'en n'ont pas, 22% ne le font pas pour des raisons de sécurité !

Côté usage, l'ordinateur familial sert aussi bien à des activités professionnelles (41% et 51% des CSP+) et vice-versa (41% et 32% des CSP+). Ce point est également constaté dans le thème « Entreprises ».

On constate une augmentation sensible de l'utilisation d'Internet hors du domicile. En effet, Internet est de plus en plus utilisé sur les lieux de vacances, dans les hôtels, les cyber-cafés (79% vs 70% en 2012).

Le stockage en ligne des données personnelles, bien qu'étant une technologie récente pour le grand public, est déjà utilisé par 38% des internautes.

91% des internautes ont effectué des achats en ligne en 2013 (plus fréquent depuis un ordinateur – 89% - que via un smartphone – 33%) et 4 personnes sur 5 utilisent les réseaux sociaux. Les internautes expriment d'ailleurs clairement certains des facteurs les confortant dans leur démarche de paiement en ligne, tels

que : les sites sécurisés en HTTPS (avec le symbole du cadenas), le mode de paiement (CB virtuelle, code unique, confirmation SMS), le fait d'avoir déjà utilisé le site en question sans problème auparavant. En revanche, un agrément par des organismes indépendants ou la localisation du site sont moins importants.

Du point de vue de la perception et de la sensibilité aux menaces et aux risques, les internautes disent avoir une conscience aigüe des problématiques de sécurité, notamment quant aux risques liés à l'utilisation d'Internet… La vision du risque encouru pour les données augmente ainsi de 29% (2012) à 44% concernant les ordinateurs et de 30% (2012) à 42% concernant les smartphones ou tablettes.

À y regarder de plus près, on constate des écarts notables en fonction des tranches d'âge, un sentiment de risque qui aurait tendance à diminuer grâce à une plus grande confiance dans les outils de sécurité, une perception accrue des risques liés à la vie privée, Internet toujours vu comme un risque pour les mineurs (91% vs 84 en 2012, mais 'seulement' 65% pour les 15-17 ans…).

Pour exemple, 36% des personnes disposant d'un profil sur les réseaux sociaux vérifie les réglages des paramètres de sécurité et de confidentialité.

35% des internautes déclarent avoir subi au moins une perte de données durant ces 24 derniers mois sur leur ordinateur et 25% sur leur smartphone. La panne (27% et 25%, respectivement 'ordinateur' et 'smartphone'), l'erreur de manipulation (27% et 30%) et le virus ou piratage (21% et 15%) restent les trois raisons majeures invoquées lors de la perte de données sur un ordinateur.

Au final, 43% (vs 32% en 2012) des internautes considèrent que les risques auxquels est exposé leur données augmentent.

En termes de comportements et par rapport à l'enquête 2012, les moyens 'classique' restent très utilisés : anti-virus (81%), pare-feu (80%), anti-spyware (77%) et anti-spam (76%).

Certains moyens de protection de l'ordinateur personnel moins 'classique' sont également utilisés. En effet, la sécurisation de la connexion wifi via une clé de chiffrement (77%, idem 2012), la sauvegarde des données sur divers supports (67% vs 69% en 2012) et la mise en place de mots de passe au démarrage des sessions sur l'ordinateur personnel (60% vs 59% en 2012) sont plébiscités par les internautes.

L'automatisation des recherches de mises à jour, voire du téléchargement et de l'installation des correctifs de sécurité, est d'une grande aide et reste largement mise en œuvre malgré une baisse sensible (74% vs 84% en 2012).

Le décalage identifié en 2012 entre les efforts faits en matière de sécurité par les internautes sur leurs équipements, selon qu'il s'agisse d'ordinateurs – plutôt « pas trop mal » gérés - ou des équipements mobiles comme les smartphones et les tablettes tant à diminuer. Pour autant, ces derniers restent moins bien protégés que les ordinateurs… Ceci reste lié au fait que l'existence d'outils de sécurisation sont peu, voire pas, connus des internautes.

A la lumière de ces résultats, on peut considérer que plus les niveaux d'automatisation des opérations de sécurité et des mises à jour seront élevés de la part des éditeurs et des fournisseurs, mieux ce sera pour le niveau de sécurité global des équipements des internautes.

En conclusion…

La menace reprend globalement (légèrement) et notre enquête montre de nouveau que les malveillances et les incidents de sécurité sont bien présents : attaques virales, vols de matériel, accroissement des problèmes de divulgation d'information et attaques logiques ciblées sont toujours au menu !

Pour les entreprises ou les hôpitaux qui n'ont encore « rien commencé », il est plus que jamais nécessaire de mettre en place le « cadre de la SSI ». Pour ceux qui l'ont mis en place, reste à mettre en œuvre et jusqu'au bout des pratiques concrètent et pragmatiques, ancrées dans les processus de la gestion de l'information afin d'assurer leur capital informationnel à leurs enjeux !

Au final, la sécurité de l'information reste un point important des organisations (jusqu'à être mise en avant dans certains secteurs comme un avantage concurrentiel) ; mais elle n'en est pas moins un domaine où il faut laisser du temps au temps. La « quantité » est (presque) là, la « maturité » augmente et la « qualité » est pour bientôt…

Alors, « au boulot » et n'oublions pas « Celui qui déplace une montagne commence par déplacer de petites pierres[2]. » !

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 »

[2] Confucius (551 av. JC - 479 av. JC).

Sommaire

Liste des figures

Méthodologie

L'enquête du CLUSIF sur les menaces informatiques et les pratiques de sécurité en France en 2014 a été réalisée de début janvier à mi-mars 2014, en collaboration avec le cabinet spécialisé GMV Conseil, sur la base de questionnaires d'enquête élaborés par le CLUSIF. Trois cibles ont été retenues pour cette enquête :

- les entreprises de plus de 200 salariés : 350 entreprises de cette catégorie ont répondu à cette enquête,
- les hôpitaux publics : 150 d'entre eux ont accepté de répondre,
- les particuliers internautes : 1009 individus, issus du panel d'internautes de l'institut spécialisé Survey Sampling International, 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 :2005 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 15, sont les suivants :

- thème 5 : Politique de sécurité,
- thème 6 : Organisation de la sécurité et moyens,
- thème 7 : Gestion des actifs et identification des risques,
- thème 8 : Sécurité des ressources humaines (charte, sensibilisation),
- thème 9 : Sécurité physique et environnementale,
- thème 10 : Gestion des communications et des opérations,
- thème 11 : Contrôle des accès,
- thème 12 : Acquisition, développement et maintenance,
- thème 13 : Gestion des incidents de sécurité,
- thème 14 : Gestion de la continuité,
- thème 15 : Conformité (CNIL, audits, tableaux de bord).

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

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

Les réponses aux questions ont été consolidées par GMV Conseil en préservant un total anonymat des informations, puis ont été analysées 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 2014, 2012, 2010 et 2008. 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 2013, 2011, 2009 et 2007.

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 « culture » et de la maturité de chaque entreprise, hôpital public ou internaute.

Entreprises

- Présentation de l'échantillon
- Dépendance à l'informatique des entreprises de plus de 200 salariés
- Moyens consacrés à la sécurité de l'information par les entreprises
- Thème 5 : Politique de sécurité
- Thème 6 : Organisation de la sécurité et moyens
- Thème 7 : La gestion des risques liés à la sécurité des SI
- Thème 8 : Sécurité liée aux Ressources Humaines
- Thème 9 : Sécurité physique
- Thème 10 : Gestion des opérations et des communications
- Thème 11 : Contrôle des accès logiques
- Thème 12 : Acquisition, développement et maintenance
- Thème 13 : Gestion des incidents – Sinistralité
- Thème 14 : Gestion de la continuité d'activité
- Thème 15 : Conformité

Les Entreprises

Présentation de l'échantillon

Pour l'édition 2014 de son enquête, le CLUSIF a repris le même échantillon d'entreprises que celui interrogé en 2012, afin de pouvoir comparer les progrès ou les éventuelles régressions sur les 2 années passées. Ainsi, la cible est constituée des entreprises de plus de 200 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 25 minutes en moyenne), avec un taux d'acceptation d'environ 10% (idem par rapport à 2012 et 2010) : sur 100 entreprises contactées, seulement 10 ont accepté de répondre à nos questions, ce qui a impliqué d'appeler environ 3 500 entreprises ! Ce taux de réponse est relativement faible et témoigne d'une certaine réticence à communiquer sur le thème de la sécurité de l'information…

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, sur la base des données INSEE.

Entreprise Taille / Secteur	200-499 salariés	500-999 salariés	1 000 et plus	Total	Total en %		Données INSEE
Banque - Assurance	26	13	17	**56**	**16,0%**	→	**7%**
Commerce	14	13	14	**41**	**11,7%**	→	**19%**
Industrie - BTP	44	56	26	**126**	**36,0%**	→	**38%**
Services	38	27	25	**90**	**25,7%**	→	**21%**
Transport – Télécoms	16	11	10	**37**	**10,6%**	→	**14%**
Total	**138**	**120**	**92**	**350**	**100,0%**		**100%**
Total en %	**39,4%**	**34,3%**	**26,3%**	**100,0%**		↑ Redressement	
Redressement →	↓	↓	↓				
Données INSEE	**65%**	**19%**	**17%**	**100%**			

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 35% (23% en 2012 et 29% en 2010) des entreprises interrogées, mais à 53% dans les plus de 1 000 salariés (45% en 2012 et 40% en 2010).

Toutes tailles et secteurs confondus, les personnes sondées sont à plus de 91% des DSI (Directeur des Systèmes d'Information), des Directeurs ou Responsables informatiques ou des RSSI (82% en 2012 et 72% en 2010).

Dépendance à l'informatique des entreprises de plus de 200 salariés

Le Système d'Information stratégique pour toutes les entreprises

L'enquête confirme cette année encore que l'informatique est perçue comme stratégique par une très large majorité des entreprises : tous secteurs confondus et quelle que soit leur taille, 77% d'entre elles jugent lourde de conséquences une indisponibilité de moins de 24h de leurs outils informatiques (avec un maximum de 95% pour le secteur de la Banque – Assurance).

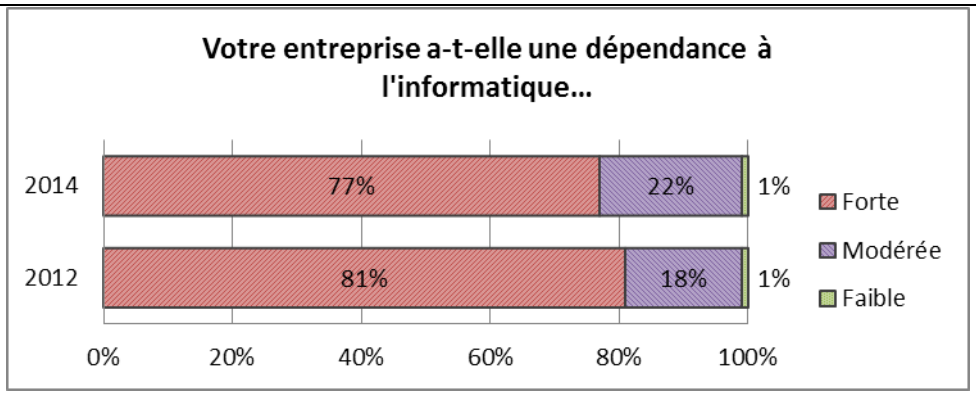

Figure 1 - Dépendance des entreprises à l'informatique

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

Un budget informatique moyen à 3,3 millions €

Le budget informatique annuel moyen est de 3,3 millions d'euros. Seul 46% des sondés ont répondus à cette question, ils étaient 42% en 2012 et 51% en 2010.

On constate que 65% ont un budget inférieur à 1 million d'euro (64% en 2012), 13% entre 1 et 2 millions (18% en 2012), 15% entre 2 et 5 millions (13% en 2012) et enfin 7% au-dessus de 5 millions jusqu'à un maximum de 120 millions (5% en 2012 avec un maximum de 40 millions).

Un budget sécurité dont le périmètre est un peu mieux cerné…

Bien que les RSSI aient encore du mal à cerner le budget qui leur est attribué par rapport au budget informatique total, ce flou diminue entre 2012 et 2014, en passant de 36% en 2012 à 25% cette année.

Tout comme en 2012, lorsque le budget est clairement identifié, la répartition est hétérogène.

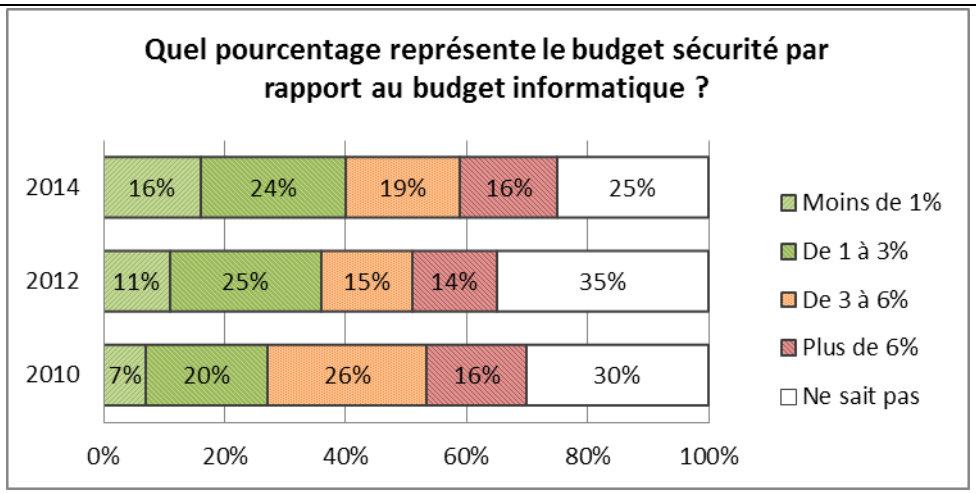

Figure 2 - Part du budget informatique alloué à la sécurité dans les entreprises

Une légère reprise des budgets sécurité

Globalement, le pourcentage des budgets « constants » diminue (54% contre 64% en 2012) tandis que 27% des budgets sont en augmentation forte ou moyenne (22% en 2012).

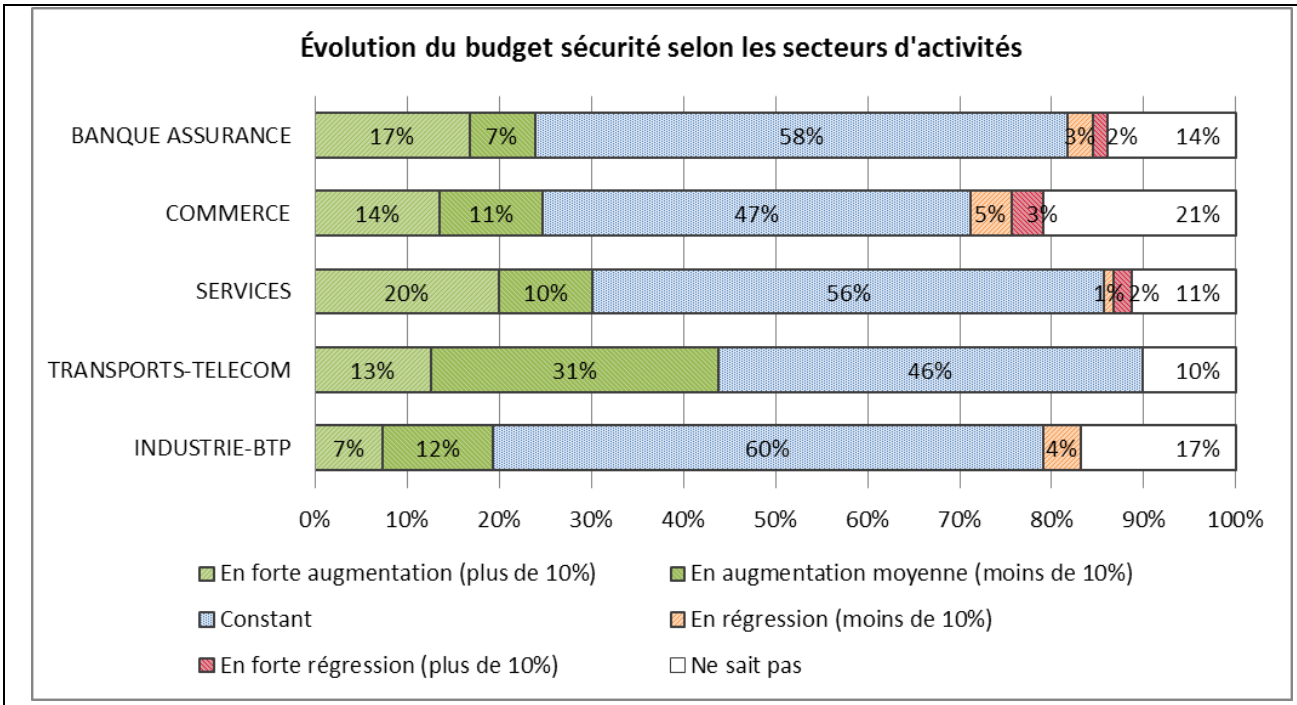

Figure 3 - Évolution du budget sécurité selon les secteurs d'activités

Toutefois, on constate que le poste ayant eu la plus grosse augmentation est une fois de plus la mise en place de solution, avec 26% (37% en 2012). On reste toujours dans la technique, pour beaucoup la sécurité reste une histoire de mise en place de solution(s) technique(s)…

Les contraintes organisationnelles et le budget freinent le RSSI

Enfin, lorsque l'on cherche à connaître les freins à la conduite des missions de sécurité dans leur entreprise, les RSSI citent par ordre d'importance décroissante :

- 1ère raison citée (34%, idem vs 2012) : le manque de budget,
- 2ème raison citée (25%, +11 points vs 2012) : le manque de connaissance,
- 3ème raison citée (22%, -7 points vs 2012) : les contraintes organisationnelles,
- 4ème raison citée (19%, -1 point vs 2012) : la réticence de la Direction Générale, des 'métiers' ou des utilisateurs,
- 5ème raison citée (16%, -5 points vs 2012) : le manque de personnel qualifié.

Le premier frein principal reste, comme en 2012, le manque de moyens budgétaires.

Le manque de connaissance passe de la cinquième (2012) à la seconde place, signe d'une certaine maturité en augmentation et liée à la croissance continue du nombre de RSSI (voir le Thème 6 ci-après).

Encore au chapitre des bonnes nouvelles, la réticence de la Direction des Systèmes d'Information reste hors du top 5 (2% seulement, idem qu'en 2012).

En fin, le manque de personnel qualifié reste dans le top 5, signe d'une continuelle agitation du marché de l'emploi dans le secteur de la SSI, comme le montre le toujours haut niveau du nombre d'offres d'embauches…

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

Stagnation de la formalisation et confirmation de son importance

Le nombre d'entreprises ayant formalisé leur PSI est quasi-inchangé depuis 4 ans (64% cette année pour 63% en 2012 et 2010). De plus, cette politique est globalement à jour dans la mesure où 85% des entreprises interrogées l'ont actualisé il y a moins de trois ans.

La PSI des entreprises reste massivement soutenue par la Direction Générale pour près de 93% des entreprises répondantes (idem 2012).

Retour de l'implication de la DSI… au déficit de la DG et du RSSI !

Alors que la PSI impacte l'ensemble de l'entreprise, certaines Directions ne s'y intéressent que de loin… Les Directions des Systèmes d'Information reprennent timidement la main (54%) face aux Directions Générales (50%), alors que le RSSI n'est toujours qu'en troisième position (39%)…

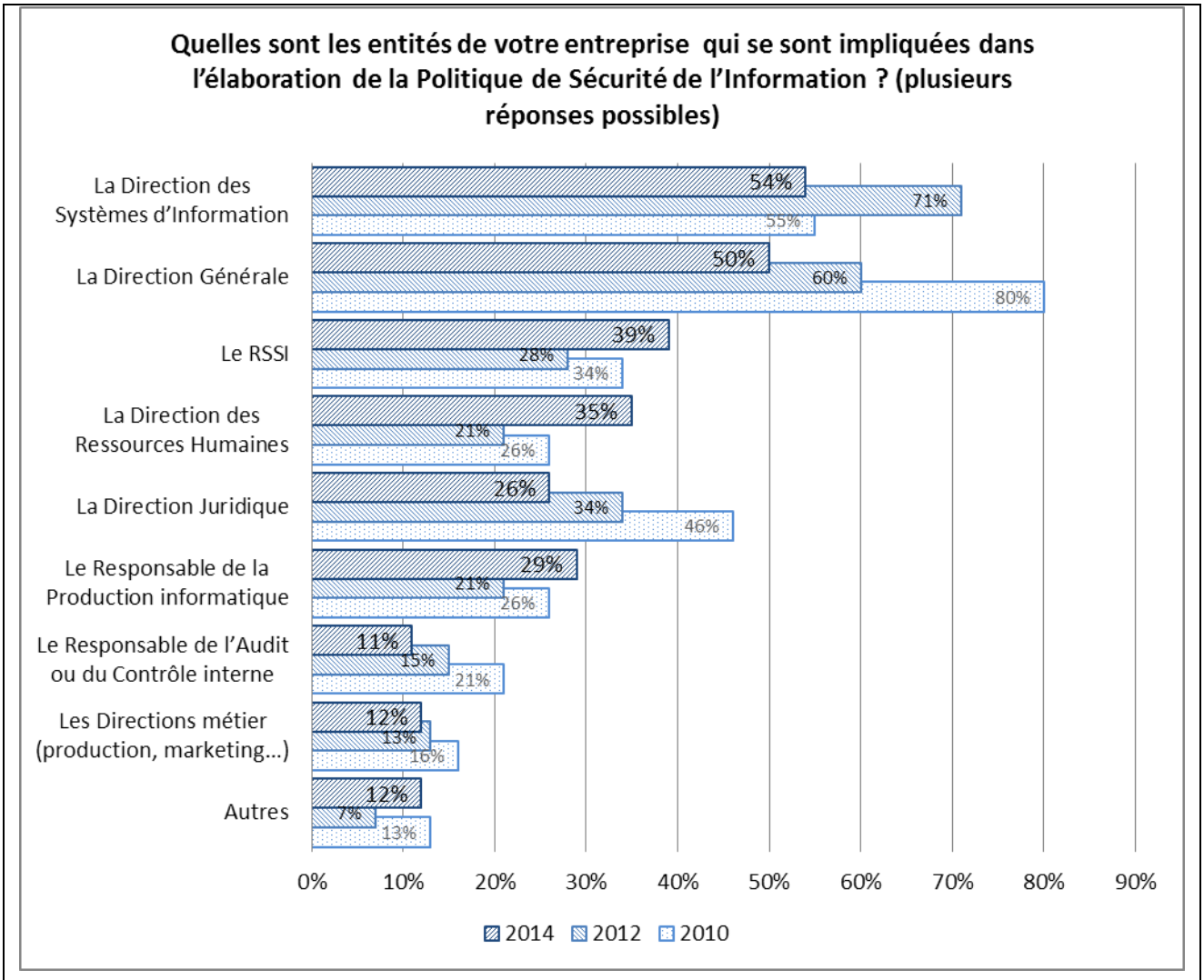

Figure 4 - Implication des différentes entités à la PSI

Les normes de sécurité poursuivent leur influence grandissante sur la Politique de Sécurité de l'Information (PSI) des entreprises, passant de 55% en 2010 à 75% en 2012 et à 79% en 2014.

La position des référentiels internes est en légère régression (16% vs 20% en 2012) ; pour autant l'influence de ces référentiels internes se confirme et semble être liée à la montée en puissance en France des exigences portées par les impératifs de contrôle interne.

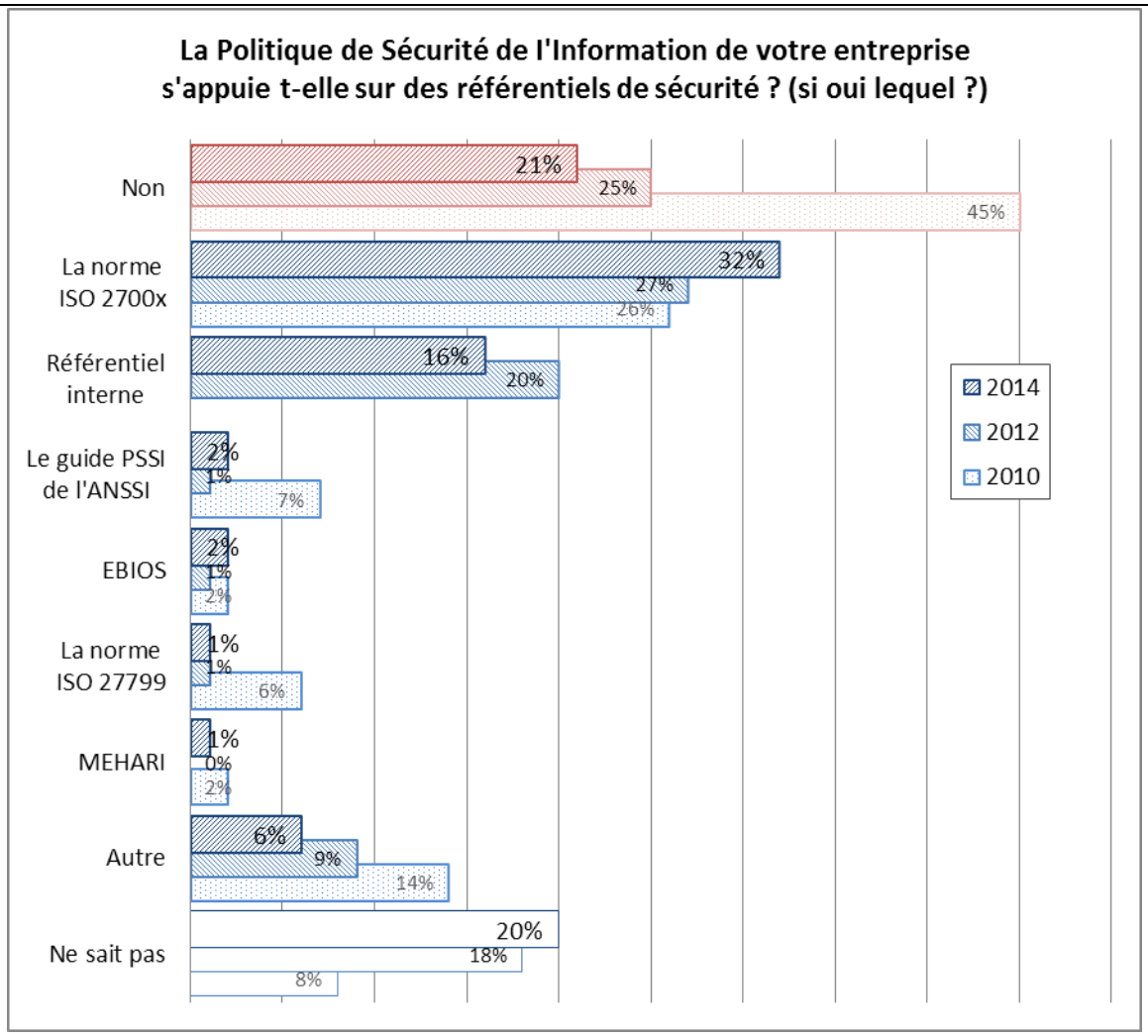

Figure 5 - Référentiels utilisés pour la formalisation de la PSI

Enfin, plusieurs référentiels apparaissent désormais d'usage marginal, tels que le guide PSSI de l'ANSSI, l'ISO 27799, EBIOS et Méhari (ces deux dernières restant avant tout des méthodes d'analyse des risques). Au global, on aboutit à une consolidation du paysage des référentiels, centré autour d'ISO 2700x et de référentiels internes, plus adaptés aux contextes des entreprises.

La PSI est communiquée à tous les acteurs du SI dans 75% des entreprises.

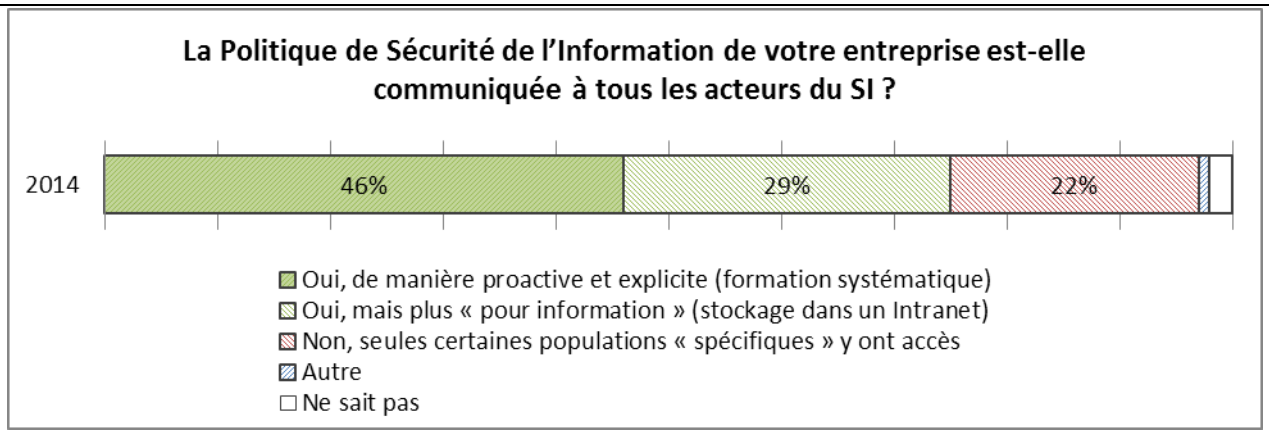

Figure 6 - Diffusion de la PSI au sein des entreprises

Thème 6 : Organisation de la sécurité et moyens

Une fonction RSSI qui continue de croître

La fonction de Responsable de la Sécurité des Systèmes d'Information (RSSI ou RSI) est de plus en plus clairement identifiée et attribuée au sein des entreprises, ce qui va dans le sens de l'histoire… La croissance est remarquable, passant de 37% (2008) à 62% (2014), soit une croissance de 168% en 6 ans !

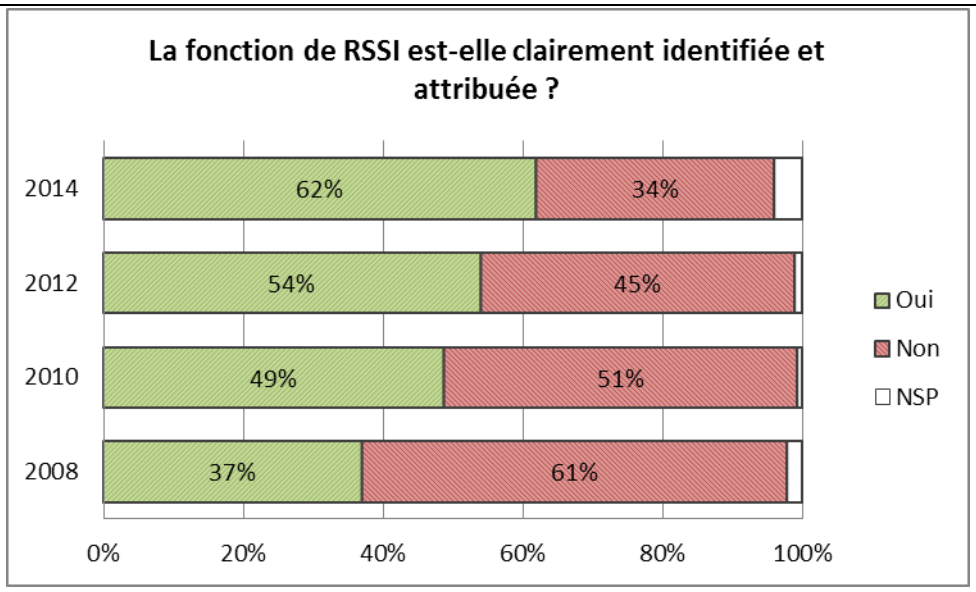

Figure 7 - Attribution de la fonction RSSI

Seuls 47% des RSSI sont dédiés à cette tâche à temps plein (vs 63% en 2012), avec toutefois des disparités fortes en fonction des secteurs d'activités (33% dans les Services pour près de 62% dans la Banque – Assurance).

Lorsque le RSSI n'existe pas, cette mission reste fortement attachée à la Direction des Systèmes d'Information.

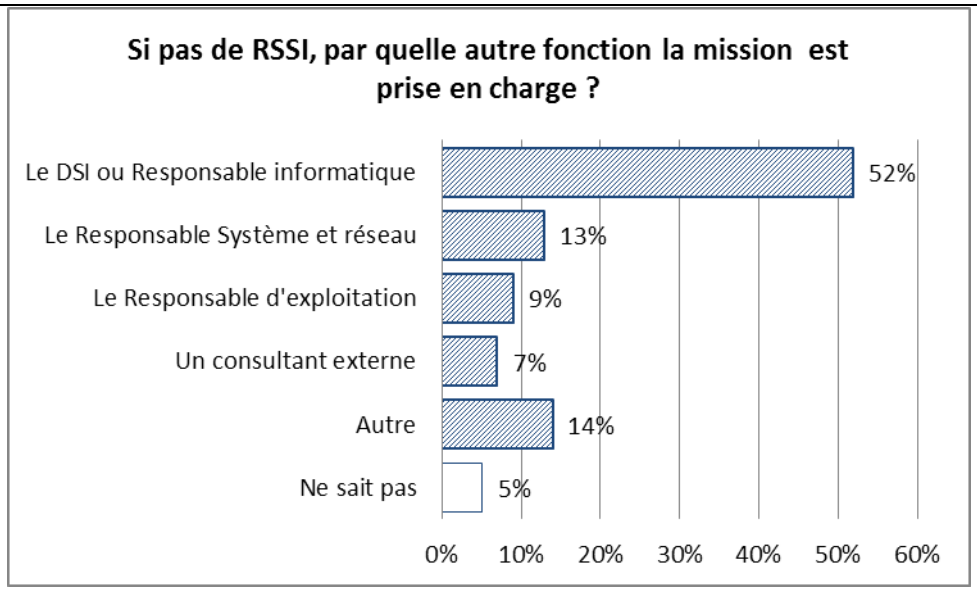

Figure 8 - Prise en charge de la fonction RSSI, lorsqu'il n'existe pas de RSSI

Un rattachement encore en perpétuelle évolution…

Le RSI ou RSSI est soit rattaché à la DSI (46%), soit à la Direction Administrative et Financière (DAF) (8%) ou directement à la Direction Générale pour 27% (-5 points vs 2012) des entreprises interviewées. Ceci s'explique encore par les arrivées plus nombreuses de RSSI au sein d'entreprises de tailles moyennes, provenant très souvent de la DSI et ayant un niveau de maturité en Sécurité des SI encore faible.

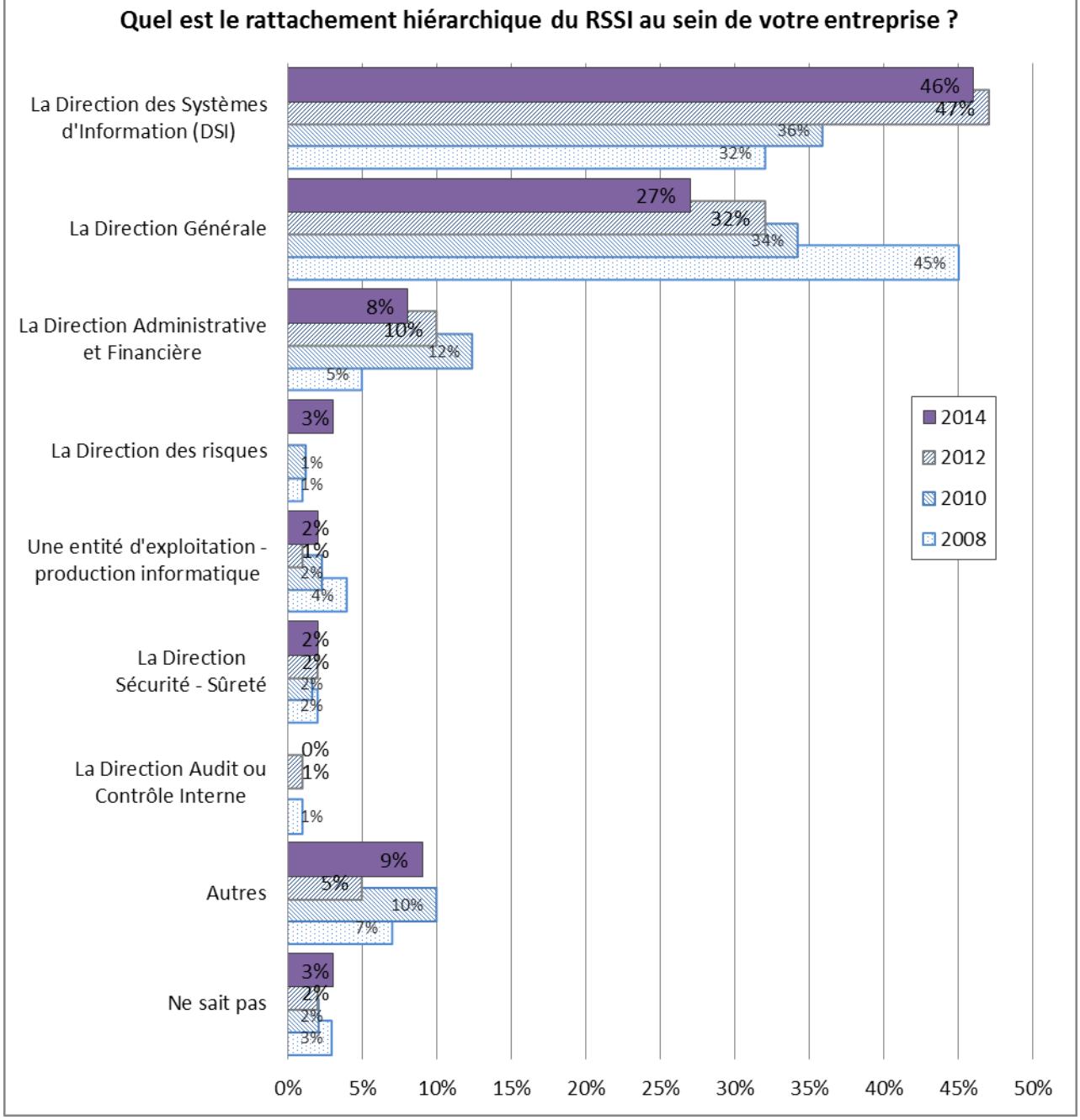

Figure 9 - Rattachement hiérarchique du RSSI au sein de l'entreprise

Globalement, la répartition des tâches du RSSI n'a que très peu évolué depuis 2010. On note toutefois que les aspects 'communication' et 'juridique' augmentent légèrement, représentant 31% à eux deux au lieu de 24% en 2012. Ce sont les aspects opérationnels qui diminuent le plus fortement (-7 points vs 2010).

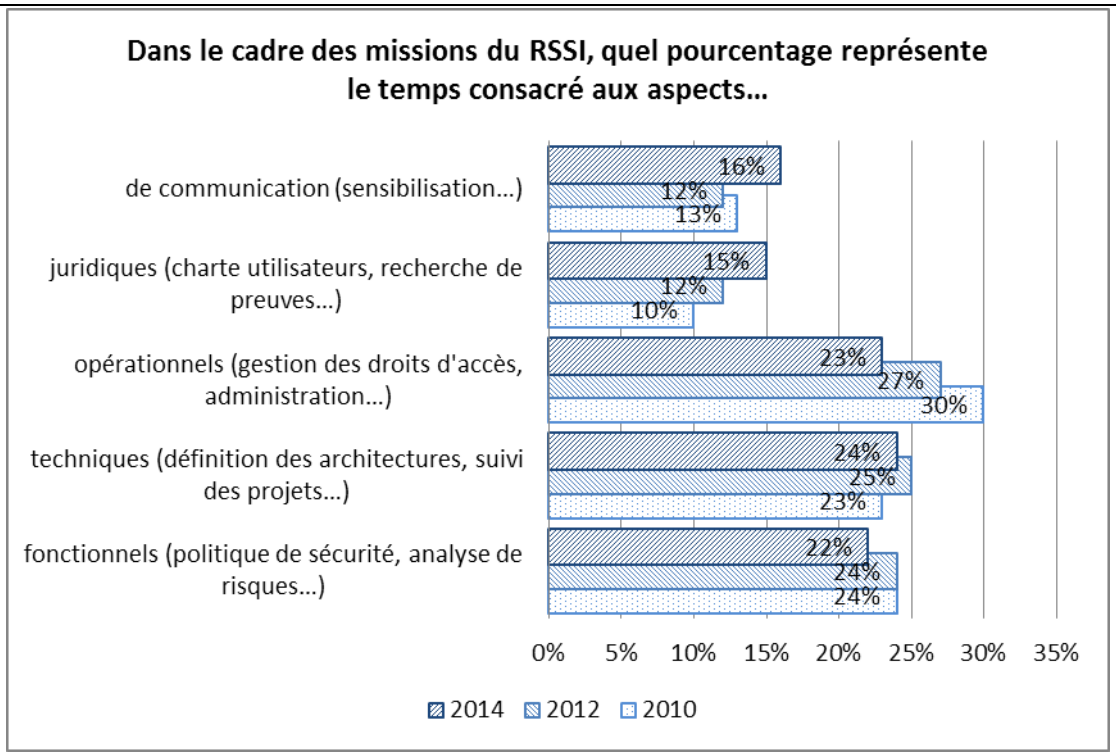

Figure 10 - Répartition des missions du RSSI

97% des entreprises ont en permanence une équipe sécurité (elles étaient 100% en 2012 !). Toutefois, dans 27% le RSSI (ou son équivalent) est 'partagé' et dans 43% des cas il est encore un homme ou une femme seul(e) ou en binôme seulement !

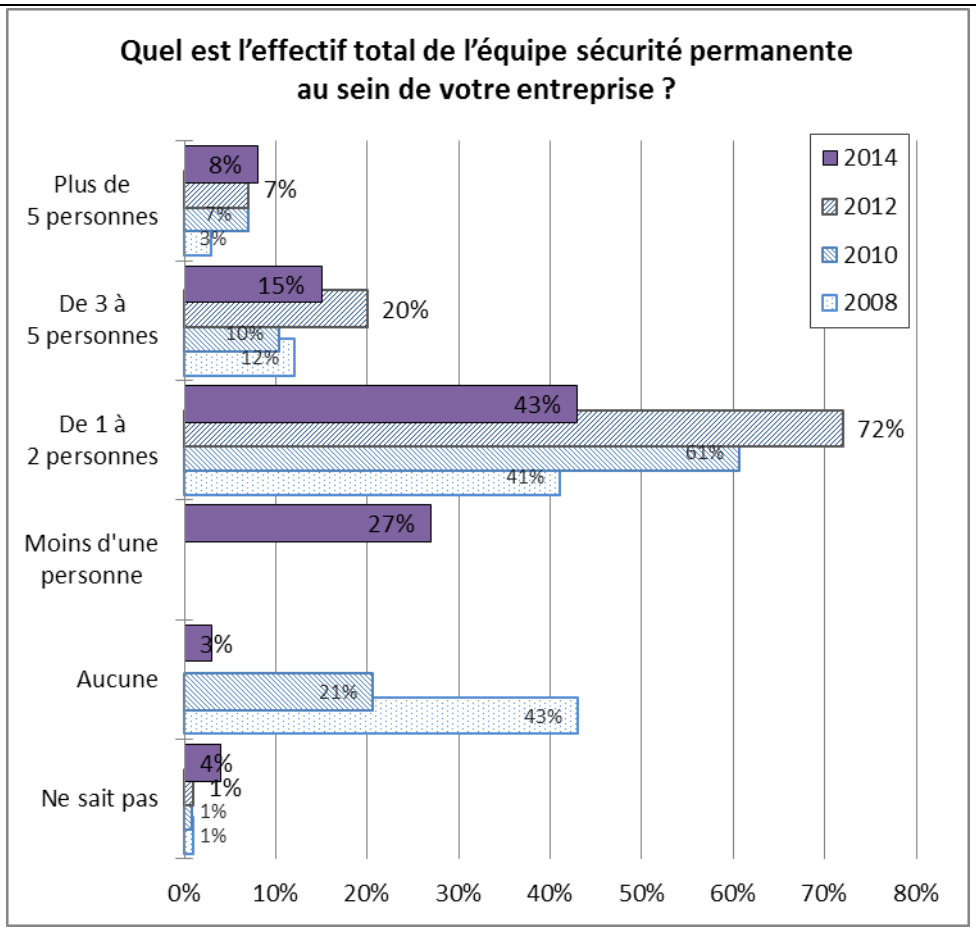

Figure 11 - Effectif total de l'équipe sécurité permanente au sein de l'entreprise

Thème 7 : La gestion des risques liés à la sécurité des SI

Inventaire et classification des informations : légère avancée en deux ans

Le nombre d'entreprises réalisant l'inventaire (66% vs 59% en 2012) de leur patrimoine informationnel et/ou la classification des informations (66% vs 56% en 2012) est en légère augmentation depuis 2012. Assez souvent ces deux thèmes sont traités simultanément, ce que reflètent bien les résultats de l'enquête.

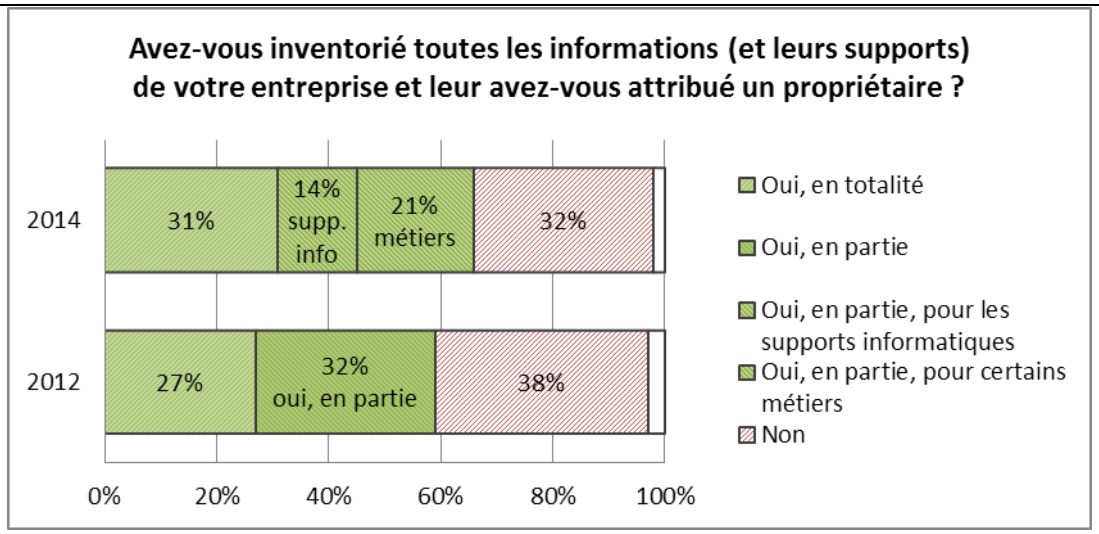

Figure 12 – Inventaire et attribution d'un propriétaire des informations de l'entreprise

L'objectif de la classification est d'identifier les informations et/ou processus les plus sensibles et les biens supports associés. Les entreprises la réalisant ont conscience du patrimoine qui participe à leur pérennité et ont, à priori, les éléments discriminants pour faire le choix des mesures de sécurité les mieux adaptées à leur contexte. Le nombre de niveaux de sensibilité des informations est majoritairement fixé à 3, pour 47% des entreprises.

Pour les 31% de sociétés qui n'ont pas réalisé de classification de leurs informations, la question se pose de savoir sur quels critères elles définissent le niveau des dispositifs de sécurité à déployer ? Dans cette catégorie, 36% des sociétés des secteurs d'activités 'Services' et 'Commerce' n'ont engagé aucune démarche de classification de leurs informations…

Reste que, si l'on considère qu'une classification partielle laisse « des trous dans la raquette », cela signifie que 69% des entreprises ne peuvent dire avec précision sur quel périmètre et avec quelle priorité il est indispensable de déployer des outils, d'augmenter les contrôles ou de renforcer les actions de sensibilisation… Il peut être intéressant de rapprocher ce chiffre du facteur n°1 de frein à la conduite de missions sécurité qui est le budget : est-ce que les RSSI (ou équivalent) utilisent des arguments suffisamment convaincants dans leur communication vis-à-vis du décideur budgétaire ou sont-ce les décideurs qui font la sourde oreille en n'étant pas réceptifs aux arguments des RSSI ?…

L'analyse des risques en légère régression…

Les entreprises ont pris la mesure de la nécessité d'avoir une vision plus large de leurs risques, elles sont, en 2014, 21% (+2 points vs 2012) à réaliser une analyse formelle sur l'ensemble de leur SI.

Le nombre d'entreprises (dont majoritairement le commerce et l'industrie) n'utilisant pas de méthodes ou de référentiels formels est en légère augmentation à 47%. Alors que cette proportion était passée de 60% en 2010 à 45% en 2012, donc nous arrivons à une légère stagnation.

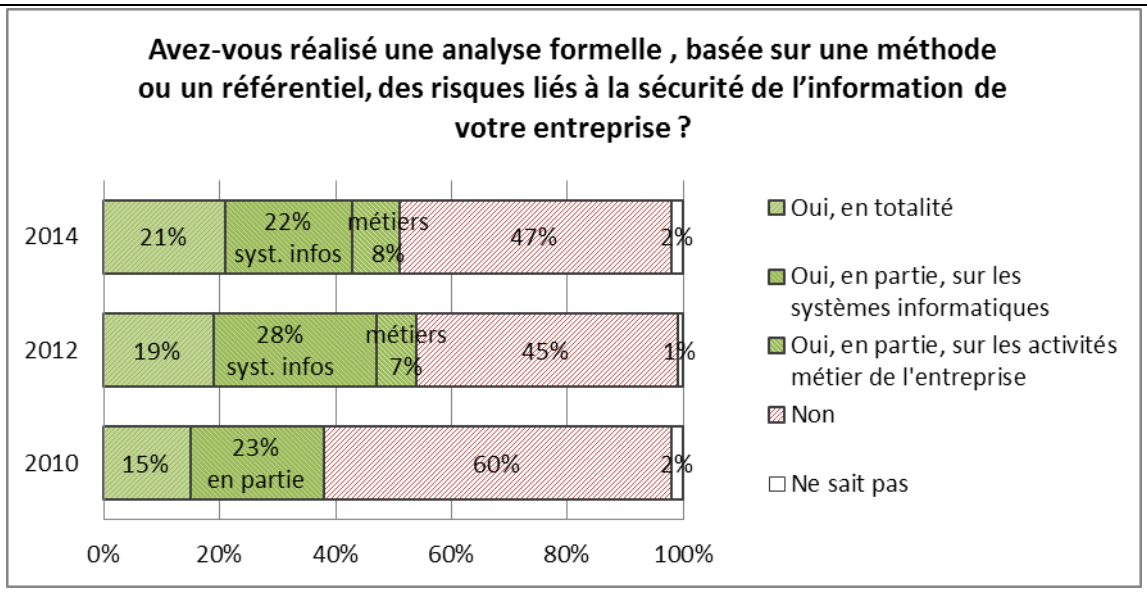

Figure 13 : Utilisation d'une méthode ou un référentiel pour réaliser l'analyse des risques

La taille de l'entreprise ne semble pas être un élément limitant la démarche, parmi les entreprises ayant réalisé en totalité une analyse nous trouvons :

- 20% des entreprises de 200 à 499 collaborateurs,
- 25% des entreprises de 500 à 999 collaborateurs,
- 26% des entreprises de plus de 1 000 collaborateurs.

Quand l'entreprise utilise une démarche formelle d'analyse de risques sur l'ensemble du périmètre du SI, elle utilise majoritairement ces résultats au profit de l'amélioration de sa sécurité. Une meilleure vision des circonstances des risques amène souvent, voire toujours, une meilleure compréhension des mesures de sécurité nécessaires à l'atteinte des objectifs identifiés lors de l'analyse.

Les entreprises n'utilisant pas les résultats de leur analyse de risques pour améliorer leur sécurité est en diminution, 16% en 2014. Signe encourageant, qui montre peut-être que les entreprises capitalisent sur leurs travaux d'analyse de risques. Le seul fait de réaliser une analyse de risques pour être conforme à un cadre ou un règlement n'est sans doute plus l'approche unique de l'entreprise.

Quel que soit le secteur d'activité, le RSSI reste leader dans la démarche de l'analyse des risques. Il est surprenant que malgré les progrès fait entre 2010 et 2012 sur la prise de possession de la démarche par les métiers que celle-ci ai aujourd'hui régressée de 20% (2012) à 15% (2014). Est-ce là un signe de maturité dans la démarche au sein de l'entreprise ? Un indicateur qui témoigne que nous sommes entrés dans une logique d'appropriation de la gestion des risques au-delà de leur seule analyse qui n'implique du coup moins les métiers, et plus les opérationnels dans la gestion des risques.

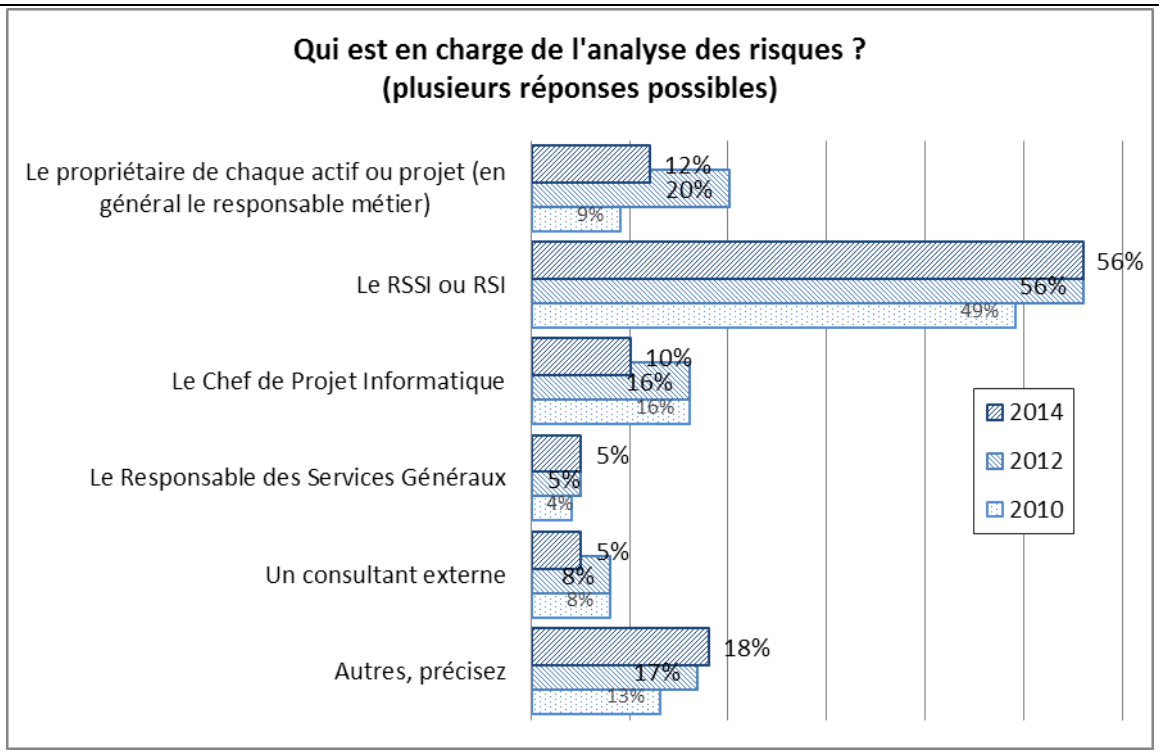

Figure 14 : Responsable de la conduite de l'analyse de risques

La qualité des méthodes d'analyse de risques ou des cadres méthodologiques de gestion des risques est restée stable. Il est intéressant de noter une forte progression de l'utilisation de la méthode EBIOS, si les entreprises citaient pour 7% d'entre-elles l'utilisation d'EBIOS en 2010, elles sont aujourd'hui 15% à utiliser la méthode. Ceci principalement dans les secteurs de la Banque-Assurance, des Services et de l'Industrie-BTP.

Il faut voir sans doute ici les effets des cadres réglementaires comme le RGS (ou la méthode CNIL) qui sous-tendent l'usage de cette méthodologie ; y compris peut-être pour des entreprises non soumises au respect de réglementation comme le RGS.

Il est à noter que le cumul fait 104%, cela laisse donc entendre que les entreprises utilisent, pour certaines d'entre-elles, plusieurs méthodes. Sans doute une adaptation des méthodes historiques en France que sont MEHARI et EBIOS avec le cadre méthodologique de la gestion des risques de l'ISO/IEC 27005. En remarque libre, les personnes interviewées ont souvent évoqué la question de l'usage de « méthodes sur la base de MEHARI ».

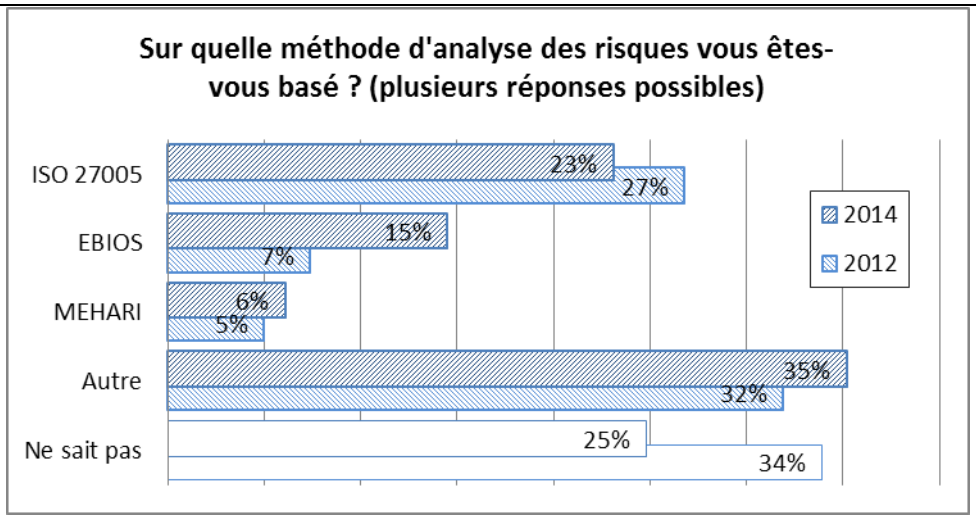

Figure 15 : Répartition des méthodes utilisée

Thème 8 : Sécurité liée aux Ressources Humaines

Les chartes d'utilisation du SI en constante progression depuis 2010

Elles gagnent encore 5 points en 2014, ce qui est très logique par rapport à la multiplicité actuelle des usages et aux possibilités de plus en plus étendues de coupler usages professionnels et personnels.

Ces chartes ont été soumises aux Instances Représentatives du Personnel (IRP) à 77%, en forte régression de 14% par rapport à 2012. Il est vrai qu'elles ne sont soumises que pour avis, sans nécessiter un accord. La charte peut, en tout état de cause, être intégrée au Règlement Intérieur et faire l'objet des formalités administratives nécessaires (greffe du conseil de prud'hommes et Inspection du Travail). Elle est ainsi opposable aux tiers sans obligation de la faire signer par chaque salarié.

Chartes fournisseurs : le déploiement

Une nouvelle question en 2014 prend en compte la situation des fournisseurs et prestataires intervenant pour un client et des engagements qu'ils doivent respecter. Les incidents majeurs de grandes entreprises qui ont eu lieu notamment dans le domaine du Cloud ne sont certainement pas étrangers à ce processus…

La nouvelle version de la norme ISO/IEC 27001:2013 consacre un chapitre sur les fournisseurs et les contrôles que doit mettre en œuvre une entité afin de s'assurer de ne pas créer de brèches dans son management de la sécurité ; ainsi, ces chartes devraient continuer à se développer.

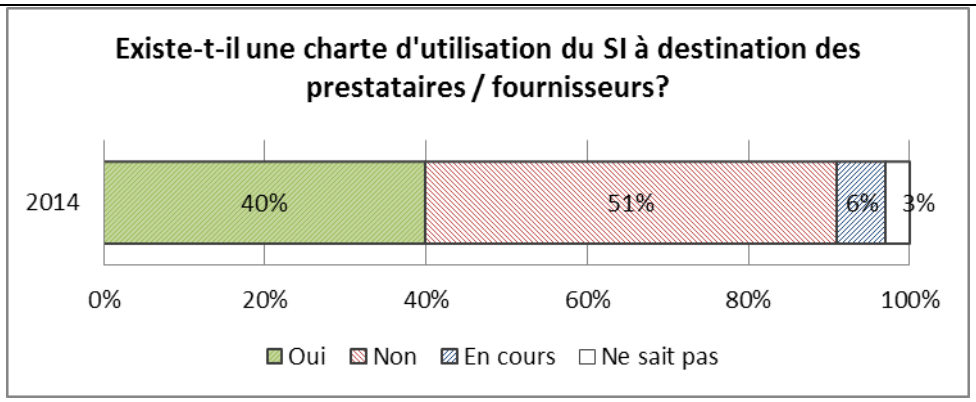

Figure 16 : Charte d'utilisation du SI à destination des prestataires et fournisseurs

Toutefois, il faut bien garder à l'esprit que ce document doit être annexé au contrat du fournisseur si l'on souhaite qu'il ait la même valeur juridique et soit opposable en cas de différent.

Calme plat sur la sensibilisation, à l'exception des VIP

Aucun changement significatif ne marque la sensibilisation, ni sur les programmes déployés, ni sur les moyens engagés, ni sur le suivi qui en est fait. Ce sont toujours les publications sur l'Intranet, par mail ou par affiches qui arrivent en tête. Elles sont privilégiées à 60% par les Transports et le Commerce.

Seule bonne nouvelle, la sensibilisation des VIP passe de 18% en 2012 à 31% en 2014. Est-ce un effet d'onde de choc suite aux révélations sur le programme PRISM ? Gageons qu'il s'agit d'une vraie prise de conscience de la valeur des informations par ceux qui doivent impulser et soutenir les actions de sécurisation.

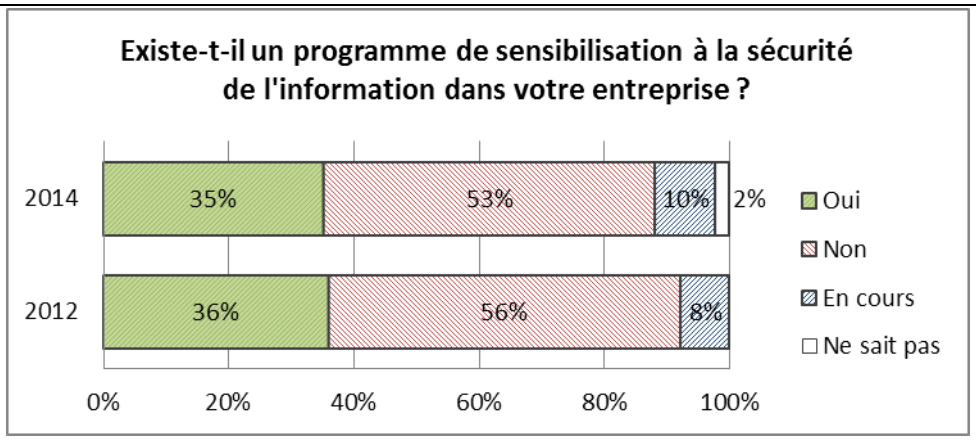

Figure 17 : Programme de sensibilisation à la sécurité de l'information

Gestion des mouvements des collaborateurs et des droits d'accès

La question suivante apporte une réponse qui pourrait sembler assez satisfaisante… Toutefois, il est intéressant de la mettre en perspective avec une des questions posées au chapitre 11 sur le contrôle d'accès logique, lorsque seulement 66% des entreprises déclarent avoir *une procédure formelle de création, modification et suppression de comptes utilisateurs nominatifs*.

Faut-il interpréter ce résultat comme une suppression des droits d'accès sans suppression des comptes, cela étant possible ?

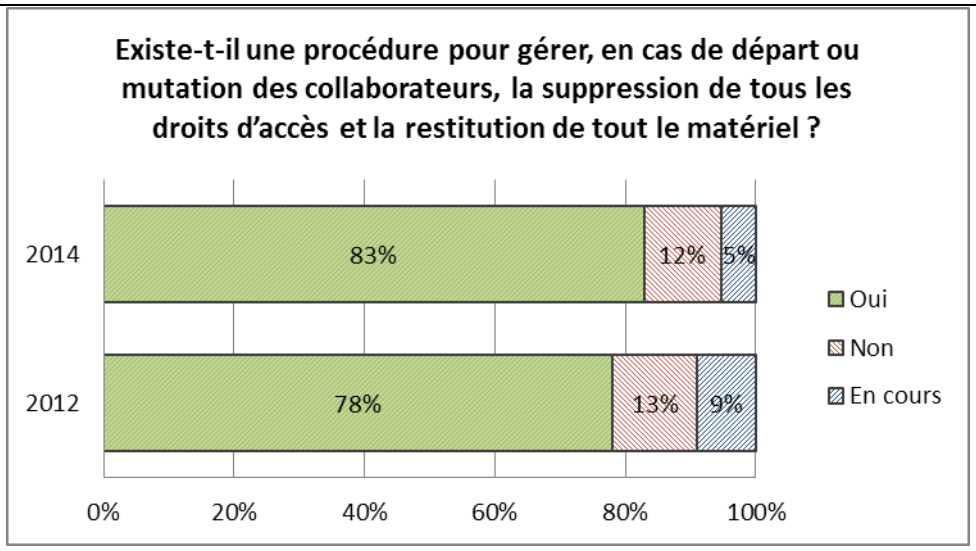

Figure 18 : Existence d'une procédure de suppression des accès et de restitution du matériel

Thème 9 : Gestion de la sécurité physique

Peut mieux faire…

Certes, en moyenne, une grande majorité des entreprises interrogées (70%) veillent à la protection des supports physiques (bandes, CD, papiers, etc.) dans le cadre de leur PSSI. Toutefois, on constate une disparité des pratiques entre les entreprises du secteur du Commerce et des Services comparées à celles des secteurs financiers et de l'industrie qui gèrent de manière plus efficace la sécurité physique de leurs données.

Par ailleurs, près du quart des entreprises en moyenne ne prennent pas en compte la protection physique de leurs données. Pourtant, cette vulnérabilité mériterait d'être systématiquement prise en compte dans la politique de sécurité des organisations.

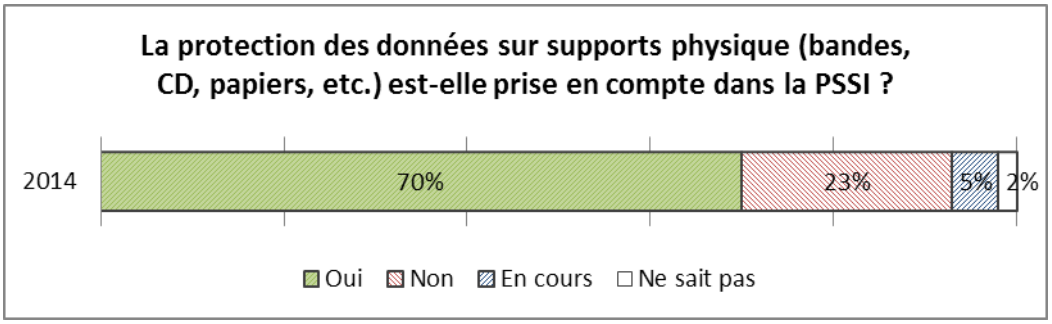

Figure 19 : Pourcentage d'entreprises prenant en compte la protection physique des données dans le cadre de leur PSSI

Un dispositif de contrôle d'accès par badge dans près d'un cas sur deux

Lorsqu'il existe, le dispositif de contrôle d'accès à la salle machine se fait par badge dans près de la moitié des cas (44%). En revanche seule une petite minorité dispose d'un contrôle à unicité de passage de type sas (2%).

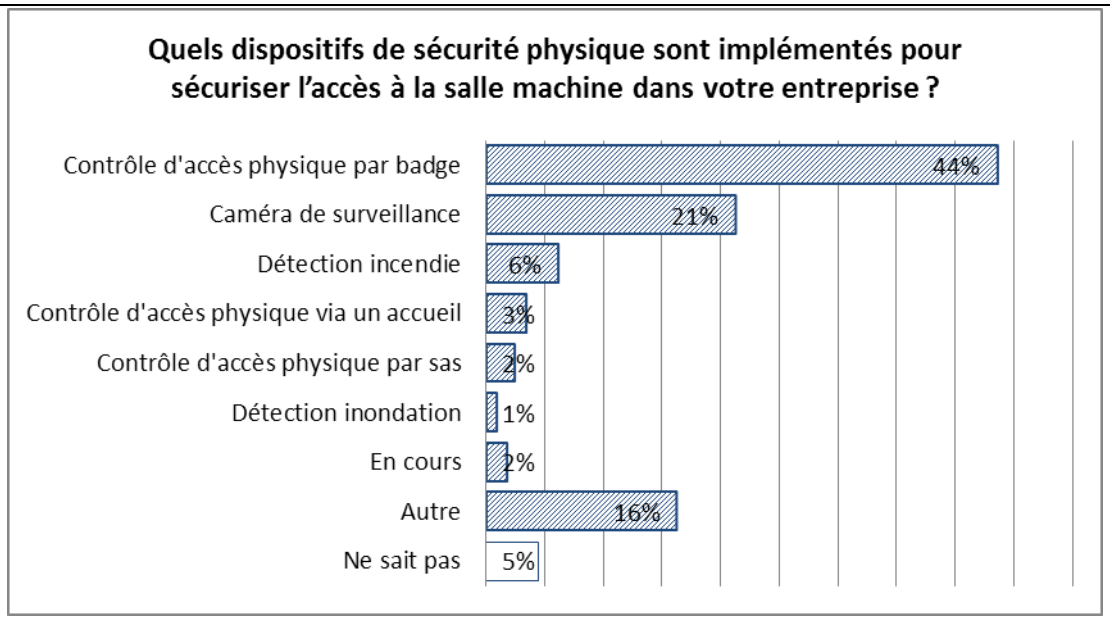

Figure 20 : Dispositifs de sécurité physique pour sécuriser l'accès à la salle machine

Thème 10 : Gestion des communications et des opérations

Ce thème aborde les éléments liés à la gestion des opérations et des communications sous 3 aspects :

- la sécurisation des nouvelles technologies,
- les technologies de protection et de gestion des vulnérabilités,
- l'infogérance.

Sécurisation des nouvelles technologies

La position des politiques de sécurité concernant l'accès au SI par des postes nomades contrôlés ou non contrôlés a peu évolué depuis 2 ans. En revanche, on note une évolution importante (environ 10%) en faveur de l'accès par un réseau privé wifi au sein de l'entreprise contrôlé ou non.

L'enquête de 2012 ne faisait pas de distinction entre les tablettes et smartphones distribués par l'entreprise et ceux du salarié (BYOD). L'enquête de 2014 fait apparaître clairement le rejet du BYOD par les entreprises.

La position concernant la voix sur IP ou la téléphonie IP n'a pas évolué. Les messageries instantanées sont mieux acceptées qu'en 2012 (environ 10%), de même que l'utilisation des réseaux sociaux dans la même proportion.

L'accès à l'Internet est majoritairement filtré (cette question n'était pas posée en 2012).

Les chiffres sont à peu près répartis de façon similaire pour tous les secteurs bien que les secteurs du Commerce et de la Banque semblent plus ouverts aux nouvelles technologies.

Figure 21 : Quel est votre politique d'accès au SI de l'entreprise ?

Technologies de protection et de gestion des vulnérabilités

Ce secteur est globalement stable, montrant que ces technologies évoluent peu au sein des entreprises. Certaines d'entre elles sont même en légère diminution tendant à prouver que les utilisateurs ne sont pas prêts à en supporter les contraintes.

Alors que les PC portables sont systématiquement équipés d'anti-virus et d'anti-malware, les smartphones et tablettes ne sont pratiquement pas traités bien que leur nombre augmente. On constate la même tendance concernant les pare-feu sur PC portables comparés aux pare-feu sur smartphones et tablettes.

Des outils complexes à déployer encore peu intégrés…

Le nombre de sondes IDS/IPS est pratiquement stable depuis la dernière enquête. Les outils de contrôle des périphériques sont en régression par rapport à la précédente enquête, le NAC (*Network Access Control*) est stable, les outils de DLP (*Data Leak Protection*) sont en régression et le nombre de SIEM (*Security Information and Event Management*) augmente très faiblement.

Tous ces outils, bien que globalement matures, restent complexes et couteux à déployer, ce qui peut expliquer leur faible pénétration au sein des entreprises…

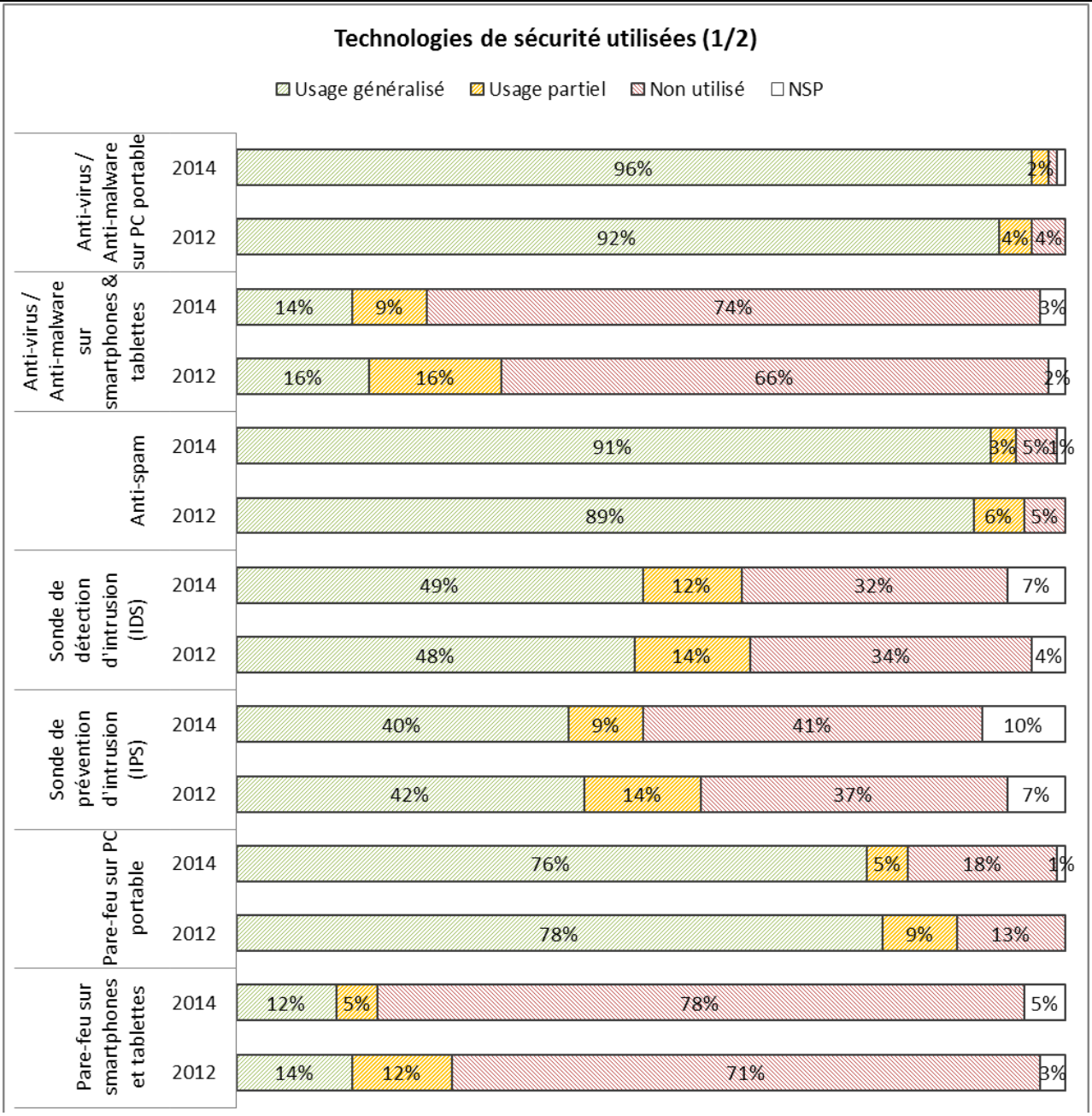

Figure 22 : Technologies de sécurité utilisée (1/2)

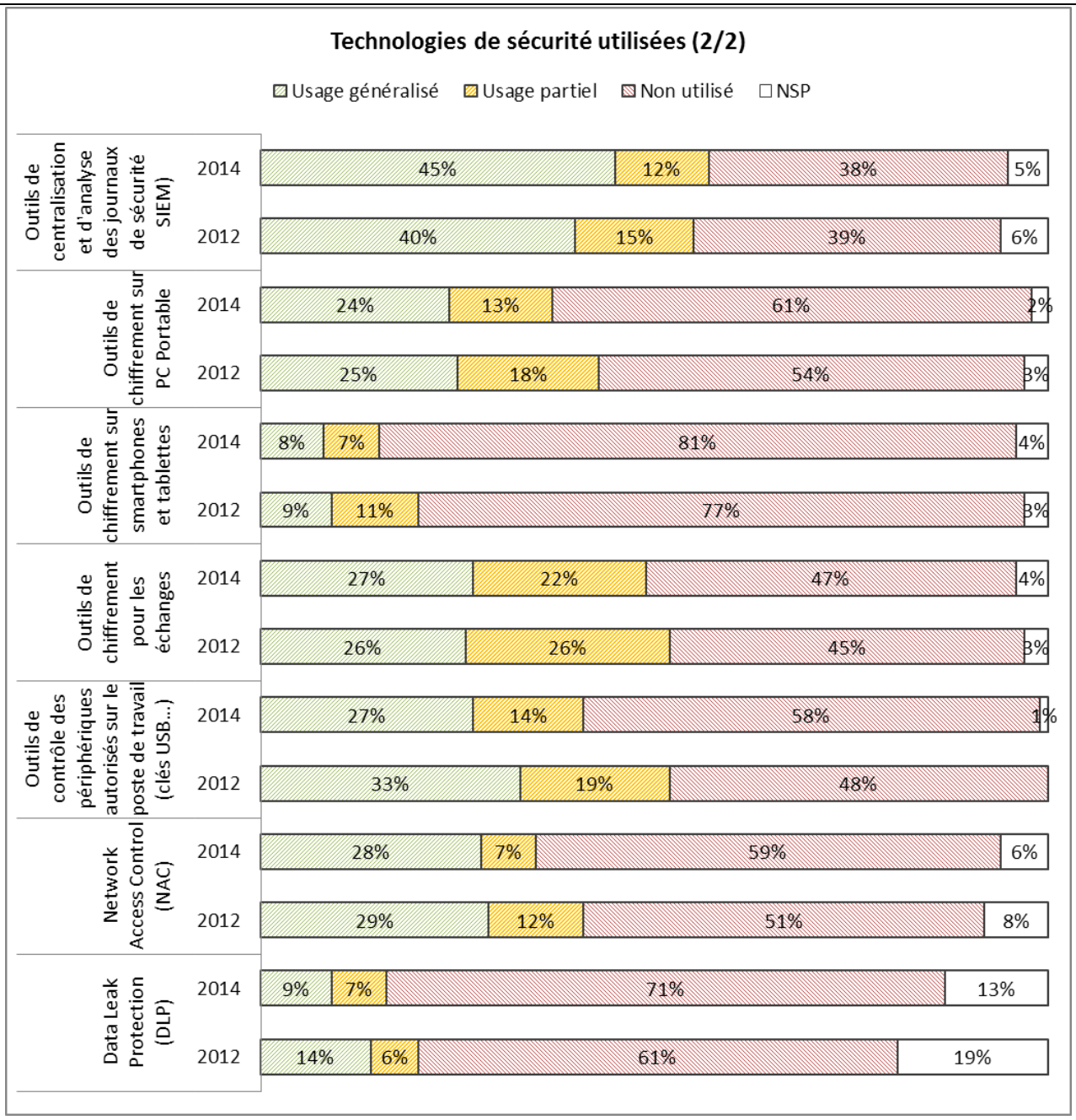

Figure 23 : Technologies de sécurité utilisée (2/2)

Le chiffrement encore peu utilisé…

Les outils de chiffrement sur PC portables ne sont utilisés que par un tiers des entreprises et leur nombre n'évolue pas. Les outils de chiffrement sur smartphones et tablettes sont encore deux fois moins utilisés et leur nombre est en régression. Les outils de chiffrement pour les échanges sont utilisés par 50% des entreprises.

Infogérance

La part de l'infogérance a globalement augmenté depuis la dernière enquête pour atteindre 50% des entreprises.

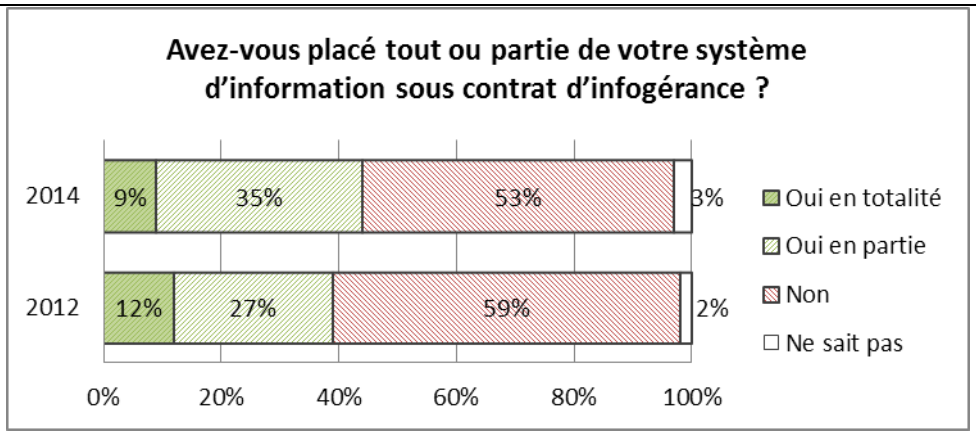

Figure 24 : Part des SI sous contrat d'infogérance

De même, le suivi de l'infogérance est aussi en progression puisque deux tiers des entreprises qui mettent leur SI sous contrat d'infogérance suivent les indicateurs sécurité alors que les audits de sécurité sont eux en diminution de10%. Ceci confirme l'influence de la diminution des budgets à moins que les entreprises soient pleinement rassurées sur les contrats qu'elles ont signés…

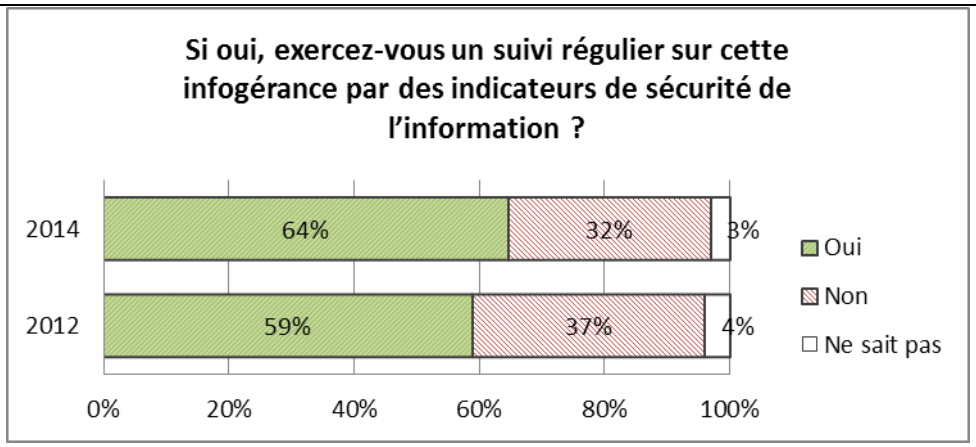

Figure 25 : Suivi de l'infogérance par des indicateurs de sécurité

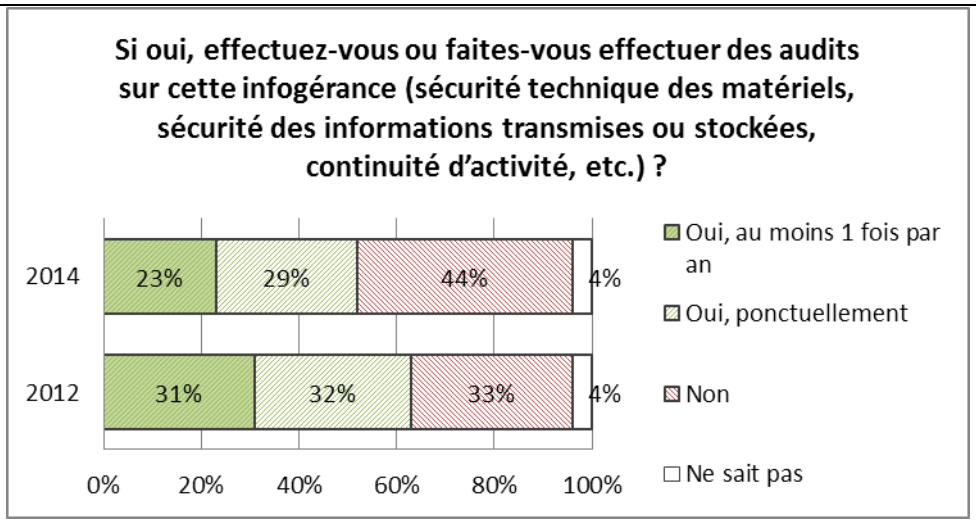

Figure 26 : Réalisation d'audit sur l'infogérance

Le Cloud de plus en plus sollicité…

L'utilisation du Cloud augmente de façon importante (38%, + 24 points vs 2012) même s'il représente moins de 50% des entreprises. La part la plus importante revient au Cloud privé même si le Cloud public est lui aussi en évolution. La part des Cloud hybrides reste stable.

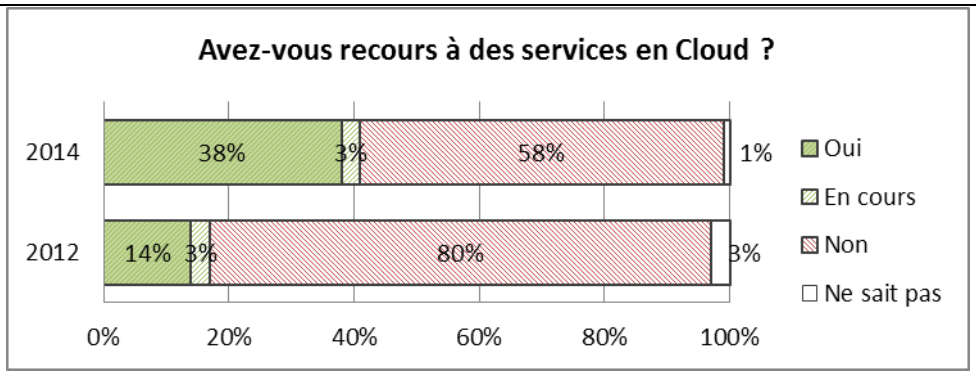

Figure 27 : Part d'utilisation de services en Cloud

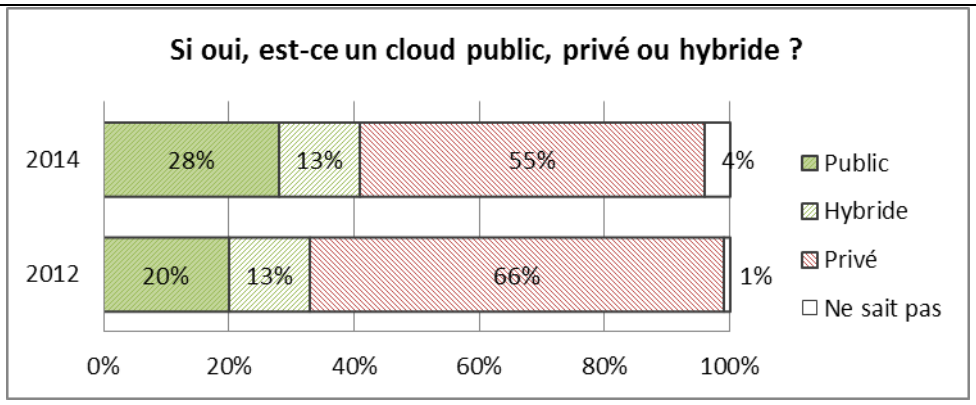

Figure 28 : Type de Cloud utilisé (public, hybride, privé)

Thème 11 : Contrôle des accès logiques

Globalement, les dispositifs de contrôle d'accès mis en œuvre stagnent ou régressent, à l'exception du SSO et du web SSO

Outre ce constat général, un autre s'impose : la 'sortie' de la biométrie du paysage des contrôle des accès logiques ! Pourtant des innovations continuent dans ce domaine, le passeport et le permis de conduire biométriques internautes sont des réalités. Faut-il chercher les raisons par rapport aux failles détectées ou à la difficulté de mise en œuvre de certains dispositifs ?

Il n'y a pas de véritable fossé dans les résultats par tranche d'effectifs. Les petites entreprises semblent privilégier l'authentification par certificat logiciel de type *token*, aussi bien en usage généralisé que partiel, tout comme la Banque-Assurance, en usage partiel.

Les Services et la Banque-Assurance préfèrent le SSO en usage généralisé, tandis que les Transports l'utilisent à 40% en partiel.

Certaines approches comme la conception de matrices d'habilitations par rôles et profils ou le provisionning sont difficiles à mettre en œuvre car elles nécessitent la participation active des métiers et une forte implication du management pour expliquer les enjeux. Ce sont des projets d'envergure qui nécessitent temps et ressources adaptés.

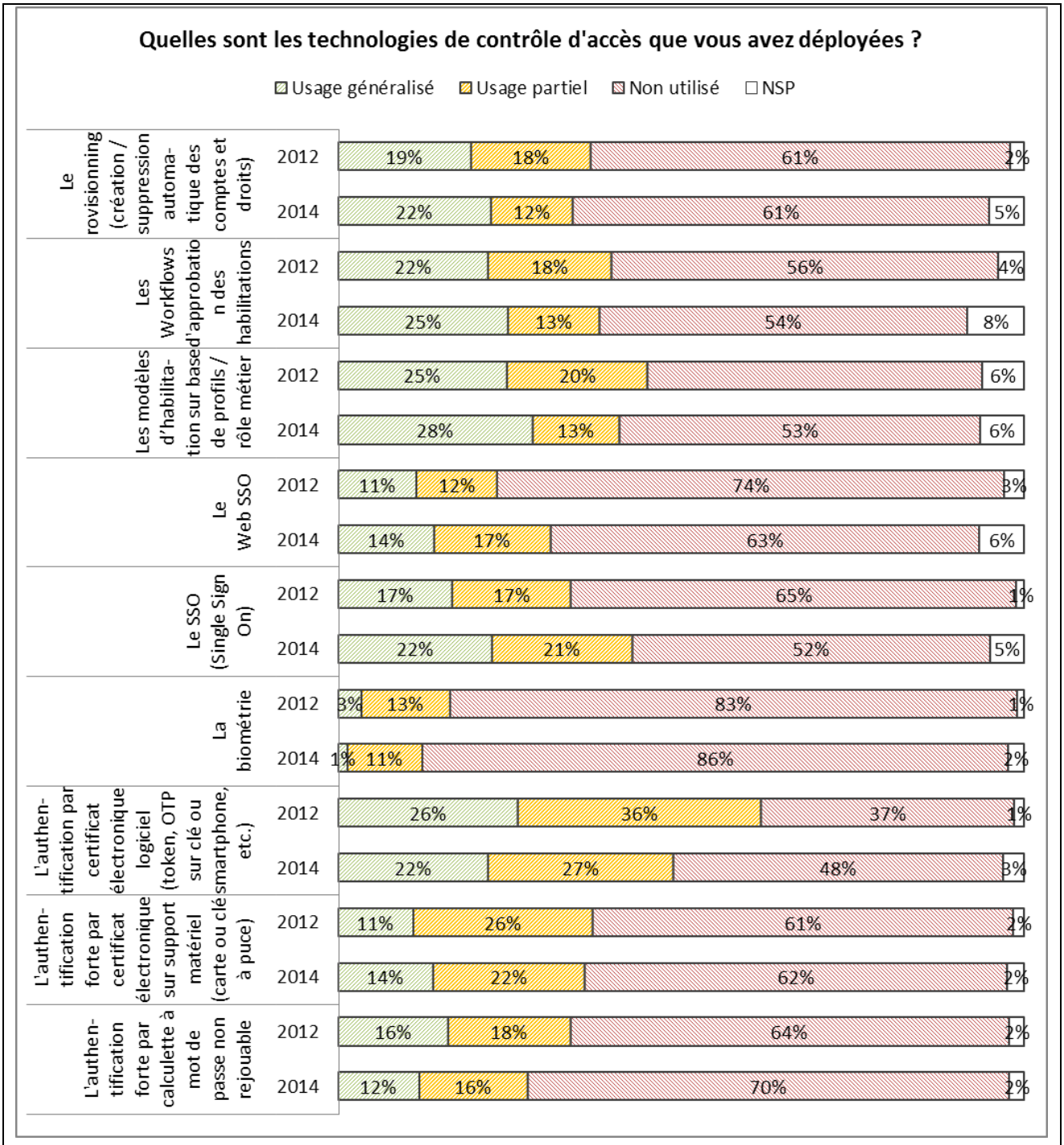

Figure 29 : Approches de sécurisation utilisées

Atteinte d'un palier dans les procédures de gestion des accès ?

Pas d'évolution dans la formalisation du processus de création de compte et de son cycle de vie ; les résultats sont très homogènes par secteur et par effectif.

Depuis 2010, c'est toujours environ 2/3 des entreprises qui contrôlent leurs accès par un processus formalisé.

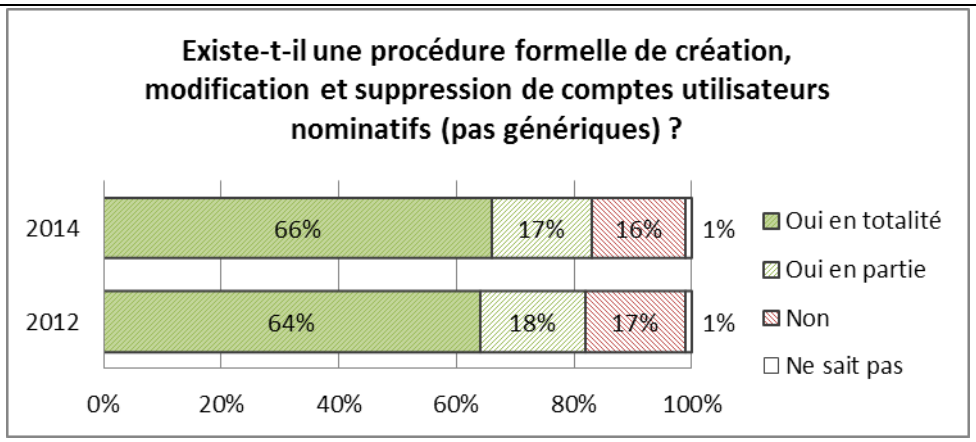

Figure 30 : Procédure formelle de création, modification et suppression de comptes utilisateurs nominatifs

Il en est de même pour les règles de constitution et de péremption des mots de passe.

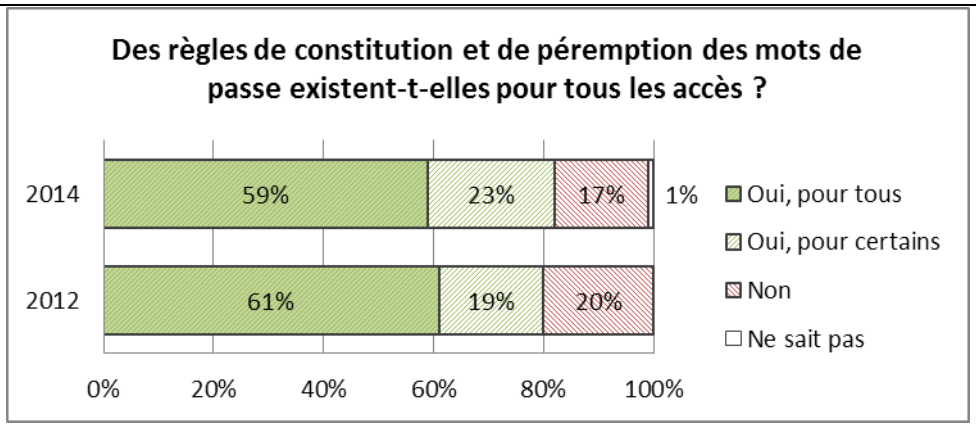

Figure 31 : Règles de constitution et de péremption des mots de passe

Ce résultat se comprend moins bien que pour la mise en œuvre de certains dispositifs de contrôle d'accès car dans la majorité des cas, ce processus peut être automatisé sans trop de difficulté.

Toutefois, l'analyse détaillée indique que ces règles sont appliquées à 76% pour tous les accès dans le secteur de la Banque Assurance.

Thème 12 : Acquisition, développement et maintenance du SI

Les Systèmes d'Information, qu'ils soient directement développés en interne ou via des prestataires, voire acquis (progiciels) se doivent d'être régulièrement surveillés concernant la sécurité. Les vulnérabilités étant monnaie courante, il convient de mettre en place une veille et des processus de mise à jour particuliers.

La veille en vulnérabilités est toujours présente au sein des entreprises interrogées. Néanmoins, et malgré le nombre d'incidents en progression constante, on ne note que peu d'évolution de la veille en vulnérabilités sur les SI. Le secteur Banque-Assurance et des Télécoms sont quant à eux les plus avancés dans cette pratique.

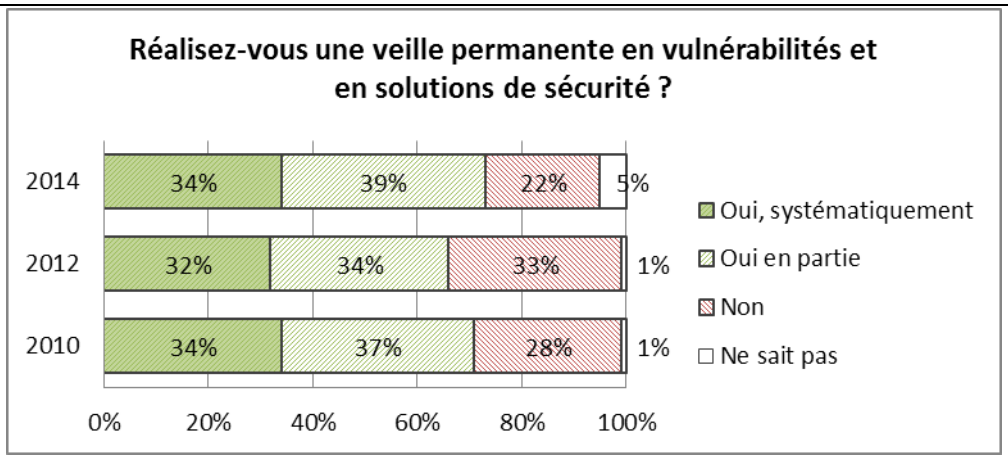

Figure 32 : Veille en vulnérabilités et en solutions de sécurité

Les procédures de gestion des correctifs de sécurité ont elles aussi peu évolué depuis la dernière enquête malgré les différentes obligations que l'on retrouve dans les règlements et/ou normes autour de la SSI.

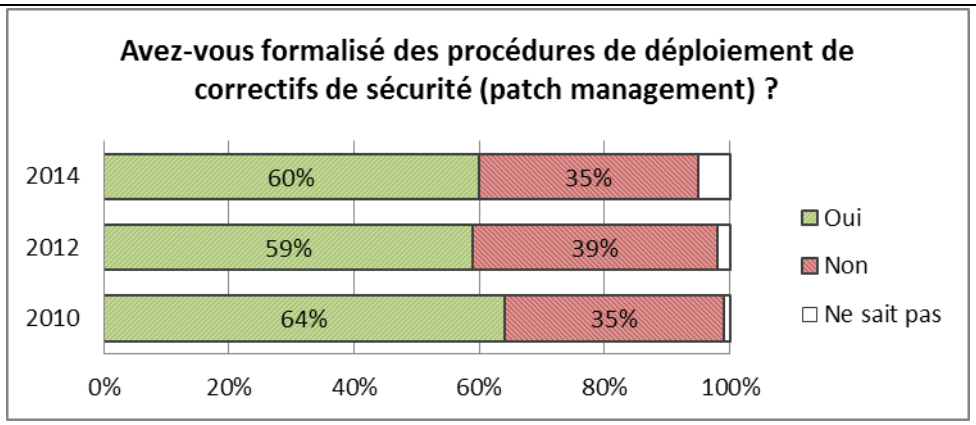

Figure 33 : Formalisation des procédures de déploiement de correctifs de sécurité

La Sécurité dans le cycle de développement progresse, mais reste toujours trop insuffisante.

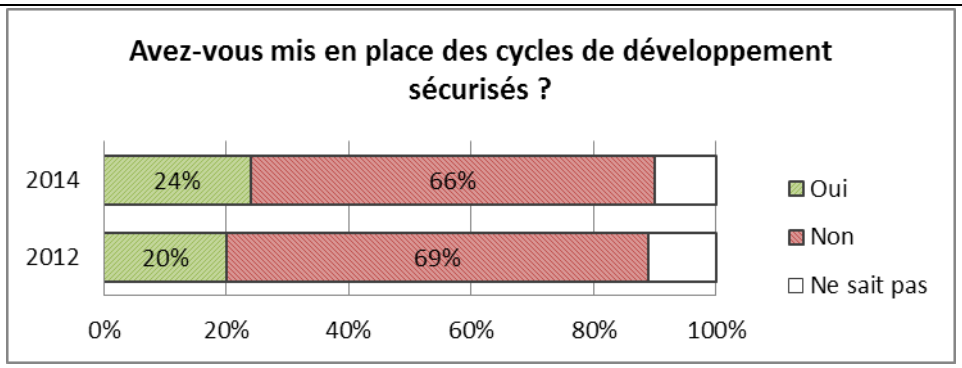

Figure 34 : Mise en place de cycles de développement sécurisé

Enfin, les entreprises ont majoritairement recours à des pratiques pragmatiques et non « standardisées » pour ce qui touche à leurs développements (49%) ; viennent ensuite dans l'ordre Microsoft SDLC (31%), INCAS (21%), OWASP CLASP (7%).

Thème 13 : Gestion des incidents de sécurité

Une nette recrudescence des dépôts de plaintes, de vols de matériels informatiques et des attaques logiques ciblées

Dans près de la moitié des cas (45%), il est toujours aussi surprenant de constater que les entreprises ne disposent pas de cellule de collecte et de traitement des incidents de sécurité de l'information. Comparé à l'étude de 2012, ce taux est en régression (- 8 points). En revanche, le pourcentage d'entreprises ayant déposé des plaintes suite à des incidents passe de 6% à 15% en 2014. Certes, plus de 80% ne déposent toujours pas de plaintes, mais l'augmentation du nombre de dépôts est significative.

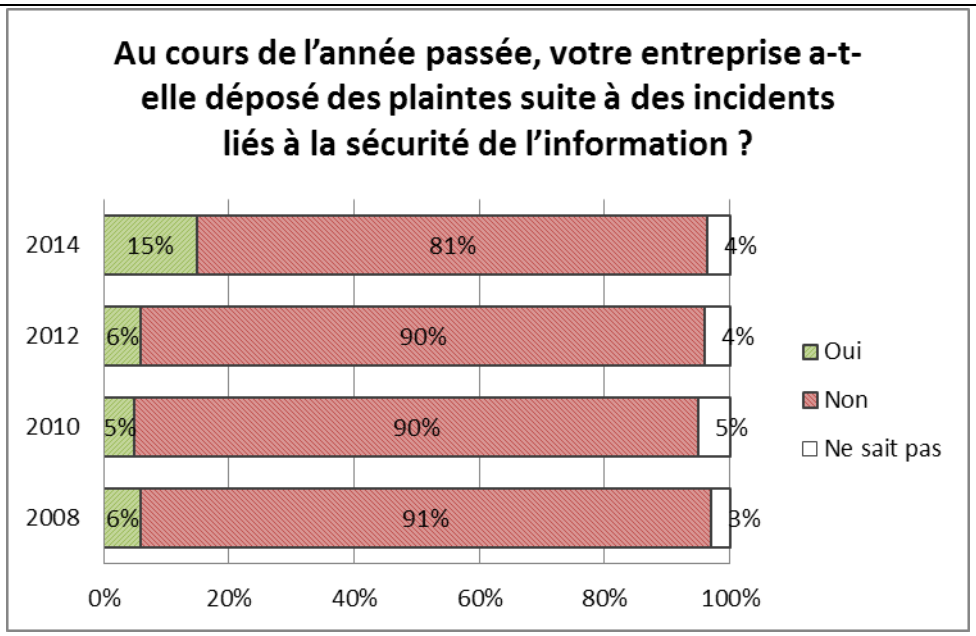

Figure 35 : Dépôt de plainte suite à des incidents liés à la sécurité de l'information

De même, le taux de vols ou disparitions de matériel informatique a pratiquement doublé par rapport à 2012. Cette hausse est probablement due à la hausse du taux d'équipements des entreprises en tablettes et autres équipements nomades.

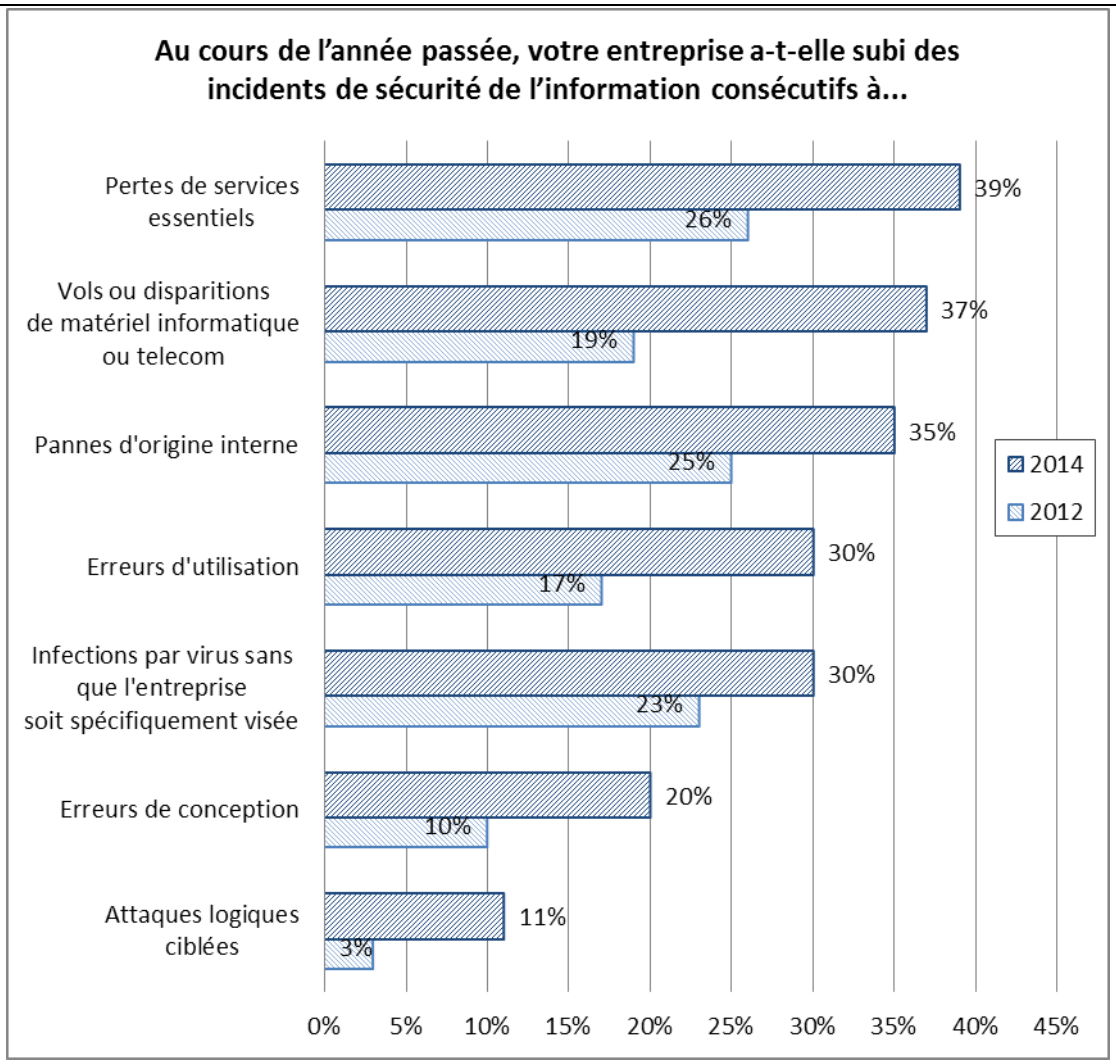

Figure 36 : Typologie des principaux incidents de sécurité

Par ailleurs, le nombre moyens d'erreurs d'utilisation passe de 7,1 à près de 19 entre 2012 et 2014 et le nombre d'attaques logiques ciblées de 2,2 à 10,5 (soit une multiplication par près de 5) expliquant probablement l'augmentation du nombre de dépôt de plaintes évoqué précédemment.

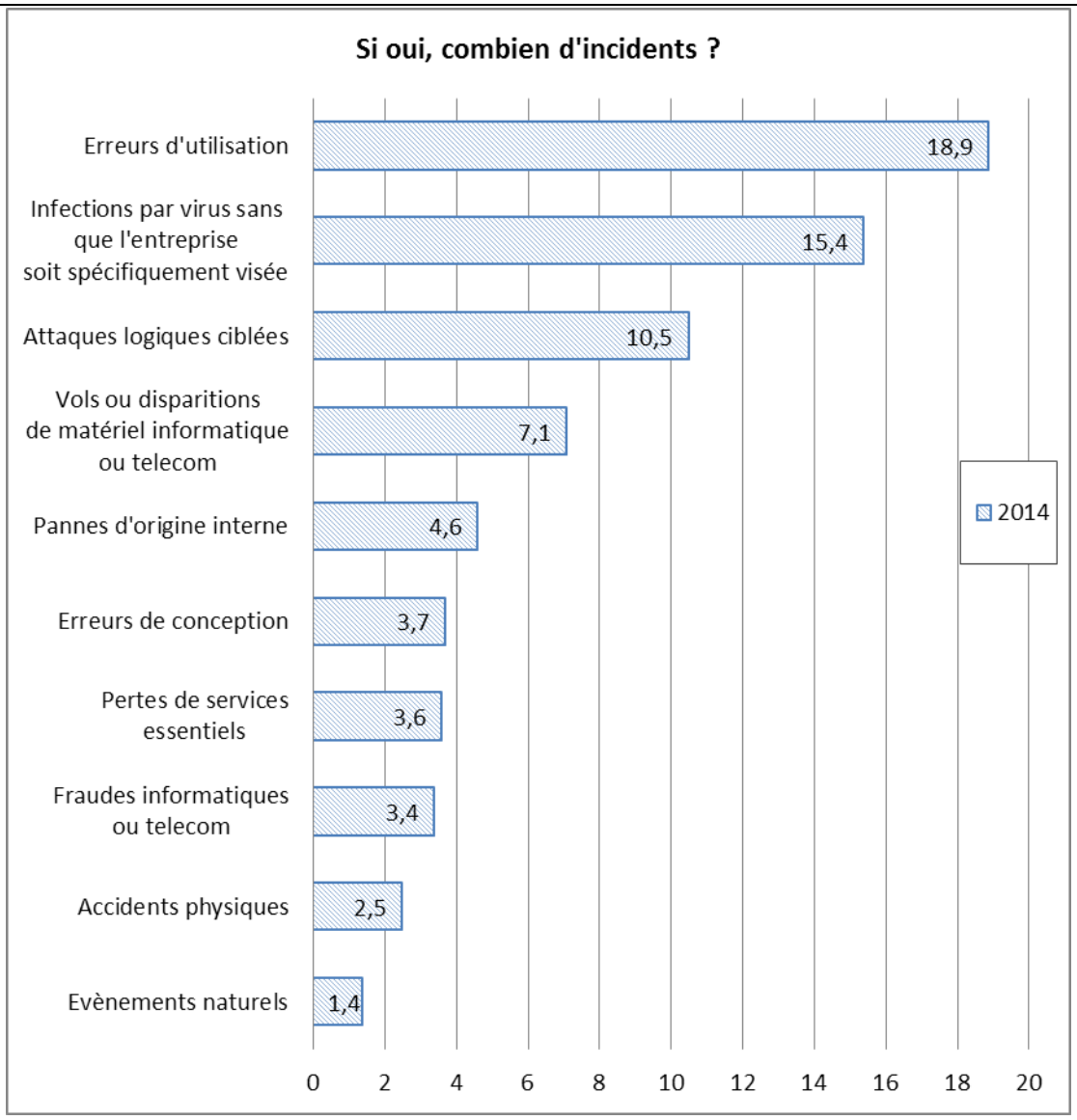

Figure 37 : Nombre moyen d'incidents par entreprise concernée pour chaque type

Thème 14 : Gestion de la Continuité d'Activité

Une gestion de la Continuité d'Activité qui régresse dans la couverture de certains scénarios d'indisponibilité

Le nombre d'entreprises qui ont un processus de Continuité d'Activité passe de 69 à 73% ce qui est plutôt rassurant.

En revanche, les entreprises semblent moins se préoccuper de l'indisponibilité d'un fournisseur essentiel dont la couverture passe en 2 ans de 26 à 18%. Ce point peut sembler inquiétant car les entreprises externalisent de plus en plus…

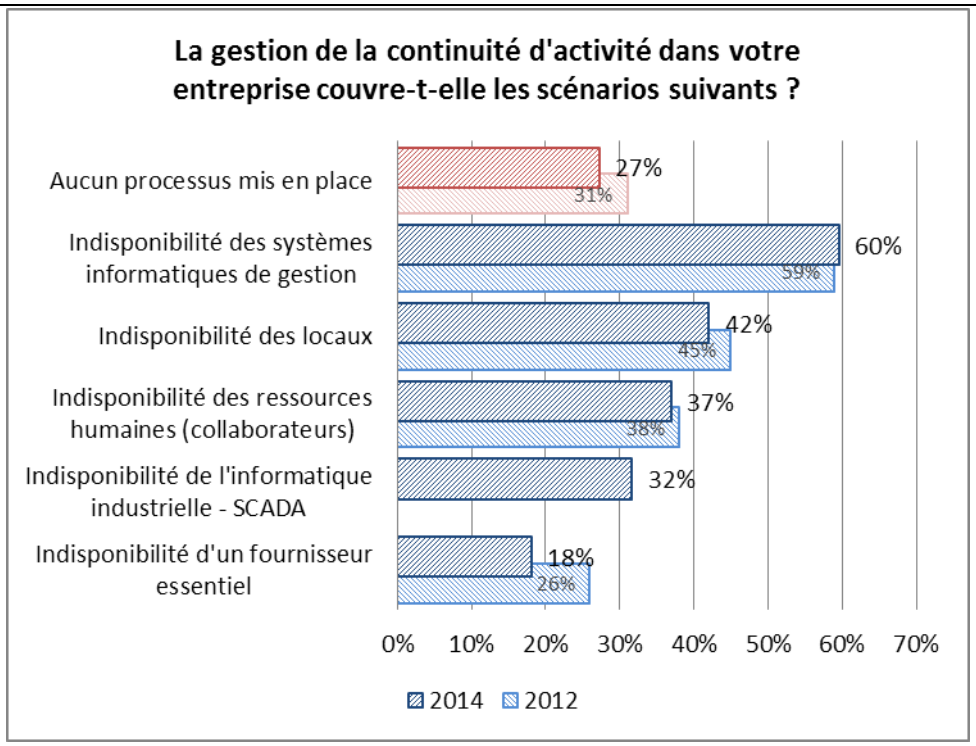

Figure 38 – Scénarii couverts par la gestion de la continuité d'activité

Confirmation de la forte progression de la prise en compte des exigences métiers

On constate sans hésiter une meilleure prise en compte des exigences Métier. La progression est de 12 points ! L'externalisation de certaines ressources (en mode PAAS, SAAS ou IAAS) en est-elle la cause ?

Serait-ce là le commencement d'un cercle vertueux dont on verra la suite dans la prochaine enquête avec une meilleure prise en comptes des scénarios d'indisponibilité ? Pour l'instant, ce résultat est paradoxal par rapport aux résultats de la question précédente.

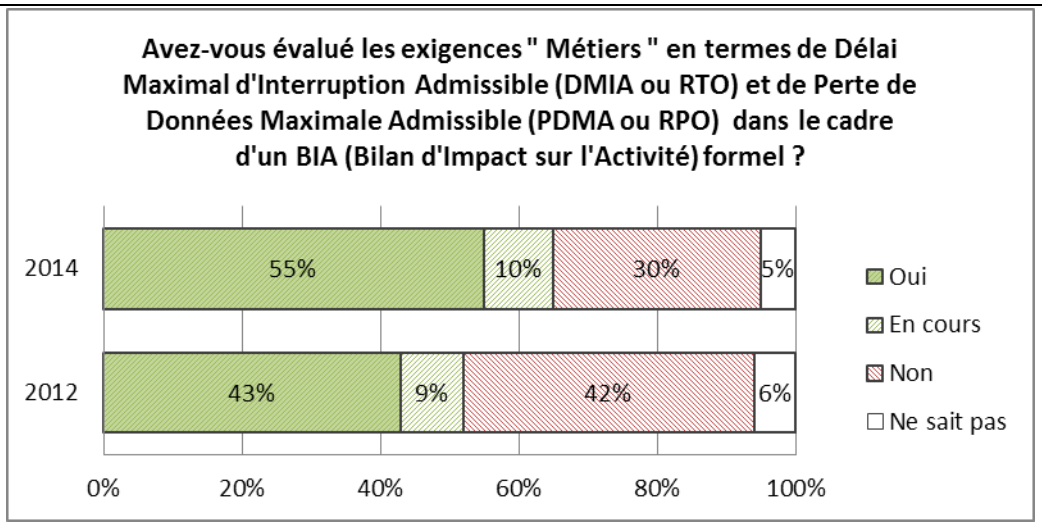

Figure 39 – Prise en compte des exigences métiers dans le cadre d'un BIA

Des exercices utilisateurs dont la fréquence s'améliore

Les exercices utilisateurs, meilleure garantie de l'opérationnalité des solutions mises en place progressent de 5 points sur la fréquence annuelle. Mais encore un quart des entreprises n'en font jamais.

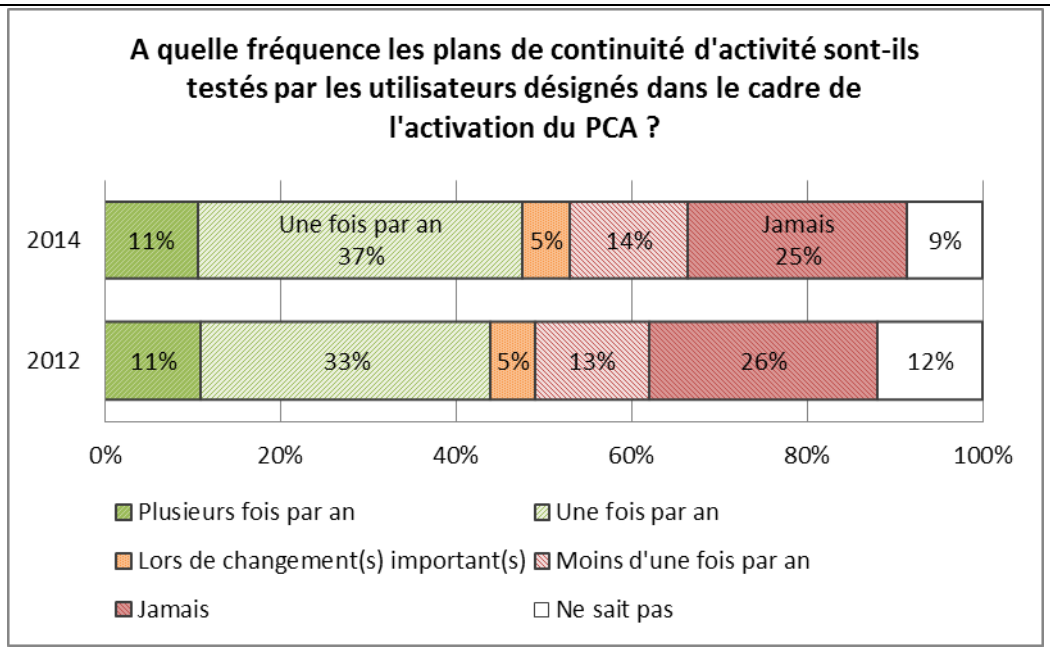

Figure 40 - Fréquence des exercices utilisateurs

Des exercices techniques dont la fréquence s'améliore doucement

Depuis la dernière étude, on constate une progression ; en effet, les entreprises qui ne réalisaient auparavant pas ou peu de tests, en conduisent désormais au moins une fois par an. Ce qui peut paraitre surprenant en comparant avec les chiffres précédents : classiquement un test technique précède un exercice utilisateurs et cela ne semble pas être systématiquement le cas.

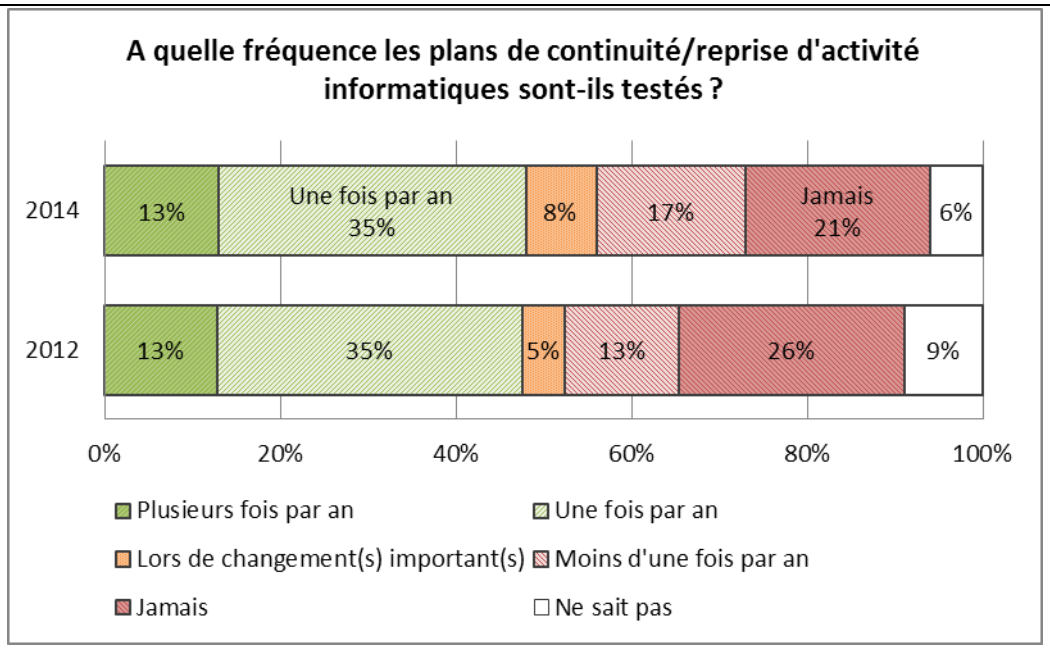

Figure 41 - Fréquence des tests techniques

Cette année une nouvelle question sur l'exhaustivité de la couverture des solutions testées a mis en évidence que 59% des entreprises couvraient de 75 à 100% de leurs solutions mises en œuvre ce qui est très positif quant au sérieux des tests effectués.

Une gestion de crise en crise !

La véritable surprise de l'enquête sur le thème de la Continuité d'Activité est dans les réponses aux questions sur la gestion de crise. Seule une moitié des entreprises a une gestion de crise formalisée (passe de 54 à 51% en 2 ans).

Les secteurs des entreprises montrent une grande disparité sur ce sujet. Les secteurs Transport-Telecom et Banque-Assurance étant les mieux équipés.

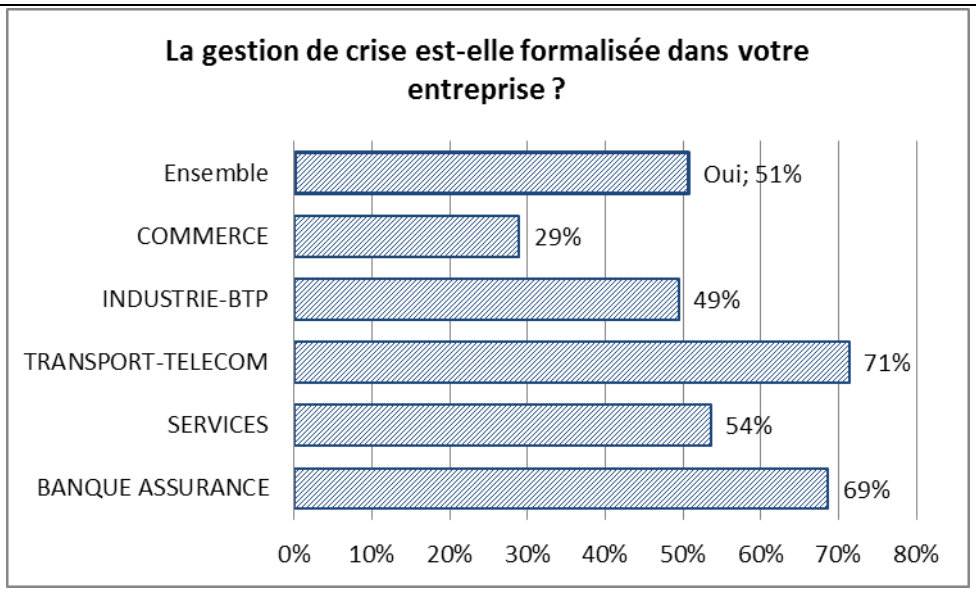

Figure 42 – Gestion de crise formalisée

L'existence de cellules de crise décisionnelle et opérationnelle montre également une prise en compte dépendante du secteur d'activité (insuffisamment prise en compte par les secteurs Industrie-BTP et Commerce).

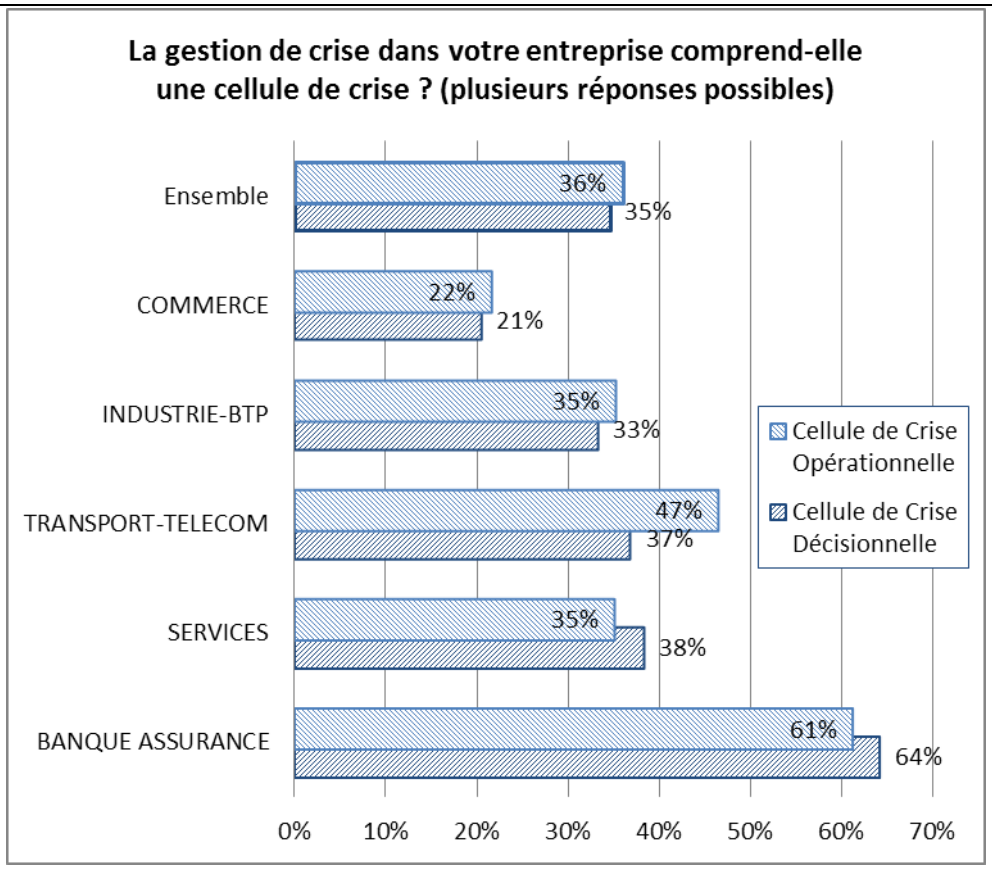

Figure 43 – Cellules de crise opérationnelles et décisionnelles

Enfin les cellules de crise comportent peu de processus d'escalade outillés et très peu de salles de gestion de crise équipée. Il parait pourtant évident qu'une gestion de crise activée rapidement et dans des locaux préparés à l'avance donne un atout majeur à l'entreprise qui subit une crise car sa rapidité de réaction peut être vitale. Là encore, selon les secteurs d'activité on constate de gros écarts.

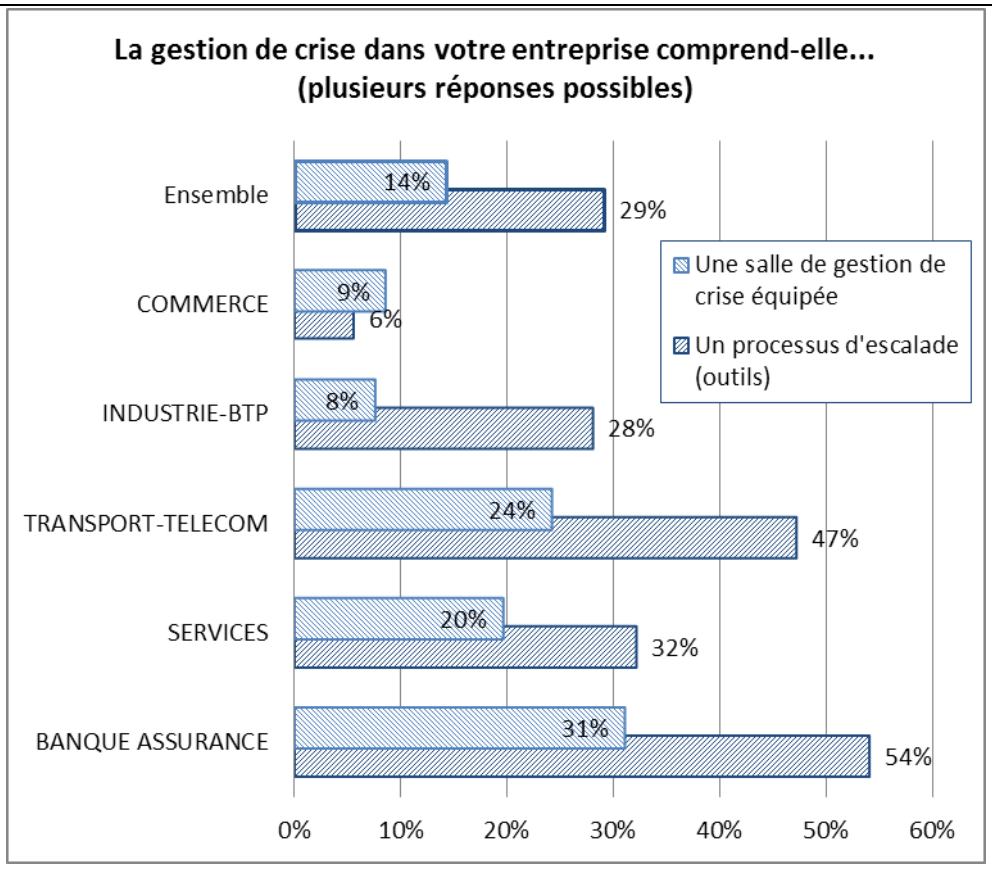

Figure 44 - Salles de gestion de crise et processus d'escalade

Thème 15 : 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 responsabilité de déclarer les traitements à la CNIL est répartie équitablement entre le DSI (22%), le service RH (21%), le service juridique (16%) et le CIL ou le RSSI (25%). Cette répartition n'est guère surprenante dans la mesure où il s'agit d'une fonction autant technique que juridique.

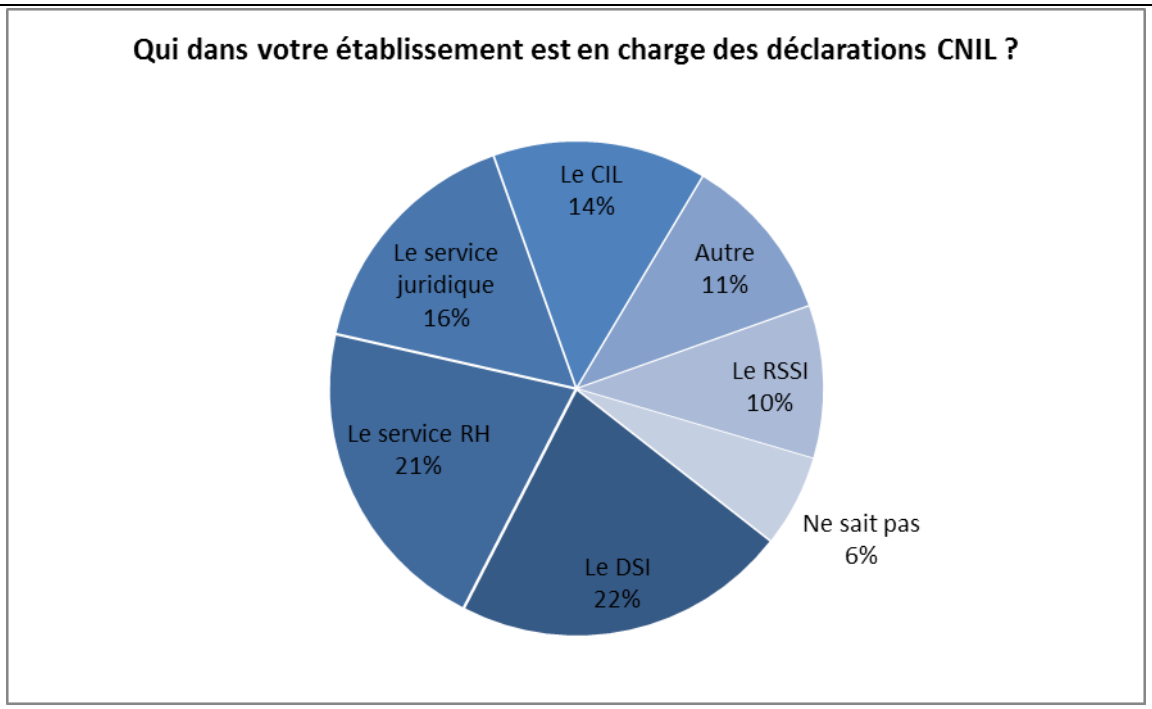

Figure 45 - Répartition de la charge des déclarations à la CNIL

On note par contre des disparités importantes selon les secteurs d'activité, par exemple pour le CIL (de 10% dans le secteur Industrie-BTP, à 28% dans la Banque-Assurance), ou le RSSI (de 1% dans le Commerce, à 16% dans la Banque-Assurance).

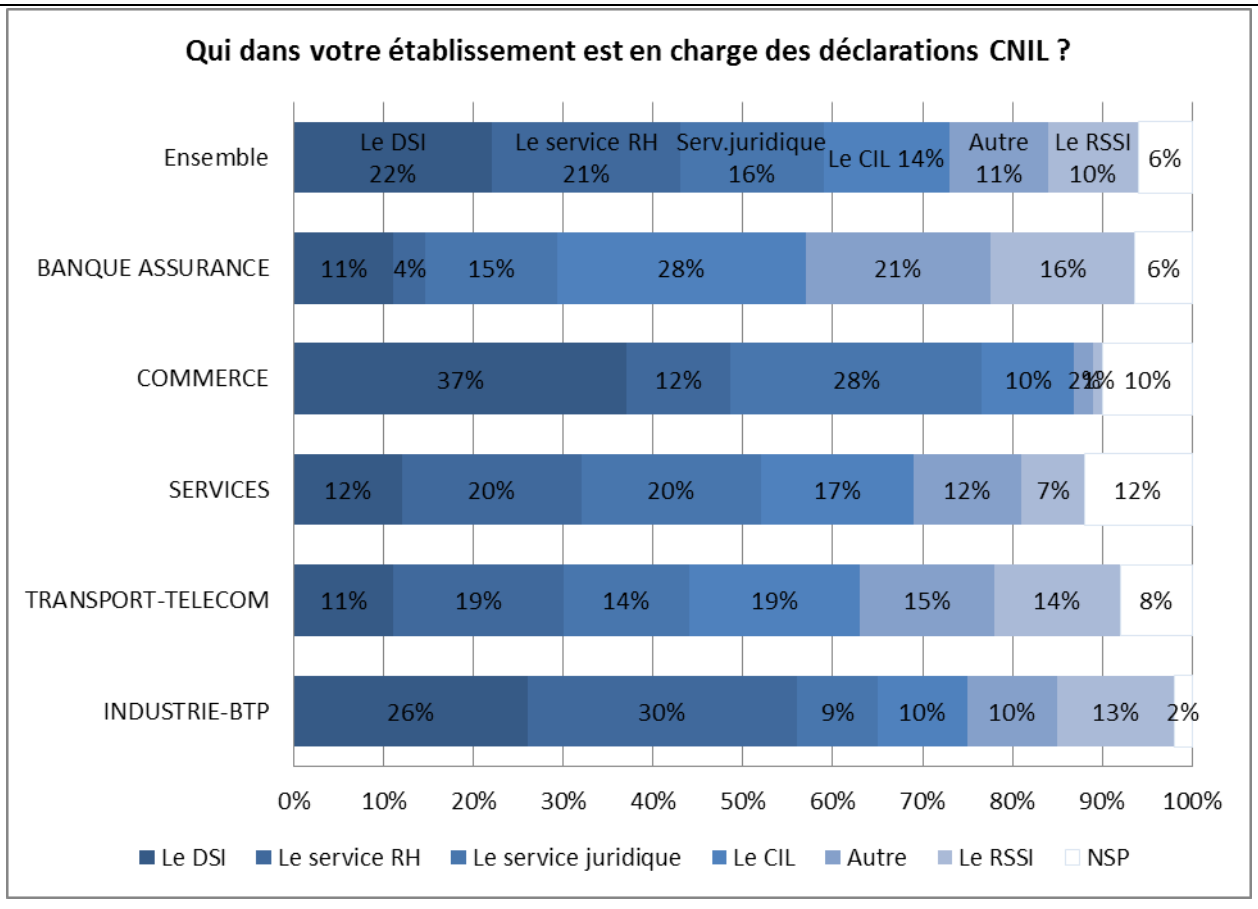

Figure 46 - Répartition de la charge de déclaration à la CNIL selon les secteurs d'activité

Ces réponses présentent toutefois un décalage sensible avec les résultats des années précédentes : dans la mesure où un Correspondant Informatique et Libertés est « déjà en place » (32% en 2010, 42% en 2012), son rôle dans les déclarations à la CNIL parait très faible (14%) !…

Les audits de sécurité

Un quart des entreprises indiquent être soumises à des lois ou règlementions spécifiques en matière de sécurité de l'information.

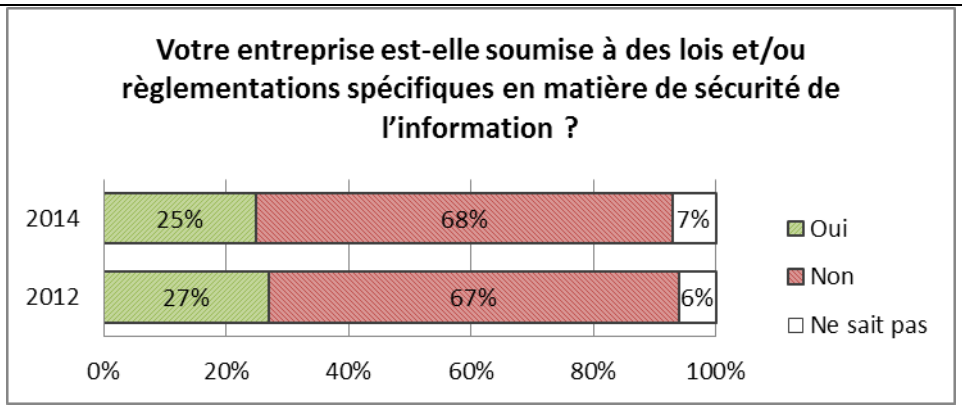

Figure 47 – Entreprises soumises à des lois/règlementations spécifiques pour la sécurité des SI

Plus de deux tiers des entreprises interrogées ont réalisé au moins un audit de sécurité au cours de deux dernières années. Ces chiffres sont relativement stables, y compris depuis l'enquête de 2010 (63%).

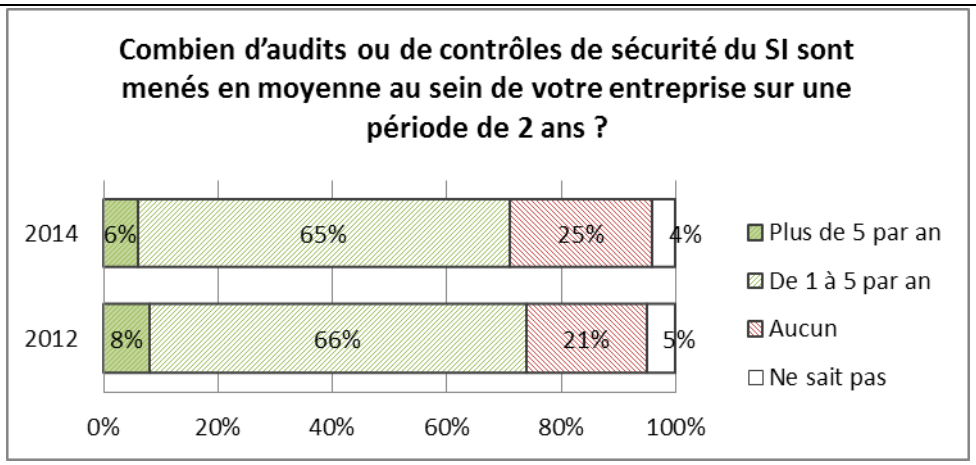

Figure 48 – Nombre d'audits de sécurité du SI réalisés sur une période de 2 ans

Les motivations de ces audits restent principalement le respect de la PSSI (43%), mais elles sont aussi motivées par des exigences contractuelles ou règlementaires (33%), ou des exigences externes, comme les assurances ou les clients (32%). La réaction à un incident reste une cause notable (19%, contre 14% en 2012).

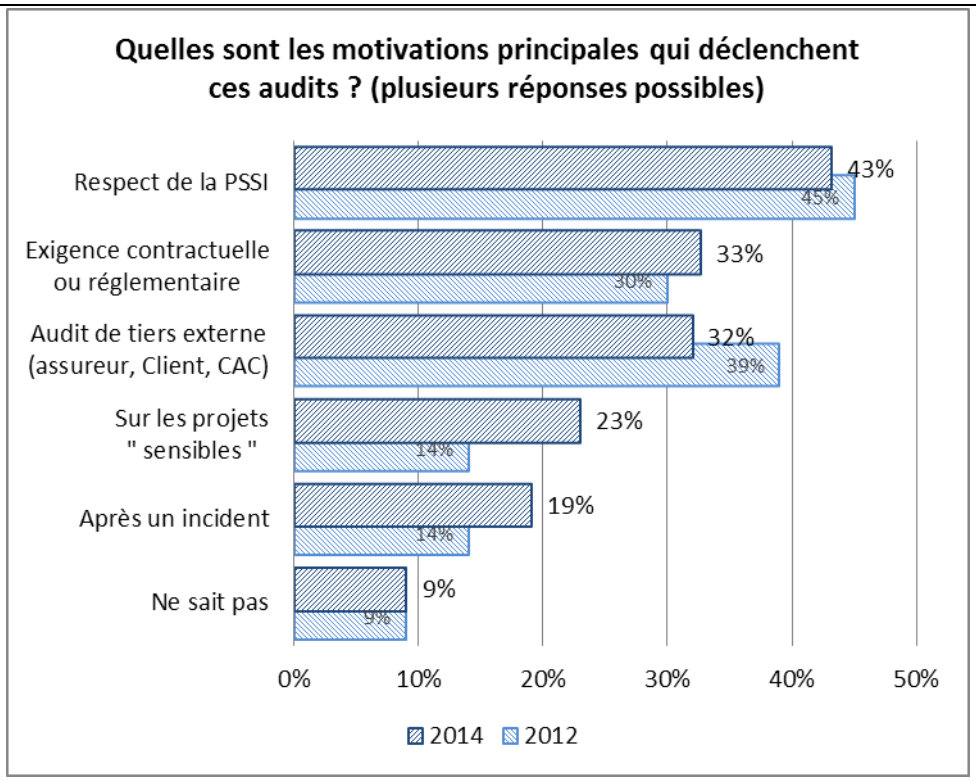

Figure 49 - Motivations déclenchant les audits de sécurité

Utilisation de tableaux de bord de sécurité

L'utilisation de tableaux de bord de sécurité reste très largement absente dans la plupart des entreprises (73%), même si on note une augmentation sensible de cette pratique (+10 points depuis 2012).

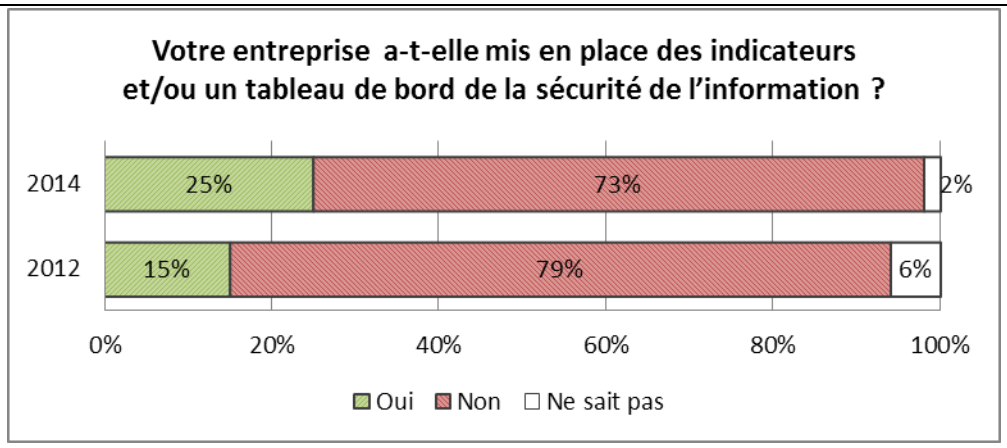

Figure 50 - Mise en place de tableaux de bord de la sécurité de l'information

La vocation opérationnelle de ces tableaux de bord se consolide (69% contre 60% en 2012), tandis que leur rôle de pilotage de la SSI diminue (35% contre 47%), de même que l'intérêt des Directions Générales (21% contre 37%).

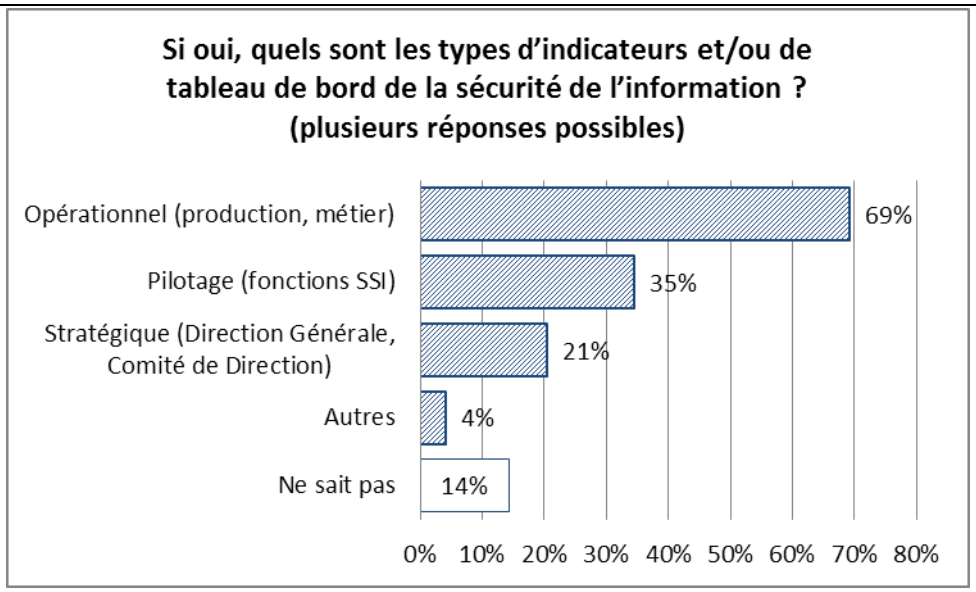

Figure 51 – Types d'indicateurs ou de tableaux de bord

Comme on le soulignait déjà en 2012, l'information des Directions Générales reste un axe d'amélioration à entretenir pour les RSSI.

Sans évolution majeure par rapport à 2012 et 2010, les indicateurs suivis restent en priorité de nature technique (taux de disponibilité, vulnérabilités détectées, taux de mise à jour).

Les indicateurs liés à l'organisation restent très présents, comme la conformité (en baisse de 70% à 50%), ou l'avancement de projets de sécurisation (en hausse de 31% à 50%).

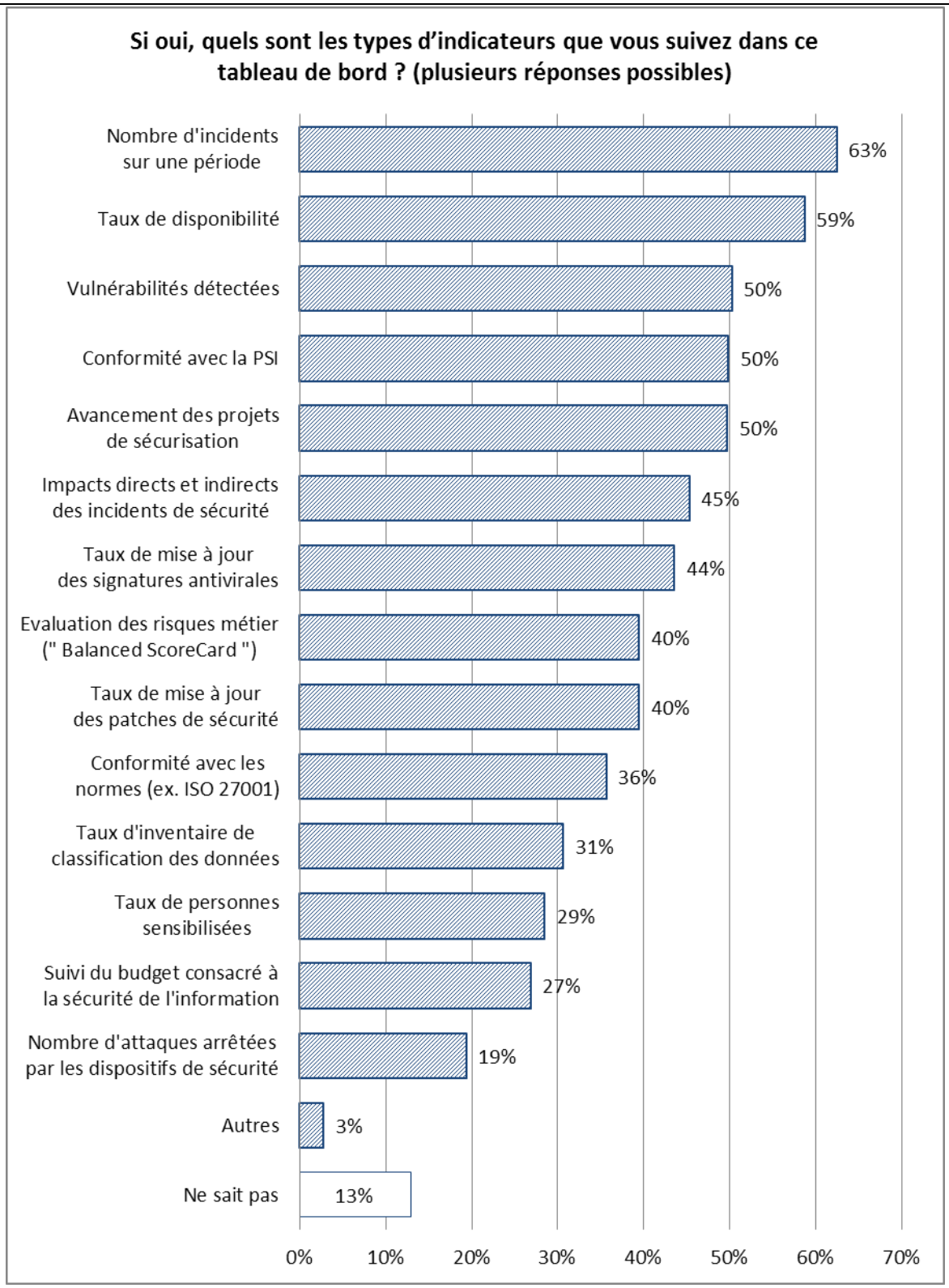

Figure 52 - Indicateurs suivis dans le tableau de bord

Hôpitaux publics

- Présentation de l'échantillon
- Dépendance à l'informatique des collectivités territoriales
- Moyens consacrés à la sécurité de l'information par les collectivités territoriales
- Thème 5 : Politique de sécurité
- Thème 6 : Organisation de la sécurité et moyens
- Thème 7 : La gestion des risques liés à la sécurité des SI
- Thème 8 : Sécurité liée aux Ressources Humaines
- Thème 9 : Sécurité physique
- Thème 10 : Gestion des opérations et des communications
- Thème 11 : Contrôle des accès logiques
- Thème 12 : Acquisition, développement et maintenance
- Thème 13 : Gestion des incidents – Sinistralité
- Thème 14 : Gestion de la continuité d'activité
- Thème 15 : Conformité

Les Hôpitaux publics

Présentation de l'échantillon

L'enquête a été réalisée par téléphone début 2014 auprès des hôpitaux publics de plus de 200 lits :

- 150 hôpitaux y ont répondu (durée moyenne de l'entretien : 25 minutes)
- 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 précédente enquête date de 2010.

Profil des hôpitaux interrogés

Les établissements de 200 à 499 lits sont toujours en majorité (la moitié), même si l'échantillon contient plus de grands hôpitaux (+ de 1000 lits) par rapport à 2010 (21% en 2014, contre 7% en 2010).

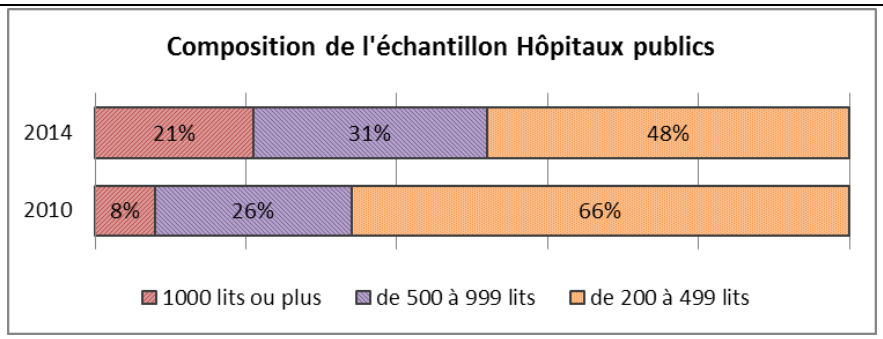

Figure 53 - Taille des hôpitaux interrogés

Seuls 19% des établissements font partie d'un groupement.

Profil des interviewés

Ce sont des responsables des Systèmes d'Information qui ont le plus souvent répondu à l'enquête (72% des cas) : Responsable des Systèmes d'Information, DSI, Directeur Informatique. Ces chiffres sont en très nette progression par rapport à 2010.

La cible prioritaire - le Responsable de la Sécurité des Systèmes d'Informations (RSSI) - n'a pu être jointe que dans 17% des cas (contre 28% en 2010) : même si les hôpitaux ont plus fréquemment un RSSI ou un « référent sécurité SI », est-ce lié au fait que les RSI se voient de plus en plus impliqués et se sentent de plus en plus responsables de la sécurité de leur SI, et donc répondent directement ?

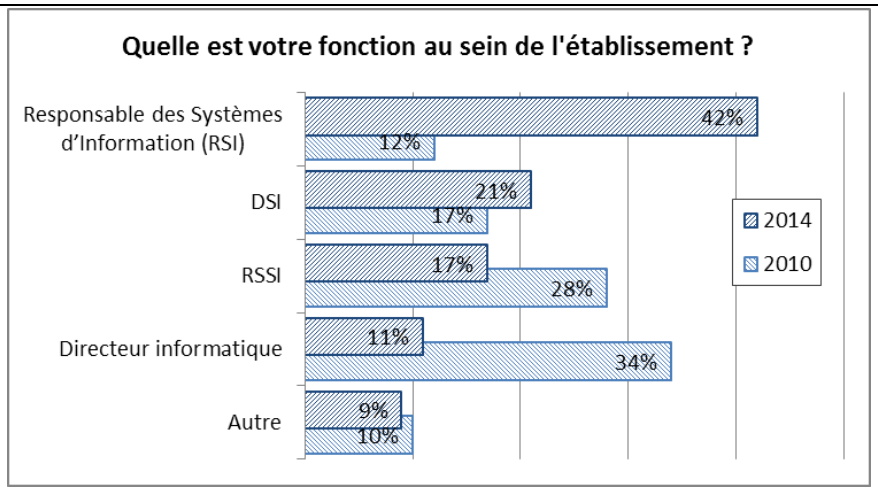

Figure 54 - Profil des interviewés

Thème 5 : Politique de sécurité de l'information

Les établissements de plus de 1 000 lits largement en tête

L'examen détaillé des réponses de l'enquête montre que 72% des hôpitaux de plus de 1000 lits ont formalisé leur politique de sécurité, alors qu'ils ne sont que 40% pour les établissements de 200 à 999 lits. Ceci est probablement lié aux ressources disponibles, bien plus importantes dans les CHU

Si en 2010, la formalisation de la PSSI avait été fortement motivée par les travaux du GMSIH (Groupement pour la Modernisation du Système d'Information Hospitalier), les résultats de l'enquête font apparaître que 17% des établissements interrogés l'ont formalisée pour être en conformité avec le prérequis du programme Hôpital Numérique.

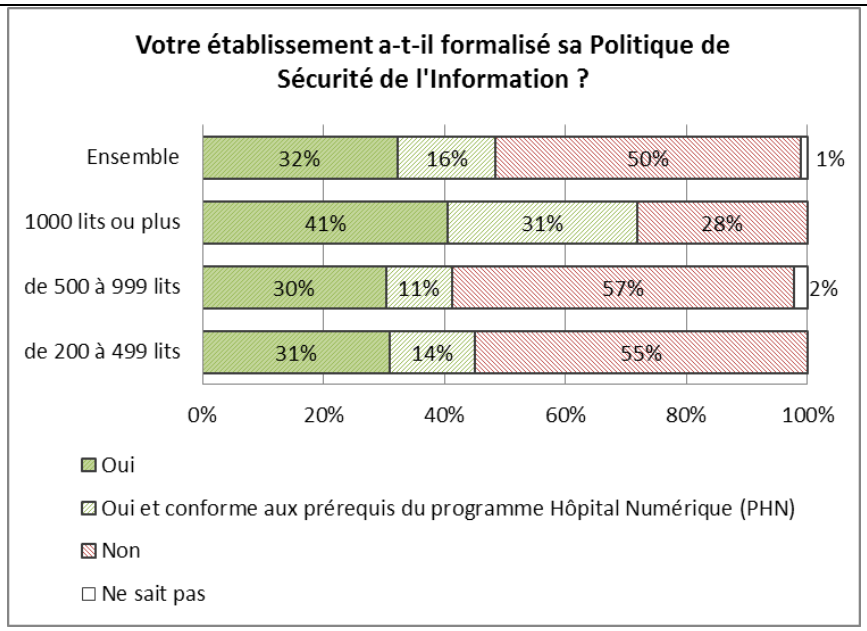

Figure 55 – Formalisation de la PSSI

Une Direction Générale toujours impliquée

Lorsque la PSSI existe, les résultats révèlent que la Direction Générale soutient cette politique à 90%. Face à une accélération soutenue de la dématérialisation des processus métiers et des échanges, la sécurité est une préoccupation de la Gouvernance des hôpitaux.

Des politiques révisées régulièrement

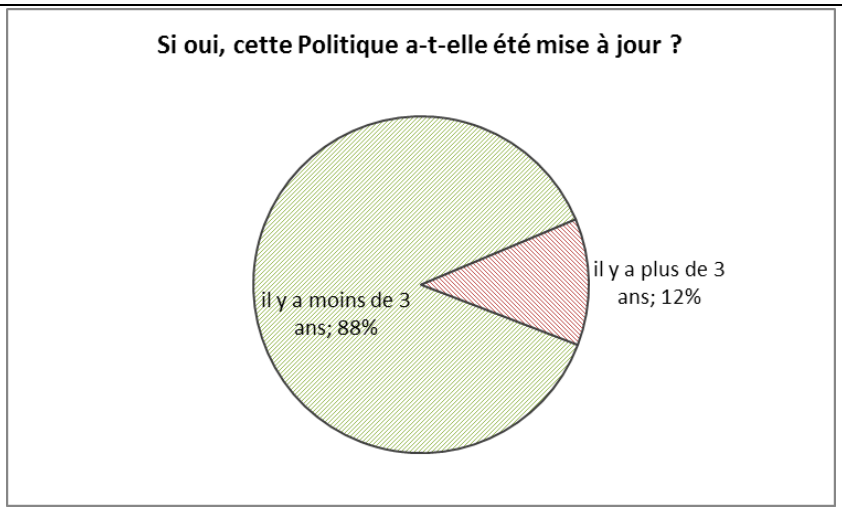

Figure 56 – Renouvellement de la PSSI

Pour ceux qui possèdent une politique, 88% déclarent l'avoir révisée il y a moins de trois ans. Si les facteurs déclenchant la révision d'une politique de sécurité ont différentes sources, on peut imaginer que la publication en 2012 par la Direction générale de l'offre des soins du guide des indicateurs des prérequis est un bon levier de cette révision.

ISO 2700x et ANSSI comme source d'inspiration

Deux corpus documentaires sont plébiscités pour aider à la formalisation de cette politique : la norme ISO 27000 et ses 11 chapitres sur les mesures de sécurité ; les 16 domaines du guide PSSI de l'ANSSI. Publié en novembre 2012 par l'ASIP, le référentiel de politique générale de sécurité des Systèmes d'Information de santé est déjà pris en compte par 4% des établissements interrogés. Par contre, la norme ISO 27799, déclinaison de la norme ISO 27002 et qui traite des besoins de gestion de la sécurité de l'information spécifiques au domaine de la santé, semble avoir été abandonnée au profit de la norme ISO 27002.

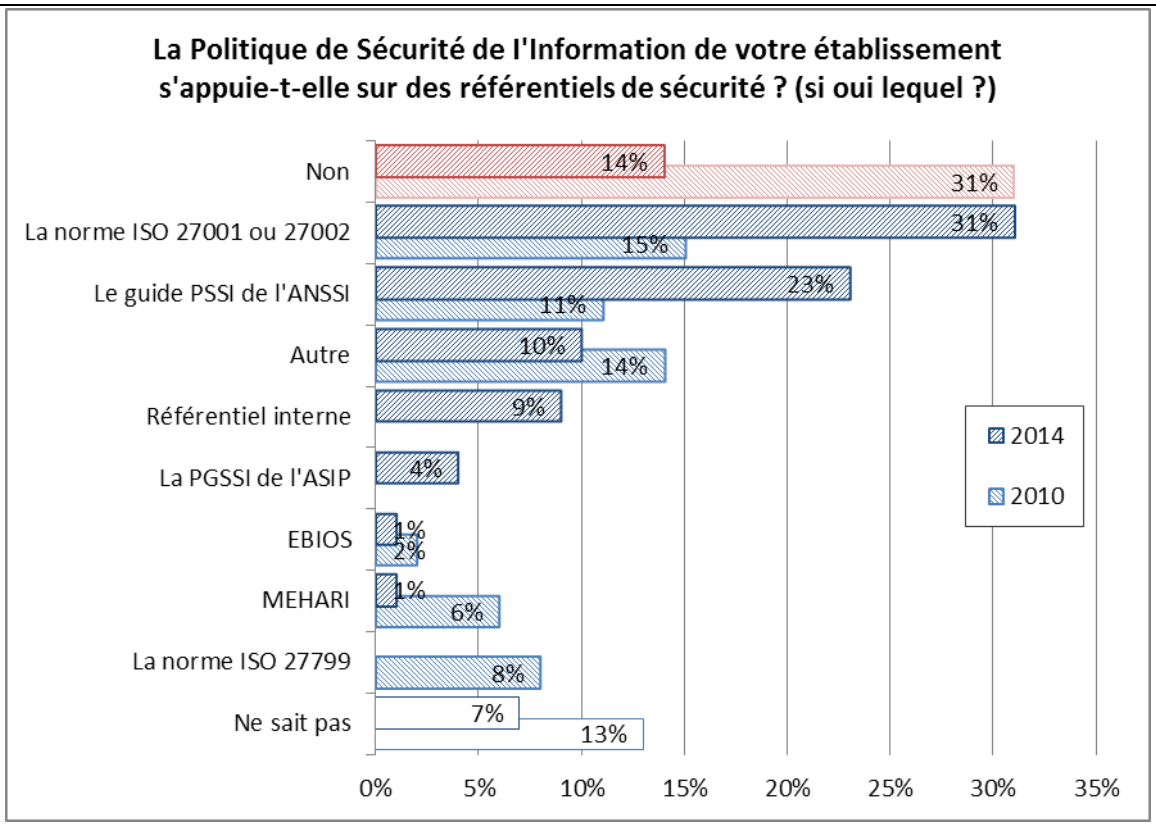

Figure 57 – Référentiel utilisé pour établir la PSSI

Thème 6 : Organisation et Moyens

RSSI : un bond en 4 ans !

Le RSSI ou référent sécurité SI s'impose désormais dans 60% des établissements hospitaliers. Il est le point de contact désigné au sein de l'établissement sur le thème de la sécurité des Systèmes d'Information. Le référent n'est pas forcément un informaticien de formation, la direction des soins ou encore le service qualité se voient souvent confier ce rôle dans les établissements de taille moyenne. Pour 74% des établissements interrogés, ce référent n'est pas à temps plein sur cette activité.

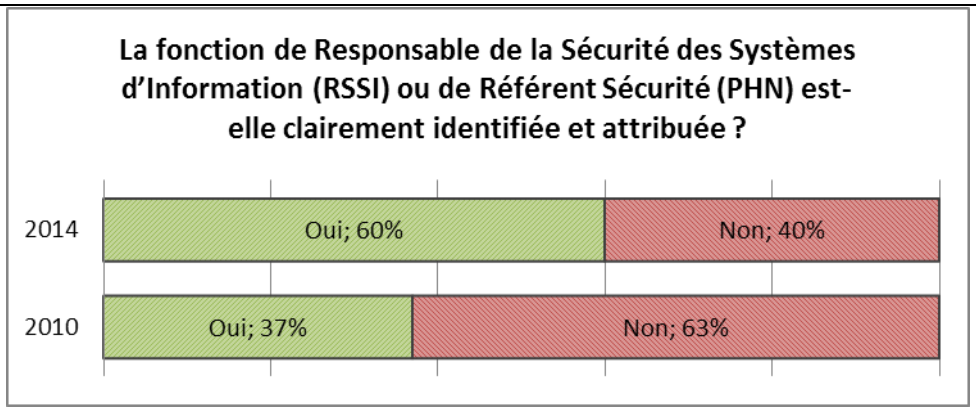

Figure 58 – Identification de la fonction de RSSI

Un rôle qui demande aussi un intérêt et des compétences pour les aspects juridiques

Les activités du référent Sécurité SI sont très variées : rédiger la politique de sécurité, participer activement à certains comité transversaux comme celui d'identitovigilance, suivre les projets techniques liés à la sécurité, sensibiliser les utilisateurs mais aussi, et de plus en plus, faire les déclarations à la CNIL et participer à l'instruction de plaintes.

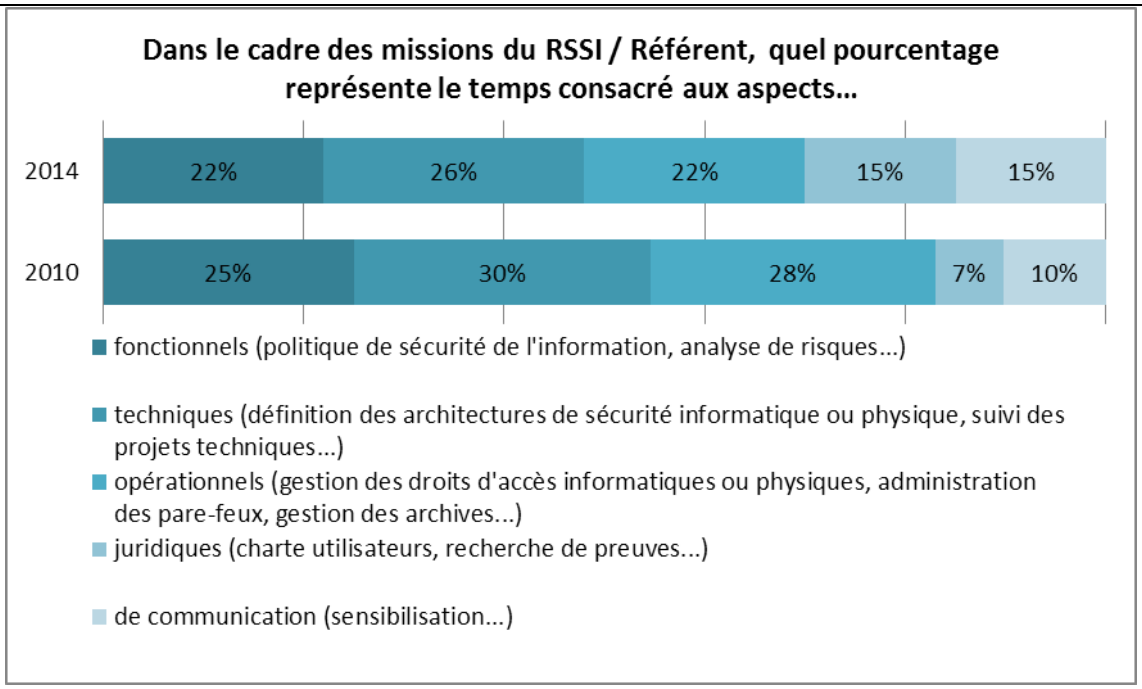

Figure 59 – Répartition du temps du RSSI

Budget informatique annuel : plus de transparence

Le taux de réponse s'est amélioré par rapport à l'enquête de 2010 (64% de répondants contre 48% en 2010).

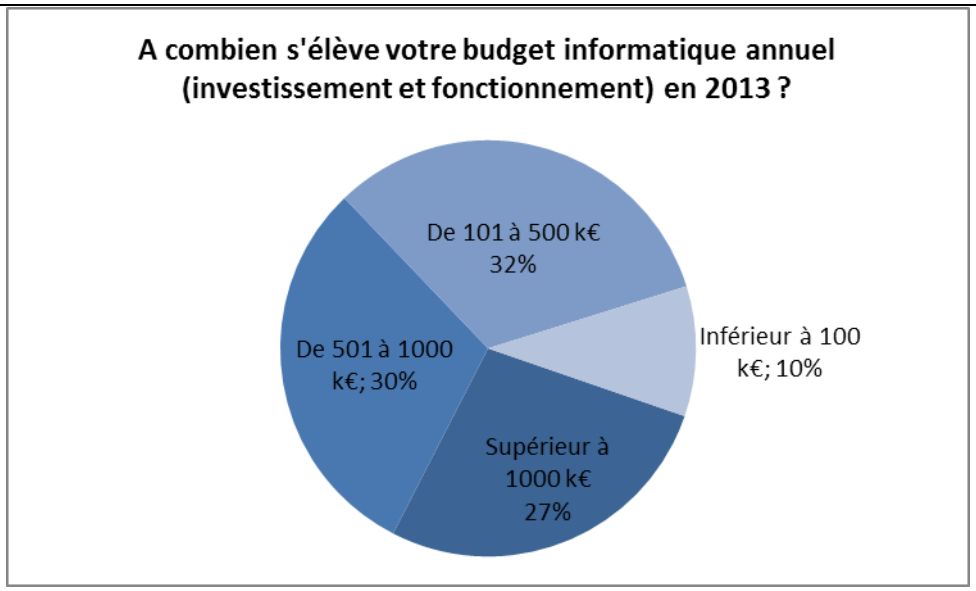

Figure 60 - Montant des budgets informatiques annuels

Alors que 40% des hôpitaux avaient un budget informatique supérieur à 400K€ en 2010, 57% ont désormais un budget supérieur à 500k€ dont 27% supérieur à 1000k€. 32% des hôpitaux ont un budget compris entre 101 et 500K€ alors que le même pourcentage en 2010 gérait un budget de 100 à 400K€. Cette augmentation des budgets est probablement liée à l'implication des directions dans la politique de sécurité SI de leur hôpital.

Pour avoir une vision plus large et plus détaillée des ressources des hôpitaux consacrées au Système d'Information hospitalier, les lecteurs peuvent se reporter à l'Atlas des SIH publié par la Direction Générale de l'Offre de Soins du Ministère de la Santé, dont la première édition est parue en 2013.

La dépendance au bon fonctionnement de l'informatique est totale

Les réponses obtenues en 2014 sont sensiblement identiques à celles obtenues en 2010 : 79% de dépendance forte, 18% de dépendance modérée.

Les DSI, les RSI et les RSSI sont tout à fait conscients des impacts d'une indisponibilité grave du Système d'Information, et ce depuis la décennie 2000 qui a vu se développer l'informatisation de la production des soins.

Cette réponse peut être corrélée en partie à l'augmentation du poste « mise en place de solutions techniques » du budget sécurité (45% de l'échantillon) : la redondance des configurations et la réplication temps réel ou en temps légèrement différé, si possible sur deux sites géographiquement séparés, demandées de plus en plus par les acteurs métiers, devient un impératif pour beaucoup de DSI d'établissements et peut expliquer cette augmentation.

La part du budget sécurité dans le budget informatique régresse…

La comparaison entre les résultats des années 2010 et 2014 montre en particulier une augmentation de la part des établissements déclarant consacrer de 1 à 3% de leur budget informatique à la sécurité du Système d'Information (25% contre 15% en 2010), et une diminution de la part supérieure à 6% (passage de 22% des réponses en 2010 à seulement 13% en 2014).

Les chiffres présentés traduisent la perception des DSI et RSI des établissements (plus que celle des RSSI qui représentent 17% de l'échantillon) : il est toujours difficile d'isoler le budget lié à des actions sécurité du reste du budget des Systèmes d'Information, en particulier lorsque l'établissement ne dispose pas d'un plan d'actions sécurité de l'information formalisé et suivi. Le pourcentage de 31% de réponses de responsables indiquant qu'ils ne connaissent pas la part du budget sécurité par rapport au budget informatique est significatif de cette difficulté ; elle s'explique néanmoins car la distinction ne peut se

faire aisément ; une des illustrations est la mise en place d'architectures sécurisées pour les projets, qui est identifiée comme une opération informatique et non une opération sécurité.

…Mais les budgets sécurité restent globalement stables

Les réponses font ressortir majoritairement une stabilité du budget sécurité, avec cependant des extrêmes (augmentation ou régression) dans un pourcentage significatif. 45% des réponses en 2014, et 41% en 2010, indiquent que le budget sécurité est constant par rapport à l'année précédente.

Une part constante d'hôpitaux (17% aussi bien en 2010 qu'en 2014) connaît une augmentation du budget sécurité de plus de 10% par rapport à l'année précédente.

On constate cependant un pourcentage plus élevé d'hôpitaux déclarant avoir un budget en régression en 2014(4% en régression et 5% en forte régression, contre respectivement 1% et 2% en 2010).

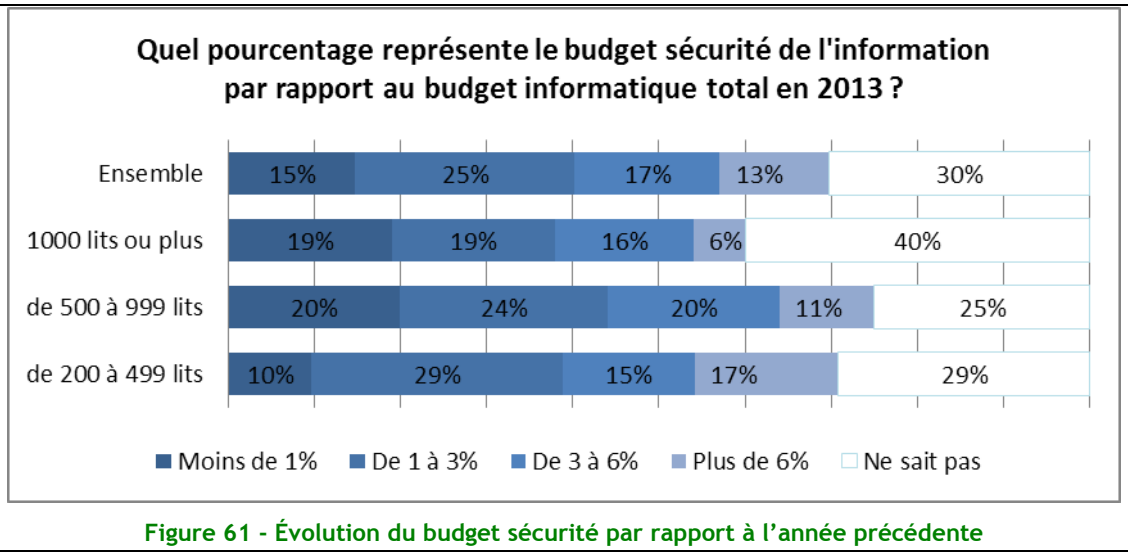

Figure 61 - Évolution du budget sécurité par rapport à l'année précédente

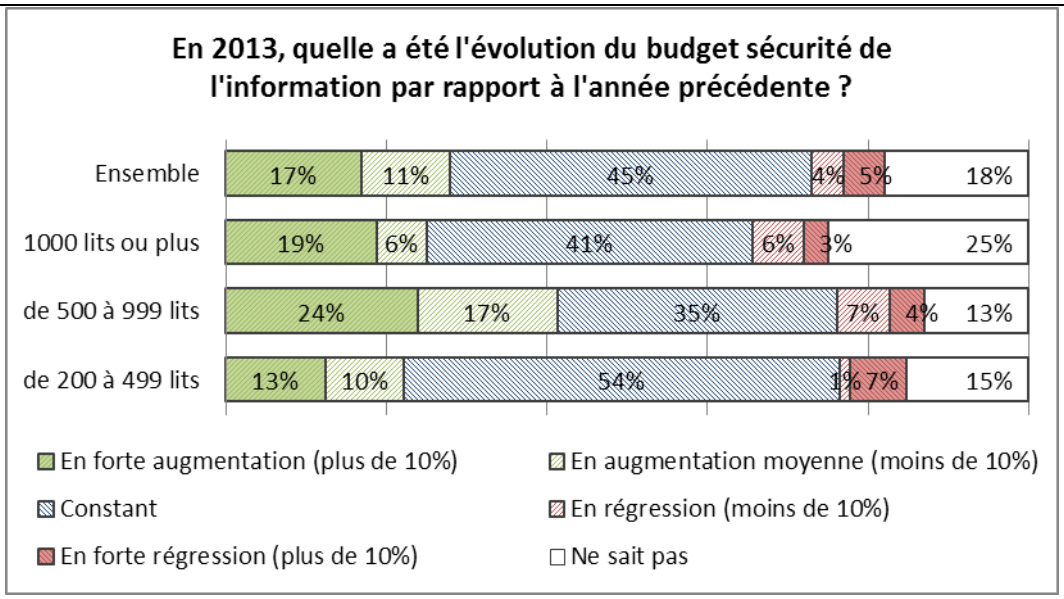

Figure 62 - Budget sécurité / budget informatique

Cette donnée devrait être suivie dans les prochaines enquêtes car elle ne reflète pas l'évolution vers la sécurisation imposée à la fois par le programme Hôpital Numérique et par la certification des comptes. Mais est-ce lié à la répartition Informatique / sécurité qui est délicate ? Et si on voulait faire la répartition, puisque l'argumentaire sécurité est fréquent, n'aurait-on pas la majorité du budget informatique sur la sécurité ? De fait, cette question de budget SSI n'a de sens que s'il existe une direction SSI, possédant son propre budget.

Augmentation du budget dédié aux solutions techniques

La plus grosse augmentation est constituée de la mise en place de solutions techniques (45% de l'échantillon connaît une augmentation), ce qui correspond au besoin de disponibilité du Système d'Information de production de soins. L'augmentation de mise en place de solutions métiers contribuant à l'informatisation du parcours de soins est une question dont la réponse peut s'interpréter de plusieurs façons : soit un recours plus important à la sécurisation applicative comme la mise en place d'un SSO, soit un renforcement de certaines fonctionnalités dans le cadre de la réduction des risques liés aux soins (par exemple renforcement des contrôles et alertes sur les processus de soins, interrogation en ligne de la base de données de référence des médicaments, développement de la traçabilité des actions présentée aux acteurs métier).

Un signal intéressant est l'augmentation dans 15% des réponses des postes contrôles/audits, mise en place d'éléments organisationnels, et formations/sensibilisations, ce qui peut indiquer une évolution vers un management de la politique de sécurité dans l'établissement.

Enfin, le pourcentage de réponses qui « ne savent pas » approche encore le quart (23%) : c'est un indicateur de l'absence d'un plan d'actions sécurité formalisé, valorisé et suivi.

Manque de budget et de personnel qualifié sont les principaux freins

Les premiers freins évoqués (52% manque de budget, 43% manque de personnel qualifié) sont significatifs de la situation des hôpitaux : mis à part les centres hospitaliers universitaires, les établissements publics et privés ont rarement les moyens de recruter un RSSI formé ou de disposer de personnel disponible et impliqué dans la sécurisation du SI.

Au plan organisationnel, les établissements désignent un « référent sécurité SI » qui est souvent issu de la Direction des Systèmes d'Information, mais on voit apparaître également des référents issus de la Direction Qualité ou de la Direction Générale.

Au plan des compétences, certaines régions s'organisent au sein d'une maîtrise d'ouvrage régionale (Groupement de Coopération Sanitaire pour l'e-santé) pour disposer d'une compétence sécurité mutualisée.

Néanmoins, l'évolution reste encore timide au regard des exigences de sécurité qui doivent s'imposer d'ici à 2017 aux établissements de santé dans le cadre des prérequis du programme Hôpital Numérique.

Thème 7 : Gestion des biens

Inventaire : processus en légère progression

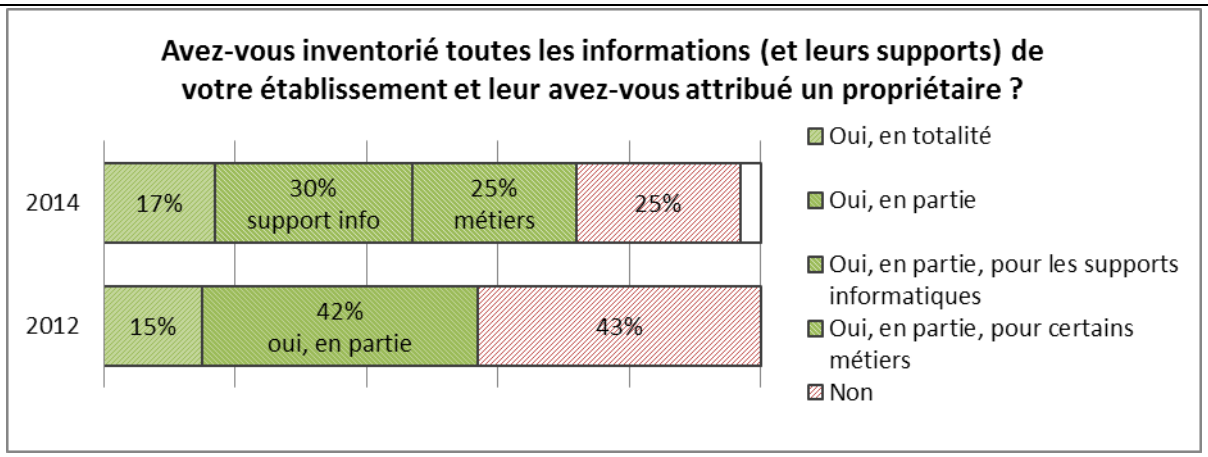

Figure 63 - Inventaire des biens

La proportion d'établissements ayant inventorié en totalité les informations et leur ayant attribué un propriétaire a augmenté seulement de 2% en quatre ans.

L'évolution des réponses ayant fait l'inventaire « en partie » en 2014 (29%+ 25%) reflète globalement une augmentation de 9% (contre 42% en 2010).

Cela peut paraître un écart peu significatif, mais l'intérêt de l'enquête de 2014 est la distinction entre inventaire des informations et inventaires des supports :

- 29% ont inventorié les supports informatiques, ce qui pourrait être un indicateur de l'augmentation du management des opérations informatiques (sauvegardes, plans de secours et de reprise,…), qui apparaît essentiellement suite à des incidents techniques impactant la disponibilité du SI,
- et 25% ont inventorié les informations et leur ont attribué un propriétaire, ce qui est probablement un indicateur du développement de l'inventaire dans le cadre d'une politique de sécurité de l'information et de la certification des comptes (l'inventaire des biens immatériels étant l'un des axes de la préparation à la certification des comptes).

Classification de l'information : bonne évolution

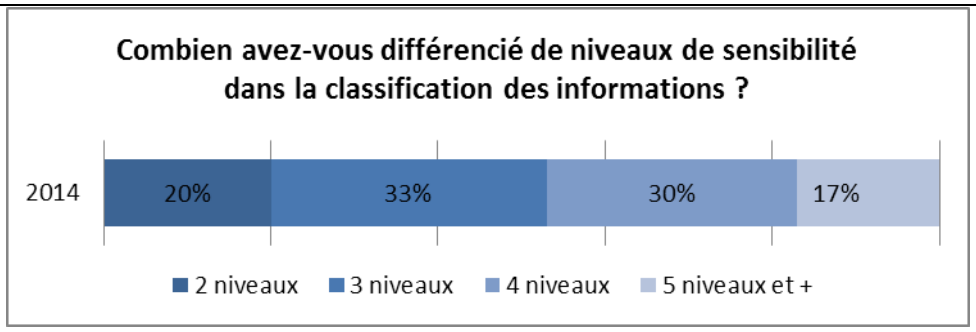

Figure 64 - Échelles de sensibilité utilisées pour la classification

Le graphique des réponses, ainsi que la comparaison avec les données de l'enquête de 2010, montrent que la situation évolue plutôt favorablement : la communauté a désormais basculé vers la mise en œuvre d'une politique de sécurité et de diffusion de l'information puisque désormais ce sont 61% des établissements qui ont commencé à classifier les informations, et que seuls 38% des établissements n'ont pas commencé (contre 51% en 2010).

L'identification de 5 niveaux ou plus, dans 18% des réponses, pourrait correspondre aux différents niveaux et périmètres de besoin de disponibilité (Dans les 4 heures, demi-journée, …) et de protection de la confidentialité de l'information médicale (dans l'unité où est pris en charge le patient, dans l'établissement, dans la communication avec les médecins correspondants,….).

60% des établissements ont réalisé une analyse de risque

L'analyse des risques liés à la sécurité de l'information est pratiquée de manière formelle dans 60% des établissements interrogés et sans équivoque par ceux qui disposent d'un référent sécurité SI. Pour 19% d'entre eux, le périmètre de l'analyse porte sur l'ensemble du Système d'Information, pour 27% sur les activités métiers qui sont au cœur du processus de soins comme le recommande la DGOS, les 13% restant étant des analyses limitées au périmètre de l'informatique.

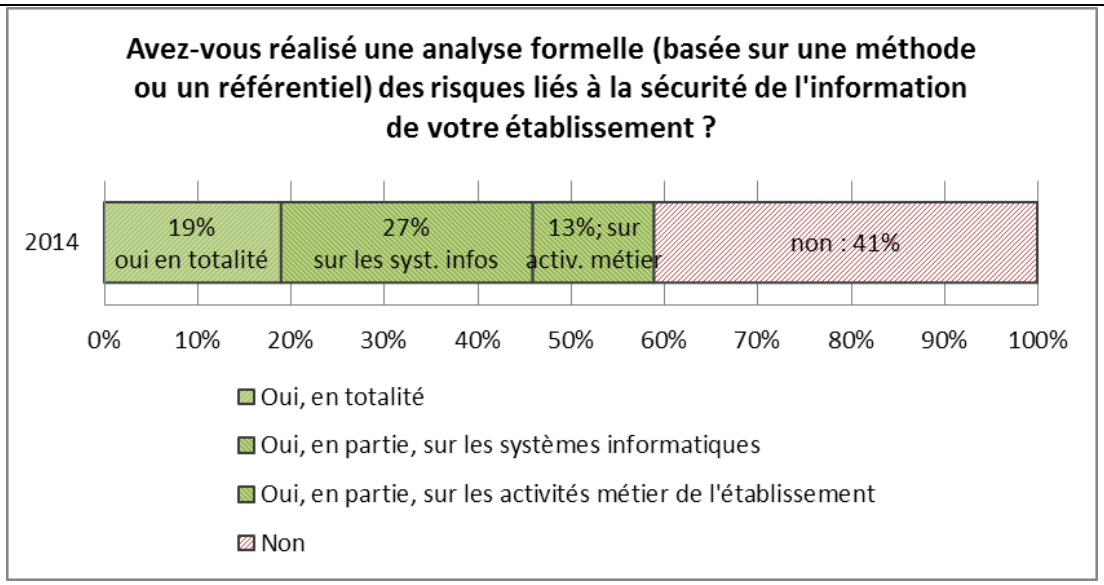

Figure 65 – Analyses de risques formalisées

EBIOS, la méthode la plus utilisée

Les méthodes les plus utilisées pour analyser les risques sont pour 26% la méthode EBIOS qui affiche une progression de 15% par rapport à 2010, probablement parce qu'elle est recommandée par le Ministère en charge de la Santé, l'ASIP Santé, et l'ANSSI, puis à hauteur de 20% la norme ISO 27005 ou des méthodes conformes aux activités décrites dans cette norme, ce qui est probablement lié aux cursus de formation des RSSI qui traitent de cette norme.

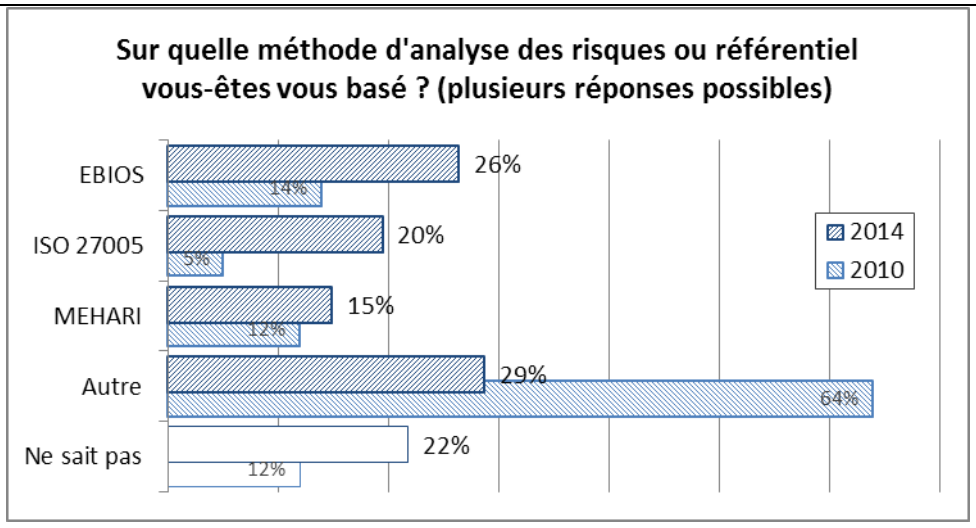

Figure 66 – Méthodes d'analyses des risques

Thème 8 : Sécurité des ressources humaines

Chartes d'utilisation du SI quasi généralisées

Près de 9 établissements de santé sur 10 disposent (89%) d'une charte d'usage ou d'utilisation du Système d'Information. Un certain nombre d'établissements (6%) ont une démarche en cours d'élaboration de la charte. La tendance est donc vers une généralisation, quelle que soit la taille de l'établissement.

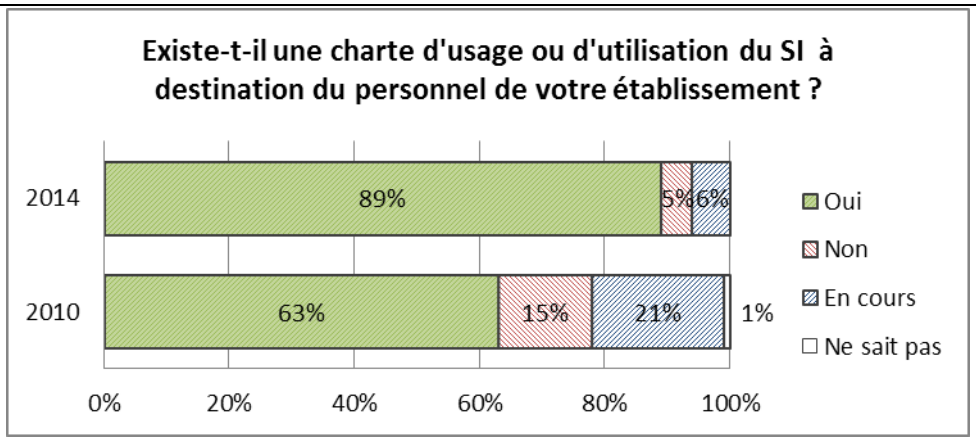

Figure 67 – Charte d'usage ou d'utilisation du SI à destination du personnel

Ces chartes sont largement communiquées. Plus de la moitié des établissements recherchent la signature de la charte par les utilisateurs, afin de s'assurer d'une prise de connaissance, et non plus de l'annexer uniquement au Règlement Intérieur (qui s'applique à tout agent intervenant dans l'établissement).

Pour plus de 8 établissements sur 10, la direction est impliquée dans l'élaboration de la charte, et est soucieuse de la soumettre aux Instances Représentatives du Personnel.

Toutefois, les chartes ciblent avant tout le personnel des établissements. Seuls 33% des établissements disposent d'une charte à destination des prestataires/fournisseurs, et 14% ont une démarche en cours.

Ces chartes constituent des outils de management et de sensibilisation à destination de l'ensemble des utilisateurs accédant au Système d'Information. Une généralisation vers les prestataires/fournisseurs accédant au Système d'Information est donc nécessaire.

Un peu plus de la moitié des établissements s'assure 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 plutôt assez bien présente dans les établissements de plus de 1.000 lits, mais la couverture à 100% n'est pas garantie.

Des programmes de sensibilisation à la sécurité de l'information toujours modestes

À peine un tiers des établissements ont un programme de sensibilisation à la sécurité de l'information. Les établissements de plus de 1 000 lits sont aussi sur cette tendance.

Toutefois, le programme Hôpital Numérique devrait permettre l'augmentation certaine de cette tendance à la hausse.

Les moyens pour assurer la sensibilisation restent relativement traditionnels. Le moyen principal reste la publication de 'news' dans l'intranet, la publication de mails, ou des articles dans le journal interne.

Des difficultés intrinsèques à mettre en place des actions périodiques et récurrentes de tout le personnel persistent. Ceci est essentiellement lié au fait que les personnels de santé consacrent leur présence dans l'hôpital aux patients et suivent en priorité les formations métier ; leur hiérarchie ne privilégie pas non plus leur inscription à des sessions de sensibilisation spécifiques à la sécurité, surtout si elles impliquent plus d'une demi-heure d'absence.

Un nombre important d'établissements (40%) développe des solutions propres pour la sensibilisation du personnel. Une connaissance de ces moyens serait intéressante, ainsi que le niveau d'efficacité associé. Il pourrait notamment s'agir de messages sécurité lors de la connexion ou en veille écran, d'informations

lors de session d'intégration, lors de formations métier ou spécifiques à la mise en œuvre de nouveaux progiciels (ex. dossier patient informatisé), voire dans le cursus des écoles et des facultés.

La mesure de l'efficacité de l'impact de ces programmes et des actions de sensibilisation est recherchée (de 20% à 28% des établissements entre 2010 et 2014) dans un souci d'optimisation des moyens, mais reste encore à développer.

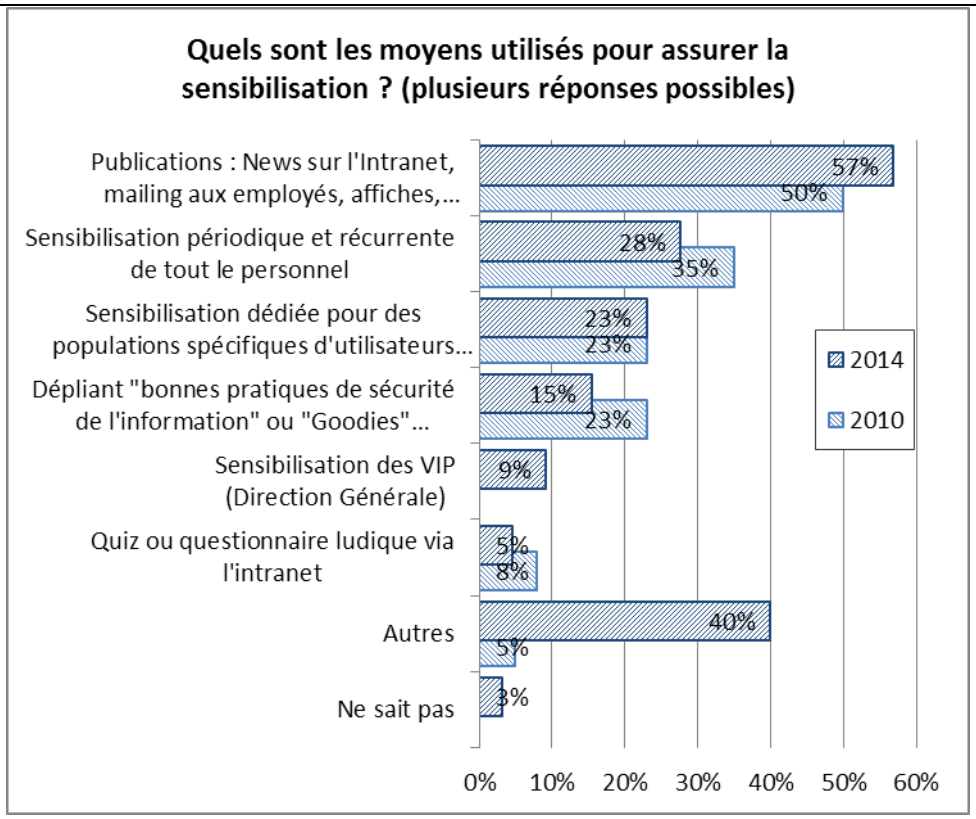

Figure 68 – Moyens utilisés pour assurer la sensibilisation

Une sensibilisation des acteurs décideurs apparaît ; dès lors qu'ils sont convaincus eux-mêmes, ceux-ci sont souvent les relais majeurs pour porter les messages à leurs équipes. Cette tendance devrait se développer avec notamment des programmes de la tutelle (ex. programme Hôpital Numérique, certification HAS,…). Le niveau de maturité à la sécurité de l'information des établissements devrait donc augmenter.

Thème 9 : Sécurité Physique

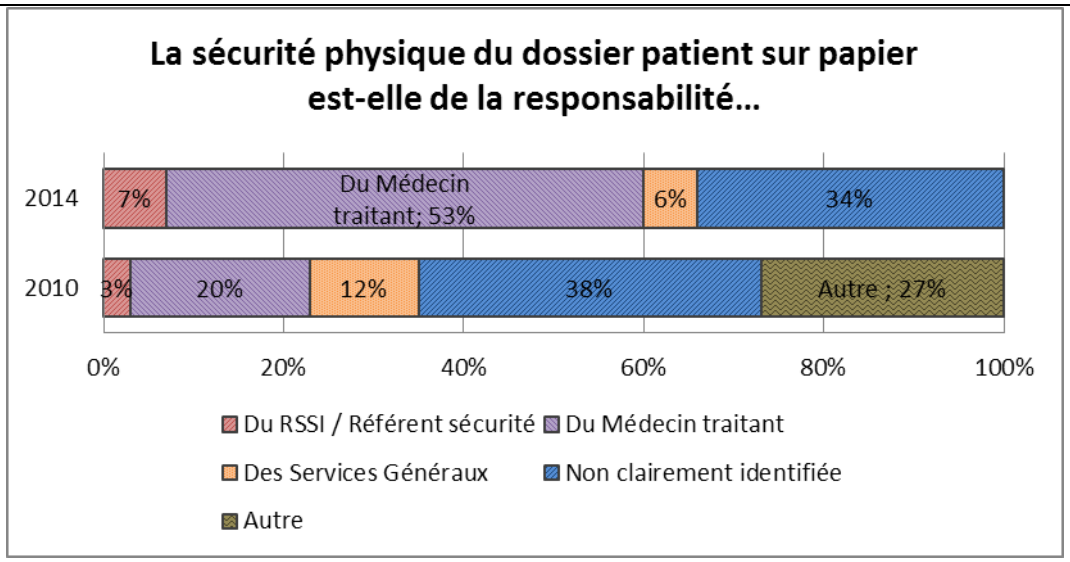

Figure 69 – Responsabilité de la sécurité physique du dossier patient

Comme en 2010, la question porte sur la responsabilité de la sécurité physique du dossier patient sur support papier.

Car, même si l'informatisation progressive des dossiers des patients (qui facilite la conservation numérique et l'accès immédiat aux données) pose la question du maintien en parallèle des dossiers patients sur papier, volumineux et de gestion lourde et coûteuse, le dossier patient sur support papier présente toujours aujourd'hui dans les hôpitaux une réalité réglementaire incontournable.

En effet, les dispositions légales relatives à la preuve écrite, visant la conformité aux exigences de la loi n° 2000-230 du 13 mars 2000, obligeraient à mettre en place, auprès des professionnels de santé des dispositifs de signature électronique dans les systèmes informatiques produisant les pièces à signer (comptes rendus, résultats d'examens), sans oublier les patients qui ont également des documents à signer, tels que ceux relatifs à leur consentement. Cette mise en œuvre exige des efforts organisationnels et des investissements techniques et financiers qui ne sont pas facilement à la portée des hôpitaux.

Des faits récents montrent aussi que l'absence de preuve signée (papier ou signature électronique), malgré la présence d'éléments enregistrés, voire validées électroniquement, ne permettent pas forcément une prise en compte sur le plan juridique ; une des illustrations, un patient décédé avait émis le souhait que son dossier ne soit pas communiqué à la famille ; cependant l'hôpital, n'ayant pu présenter de preuve signée par le patient, n'a pu faire valoir le seul enregistrement dans le SI de son souhait et a dû communiquer le dossier aux ayants-droits.

En 2014, pour 53% des personnes interviewées (composées de 73% de de responsables / directeurs des Systèmes d'Information ou informatiques et 17% de RSSI), la sécurité physique du dossier papier est du ressort des professionnels de santé (contre 20% en 2010).

6% (contre 12%) estiment que la responsabilité est portée par les services généraux, ce qui peut concerner les archives rattachés aux services généraux.

Mais comment se fait-il que pour 34% des personnes la responsabilité de la sécurité physique du dossier papier n'est pas clairement identifiée (contre 26% en 2010) ? N'est-ce pas tout simplement parce la responsabilité de cette sécurité physique est prise « au pied de la lettre », et dépend donc du lieu de stockage ? Sous responsabilité du service de soins quand le patient est présent, puis sous responsabilité des archives quand le patient est sorti ? En tout cas, la réponse ne varie pas sensiblement en fonction de la taille de l'hôpital.

Thème 10 : Gestion des communications et opérations

Un nomadisme qui augmente mais sous le contrôle de la DSI

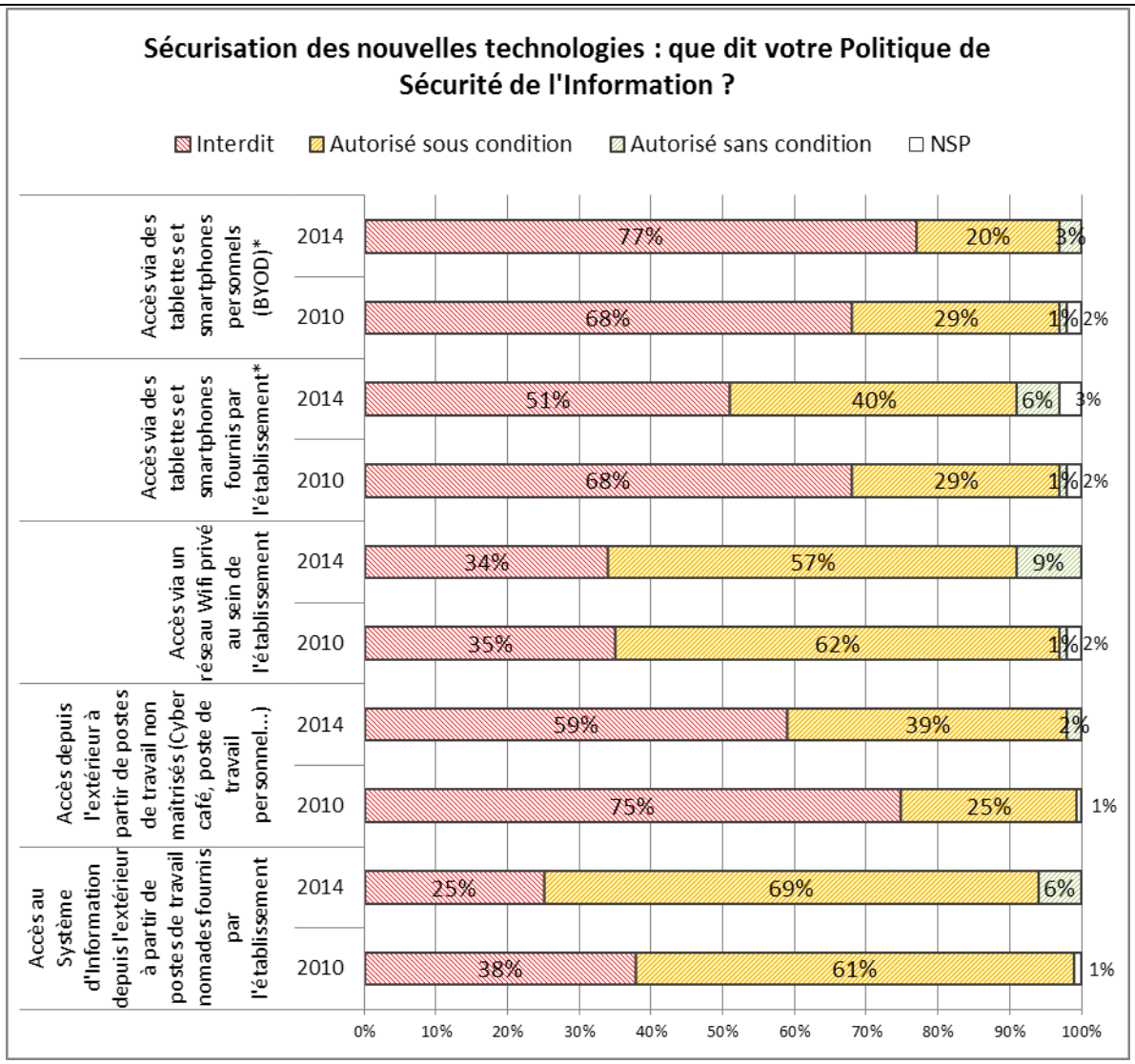

Figure 70 – Position de la PSSI sur les accès extérieurs au SI

Les hôpitaux continuent à ouvrir l'accès à partir de l'extérieur au Système d'Information, même si cela se fait majoritairement à partir d'équipements fournis par les établissements, que ce soit ordinateurs portables (75% l'autorisent, +14 points par rapport à 2010) ou tablettes/smartphone (46% l'autorisent, mais assurément moins en 2010 ; pas de comparaison avec 2010 possible, car le critère « BYOD/fournis par l'établissement » n'était pas pris en compte).

En ce qui concerne l'accès au S.I. des hôpitaux à partir de smartphone et autres tablettes appartenant au personnel (BYOD), celui-ci est plutôt limité (seulement 23% des établissements l'autorisent). L'analyse bénéfice/risque de l'usage des équipements mobiles dans les hôpitaux s'est semble-t-il orienté vers un besoin de contrôle, par les DSI, des équipements connectés, et ce malgré l'existence d'un phénomène de mode en faveur du BYOD ces dernières années. Pour autant, les DSI ont investi pour permettre à leurs utilisateurs de se connecter à partir de postes de travail non maitrisés, que ce soient dans les cybercafés ou à partir de leurs ordinateurs personnels, (41% des établissements l'autorisent, +16 points par rapport à 2010), cela devrait à terme se traduire par une autorisation d'accès indifférenciée pour tous les périphériques.

Messagerie instantanée et Réseau Sociaux peu autorisés

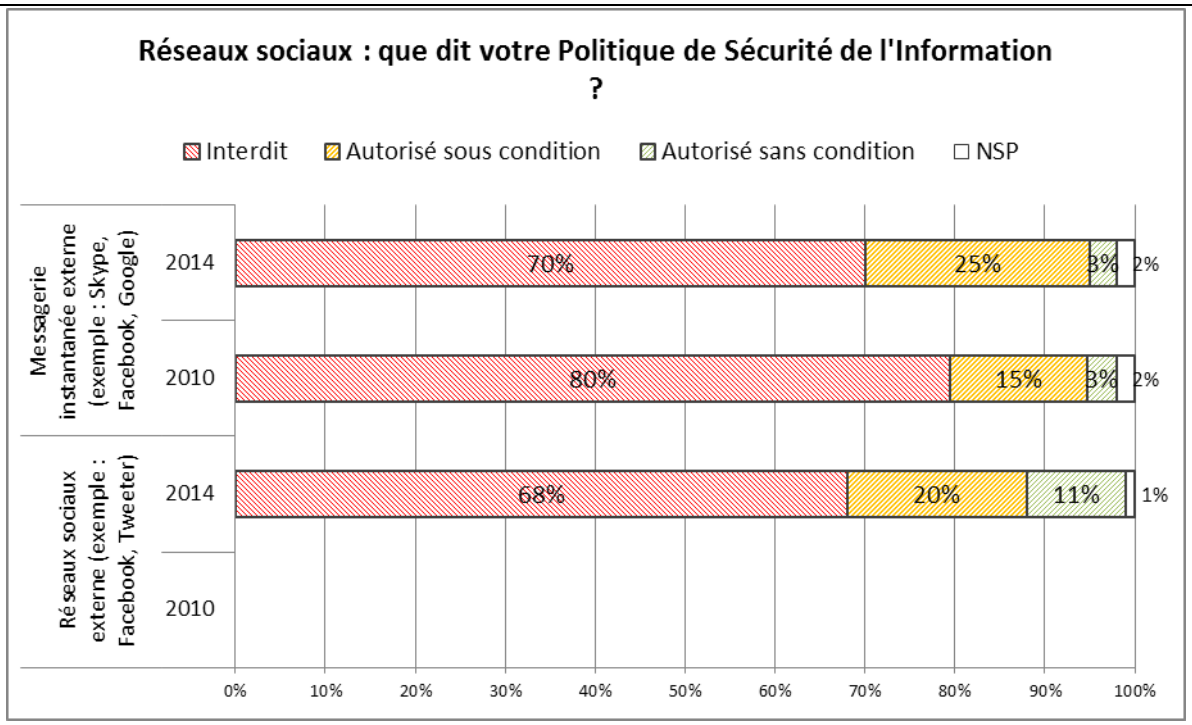

Figure 71 – Utilisation des réseaux sociaux et messageries instantanées

L'accès aux outils de messagerie instantanée externe et aux réseaux sociaux reste globalement interdit (70% des cas) aux personnels des hôpitaux. Ce qui ne veut pas dire que les hôpitaux rejettent les réseaux sociaux, bien au contraire, ceux-ci étant de plus en plus souvent utilisés dans les plans de communication. Ces technologies n'étant pas liées à l'activité professionnelle des utilisateurs, elles apparaissent comme des sources de risques (problème de confidentialité, divulgation d'information, diffusion de virus, absence de moyens de contrôle, perte de productivité, …).

L'interdiction de ces technologies Internet est à mettre en opposition avec le chiffre de 86% des établissements indiquant autoriser l'accès à internet sans filtrage ni d'URL, ni protocolaire. Comment ces établissements peuvent-ils contrôler réellement l'interdiction de la messagerie instantanée ou des réseaux sociaux ?

Le déploiement de la VOIP et de la TOIP continue

Se basant sur un marché technologiquement mature et permettant un retour sur investissement bien évalué, l'adoption par les hôpitaux des technologies de VOIP et de TOIP continue (+20 points en 4 ans pour arriver à 51%).

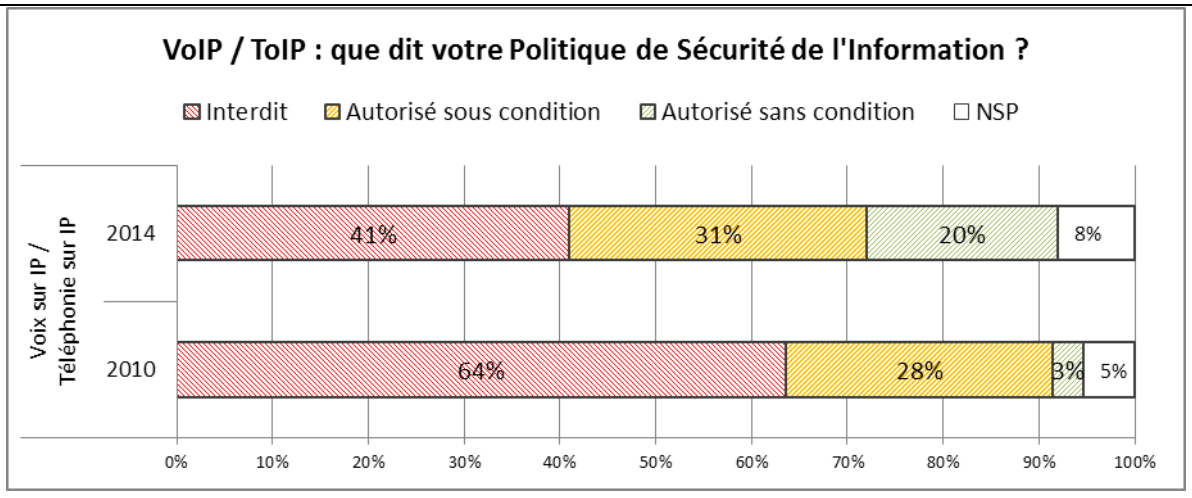

Figure 72 – Utilisation de la VoIP / ToIP

Lutte antivirale, protection contre les intrusions et gestion des vulnérabilités

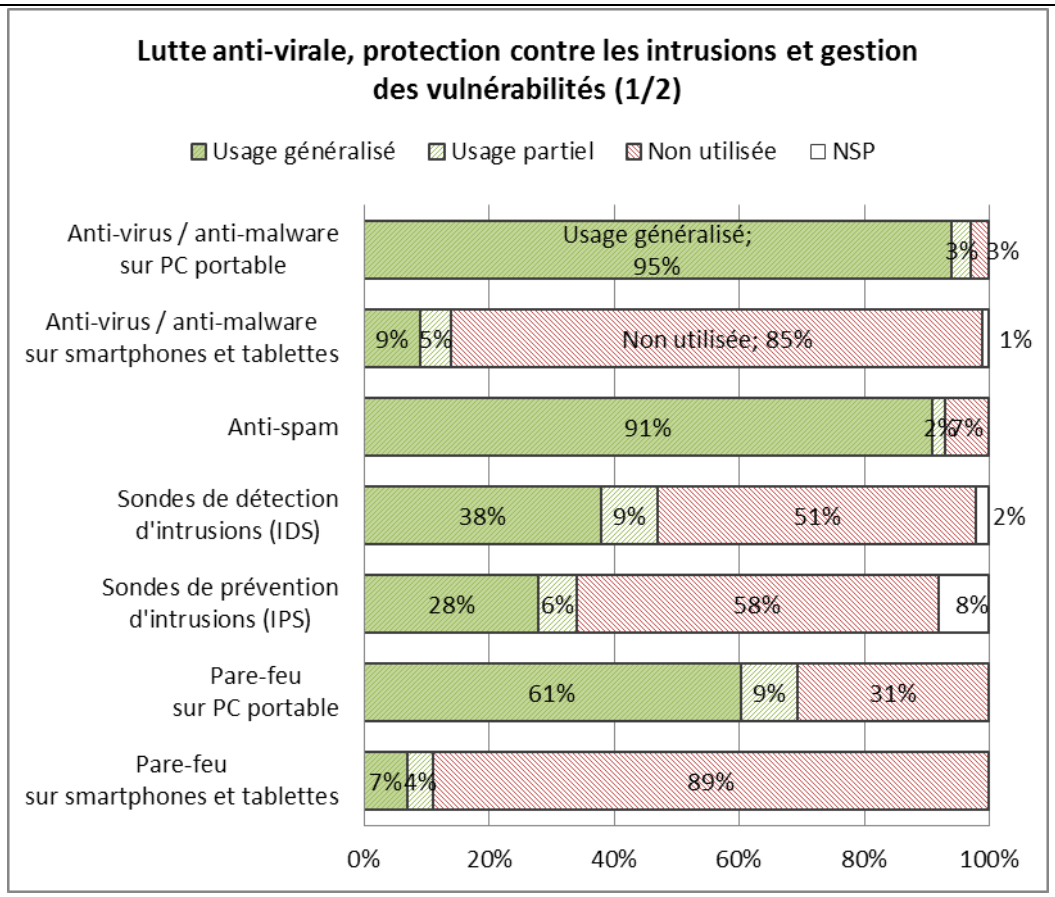

Figure 73 – Lutte contre les vulnérabilités et les intrusions (1/2)

Si les ordinateurs (fixes et portables) maintiennent un niveau de protection très élevé vis-à-vis des risques « classiques » (anti-virus, pare-feu, anti-spam), protéger les équipements mobiles (smartphones et tablettes) ne semble pas être à l'ordre du jour. La protection de ces derniers présente en effet des difficultés techniques mais aussi juridiques dans le cadre du BYOD (intervention sur des équipements appartenant à l'utilisateur).

L'adoption du chiffrement des données sur les équipements mobiles reste très faible, moins de 20% sur les ordinateurs portables et il est inexistant sur les smartphones ou tablettes. Ces chiffres relativement faibles peuvent en partie être expliqués par l'usage fait des ordinateurs portables dans les hôpitaux. Ceux-ci servent surtout à la mobilité à l'intérieur de l'établissement, et donc contiennent pas ou peu de données sensibles.

Par contre, dans le contexte de l'échange de données, les hôpitaux adoptent largement les technologies de chiffrement (75% des établissements, voir même plus de 90% pour les établissements de plus de 1000 lits). Au regard des obligations liées à l'échange des données de santé, ce taux devrait continuer à augmenter.

On traite dans ce cadre aujourd'hui principalement le chiffrement du flux et non des données.

L'utilisation d'IDS et d'IPS est moins répandue dans les hôpitaux que dans l'industrie, et ce alors que ces solutions sont de plus en plus souvent intégrées aux boitiers firewall. Ces outils permettent pourtant de détecter et de bloquer la propagation d'un certain nombre d'attaques avec un impact réduit sur le Système d'Information lors de leur installation. Est-ce une méconnaissance du potentiel des outils ? Ou l'absence de personnel compétent en ce domaine ?

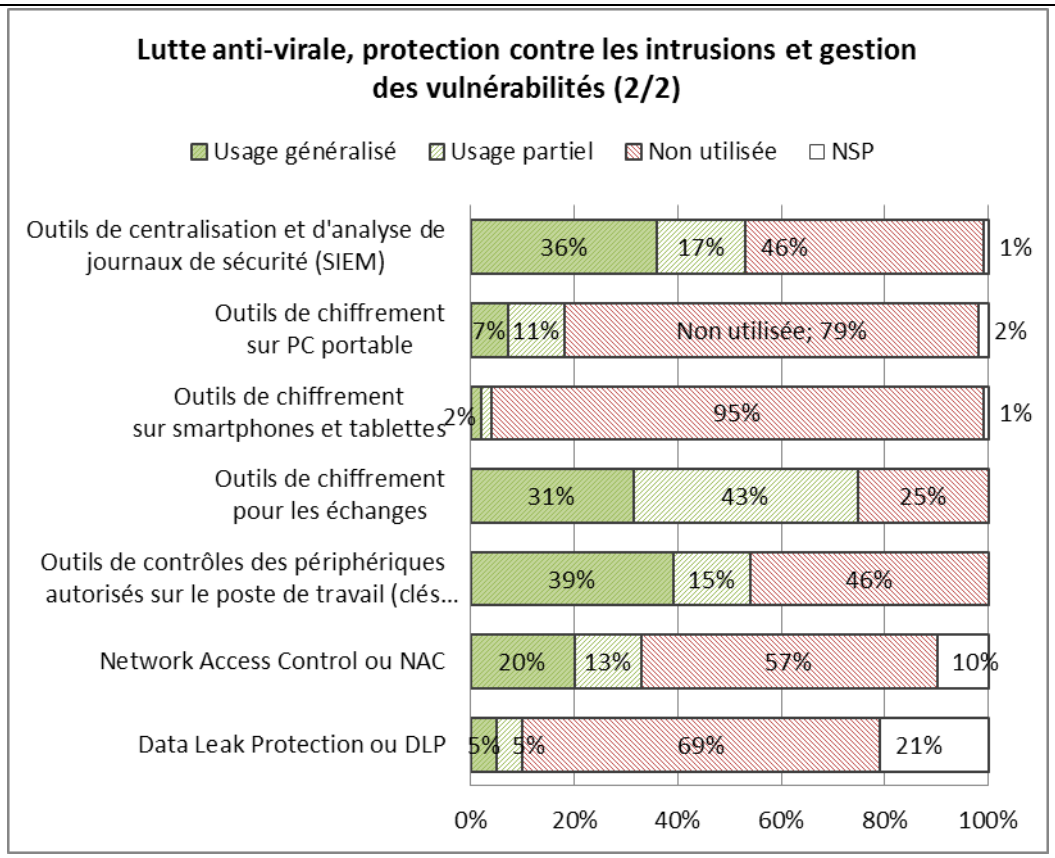

Figure 74 - Lutte contre les vulnérabilités et les intrusions (2/2)

Le déploiement des SIEM (outils de centralisation et d'analyse des journaux de sécurité) continue au sein des hôpitaux avec 1 établissement sur 2 équipé d'une telle solution. L'utilisation de ces outils est pertinente au regard de l'augmentation de la complexité des attaques informatiques auxquelles sont exposés les Systèmes d'Information et aux besoins de réactivité et d'analyse des incidents constatés. Les éditeurs de solution de sécurité avancent dans cette direction avec leurs nouveaux produits, puisque pour la détection des APT (Advanced Persistent Threats) ils cherchent à corréler l'ensemble des détections pour repérer ces attaques.

Le NAC (Network Access Control) et le DLP (Data Leak Protection) restent des technologies peu utilisées au sein des dispositifs de sécurité des hôpitaux. Si ces deux technologies ont fait leurs preuves dans le contrôle, pour la première, de l'accès physique aux réseaux et des flux d'informations pour l'autre, ce sont des technologies dont la mise en œuvre reste délicate.

Le recours à l'infogérance stagne, avec un manque de suivi par des audits ou des indicateurs

Il n'y a pas de changement significatif sur la part de systèmes informatiques placés sous contrat d'infogérance en 2014 : 28% des hôpitaux en ont placé une partie et 3% la totalité, contre respectivement 25% et 1% en 2010.

Mais si l'on considère les tailles d'établissements, on constate alors une grande disparité entre les gros établissements (1000 lits et supérieurs), qui ne confient leurs SI en infogérance qu'à 18%, et les autres établissements, qui, eux, en confient en moyenne 35%.

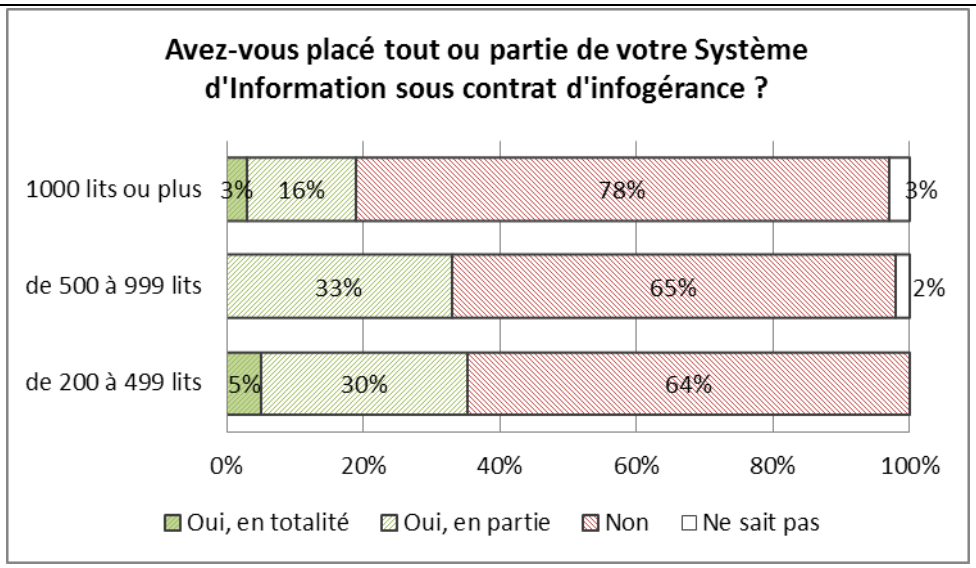

Figure 75 - Recours à l'infogérance

La part d'infogérance n'a pas encore rattrapé ses niveaux de 2005 (27% et 10% en 2005), probablement la conséquence des plans nationaux successifs, visant à une meilleure maitrise de ses SI.

Comme il y a 4 ans, les hôpitaux qui ont placé leur SI (en totalité ou pour partie) en infogérance sont 66% à ne pas établir d'indicateurs de suivi sur cette infogérance, sauf les plus gros établissements qui en font dans 50% des cas.

De même, les hôpitaux sont 70% à ne pas auditer leur infogérance (à l'exception, là aussi, des gros établissements de plus de 1000 lits, qui réalisent des audits dans 50% des cas, une fois par an ou ponctuellement). Ces chiffres montrent une légère dégradation de la situation par rapport à 2010.

Les technologies de Cloud Computing sont principalement privées

Concernant les technologies de Cloud Computing, un hôpital sur 5 y a recours. Les types d'architectures utilisées sont, dans 65% des cas, des Cloud privés, dans 13% des cas des Cloud hybrides, et dans 19% des cas des Cloud publics.

Thème 11 : Contrôle des accès

Technologies ou approches de sécurisation utilisées : plusieurs facteurs concourent à développer la carte d'établissement multifonction.

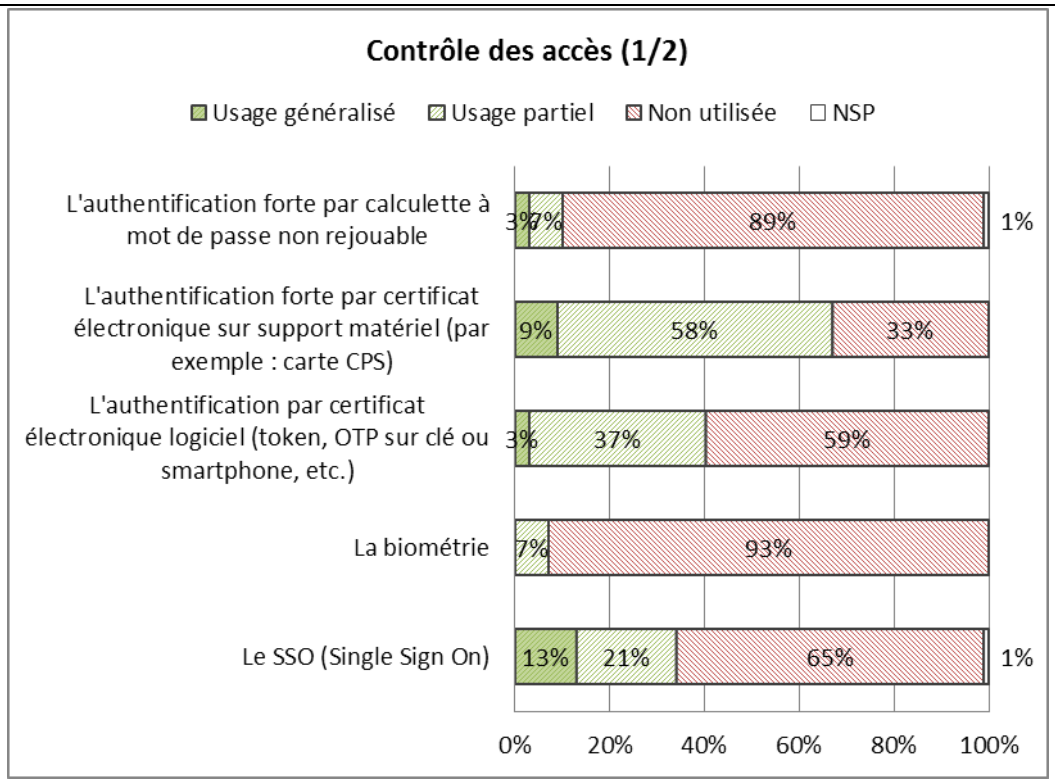

Figure 76 - Technologies ou approches de sécurisation utilisées pour le contrôle des accès (1/2)

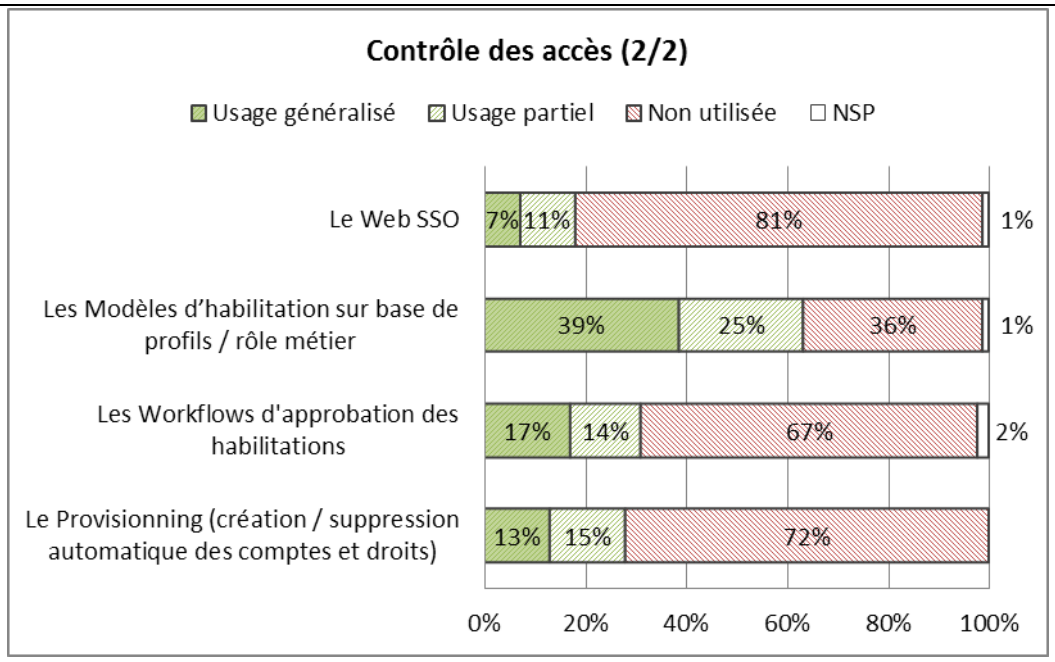

Figure 77 - Technologies ou approches de sécurisation utilisées pour le contrôle des accès (2/2)

Ces chiffres s'inscrivent dans le contexte d'authentification forte imposée par la réglementation hospitalière (Cf. décret de confidentialité des données de santé dans le cadre du projet Hôpital 2012).

L'usage de la calculette est très peu répandu (10%) : cela représente une perte de temps pour l'utilisateur (saisie de l'identifiant et du code unique à chaque connexion), un risque de perte du dispositif, et le coût d'acquisition est important pour l'établissement. D'où le fait que cette solution reste marginale dans les hôpitaux.

L'emploi d'une carte contenant le certificat numérique est le mode d'authentification forte le plus répandu (67%) : Tout d'abord à cause d'une incitation forte par le décret, afin de permettre le déploiement d'une solution pour la confidentialité des données de santé. Un existant est repris par rapport à la carte CPS, distribuée gratuitement aux professionnels de santé des hôpitaux depuis 2013, et déployée dans quelques hôpitaux pour l'accès au SI et la validation des médecins. Ce principe se généralise dans certains hôpitaux sous la forme d'une carte d'établissement multifonction (contrôle accès logiciel, locaux, self, identification visuel du personnel, …) avec des cartes hybrides puce IAS ECC et une puce sans contact Mifare.

L'authentification par certificat logiciel reste contraignante pour les utilisateurs, bien qu'étant employée dans 40% des hôpitaux. La solution consistant, pour chaque connexion, à envoyer un SMS est difficilement gérable pour le personnel dans un hôpital.

Quant à la biométrie, elle est refusée par la CNIL et rejetée par les utilisateurs (remontée des syndicats), car est vue comme une atteinte à la personne.

Le SSO est utilisé dans 34% des établissements : il permet la gestion des mots de passe des utilisateurs dans les unités de soins, facilite et optimise l'utilisation des applications très diverses dans le monde hospitalier. Il apporte du confort à l'utilisateur qui a souvent 5 à 10 applications métier différentes, d'où sa tendance à se développer. Couplé souvent avec le projet carte d'établissement, il nécessite qu'un agent soit présent sur le poste de travail.

WebSSO (18%) : il apporte une contrainte, le passage obligé par un navigateur WEB. Moins souple il est cependant intéressant pour les connexions distantes. Son utilisation reste limitée en interne, surtout vu les risques dans le cadre des postes partagés, qui sont majoritaires dans les services de soins.

Modèle d'habilitation (64%) : cette organisation constitue un gain très important pour l'hôpital car elle automatise ou a minima optimise la génération des comptes et droits associés dans les multiples applications métiers, et évite les problèmes de ressaisie et d'incohérence des droits applicatifs. La gestion des droits est habituellement une opération très chronophage, qui demande des ressources en personnel, surtout si l'on veut s'assurer d'une conformité dans ce cadre.

Les Workflow d'approbation, utilisés dans 31% des établissements, ont cependant peu d'intérêt si des systèmes de provisionning sont mis en place (28%).

Ce dernier apporte l'informatisation des modèles d'habilitation. C'est un projet majeur, qui nécessite la mise en œuvre et la définition de règles. De plus en plus de directions y voient un intérêt et adhèrent à la solution. Mais sa mise en œuvre informatique reste difficile car elle nécessite une analyse rigoureuse et une réactivité pour l'évolution des matrices d'habilitations à la demande des métiers.

Autre contrainte : l'interface entre les différentes applications hospitalière, car les échanges inter applicatifs sont peu normés et peu prévus par les éditeurs. Le provisionning tend cependant à se développer, la prise de conscience a commencé.

Forte progression des procédures de création/modification/suppression des comptes utilisateurs nominatifs

L'augmentation de 2010 vers 2014 s'explique par la mise en place du décret sur la confidentialité des données de santé, qui impose la responsabilisation nominative sur les données médicales (médecins, infirmières, etc.).

L'informatisation touche l'ensemble des fonctions sensibles de l'hôpital et tous ses domaines. Il y a un net renforcement de la sensibilisation à la sécurité dans les hôpitaux, notamment avec l'ouverture vers les réseaux externes (médecine de ville, échange inter hôpitaux, etc.), l'accès au SI par des acteurs multiples ou non permanents (étudiants, internes, intérimaires, etc.), et le besoin de traçabilité (y compris des applications métiers).

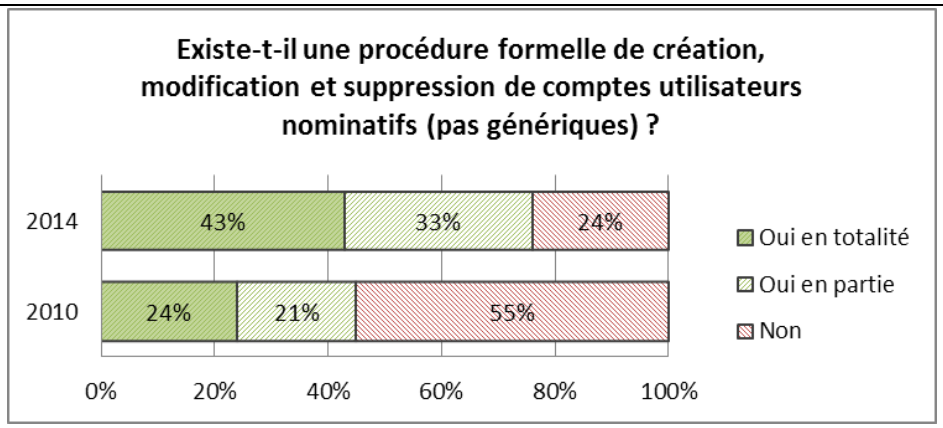

Figure 78 - Existence de procédures de gestion des comptes utilisateurs nominatifs

Cette procédure existe aussi spécifiquement pour les administrateurs, même si elle progresse moins. Il reste cependant des contraintes liées aux applications (compte de service inter applicatifs).

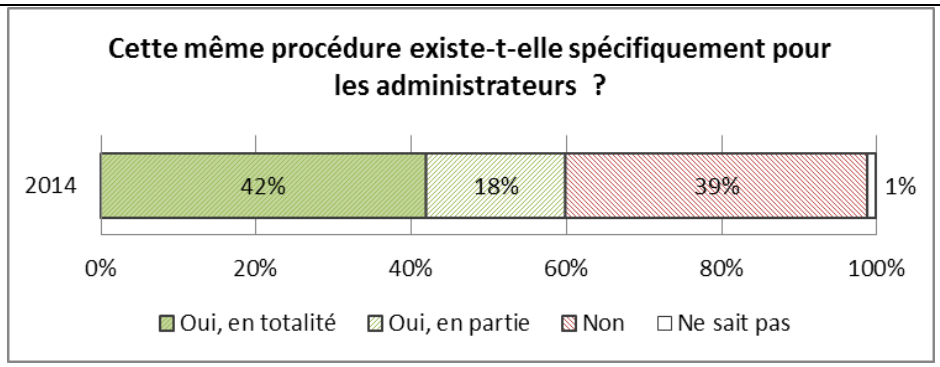

Figure 79 - Existence de procédures de gestion des comptes administrateurs

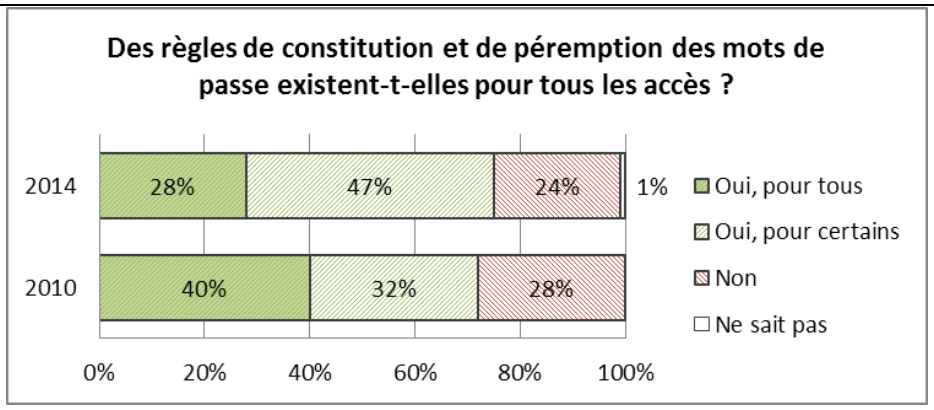

Figure 80 – Existence de règles de gestion des mots de passe

En matière de gestion des mots de passe (règles de constitution et de péremption), il y a une évolution notable des bonnes pratiques initiées depuis 2010. Ceci peut s'expliquer par l'importance des données médicales et sensibles dans le milieu hospitalier.

Mais le renforcement de la dureté du mot de passe est contraignant voire perturbant pour l'utilisateur malgré une bonne sensibilisation à la sécurité.
L'augmentation de la mise en place d'authentification (Windows) primaire forte (carte à puce avec code PIN) peut expliquer le recul de la constitution et de la péremption des mots de passe pour certaines applications. En effet, la mise en œuvre de mécanismes d'authentification forte au niveau de l'ouverture de la session du poste de travail garantit un très bon niveau de sécurité. Il est généralement couplé avec un logiciel SSO qui facilite l'accès aux applications par les utilisateurs qui n'ont plus à renseigner leur login et mot de passe dans les applications métier.

Thème 12 : Acquisition, développement et maintenance des SI

Les S.I, qu'ils soient directement développés en interne ou via des prestataires, voire acquis (progiciels), se doivent d'être régulièrement surveillés concernant la sécurité. Les vulnérabilités étant monnaie courante, il convient de mettre en place une veille et des processus de mise à jour particuliers.

Bien qu'elle progresse depuis 2010, la veille en vulnérabilités n'est pas encore arrivée à un niveau de maturité suffisant pour être systématisée au sein des hôpitaux.

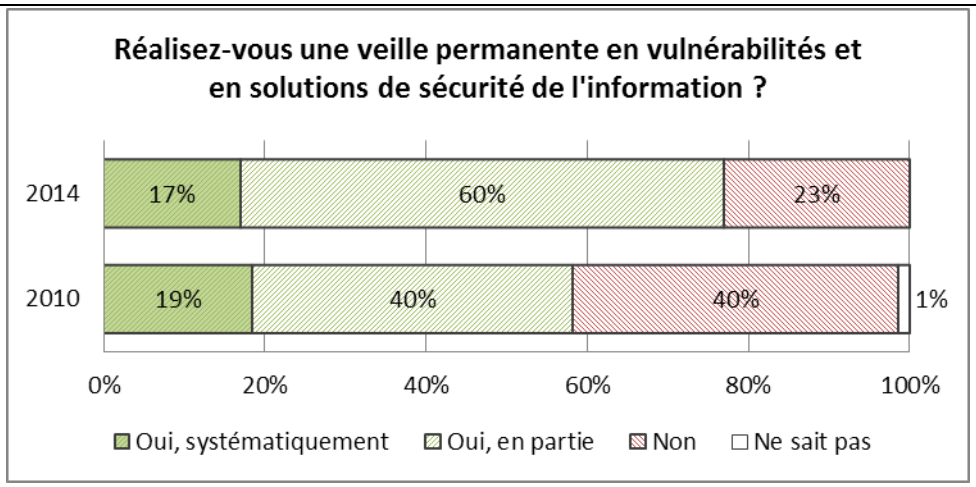

Figure 81 - Veille en vulnérabilités et solutions

Les procédures de gestion des correctifs de sécurité sont en léger recul, effet probable d'une forte augmentation de l'informatisation des hôpitaux et du parc installé de matériel parfois très spécifique.

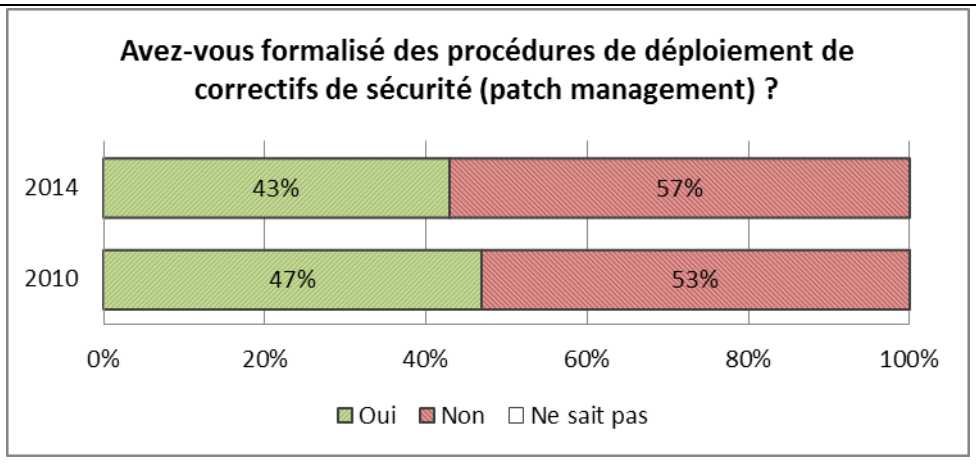

Figure 82 - Gestion des correctifs

Le développement sécurisé quasi-inexistant

On peut se demander si cela est dû à la forte place des progiciels ou matériels spécifiques ? Ou si c'est parce que les métiers et directions privilégient la mise en œuvre très attendue des aspects fonctionnels et techniques dans leurs solutions, en oubliant ou décalant un peu la sécurité ?

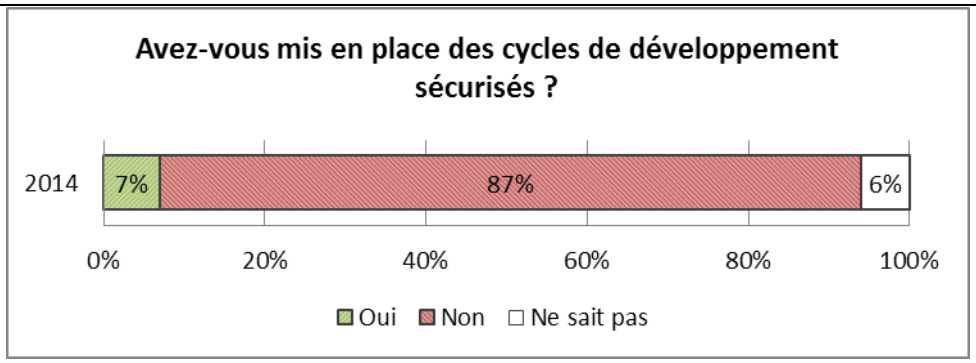

Figure 83 - Développements sécurisés

Pour que ce taux augmente, faudra-t-il une prise de conscience plus forte des développeurs, des chefs de projet informatiques et des directeurs des risques encourus dans les développements non sécurisés, voire des impacts plus visibles des incidents avérés ?

Thème 13 : Gestion des incidents

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

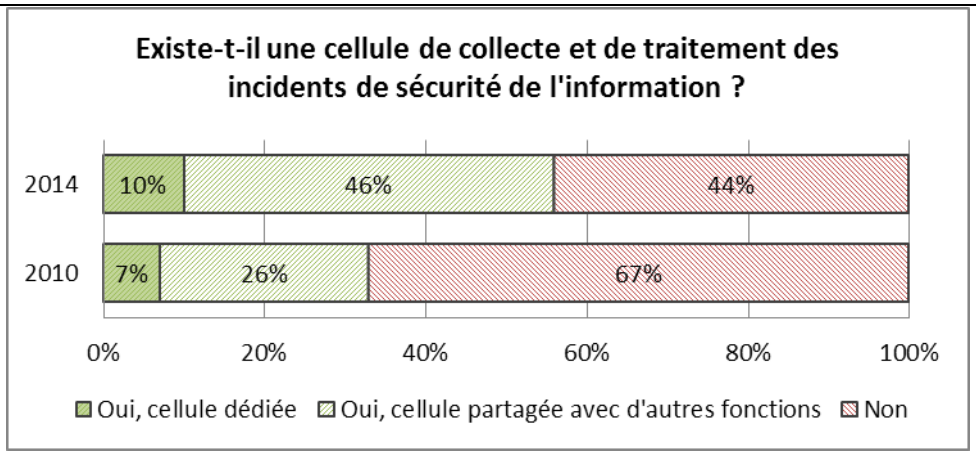

Figure 84 - Organisation de la gestion des incidents

De plus en plus d'hôpitaux (56% contre 33% en 2010) disposent d'une équipe chargée de collecter et traiter les incidents de sécurité.

Sur les 9% d'hôpitaux qui disposent d'une cellule dédiée, les hôpitaux de grande taille représentent 19%, et les petits hôpitaux seulement 5%. Par contre, les 47% d'hôpitaux ayant des cellules partagée avec d'autres fonctions sont répartis à 51% de petits hôpitaux et 41% d'hôpitaux de grande taille. Ceci est a priori lié à une optimisation des ressources disponibles.

Et pourquoi pas la mise en œuvre d'une cellule de gestion des incidents 'sécurité de l'information', qui déclinerait également les 'risques médico-légaux' en liaison avec les juristes de l'établissement ?

Types d'incidents de sécurité collectés par la cellule

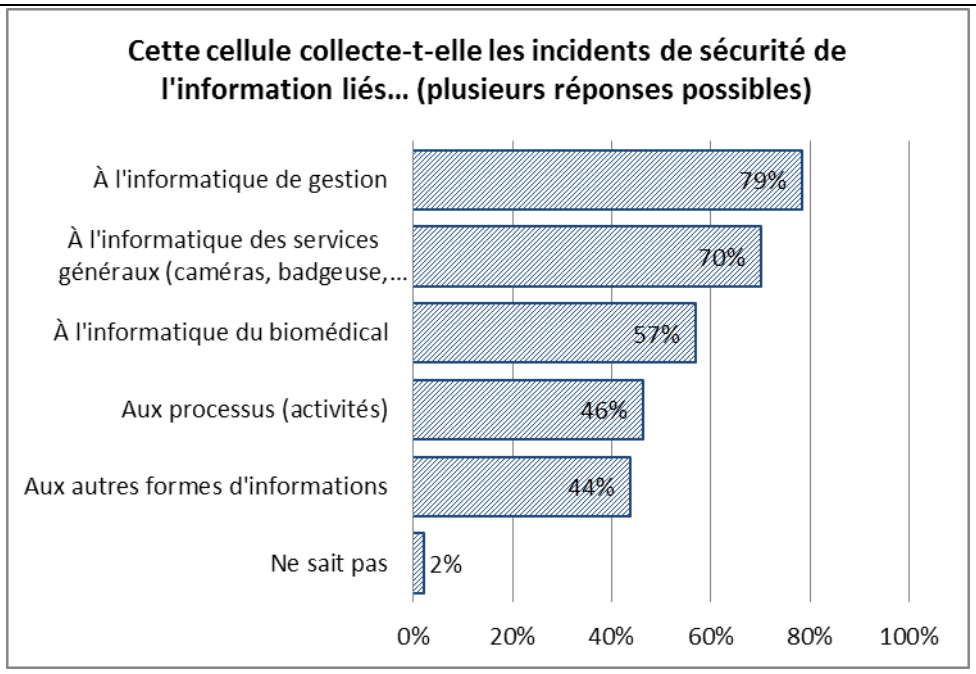

Figure 85 – Types d'incidents collectés

Les incidents de sécurité liés à l'informatique de gestion et des services généraux représentent la part la plus importante, soit respectivement 79% et 70%, voire 90% pour les moyens et gros hôpitaux.

Les incidents liés à l'informatique des dispositifs biomédicaux sont à 57%, ce qui n'est pas négligeable vu la difficulté d'intégrer dans le SI ces dispositifs. L'identification de ces incidents est motivante pour les DSI, car elle présente un bon levier pour traiter ce sujet.

Et nous constatons que les incidents liés aux processus et autres formes d'informations sont significativement moins associés aux incidents de sécurité du SI, probablement car ils sont gérés directement par les équipes qualité et risques des hôpitaux.

Dépôt de plaintes suite à des incidents liées à la sécurité de l'information

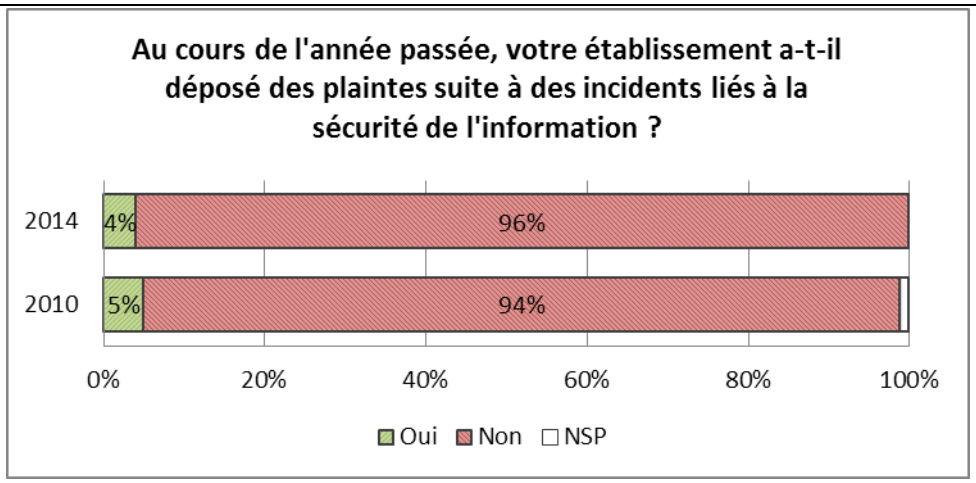

Figure 86 – Dépôt de plainte suite à des incidents SSI

Alors que les incidents de sécurité du SI sont de plus en plus fréquents dans les hôpitaux, et donnent parfois lieu à publication par les médias (surtout en cas de plainte d'un patient), les dépôts de plainte n'augmentent pas depuis 2010, même si les hôpitaux de taille importante sont à plus de 9% à avoir au moins une fois déposé plainte.

Probablement que les établissements de santé devraient porter plus systématiquement plainte, dans les prochaines années, en cas d'incident de sécurité.

Le dépôt de plainte est en effet nécessaire 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.

Une sinistralité mesurée en recul…

On observe un recul global de la sinistralité. Ce qui, mis en parallèle avec le développement des cellules de traitement et de suivi des problèmes liés au Système d'Information, indique que les différentes mesures prises par les DSI (lutte contre les attaques, PRA, formation…) ont un impact concret sur la survenue des incidents ou tout du moins sur leur connaissance et leur traitement.

L'ordre du classement évolue peu par rapport à la précédente étude, avec, dans le trio de tête des incidents auxquels le plus d'établissement sont confrontés, la panne d'origine interne, le vol ou la disparition de matériel, et la perte de services essentiels.

Si 30% des établissements remontent au moins un incident lié à une infection virale, 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.

Il est à noter que malgré cette sinistralité liée à des actes malveillants détectée et mesurée, il y a toujours très peu d'hôpitaux qui déposent des plaintes.

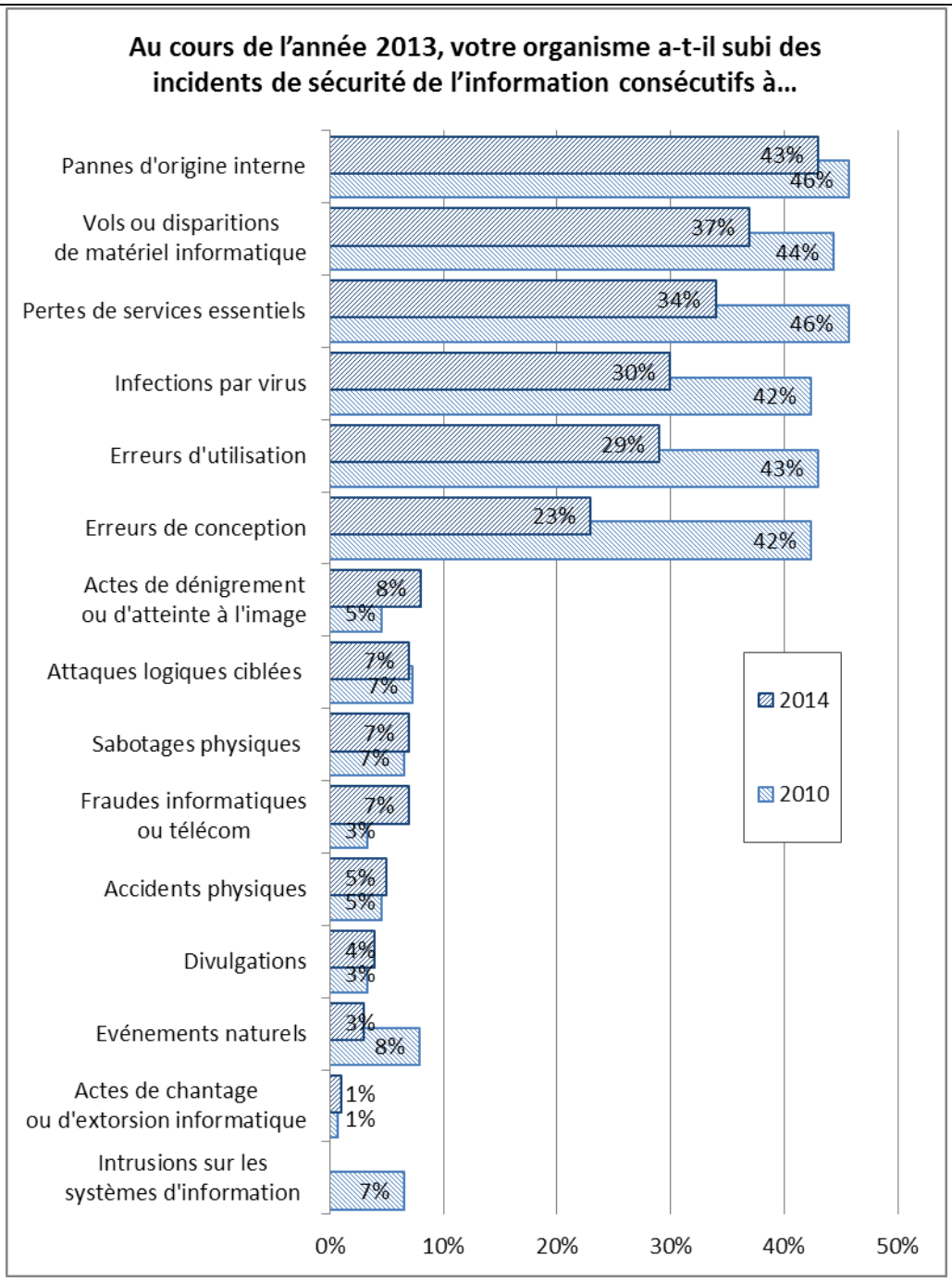

Figure 87 – Types d'incidents survenus

La perception des incidents doit cependant être différente suivant les établissements. En effet, en rapprochant le nombre moyen d'incidents pour ceux qui en ont déclarés et le nombre d'établissement déclarant avoir été confronté au dit incident, il y a des résultats surprenants. Si l'on s'intéresse aux incidents liés aux infections par virus, la moyenne d'occurrence de survenue est de 8,9 pour les hôpitaux en ayant au moins rapporté un. Mais comme 70% ne rapporte aucun incident liés à une infection par virus (alors qu'ils ont très probablement tous eu au moins une alerte de détection d'un virus), cela peut supposer que certains établissements caractérisent la détection d'un virus comme un incident de sécurité, alors que pour d'autres le seuil de caractérisation est lié à des conséquences plus graves.

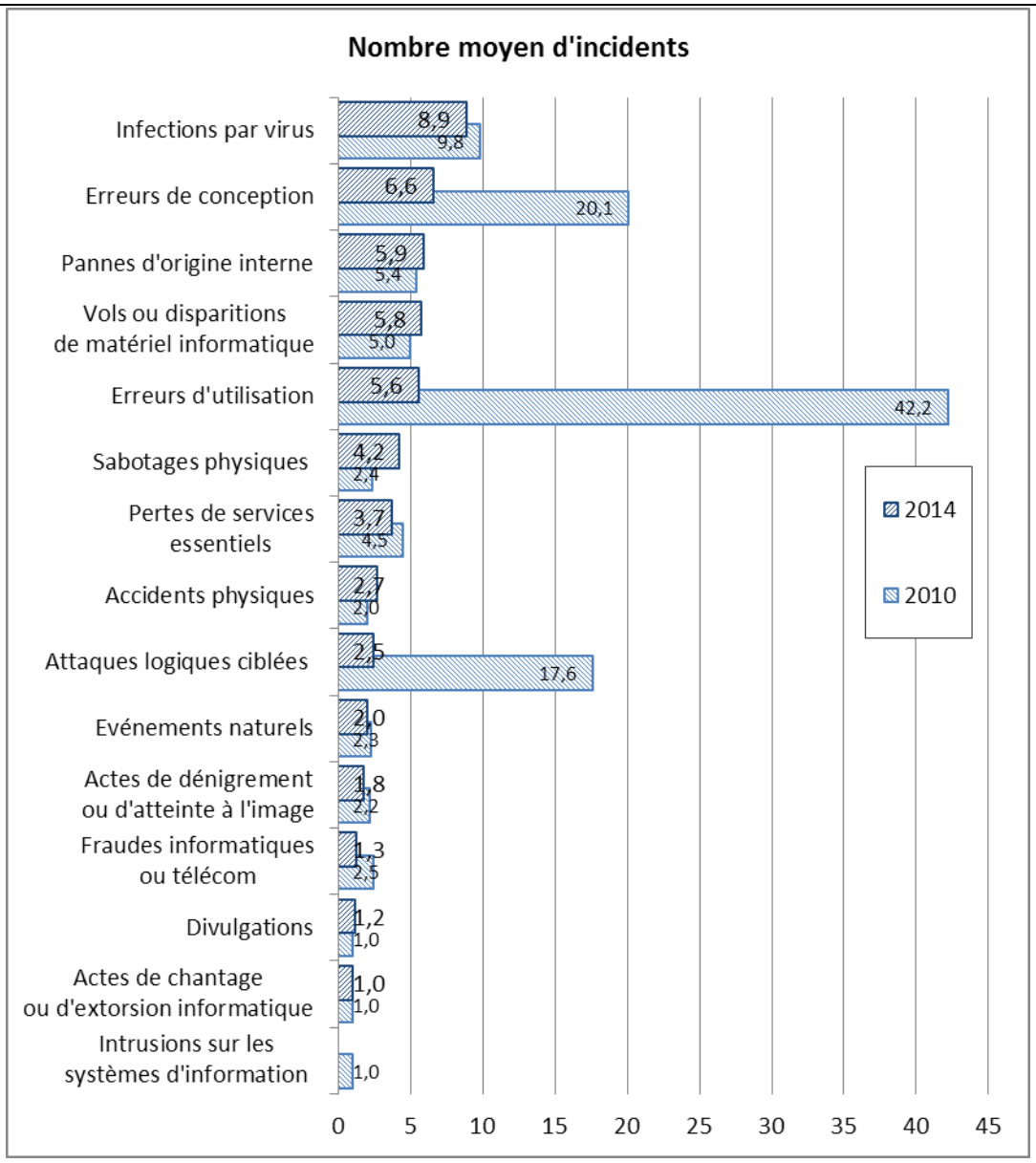

Figure 88 – Nombre moyen d'incidents par hôpital

Peu d'analyse des impacts financiers

Peu d'hôpitaux (moins de 1 sur 3) font une analyse de l'impact financier des incidents survenus sur le Système d'Information, et c'est une pratique que l'on retrouve principalement dans les grands établissements.

Quand cet impact financier est quantifié, on observe qu'il est principalement couvert soit par un financement préventif du risque (police d'assurance) ou intégré au budget courant.

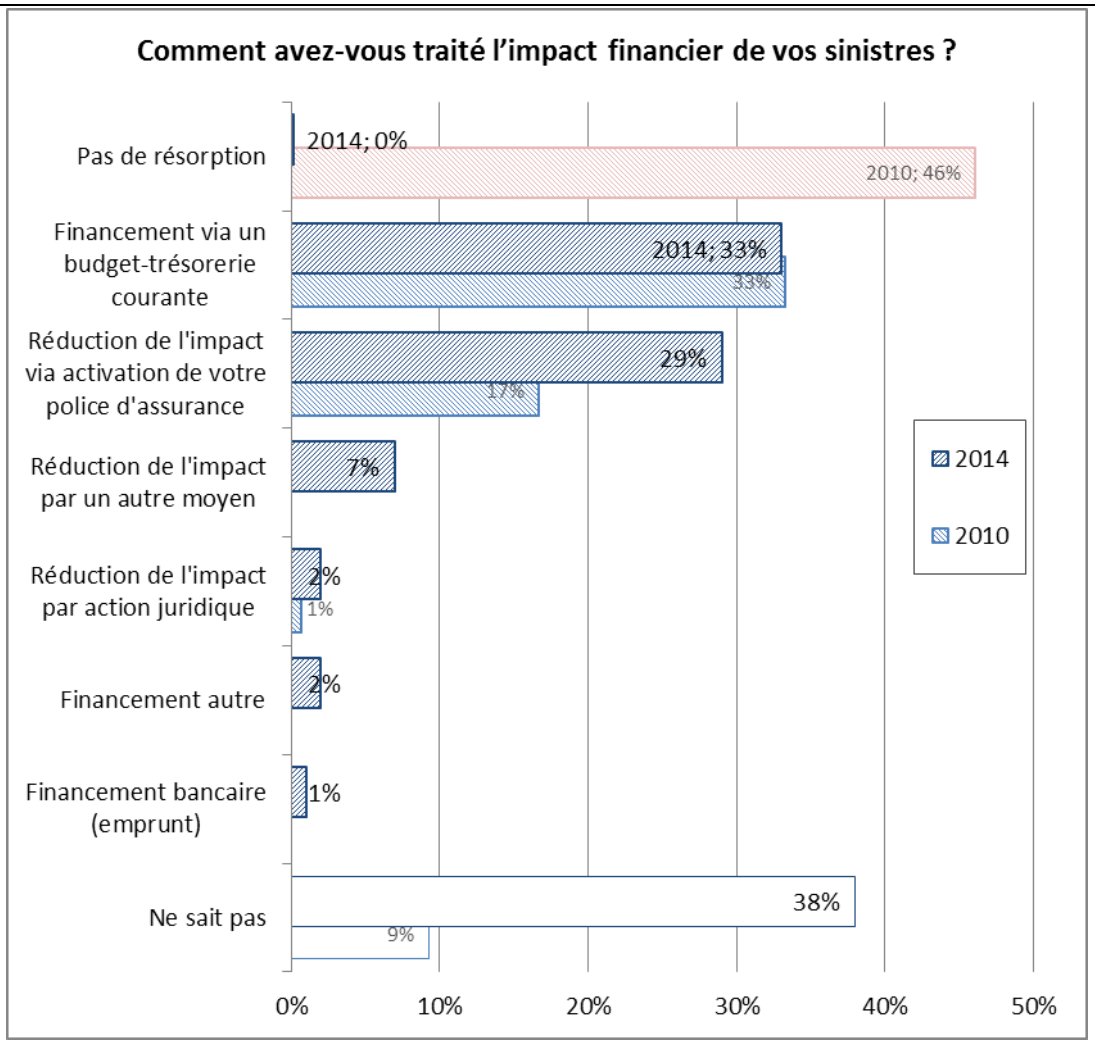

Figure 89 - Traitement de l'impact des sinistres

Thème 14 : Gestion de la Continuité

Une gestion de la Continuité d'Activité qui progresse dans le monde des hôpitaux.

Les hôpitaux traitent en majeur partie l'indisponibilité du SI (65%) et plus d'un hôpital sur deux a pris en compte l'indisponibilité de leurs locaux. Tout comme le monde de l'entreprise, on peut en revanche toujours s'interroger sur le fait que l'indisponibilité d'un fournisseur essentiel ne soit prise en compte que dans un cas sur 5.

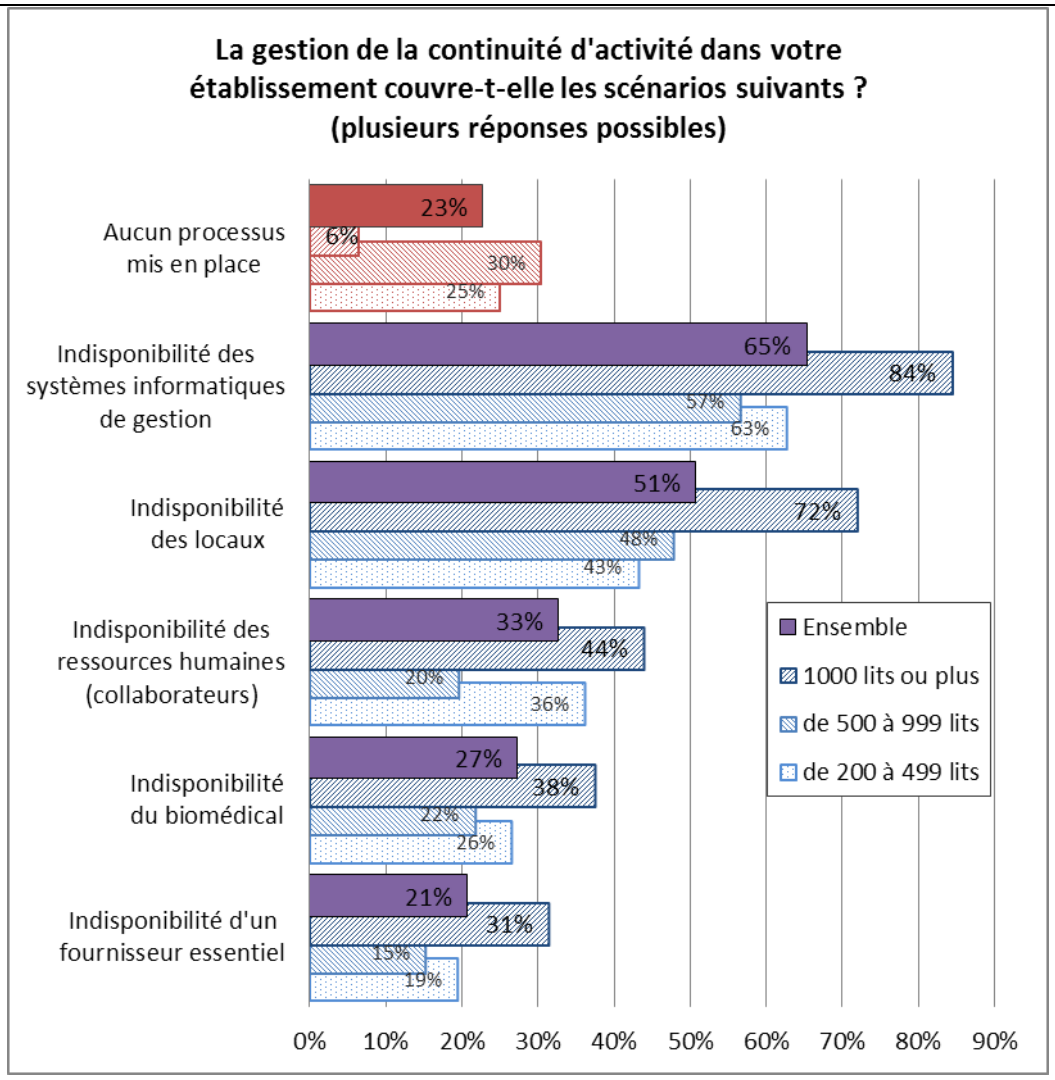

Figure 90 - - Scénarii couverts par la gestion de la continuité d'activité

Confirmation de la progression de la prise en compte des exigences métiers

Le nombre d'hôpitaux ayant un processus formalisé de Continuité d'Activité représente plus de 40%. Ce résultat est en net progrès et est plutôt rassurant par rapport à l'étude de 2010 qui en comptabilisait près de 50% en moins !

Il reste néanmoins beaucoup à faire à l'avenir. En effet, près d'un hôpital sur 4 annonce toujours ne pas avoir réalisé d'évaluation de ses exigences de continuité Métier.

Tout comme pour le monde des entreprises, le fondement peut éventuellement provenir de la possible externalisation de certaines ressources (PAAS, SAAS ou IAAS).

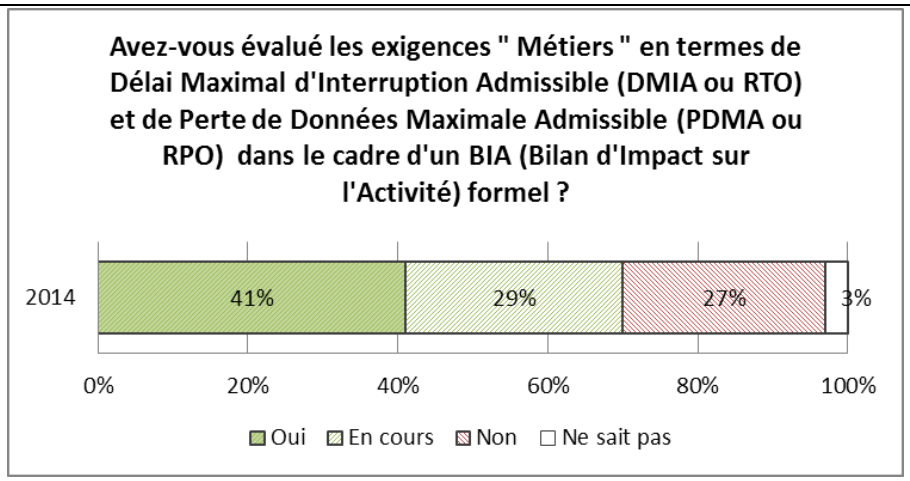

Figure 91 - Prise en compte des exigences métiers dans le cadre d'un BIA

Des exercices utilisateurs dont la fréquence a en moyenne diminué considérablement

En l'espace de 4 années, les résultats s'avèrent insolites. En effet, par rapport à 2010, on constate une très forte baisse en termes de fréquence des exercices et particulièrement pour ceux situés dans la tranche « Jamais ». Cela résulte-t-il de notre contexte économique, ou bien d'une difficulté certaine à réaliser des exercices utilisateurs, ou encore de la complexité pour la compréhension de ce qui doit être couvert par les tests ?

Il n'en demeure pas moins que l'étude nous interpelle sur ces résultats inquiétants. À l'avenir, les personnes en charge de la Continuité d'Activité dans les hôpitaux devront inclure davantage la participation des « Métiers ».

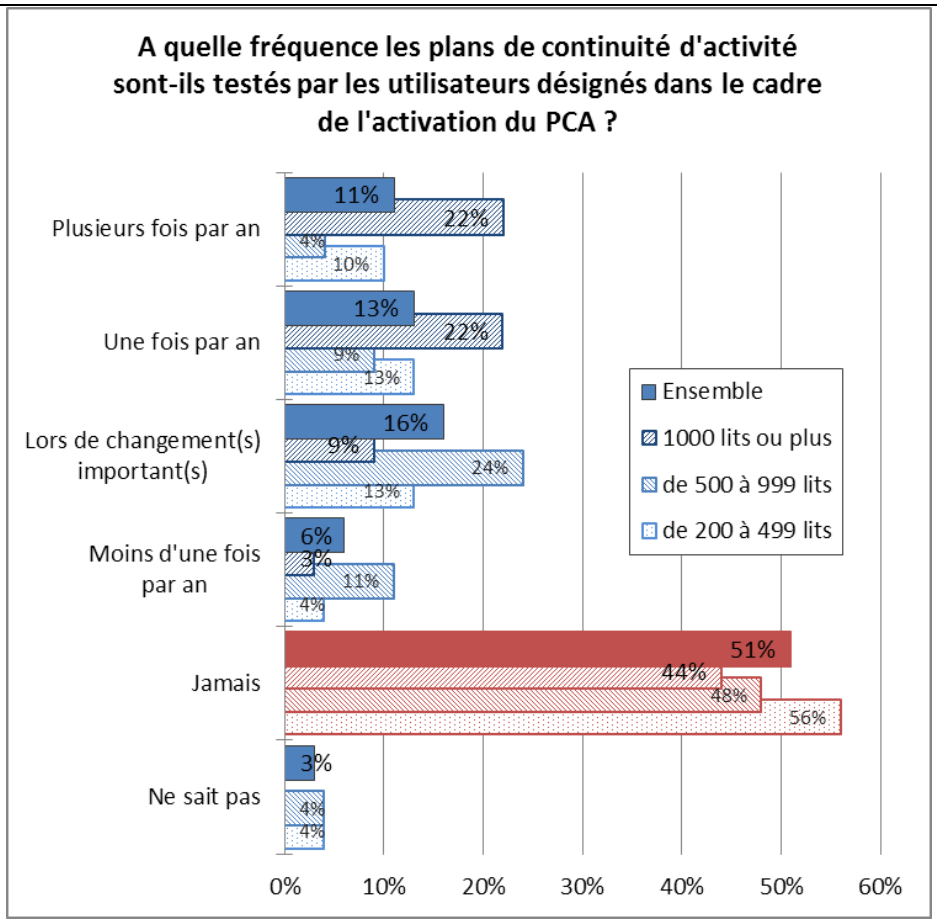

Figure 92 - Fréquence des exercices utilisateurs

Des exercices techniques dont la fréquence va devoir progresser

Tout comme pour les exercices Métier, près de la moitié des hôpitaux n'effectuent jamais de test technique. Ceci se révèle également vrai quelle que soit leur taille. Seuls 11% d'entre eux affirment réaliser plusieurs tests techniques au cours d'une même année.

Ceci est singulièrement inquiétant au regard de la forte dépendance des services hospitaliers à leurs Systèmes d'Informations et au regard des incidents. A-t-on peur du risque technique que l'on prend à effectuer ces tests ? A-t-on peur de ne pas pouvoir revenir à une situation normale dans les délais attendus ?

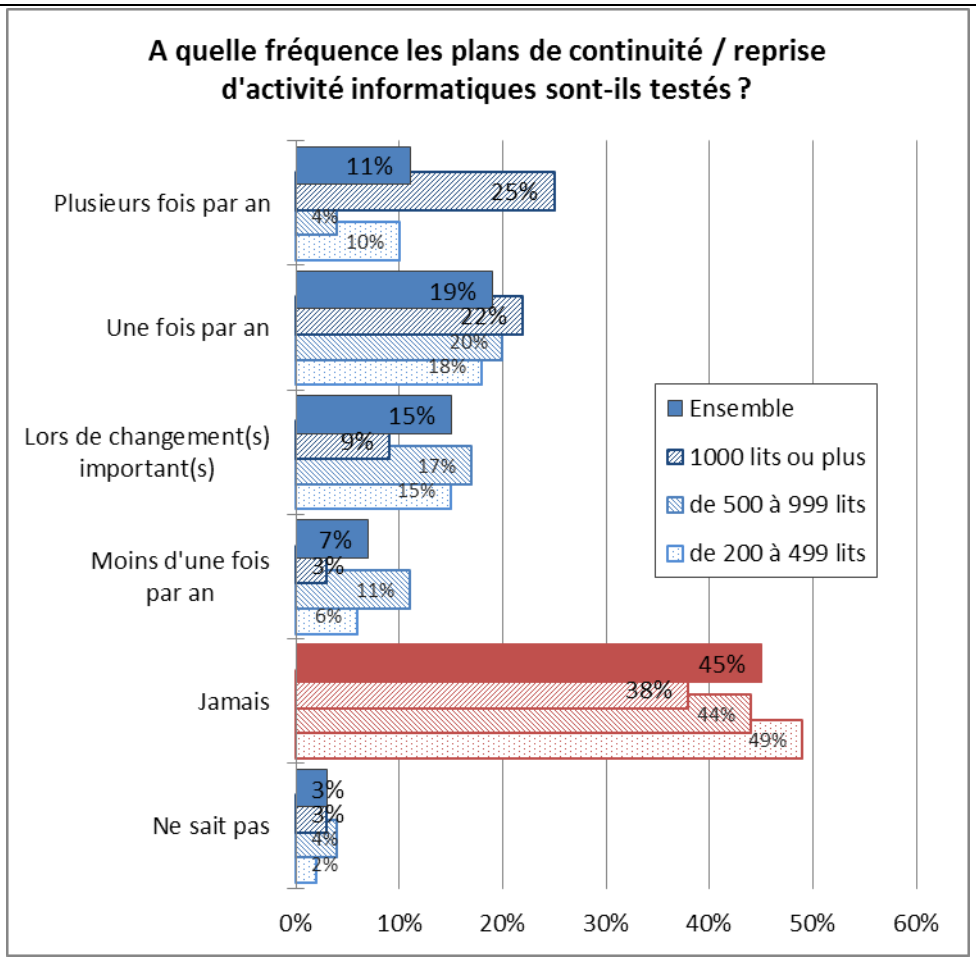

Figure 93 - Fréquence des tests techniques

Tout comme pour les entreprises, cette année l'étude a présenté les résultats sur une question touchant à l'exhaustivité de la couverture des solutions testées. Là encore, les résultats sont malheureusement inquiétants. En effet, seuls 10% des hôpitaux couvrent 100% de leurs solutions mises en œuvre ce qui est très peu. Ajoutons à cela que des tests réalisés même jusqu'à 75% de leur exhaustivité ne peuvent en aucun cas refléter la réalité en cas de sinistre.

Les hôpitaux vont devoir s'améliorer considérablement dans la prise en compte de leurs tests qu'ils soient Métiers ou technique, dans leurs fréquences tout comme dans leur intégralité.

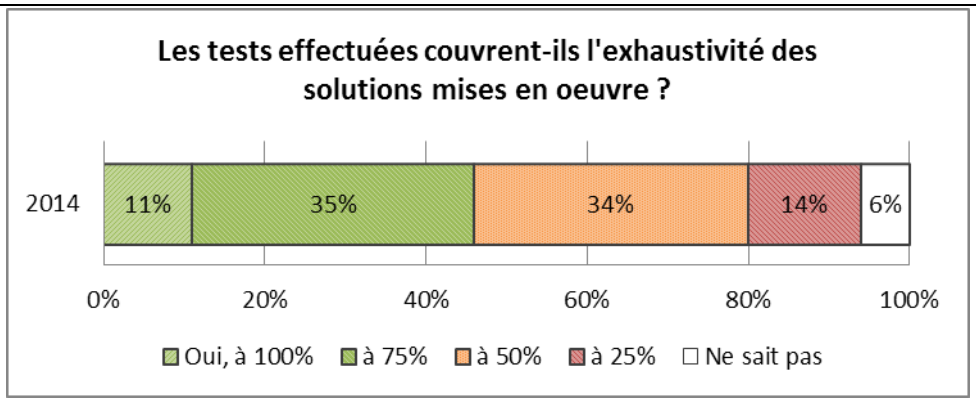

Figure 94 - Couverture des solutions testées

Une gestion de crise très insuffisamment prise en compte !

Sur cet aspect également les hôpitaux, et ce quelle que soit leur taille, vont être amenés à progresser à l'avenir en s'attachant à prendre en compte la gestion de crise.

En effet, la question sur la constitution de la gestion de crise au sein des hôpitaux démontre que seul un peu plus de la moitié des services hospitaliers dispose d'une cellule de crise (qu'elle soit décisionnelle ou opérationnelle). Ceci affiche un résultat faible au regard des enjeux d'un hôpital.

On note également que plus d'un hôpital sur 4 ne dispose d'aucun processus formalisé de gestion de crise, et souvent lors de la survenue d'un incident, on évite le déclenchement de crise ou on hésite.

Il est vrai cependant qu'en comparaison avec le secteur des entreprises qui disposent souvent d'un département communication, ce type de service de gestion de crise reste peu répandu dans les services hospitaliers; est-ce là un début d'explication ?

Thème 15 : Conformité

Le programme Hôpital Numérique comme moteur de la conformité

Près de 9 établissements sur 10 affirment être, ou en cours, de conformité aux prérequis sécurité d'Hôpital Numérique (fiabilité, disponibilité, confidentialité).

Le programme Hôpital Numérique et les exigences de la certification de la HAS (Haute Autorité de Santé) sont de véritables leviers, des moteurs pour élever le niveau de maturité et de maîtrise de la sécurité de l'information dans un établissement de santé, quelle que soit sa taille.

La conformité par rapport à la Loi Informatique & Libertés reste à améliorer. Ce sujet, quand il est pris en compte, est plutôt considéré comme un sujet technique du Système d'Information. La fonction de CIL (Correspondant Informatique et Liberté) est largement à développer. Mais ne faut-il pas au préalable une prise de conscience par les responsables de traitements de ce que signifie la conformité ?

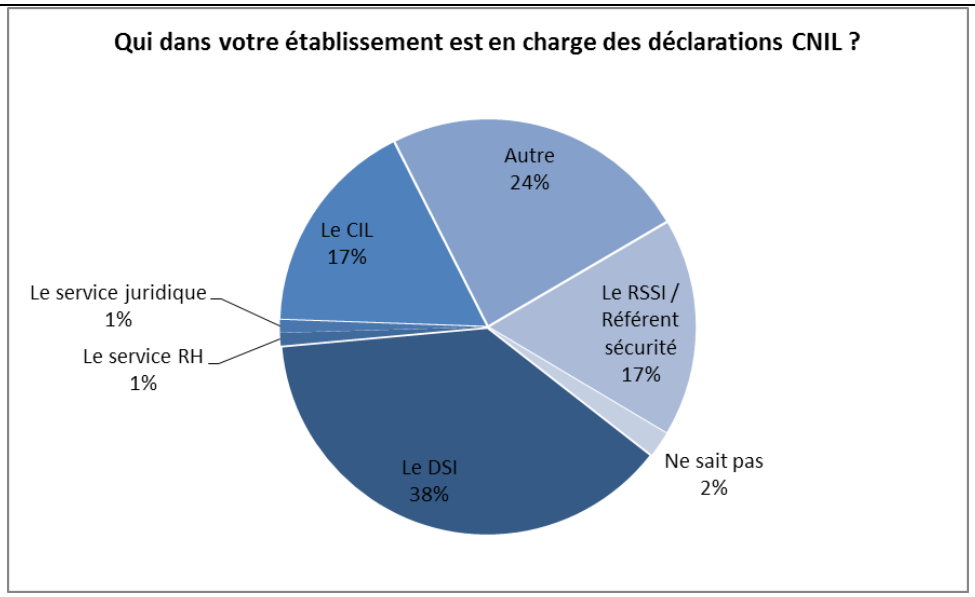

Figure 95 - Qui dans votre établissement est en charge des déclarations CNIL ?

Une démarche d'amélioration continue

Dans le cadre d'une démarche de conformité SSI, des audits périodiques sont nécessaires. À peine, la moitié des établissements réalisent au moins un audit par an.

Ces audits sont autant techniques qu'organisationnels, pour 60%. Les audits techniques intrusifs restent assez faibles. Ces audits sont mal perçus, ou bien les établissements ne considèrent pas que la menace peut venir des connections à des réseaux non sûrs (par exemple : Internet).

L'audit et les contrôles de sécurité pour les applications restent à développer.

Cependant, la tendance est bien à une augmentation des audits, dans une démarche d'amélioration continue, type PDCA (Plan, Do, Check, Act).

Les audits, avec les plans d'actions associés, participent à l'augmentation du niveau de maturité SSI des établissements.

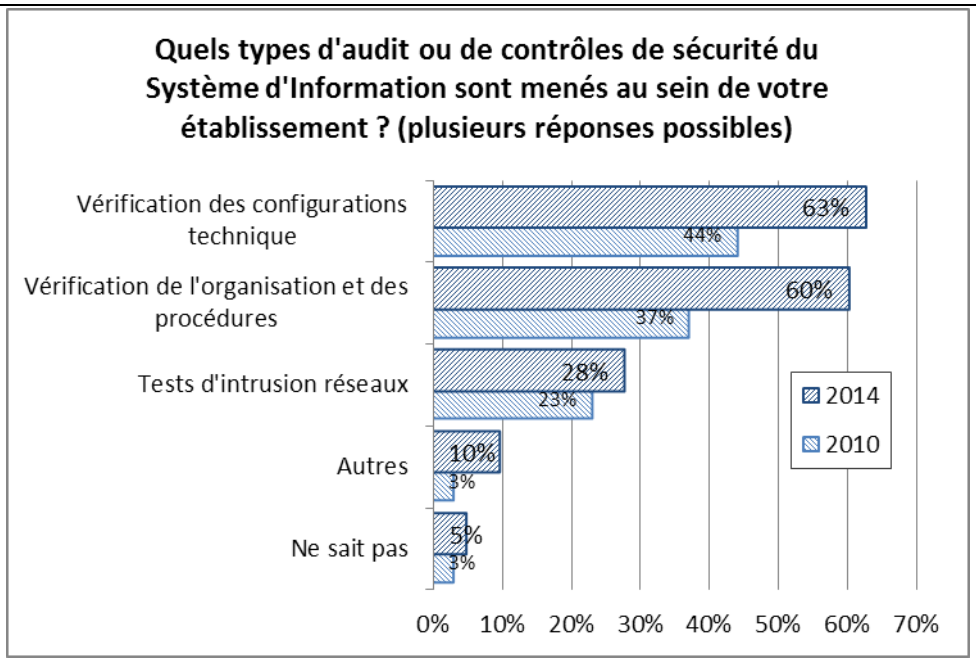

Figure 96 – Quels types d'audits ?

La motivation à lancer un audit se positionne bien sur des objectifs de conformité à la PSSI, à des aspects réglementaires, et d'audit par des tiers (HAS, commissaires aux comptes, etc.). L'auditabilité des Systèmes d'Information dans le cadre de la certification des comptes devrait fortement accentuer cette tendance.

L'audit suite à un incident est de moins en moins vrai. La tendance est de réaliser des audits préventifs, et d'améliorer l'organisation et les procédures.

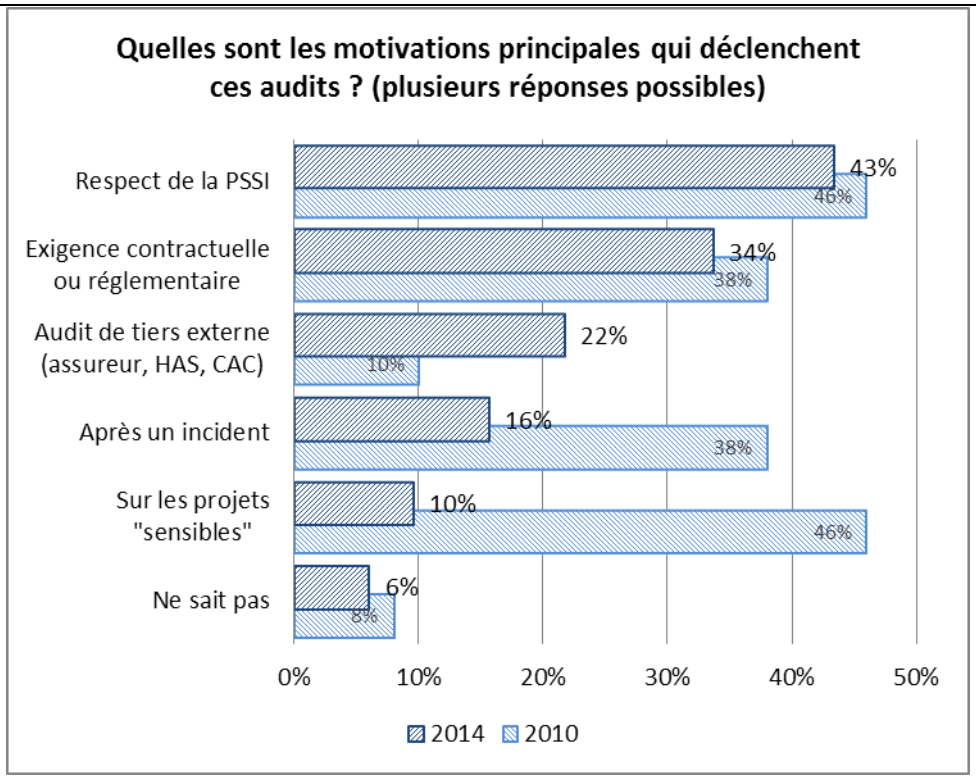

Figure 97 – Quelles motivations déclenchent les audits ?

Tableaux de bord : la disponibilité comme principale préoccupation

La mise en œuvre de tableaux de bord SSI reste assez faible, même si on constate une nette progression de l'utilisation d'indicateurs de suivi de la sécurité de l'information entre 2010 et 2014 : de 7% à 25% !

C'est un marqueur du développement de la sécurité des SIH (Système d'Information Hospitalier), bien que sa valeur puisse paraître faible au regard d'autres secteurs d'activités.

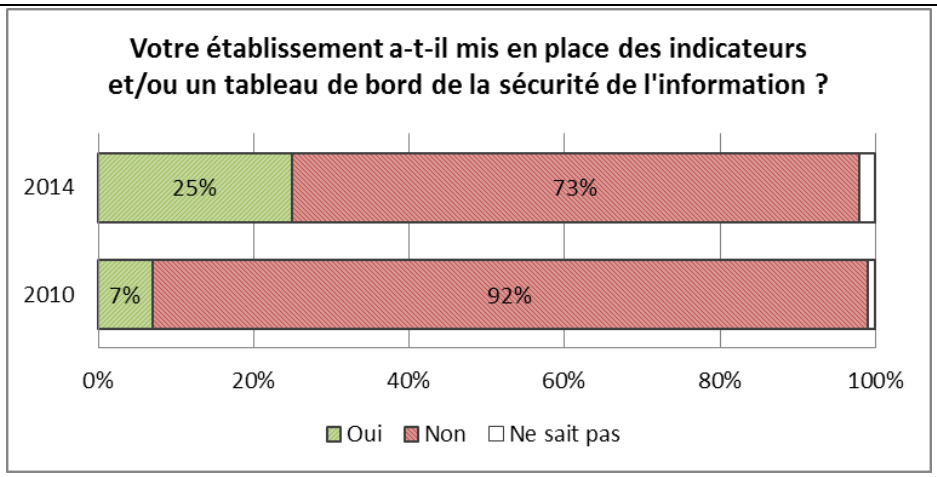

Figure 98 – Existence d'indicateurs et/ou tableaux de bord

Corrélé aux résultats de l'enquête sur les audits, la continuité de l'activité, la classification des informations, etc., ce résultat montre qu'un quart des répondants est entré dans le management de la sécurité.

Les indicateurs sont plutôt d'ordre technique (taux de disponibilité, etc.) : 80% des répondants.

Des indicateurs ou tableaux de bord à destination du pilotage et de la stratégie SSI, à destination de la direction et du Comité de direction, se développent.

La disponibilité est la principale préoccupation des établissements (76%).

La conformité aux normes (ex. ISO27001) est en net retrait (26% en 2014 contre 66% en 2010). Cependant, les principes de la norme se retrouvent dans les programmes de la tutelle.

Le taux d'inventaire de classification apparaît (37%), reflétant un besoin de connaissance et de maîtrise du Système d'Information.

Les indicateurs mesurés les plus importants reflètent les exigences des programmes de la tutelle (Hôpital Numérique, certification HAS).

De nouveaux indicateurs sont suivis en 2014, par exemple la conformité aux exigences de la politique du Ministère de la Santé pour 53% des réponses.

Très peu d'établissements suivent le taux de personnes sensibilisées à la sécurité, même si la proportion augmente légèrement en 2014 (21% contre 16% en 2010). La difficulté réside dans les moyens de sensibilisation des professionnels de santé qui sont rarement du présentiel. Ceci n'est pas forcément significatif de la politique des établissements en la matière, en particulier dans un secteur où la sensibilisation à la sécurité de l'information médicale est intrinsèquement liée aux enseignements et aux pratiques. Néanmoins, sur le terrain, dès lors que les TIC (Technologies de l'Information et de la Communication) sont utilisées pour la communication entre entités juridiques différentes, on constate un besoin de poursuivre la sensibilisation des professionnels de santé à la sécurité des communications électroniques et aux dispositifs de protection mis en œuvre.

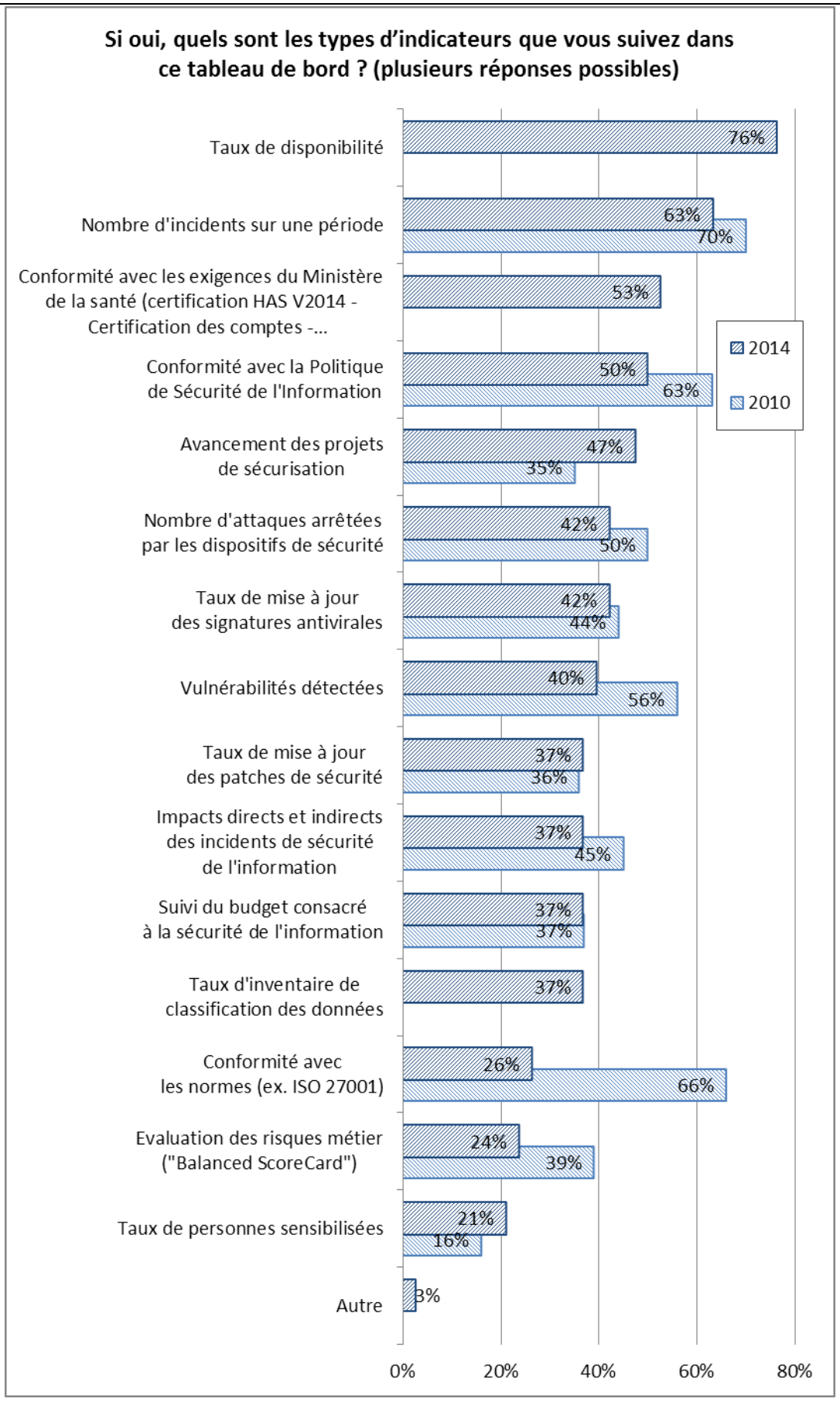

Figure 99 – Types d'indicateurs suivis dans les tableaux de bord

Internautes

- Profil des internautes et inventaire informatique
- Usages des internautes
- Perception et sensibilité aux menaces et aux risques
- Moyens et comportements de sécurité

Les internautes

Présentation de l'échantillon

Dans la continuité des années précédentes, le CLUSIF continue de remonter les perceptions et comportement des internautes français vis-à-vis du monde de l'Internet. Cette étude a été réalisée sur un millier d'internautes représentatifs de la population française actuelle en fonction de données socio-professionnelles : 56% du panel étant dans la tranche des actifs et 44% dans la tranche des inactifs et une parité homme/femme.

Les statistiques issues de cette enquête ont été réalisées par le cabinet spécialisé GMV Conseil s'appuyant sur un panel d'internautes géré par Harris Interactive.

L'échantillon final a fait l'objet, comme lors des études précédentes, d'un redressement sur les données de signalétique et par rapport aux données connues sur le plan national : sexe, âge, région, type d'agglomération, FAI, pratique d'Internet, etc.

Partie I - Identification et inventaire ordinateur et smartphone

En 2014, l'ordinateur fixe ou portable constitue toujours l'équipement le plus utilisé pour la connexion à Internet au sein des familles françaises avec une préférence pour les ordinateurs portables.

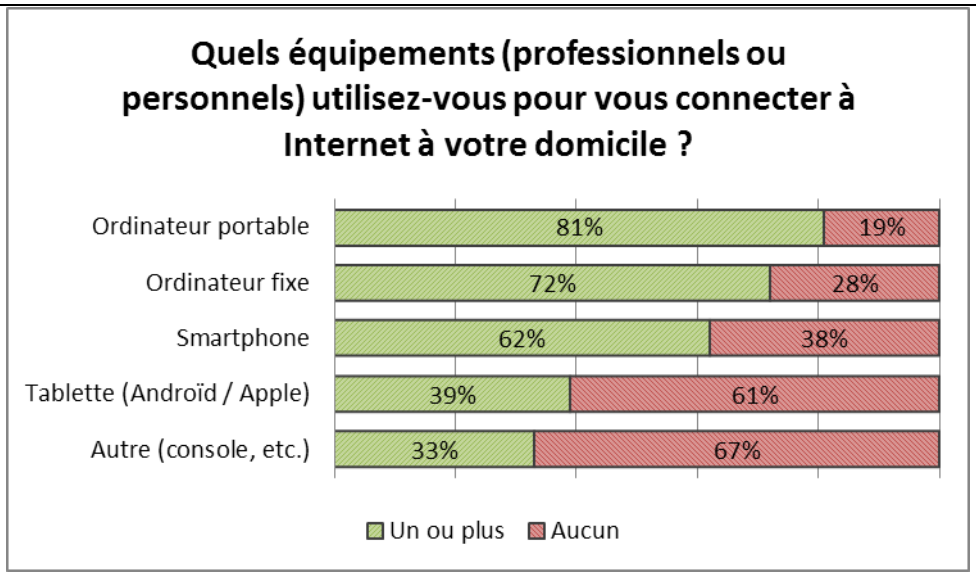

Figure 100 - Équipements utilisés par les internautes pour se connecter à Internet

L'utilisation de l'Internet via des smartphones est aussi présente dans les foyers français avec 62% du panel qui utilise son smartphone pour se connecter à internet. A contrario pour le moment, seulement 39% du panel utilise les nouveaux objets digitaux comme les tablettes pour se connecter au monde internet.

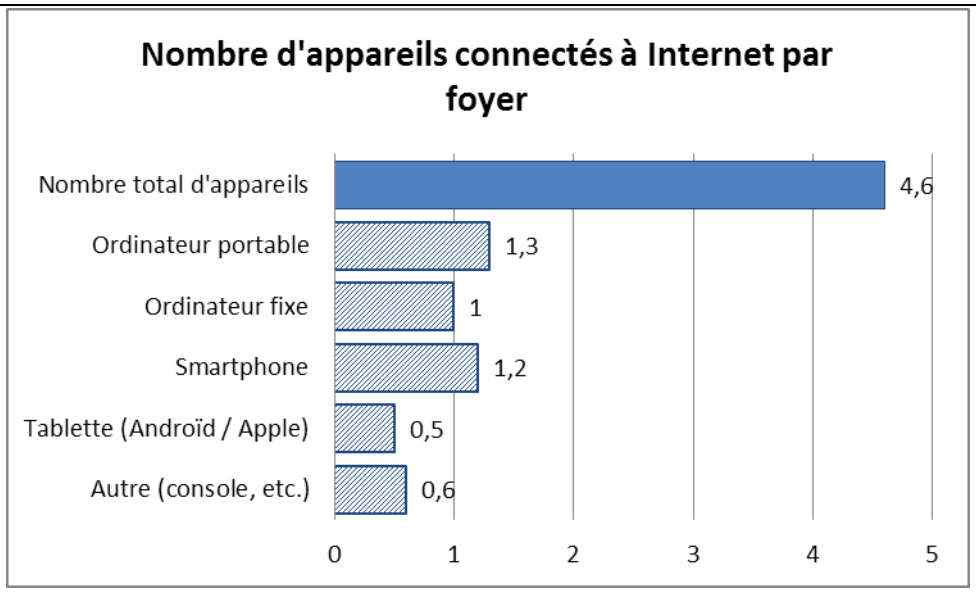

Figure 101 - Nombre d'appareils connectés à Internet par foyer

Concernant la mobilité, les français toujours connectés à Internet via leur équipement mobile ont augmenté de 5% en 2 ans alors que ceux qui ne sont jamais connecté à internet via leur équipement mobile a diminué de 7%.

L'enquête montre aussi une émergence des objets du quotidien connectés à Internet. En effet bien que très faible, représentant moins de 10% des réponses des français, le nombre de radios, alarmes et vidéosurveillance connectés à internet a doublé et le nombre d'appareils domotiques (hors alarme et vidéosurveillance) connectés à Internet a triplé. L'autre tendance sur les appareils domestiques connectés est l'augmentation de 10% en moyenne des appareils multimédia (TV, chaine, console de jeu, gadgets HIFI, etc.) par rapport à la dernière enquête MIPS.

Cet inventaire 2014 des équipements informatiques connectés à Internet confirme l'augmentation actuelle du « tout connecté » au sien des foyers français.

Partie II – Usages des internautes

De plus en plus de wifi

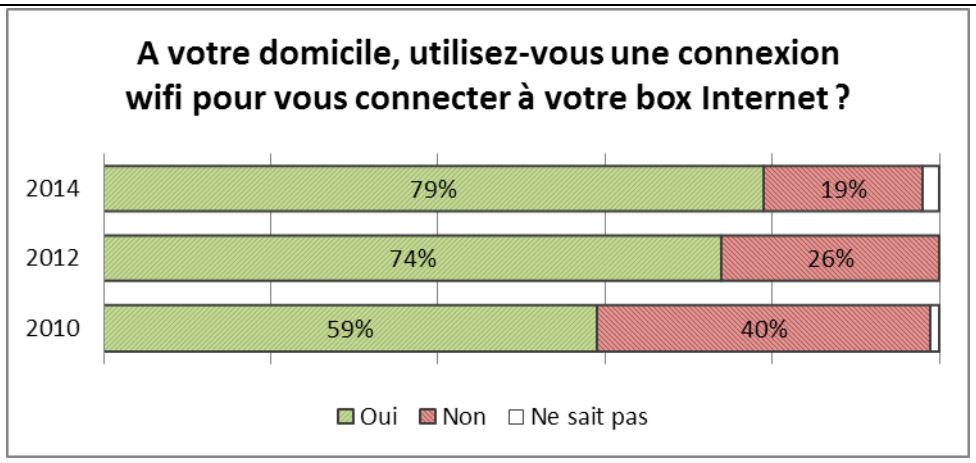

Figure 102 - Utilisation du wifi

En 2014, près de 80% des internautes sont connectés à leur box (et donc à Internet) en wifi. Ce mode de connexion, obligatoire pour les équipements mobiles (smartphone et tablette), est en constante augmentation depuis que le CLUSIF propose cette enquête. Les 20% qui n'utilisent toujours pas le wifi le font pour diverses raisons :

- Le manque d'équipement (ordinateur fixe non équipé de carte wifi) pour 40% d'entre eux,
- La sécurité pour 22% d'entre eux. Autrement dit, 4% des internautes (22% des 19% qui n'utilisent pas le wifi) choisissent de ne pas utiliser le wifi à leur domicile pour diminuer les risques d'intrusion sur leur Système d'Information personnel,
- Par habitude et du fait de la proximité du PC/box pour 15% d'entre eux.

23% des internautes ne savent pas pourquoi et laissent certainement la tâche d'administrer le réseau local familial à un autre membre de la famille plus compétent.

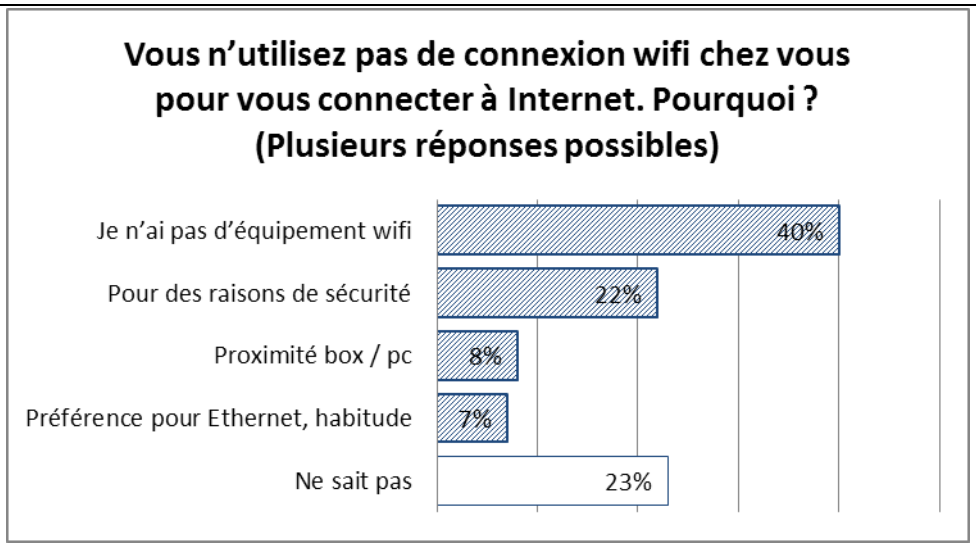

Figure 103 - Raisons pour lesquelles les internautes français ne sont pas connectés à internet via wifi

Un cadre sur deux travaille avec son propre équipement

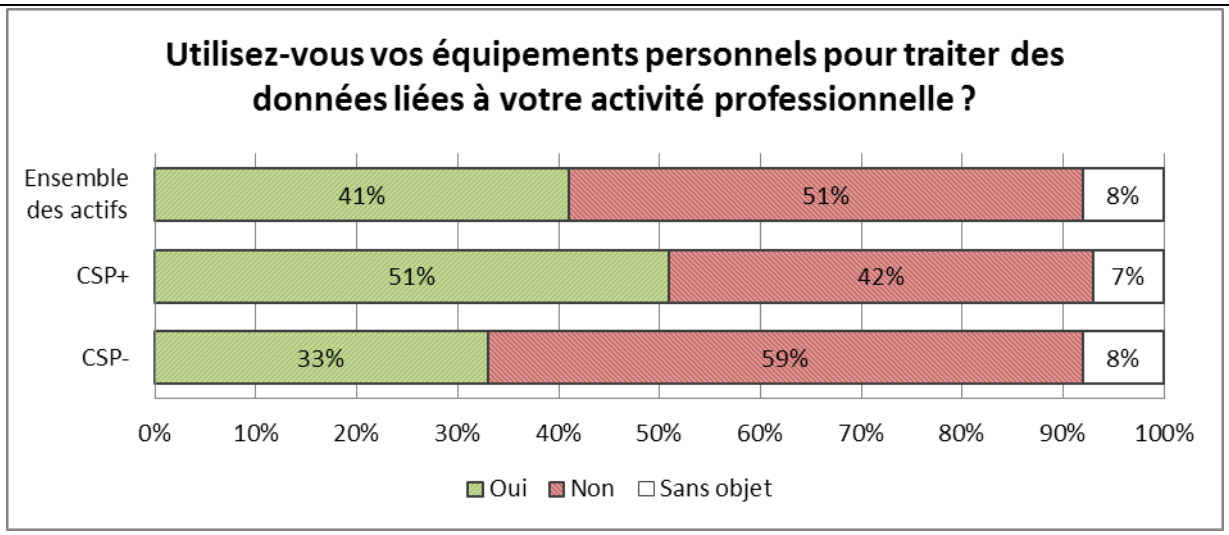

Figure 104 - Utilisation des appareils personnels pour l'activité professionnelle

L'utilisation d'un équipement personnel dans le cadre d'une activité professionnelle concerne, à l'échelle nationale, 41% des Français (+9% par rapport à 2012). Pour les catégories socioprofessionnelles supérieures, le BYOD (*Bring Your Own Device*) touche 1 personne sur deux (+3% par rapport à 2012). Ces chiffres, en augmentation par rapport à l'étude 2012, semblent indiquer que la limite entre les sphères professionnelles et privées est plus floue d'année en année.

L'inverse est également vrai, 41% des interrogés utilisent leur équipement professionnel pour consulter des données personnelles.

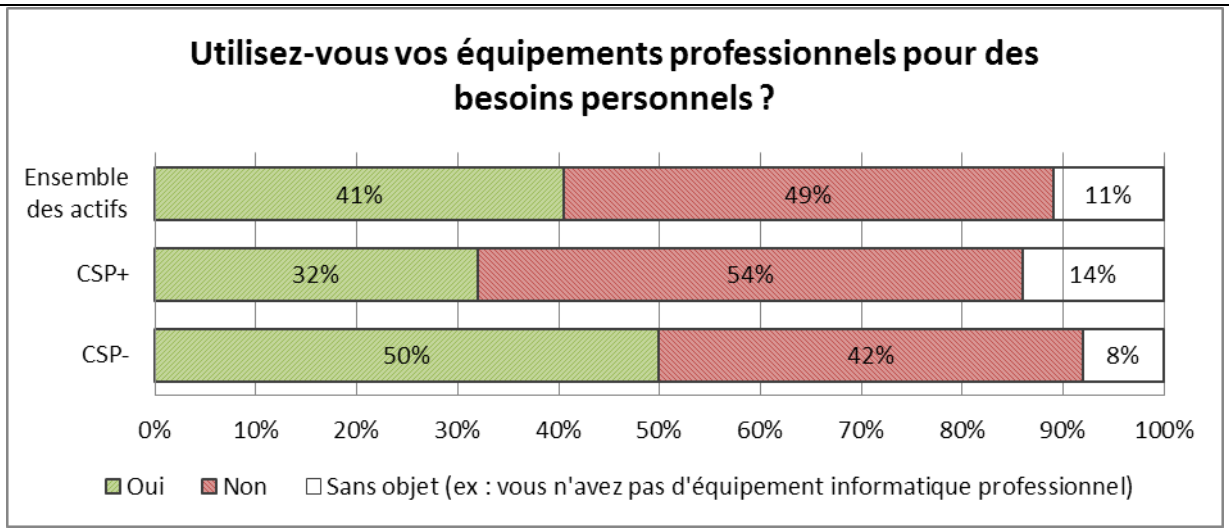

Figure 105 - Utilisation des appareils professionnels à des fins personnelles

Il apparait que les vies personnelles et professionnelles sont quasi mélangées l'une à l'autre. Les Français font de moins en moins la part des choses entre les deux vies. Ceci est probablement dû à l'augmentation de la mobilité/connectivité des outils professionnels et à la dématérialisation des données.

Pour la vie personnelle, l'essor des solutions de « Cloud » et coffre-fort numérique pour les données personnelles ainsi que l'augmentation des services à la personne en ligne, comme les impôts, ou l'accès au contenu multimédia (vidéos, musiques) contribuent au fait que plus de 40% des personnes interrogées utilisent des équipements informatiques professionnels à des fins personnelles.

Forte progression de la connexion nomade à Internet

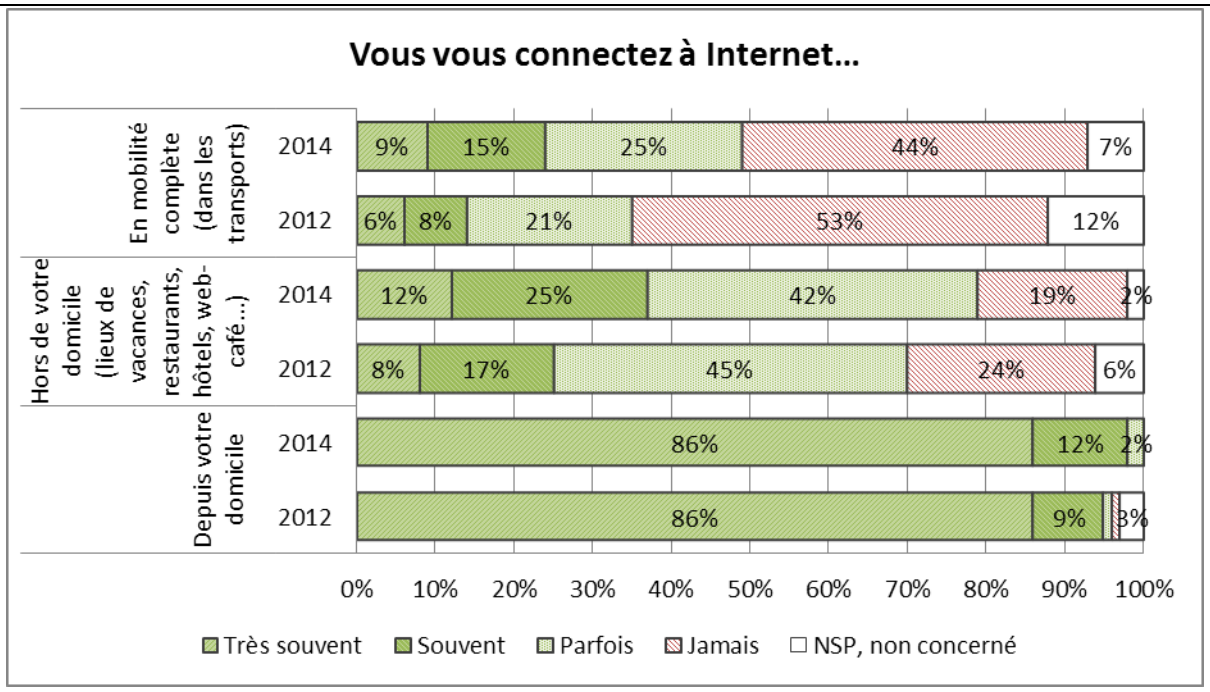

Figure 106 - Connexion à Internet en sédentaire et en mobilité

On constate une nette augmentation de l'utilisation d'Internet hors du domicile. En effet, Internet est de plus en plus utilisé sur les lieux de vacances ou les hôtels, les cyber-cafés. En 2012 les internautes étaient environ 70% à se servir d'Internet hors de leur domicile, contre presque 80% aujourd'hui.

L'augmentation la plus significative de l'utilisation d'Internet se trouve dans son utilisation en mobilité totale (dans les transports par exemple), avec pratiquement 1 internaute sur 2 qui surfe sur Internet en 4G/3G ou wifi des opérateurs. En 2012, ils n'étaient que 35% même pour une utilisation occasionnelle.

Utilisations principales d'Internet

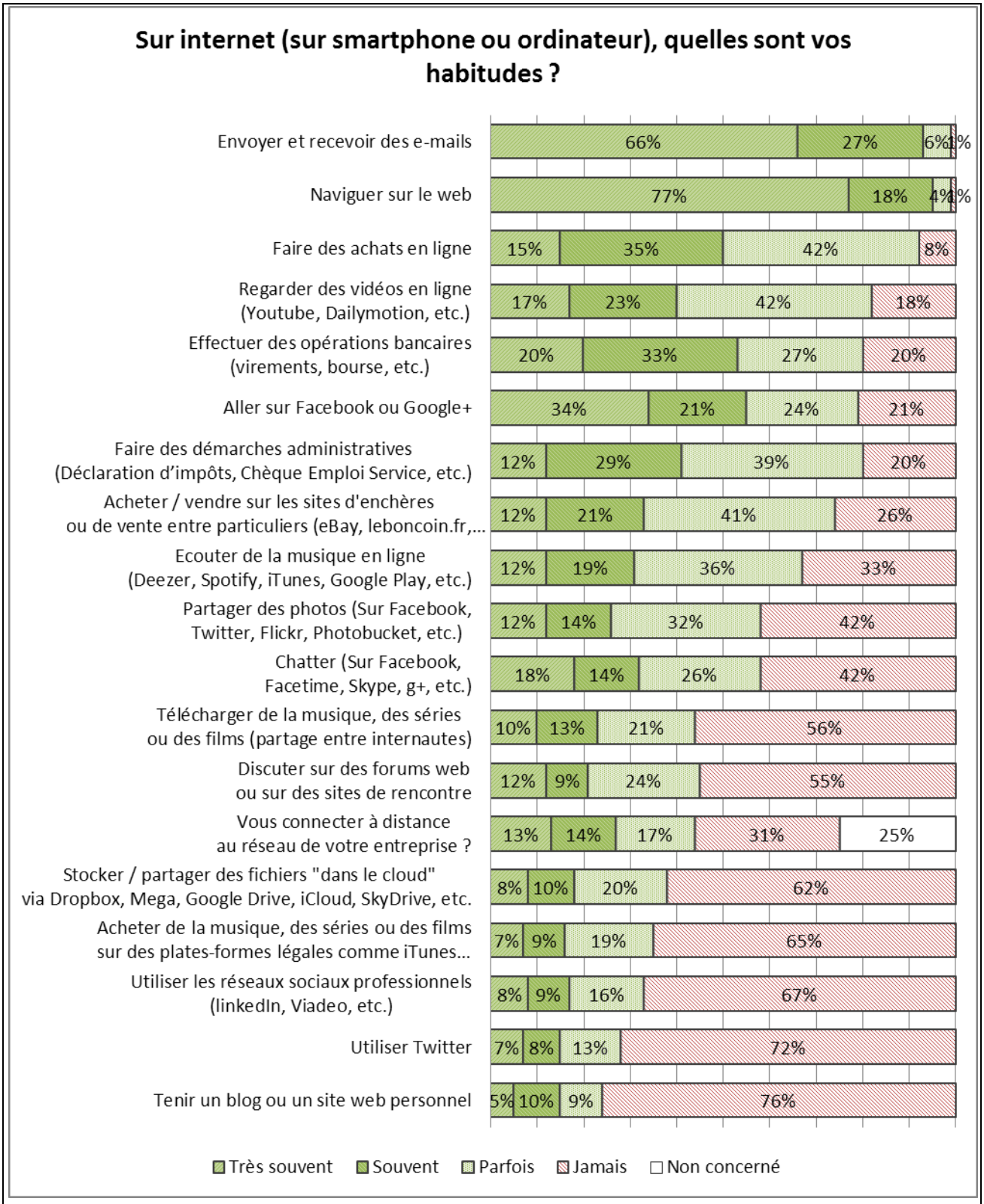

Figure 107 - Les différentes utilisations d'Internet

Hormis pour surfer ou consulter ses mails, qui arrivent évidemment en tête du sondage, des écarts entre les différentes utilisations d'Internet sont constatés.

Réseaux sociaux, des résultats hétérogènes

Quatre personnes sur 5 utilisent les réseaux sociaux (Facebook, Google+). Ces réseaux sociaux sont d'autant plus populaires chez les 15-34 ans avec une plus forte proportion de femmes que d'hommes. Le réseau Twitter, lui, peine à s'installer en France, même si 40% de la catégorie CSP+ l'utilise de « très souvent » à « parfois ». Même constat pour les réseaux sociaux professionnels (Viadeo et LinkedIn) utilisés par 50% des CSP+ et beaucoup moins par les autres catégories socio-professionnelles.

Acheter en ligne est devenu naturel…

91% des internautes ont effectué des achats en ligne en 2013. La moitié achète « très souvent » ou « souvent » en ligne. De même, 80% des internautes se connectent à leurs comptes bancaires ou effectuent des démarches administratives en ligne. Ces habitudes révèlent chez les internautes une confiance certaine dans ces services commerciaux ou financiers.

Écouter ou télécharger de la musique, regarder des vidéos, partager ses photos, dialoguer via Internet sont des activités pratiquées par plus d'une personne sur deux. À noter que 45% des internautes fréquentent les sites de rencontre ou les forums de discussion.

Le stockage en ligne des données personnelles (Google Drive, dropbox, Cloud, etc.), bien qu'étant une technologie très récente pour le grand public, est déjà utilisé par 38% des internautes.

Connexion au réseau de l'entreprise pour 60% des personnes concernées

Les internautes (hors inactifs) concernés par la question (travaillant en entreprise avec un réseau ouvert à l'extérieur) sont 60% à se connecter à ce réseau d'entreprise (44% des 75% d'actifs concernés) pour travailler de chez eux ou simplement lire leurs e-mails. L'interpénétration de la vie personnelle et professionnelle se généralise.

Je paye en ligne…

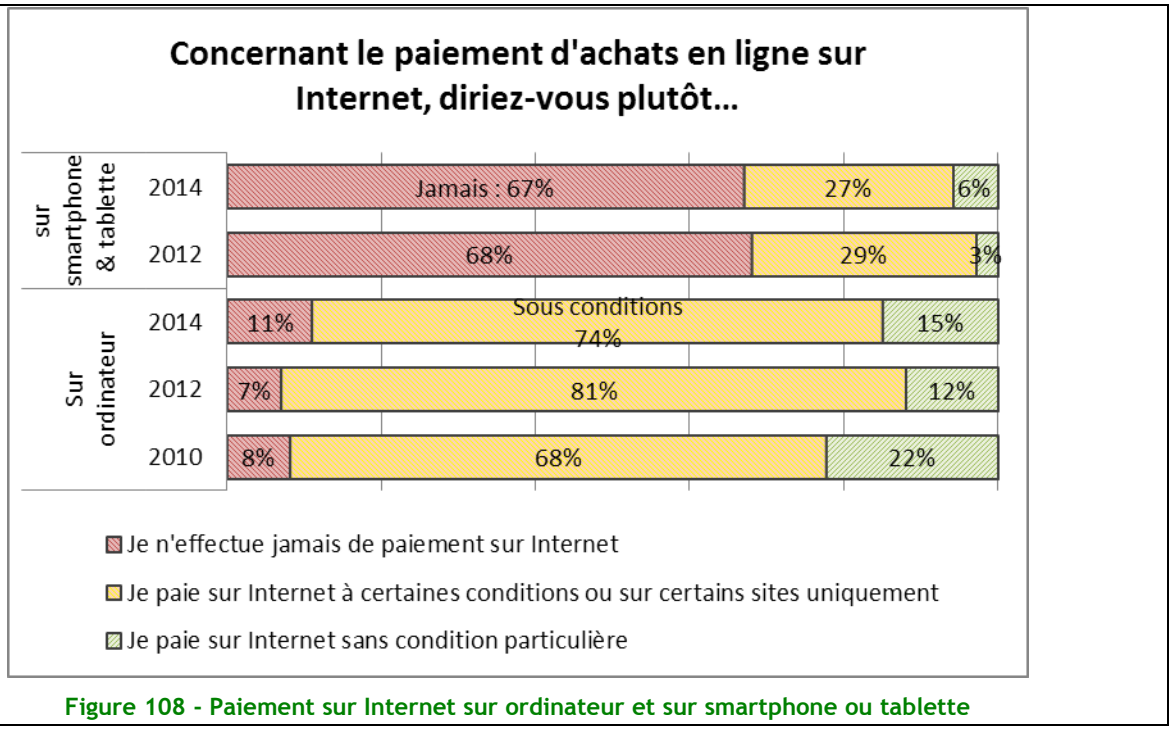

Figure 108 - Paiement sur Internet sur ordinateur et sur smartphone ou tablette

Pour le paiement en ligne, les comportements ont évolué depuis 2 ans. Concernant la partie smartphone/tablette, les internautes ont tendance à payer un peu plus sans condition particulière : +3%. Cette augmentation est en grande partie due aux achats de petites applications payantes.

Hormis cette évolution, la majorité des internautes n'est pas prête à payer via smartphone/tablette. Seulement un tiers des internautes consentent à payer via support de paiement à des conditions particulières.

Concernant les paiements à partir d'un ordinateur, la tendance est la même que via smartphone/tablette avec une augmentation de 4% des internautes prêts à payer sans condition particulière. Paradoxalement, l'enquête 2014 monte également une augmentation du nombre de personnes affirmant ne jamais payer sur internet.

…oui mais à certaines conditions

Pour les internautes qui acceptent de régler en ligne, c'est à certaines conditions : au moins 3 en moyenne. En tête de cette liste, il y a :

- Les sites sécurisés en HTTPS, avec le symbole du cadenas,
- Le mode de paiement (CB virtuelle, code unique, confirmation SMS),
- Le fait d'avoir déjà utilisé le site en question sans problème auparavant.

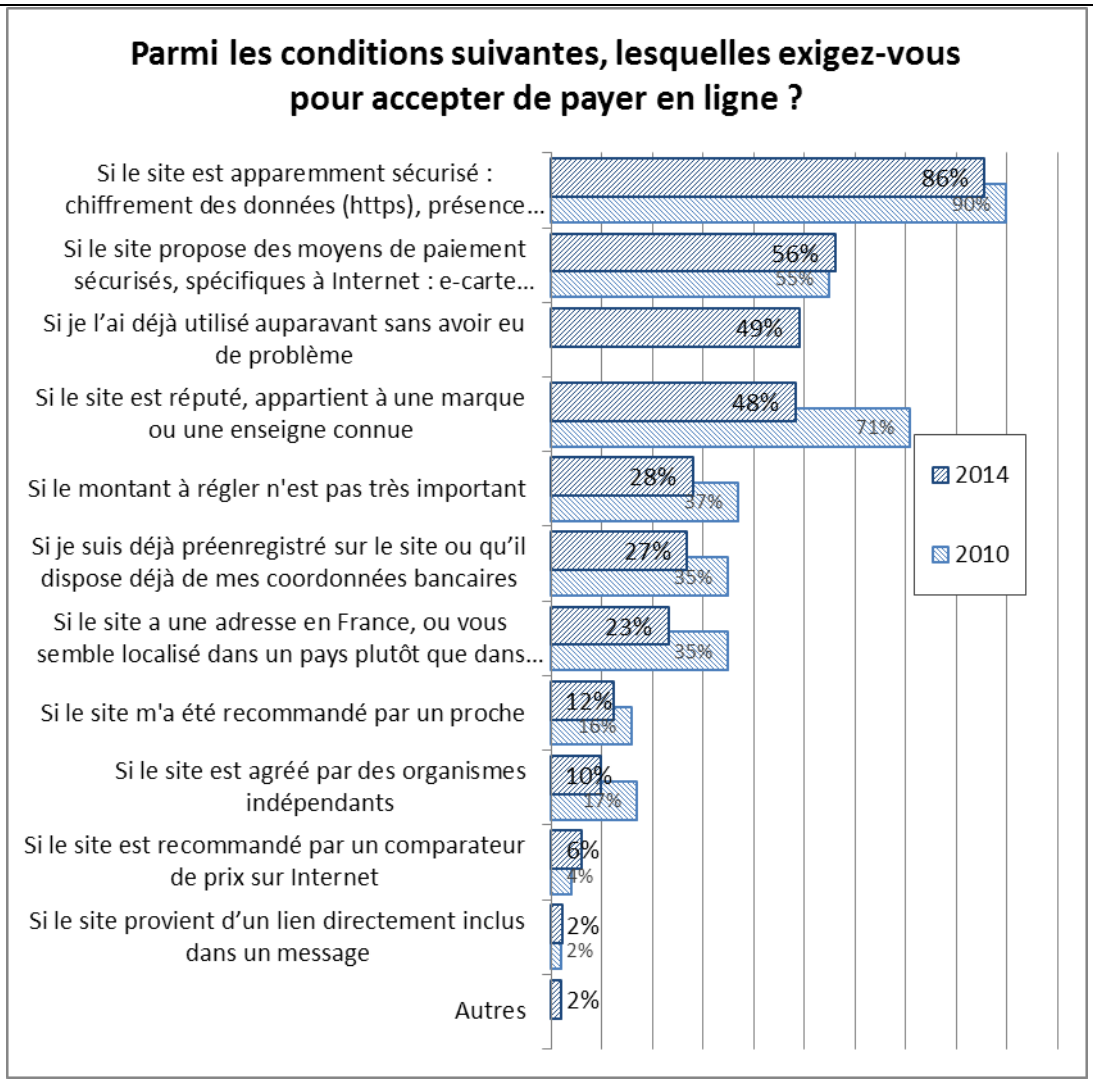

Figure 109 - Critères de confiance dans la sécurité pour les paiements en ligne

Vie privée : Attention !

En général, les deux tiers des personnes acceptent de remplir des formulaires demandant des informations personnelles seulement s'ils ont confiance dans le site. Néanmoins, ils sont encore 13% à le faire sans condition. Cette statistique a doublé par rapport à 2012.

Alors, baisse de vigilance ou excès de confiance ?

Partie III – Perception et sensibilité aux menaces et aux risques

Internet : nouvelles menaces ?

Le nombre d'internautes qui pensent faire courir des risques importants à leurs données personnelles (documents, photos, vidéos) sur leur ordinateur fixe ou portable du fait d'être connecté à Internet est en nette augmentation par rapport à l'enquête de 2012.

De même, une grosse perte de confiance est à signaler concernant les smartphones et tablettes. Là où, en 2012, 61% des internautes ne percevaient aucun ou peu de risques pour leurs données, ils ne sont plus que 30% à le penser. Ils sont désormais 42% à craindre pour leurs données stockées sur leur tablette ou smartphone et 28% à ne pas savoir quoi vraiment penser. Tout laisse à penser qu'ils manquent de visibilité sur ce sujet : les internautes ont acquis une conviction concernant la sécurité de leurs données sur leur ordinateur mais ne savent pas bien à quoi s'en tenir pour les tablettes et smartphones.

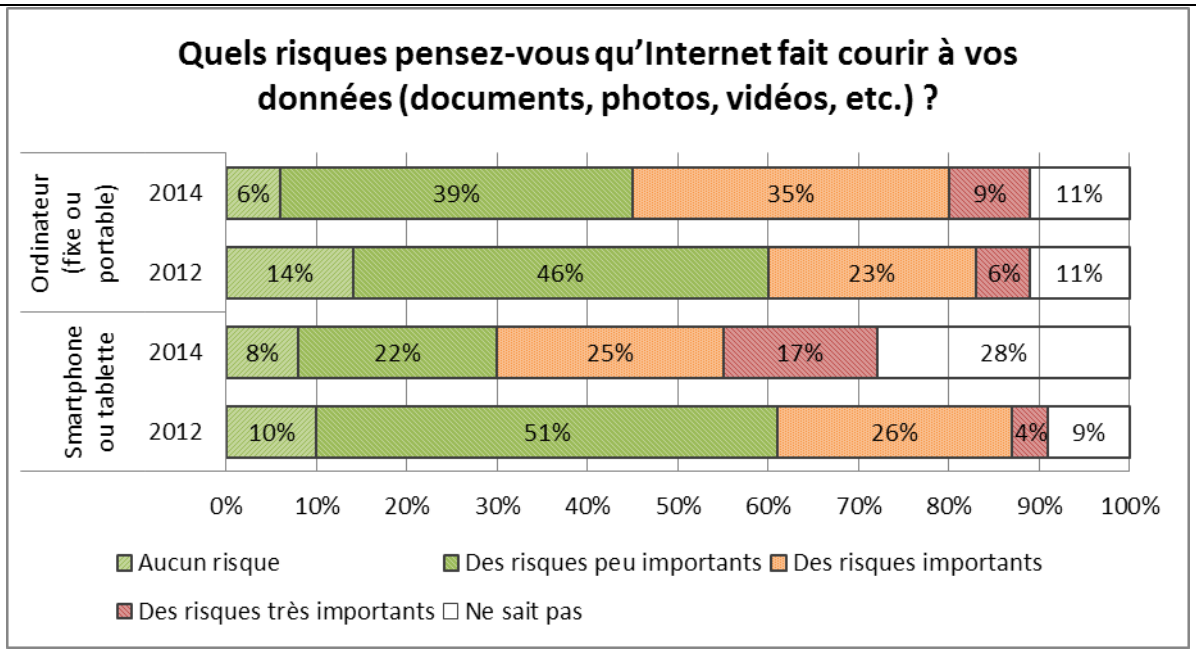

Figure 110 - Perception du risque concernant les données personnelles stockées sur des équipements connectés

Vie privée sur internet : la jeune génération moins consciente des risques qu'auparavant

Les jeunes baissent la garde. Bien qu'ils soient d'assidus consommateurs d'internet, les jeunes deviennent moins vigilants quant à l'exposition de leur vie privée sur les réseaux.

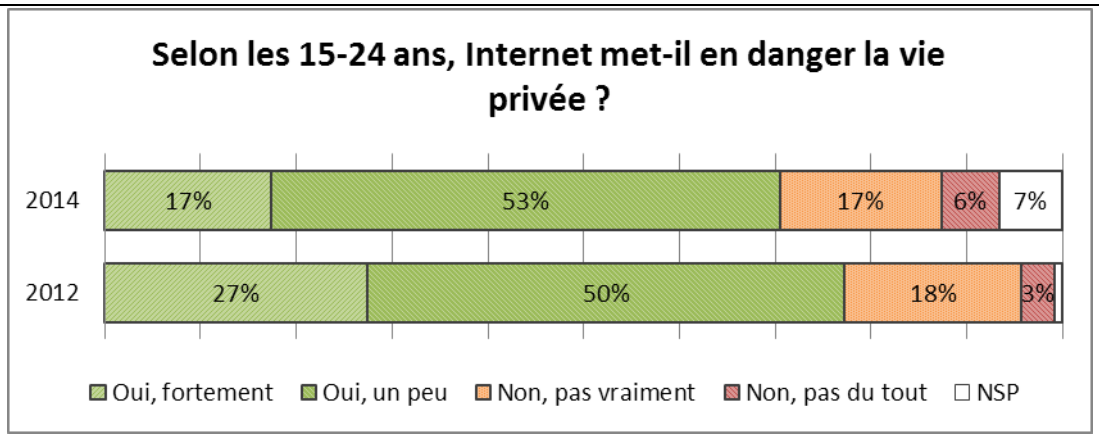

Figure 111 - Perception du danger d'Internet par rapport à la vie privée, pour les 15-24 ans

Alors que les 15-24 ans étaient 77% il y a 2 ans à penser qu'Internet pouvait mettre en danger leur vie privée, ils ne sont plus que 70% à le penser en 2014.

Plus inquiétant encore peut-être : les 15-17 ans pensent pour 19% d'entre eux que la protection de leur vie privée sur internet n'est pas du tout ou peu importante. Sur l'ensemble de la population, un peu plus d'une personne sur 10 pense la même chose.

Environ 92% des jeunes utilisent leur vraie identité sur les réseaux sociaux et délivrent beaucoup d'informations personnelles[3]. La combinaison de ces deux constats ne peut qu'inquiéter. Les récentes dispositions européennes en matière de droit à l'oubli ne pourront pas réparer tous les torts causés par ce manque de vigilance. L'éducation de la jeune génération doit se renforcer en matière de protection de la vie privée sur Internet.

Le point de vue des parents : décalage entre la théorie et la pratique…

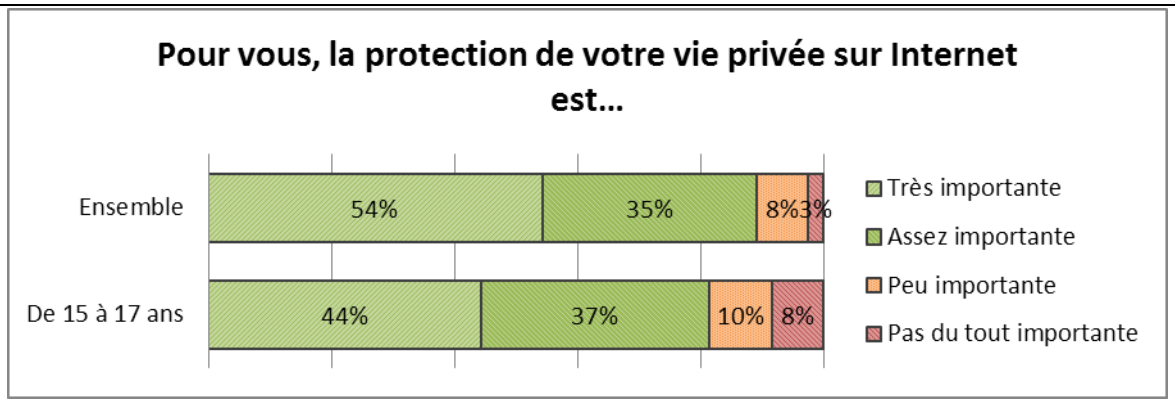

Figure 112 - Importance de la protection de la vie privée

Les parents semblent beaucoup plus conscients que leurs enfants de l'importance qu'il y a à protéger leur vie privée sur internet (seulement 71% des 15-24 ans pensent que c'est important, contre 89% de l'ensemble de la population). Toutefois, seulement les 64% des internautes vérifient les réglages de sécurité et de confidentialité de leur profil sur les réseaux sociaux.

Selon la CNIL[4], sans paramétrage, tout ce qui est mis sur un réseau social peut être vu et utilisé par tout le monde. Les plus jeunes semblent mieux maîtriser les options et les paramètres, assez complexes il est vrai, des réseaux sociaux : ils sont 74% à vérifier ces paramètres de confidentialité.

[3] Source : http://www.jeunes.cnil.fr/parents/les-constats-de-letude/

[4] Source : http://www.jeunes.cnil.fr/parents/etude%20-%20reseaux%20-%20sociaux/

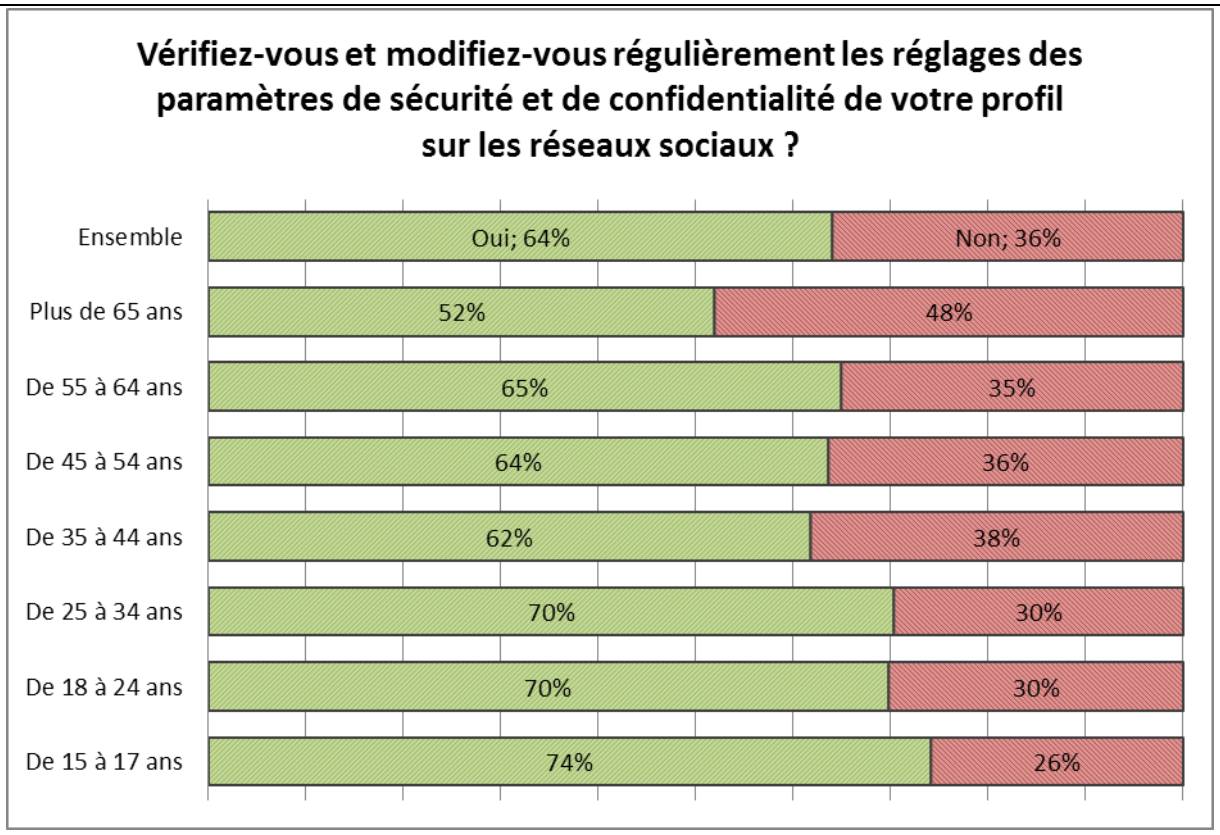

Figure 113 - Réglage des paramètres de sécurité et de confidentialité des réseaux sociaux (personnes disposant d'un profil uniquement)

Par ailleurs, lorsqu'on leur pose directement la question, les internautes pensent très majoritairement qu'internet représente un danger pour les mineurs, avec, ici encore, de grandes disparités en fonction de l'âge du répondant et également une différence entre les hommes et les femmes (les femmes en moyenne sont 10% plus inquiètes que les hommes).

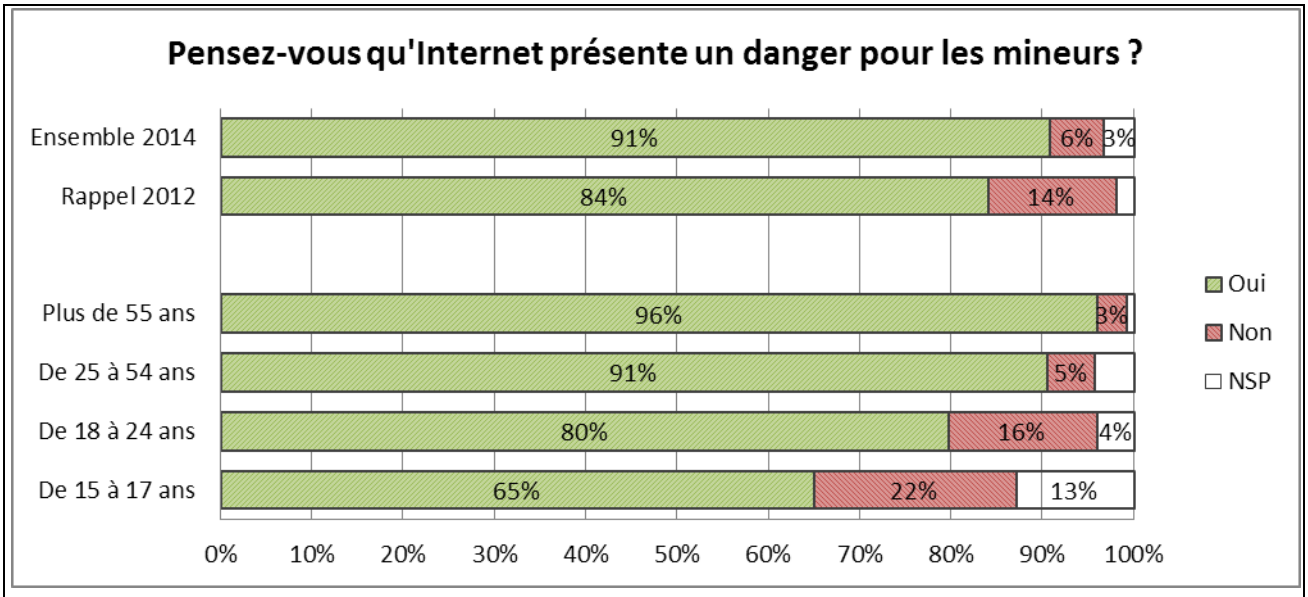

Figure 114 - Internet, un danger pour les mineurs ?

Le smartphone : « cet ami qui vous veut du mal » ?…

Quant à la relation entre les outils utilisés pour se connecter à Internet et la perception du danger pour les mineurs, notre enquête apporte un premier éclairage à suivre au fil des ans. Dans la pratique, la technologie embarquée sur les équipements mobiles communicants actuels détourne les usages vers des applications susceptibles d'engendrer à leur tour d'autres problèmes : prise de photographies ou de vidéos à l'insu des protagonistes, diffusion de ces fichiers entre mineurs ou sur des réseaux sociaux, commentaires moqueurs ou intimidants voire à caractère discriminatoire ou injurieux, accès illimité et sans contrôle parental ni éducatif à internet. Dans certains collèges, 70% des motifs de conseil de discipline sur les 2 dernières années sont rattachés au téléphone portable[5].

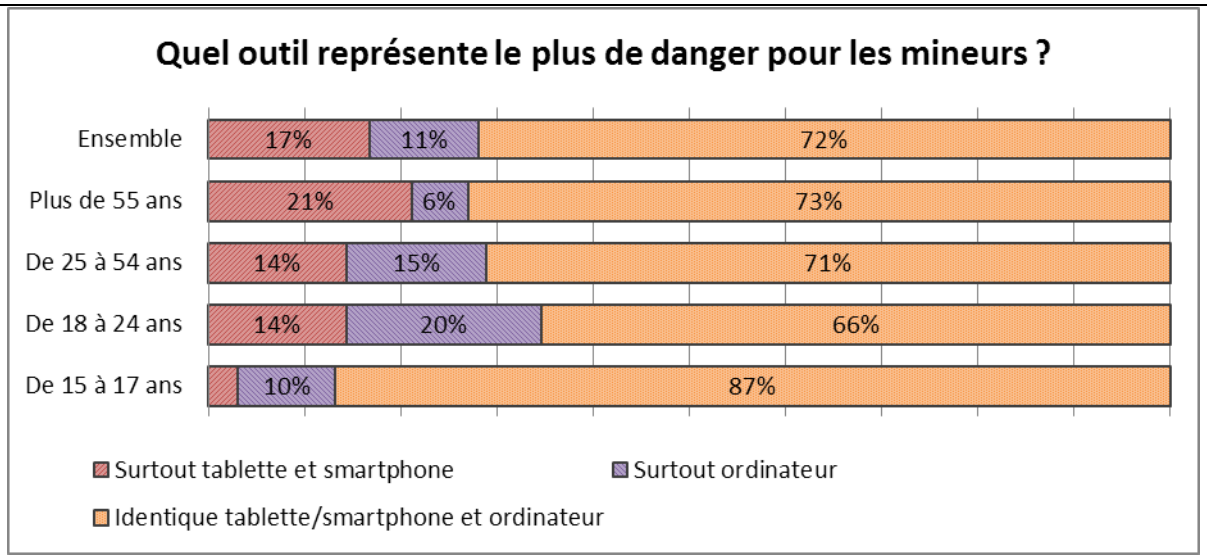

Figure 115 - Perception du danger pour les mineurs représenté par les outils communicants

A la lecture des résultats de l'enquête, il ressort que les adolescents ne sont absolument pas conscients du danger prédominant – ou peut être refusent-ils de l'admettre – que peuvent représenter leur smartphone pour eux. Sans doute préfèrent-ils pouvoir continuer à naviguer et communiquer en toute liberté sur leur équipement mobile personnel plutôt que sur l'ordinateur familial, plus bridé et soumis à la surveillance parentale.

Que deviennent nos données personnelles ?

Les internautes semblent, toutes tranches d'âge confondues, conscients de la complexité du problème de stockage de leurs données. Deux alternatives s'offrent à eux : sauvegarder leurs données « en local » (sur un disque interne, externe, une clé USB, des DVD, etc.) ou sauvegarder leurs données « dans le Cloud », en souscrivant l'un des nombreux services gratuits ou payants. Lorsqu'on leur demande quelle solution apporte le plus de garanties de sécurité en termes de confidentialité (protection contre le vol et la divulgation de données) et de disponibilité (protection contre la perte et/ou la destruction des données), force est de constater que les avis sont plus que vagues.

En effet, 40% du panel n'a pas d'avis, les autres 60% se répartissent à peu près équitablement sur les 3 autres réponses possibles. Ce manque de connaissance sur le domaine prolonge le statuquo, poussant les internautes à considérer le niveau de sécurité de leurs données personnelles équivalent, que celles-ci soient situées sur leur ordinateur ou dans le Cloud.

[5] Source : courrier adressé aux parents d'élèves en mai 2014, académie de Versailles.

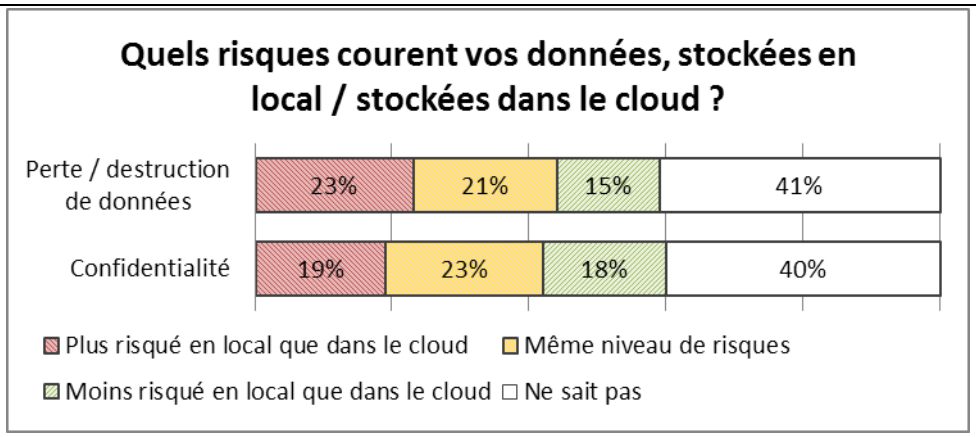

Figure 116 - Niveau du risque perçu par les internautes concernant le stockage de leurs données en local plutôt que dans le Cloud

Les particuliers, utilisateurs finaux des solutions de stockage de données, sont donc bien plus influencés par leurs fonctionnalités, confort d'utilisation, et intégration à leur écosystème habituel (accès depuis le système d'exploitation, depuis une boite mail, partage simplifié avec ses connaissances) que par la composante sécurité de la solution.

Perte de données en hausse sur les smartphones

La tendance mise en avant lors en 2012 se confirme cette année : 35% des internautes déclarent avoir subi au moins une perte de données durant ces 24 derniers mois, donc depuis la dernière enquête !

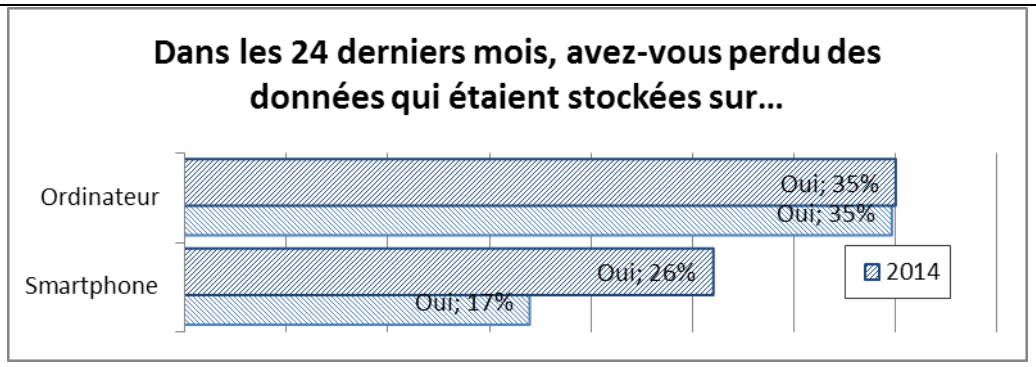

Figure 117 - Perte de données subies sur ordinateur et smartphone / tablette

La panne et l'erreur de manipulation restent les deux raisons majeures invoquées lors de la perte de données sur un ordinateur. Les 15-24 ans ont une plus forte propension aux erreurs de manipulation… ou une plus grande facilité à les reconnaître.

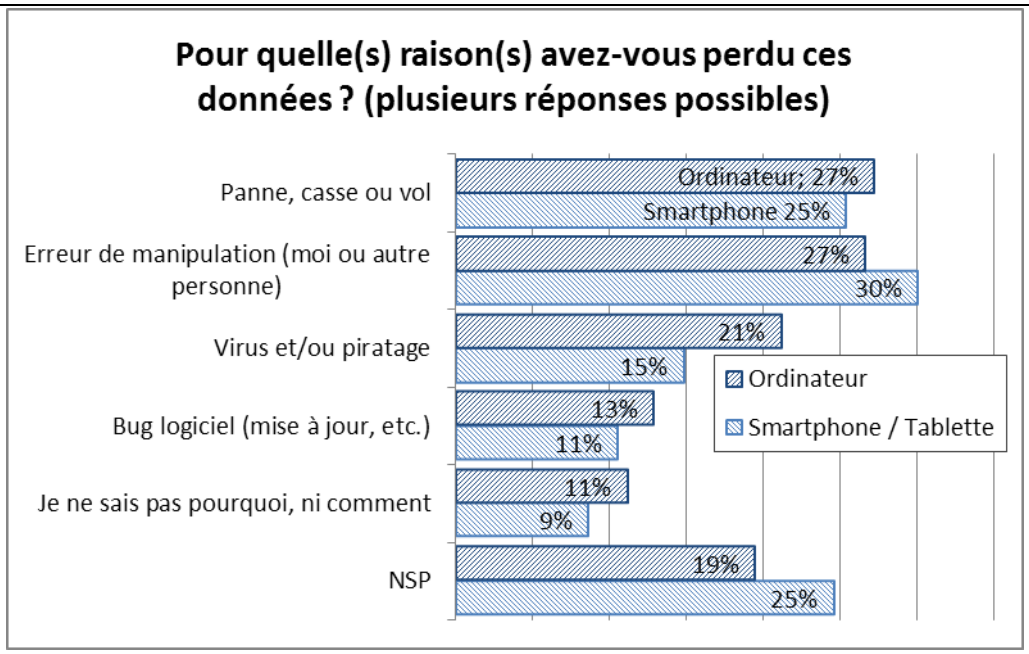

Figure 118 - Raison des pertes données sur ordinateur et smartphone / tablette

Plus d'un quart du panel utilisateurs de smartphones ou tablettes déclare avoir subi au moins une perte de données ces 24 derniers mois. Ce chiffre, en forte hausse par rapport à 2010 (+65%) est toutefois bien moindre que le taux de perte de données stockées sur un ordinateur. Ils sont néanmoins à rapprocher des usages comparés de ces deux médias.

Enfin, plus de 90% des plus de 55 ans déclarent n'avoir pas subi de pertes de documents sur leur smartphone ou tablette lors des 24 derniers mois. Cette population a-t-elle conscience des dangers liés à ces nouveaux objets communicants ?

Évolutions de la menace sur les équipements informatiques ?

43% des internautes considèrent que les risques auxquels sont exposées leur données augmentent. Et ils sont plus nombreux à le penser qu'en 2012 (32%). Le sentiment d'insécurité en ce qui concerne leur ordinateur augmente donc. L'âge est un critère important dans l'évaluation de cette menace puisqu'une augmentation du ressenti avec l'âge est constatée. 26% des internautes de 15-17 ans considèrent les risques en hausse alors que ce ratio représente 50% des internautes de plus de 65 ans.

Si l'évaluation des risques liés à l'utilisation d'un ordinateur semble entrer dans les mœurs des internautes, il n'en est clairement pas de même pour les usages nomades. En effet, 25% des utilisateurs estiment ne pas connaître l'évolution des risques sur smartphones ou portable (contre 12% sur ordinateur). Par contre, une forte proportion du panel (28%) estime tout de même que le niveau de risque n'a pas vu d'évolution notable ces dernières années.

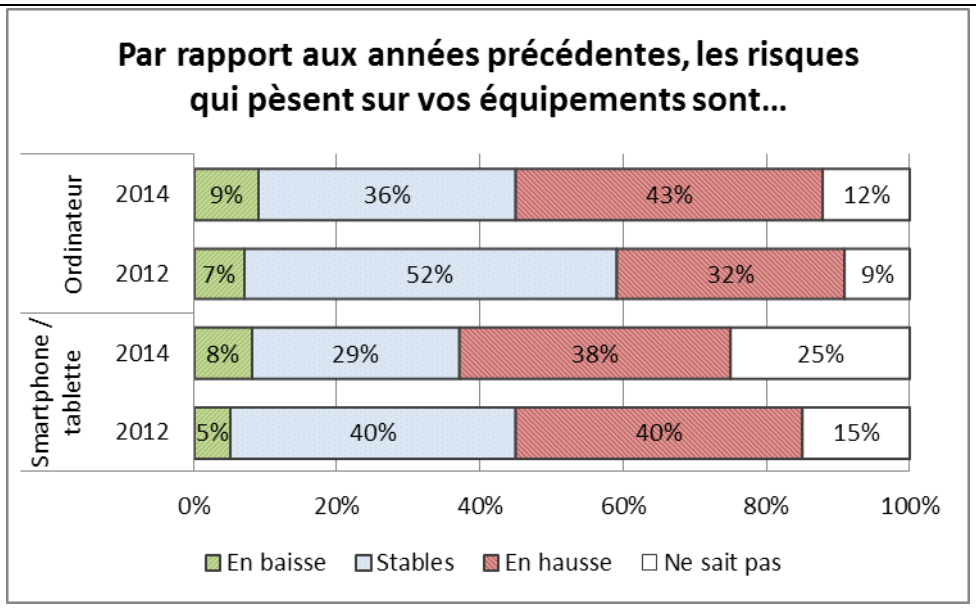

Figure 119 - Évolution de la perception de la menace sur les appareils connectés

Exception faite des usages les plus récents ou des problématiques les plus techniques, les internautes se sentent à même d'évaluer les risques pesant sur l'informatique personnelle. Sur 20 menaces présentées aux utilisateurs, 10 sont considérées comme représentant des risques très importants, parmi lesquels :

- Le virus : la crainte du virus, tant sur l'ordinateur que sur le smartphone ou la tablette est en relation directe avec la tranche d'âge des utilisateurs puisqu'il y a un écart de 20% entre les 15-17 ans (plus confiants) et les 55-64 ans. Ainsi, si le dernier rapport illustrait une tendance à la baisse du risque perçu en l'absence d'antivirus, cette préoccupation reste fortement présente dans l'esprit des internautes,
- Logiciel espion : plus de 40% des internautes considèrent aujourd'hui la présence de logiciels espions sur leur ordinateur comme un risque très important. De plus, 18% des internautes ne se sentent pas en mesure d'évaluer le niveau de risque présenté par la présence d'un logiciel espion sur leur smartphone ou tablette. Ainsi, si les logiciels espions et la peur de l'escroquerie à la carte bleue restent à l'esprit des utilisateurs d'ordinateurs, les usages différents des smartphones et tablettes rendent une part de mystère à une menace pourtant connue des utilisateurs,
- Vol d'identité : à l'exception des 15-17 ans, un consensus s'est établi sur le « risque très important » représenté par les vols d'identités. Il est probable que la communication autour d'assurances relatives à l'identité et l'e-réputation ont ouvert l'esprit des gens à ces problématiques.

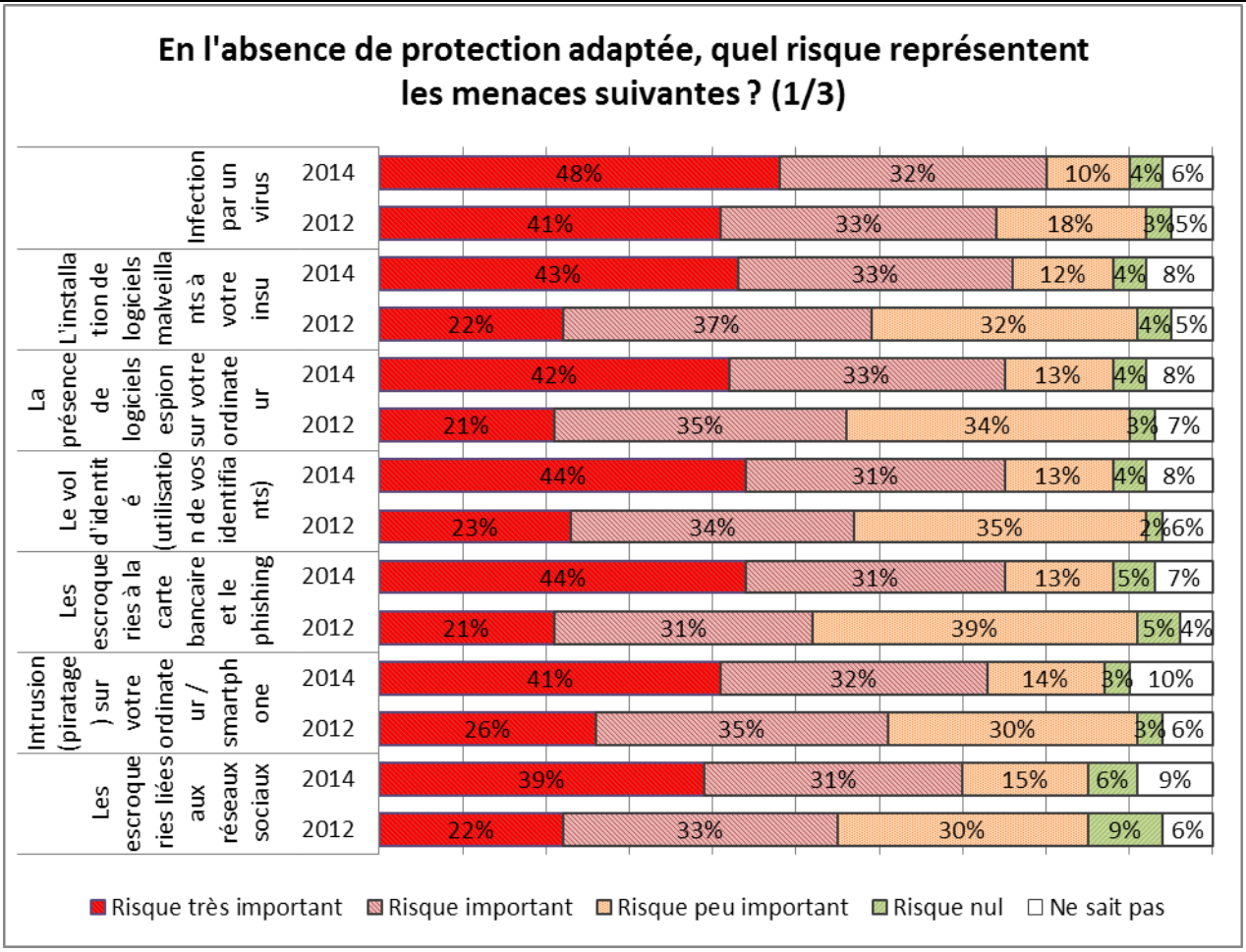

Figure 120 – Perception de la gravité de la menace en l'absence de protection adaptée (1/3)

Intrusion sur l'équipement : la peur du pirate est toujours fortement présente. Elle semble toutefois moins présente chez les jeunes puisque près de 27% des 15-17 ans ne se prononcent pas. Ceux-ci ont grandi dans un paysage médiatique plus au fait de la sécurité informatique et se détournant (difficilement) peu à peu de l'image du grand méchant pirate cagoulé, tapant à toute vitesse dans un vieil entrepôt désaffecté.

Piratage de l'accès wifi : seule étape d'un accès internet qui peut sortir du domicile de l'utilisateur, le wifi reste un élément difficilement maîtrisable en dépit des différentes méthodes de sécurisation. Le risque ressenti est relativement faible chez les jeunes (seulement 21% des jeunes le considèrent comme un risque fort), il atteint son paroxysme chez les utilisateurs ayant débuté leur découverte d'Internet par le biais de connexions nécessairement filaires (47% des 45-54 ans estiment qu'il représente un risque très important).

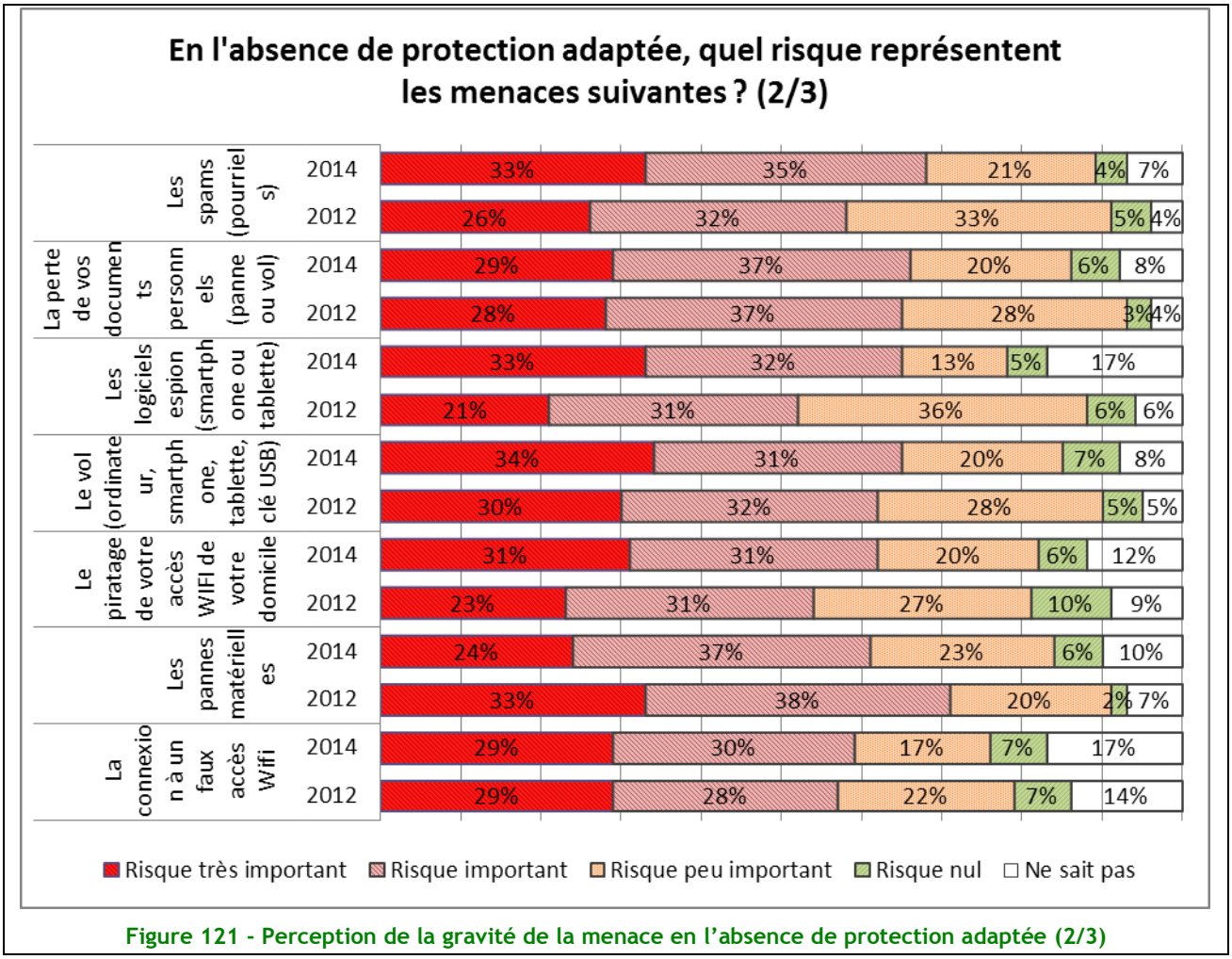

Figure 121 - Perception de la gravité de la menace en l'absence de protection adaptée (2/3)

Escroqueries liées aux réseaux sociaux : au même titre que le vol d'identité, les escroqueries liées aux réseaux sociaux représentent une crainte importante des utilisateurs puisque près de 40% des utilisateurs considèrent qu'il représente un risque très important. Exception faite des 15-17 ans qui ne se sentent pas à même d'évaluer le risque que représentent ces escroqueries, aucune catégorie d'âges ne se démarque puisque toutes s'accordent sur un niveau de risque très important à important.

Escroqueries à la carte bancaire via phishing : les compétences de plus en plus poussées des pirates informatiques permettent l'apparition de faux messages de plus en plus aboutis. Cela fait peser sur les internautes une menace de plus en plus présente. En effet, actuellement 44% du panel considèrent ce risque comme « très important » et cette statistique devrait continuer de croître, notamment en raison de l'émergence de phishing téléphonique directement auprès du grand public.

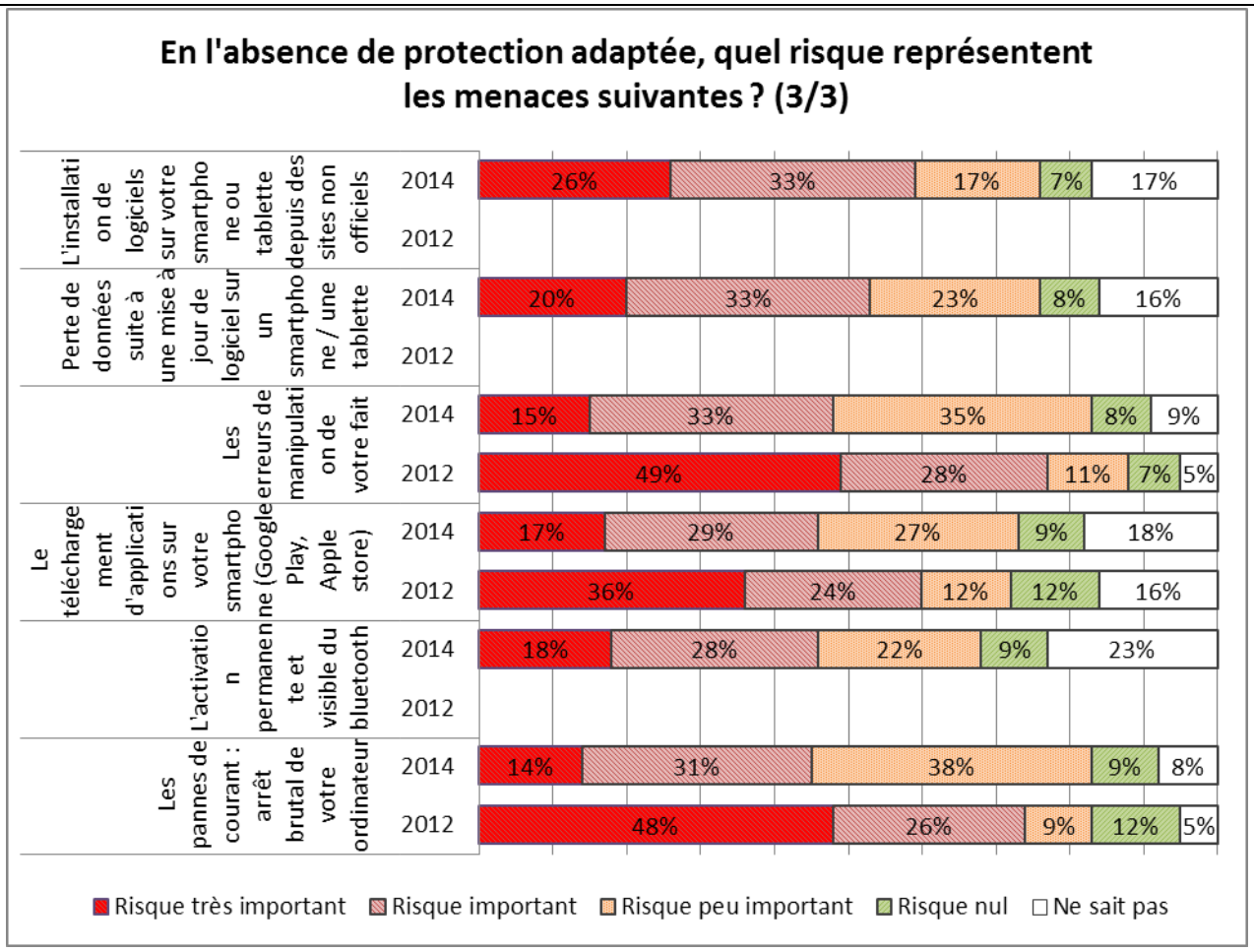

Figure 122 - Perception de la gravité de la menace en l'absence de protection adaptée (3/3)

Paiement sécurisé à partir de quel dispositif ?

Notre rapport précédent avait montré que plus de 9 internautes sur 10 avaient déjà réalisé des achats en ligne. Les smartphones et tablettes passant progressivement du statut d'objet d'accès l'information à celui d'ordinateur d'appoint. Une réticence globale reste présente lorsqu'il s'agit de réaliser des achats sur Internet. De fait, 40% des internautes se sentent plus en sécurité lorsque leurs achats sont réalisés sur un ordinateur que sur une tablette ou un smartphone.

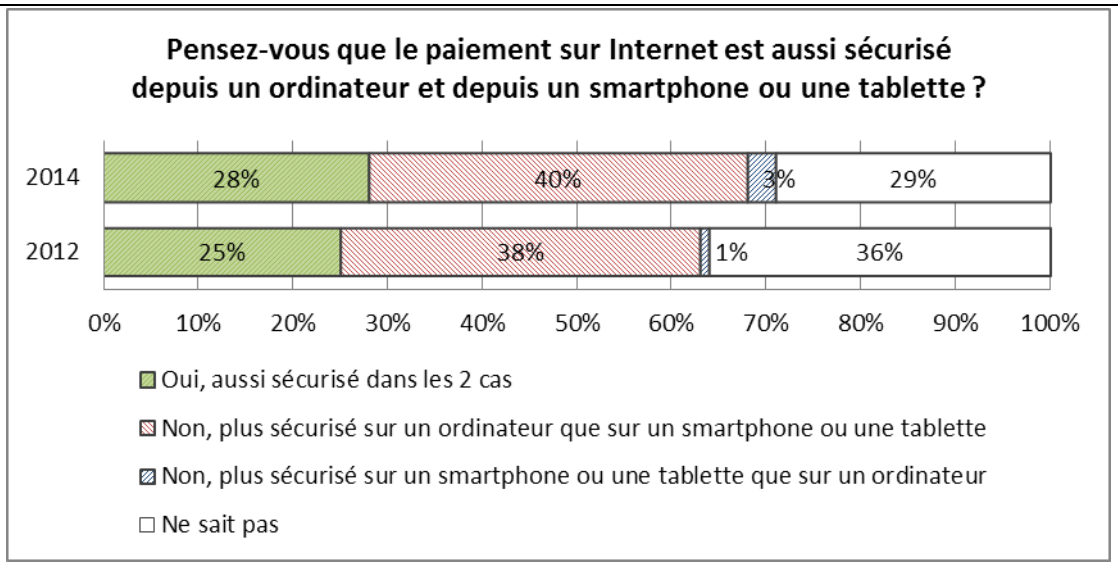

Figure 123 - Perception de la sécurité du paiement en ligne sur un ordinateur vs sur un smartphone

Cependant, la question laisse de nombreux utilisateurs en difficulté puisqu'un tiers des utilisateurs ne se prononce pas (de 20% chez les 15-17 ans à presque 35% chez les plus de 65 ans).

Les menaces actuelles d'Internet…

L'antivirus tient toujours une place prépondérante dans l'écosystème sécurité des internautes. Il en va de même pour les composants qui font la une des recommandations habituelles d'hygiène informatique. Ainsi, 85% des utilisateurs (d'ordinateurs) estiment que la navigation sans antivirus augmente fortement les risques (64% sur smartphone et tablette). De même, plus de 82% retirent leur confiance à leur solution antivirale dès que celle-ci n'est pas mise à jour. L'exposition aux menaces les plus récentes entraîne les plus grandes inquiétudes. Par opposition, seulement 17% des 15-24 ans estiment (à raison !) la mise à jour du système d'exploitation comme nécessaire à une navigation sécurisée.

De façon analogue, 78% des utilisateurs considèrent leur navigation comme risquée dès lors qu'une solution de pare-feu n'est pas présente sur la machine.

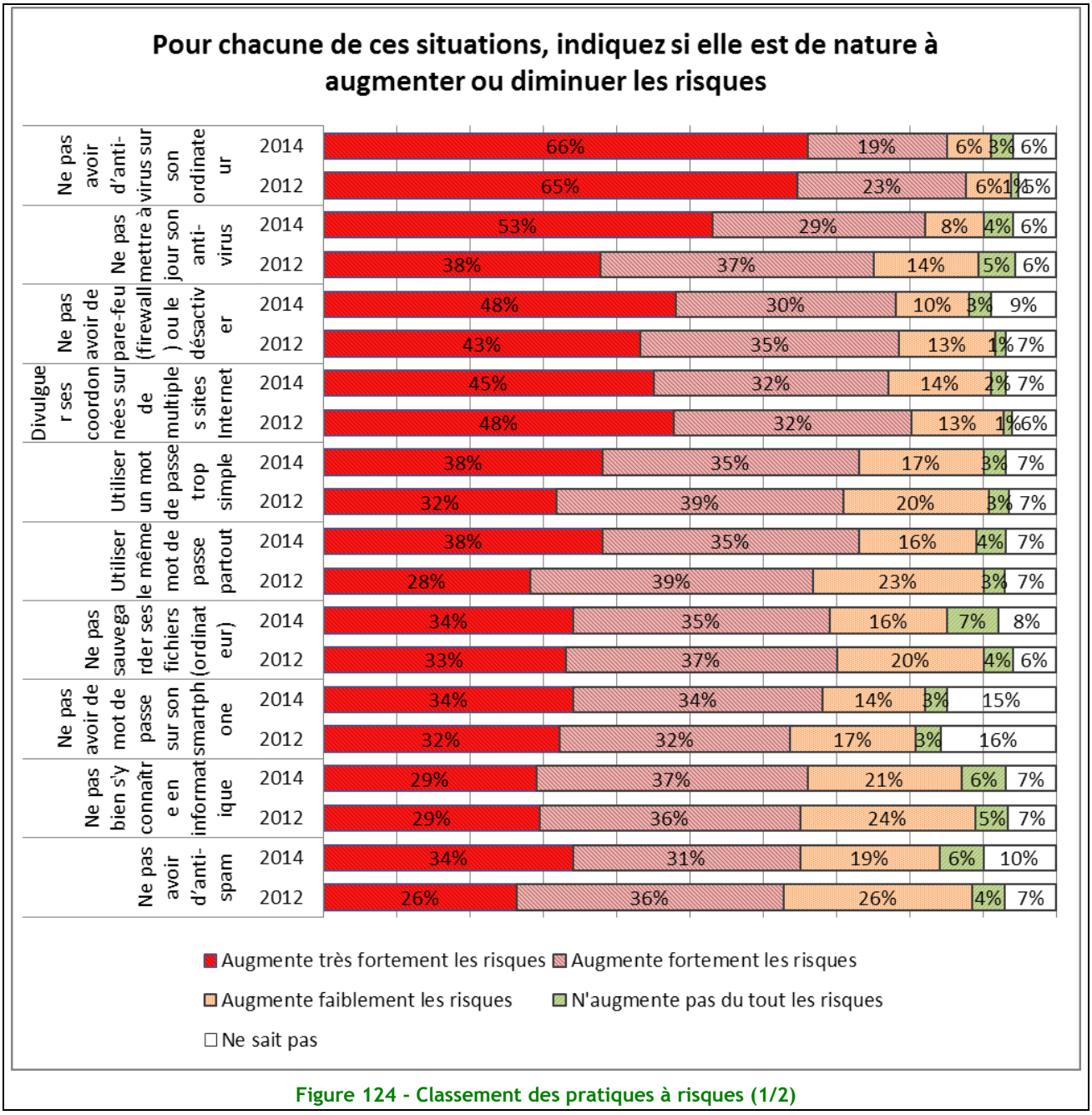

Figure 124 - Classement des pratiques à risques (1/2)

Si 45% des plus de 55 ans estiment que naviguer sans antispam augmente très fortement les risques, à peine 20% des 15-24 ans considère celui-ci comme nécessaire à une navigation sécurisée.

En apparente opposition avec le constat dressé précédemment sur les pertes de données, les internautes semblent, avec l'âge, se préoccuper de plus en plus de la sauvegarde de leurs données (13% des 15-17 ans pour 45% des plus de 55 ans). Les sauvegardes de données des smartphones ou tablettes (agenda, carnet d'adresse, etc.) sont en net recul, celles-ci étant en grande partie hébergées nativement dans le Cloud.

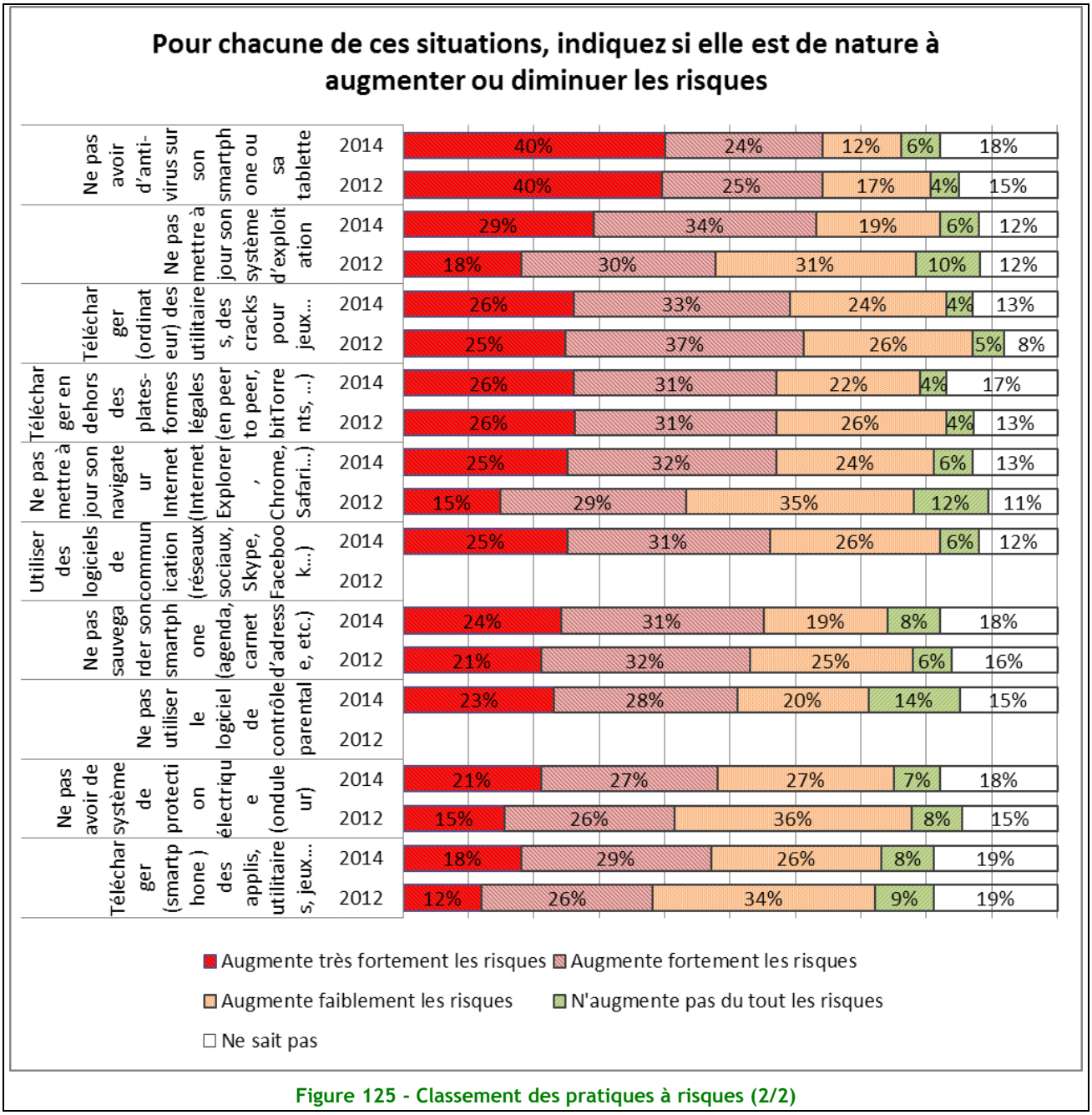

Figure 125 - Classement des pratiques à risques (2/2)

En dépit des fuites de comptes utilisateurs tendant à prouver que cette recommandation n'est que peu suivie, les utilisateurs sont majoritairement conscients du risque engendré par l'utilisation d'un mot de passe unique sur différents sites / différents matériels. En effet, 73% des utilisateurs considèrent que cela augmente fortement ou très fortement les risques.

Les utilisateurs prennent progressivement conscience de la nécessité de disposer de mots de passe robustes puisque 73% des utilisateurs estiment qu'un mot de passe trop simple pour protéger ses accès augmente fortement ou très fortement les risques.

Enfin, le manque de repères des internautes quant au risque représenté par l'installation d'applications diverses sur son ordinateur ou son téléphone semble toujours aussi présent.

Partie IV – Moyens et comportements de sécurité

Les meilleurs moyens de protéger nos équipements communicants

Par rapport à l'enquête 2012, certains moyens de protection de l'ordinateur personnel restent très utilisés. En effet la sécurisation de la connexion wifi via une clé de chiffrement, la sauvegarde des données sur divers supports (CD, en ligne, clé USB, etc.) et la mise en place de mots de passe au démarrage des sessions sur l'ordinateur personnel sont plébiscités par les internautes à plus de 60%.

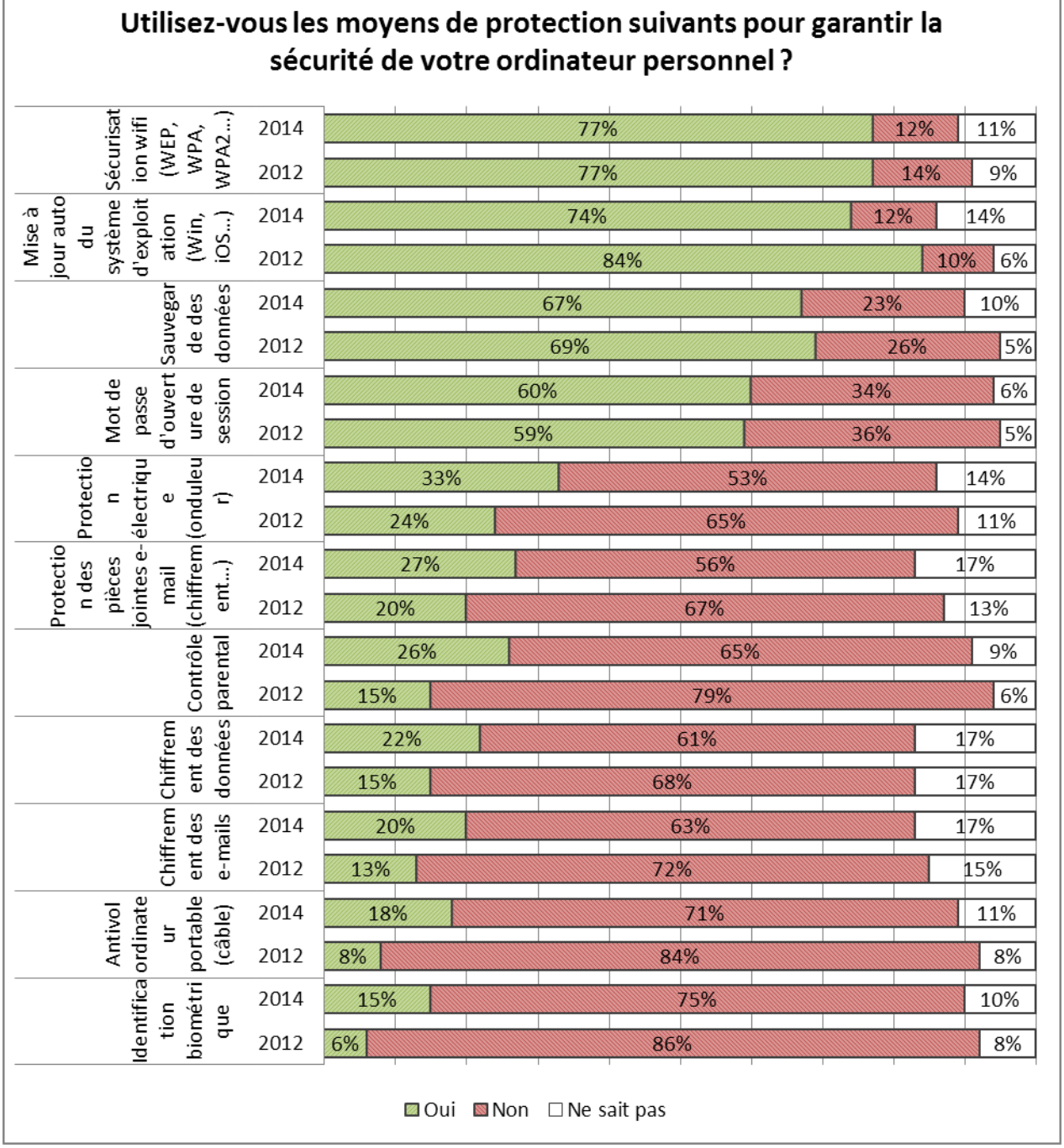

Figure 126 - Moyens de protection de l'ordinateur utilisés (1/2)

Le sentiment d'insécurité sur internet déjà montré à plusieurs reprises dans cette étude a conduit les internautes à, globalement, mieux s'équiper de moyens de protection. Dans l'ensemble, tous les moyens de protection progressent, parfois de plus que 10%. Seule ombre à ce tableau, la diminution de la mise à jour automatique du système d'exploitation. Cette tendance devra être examinée avec attention dans les éditions à venir.

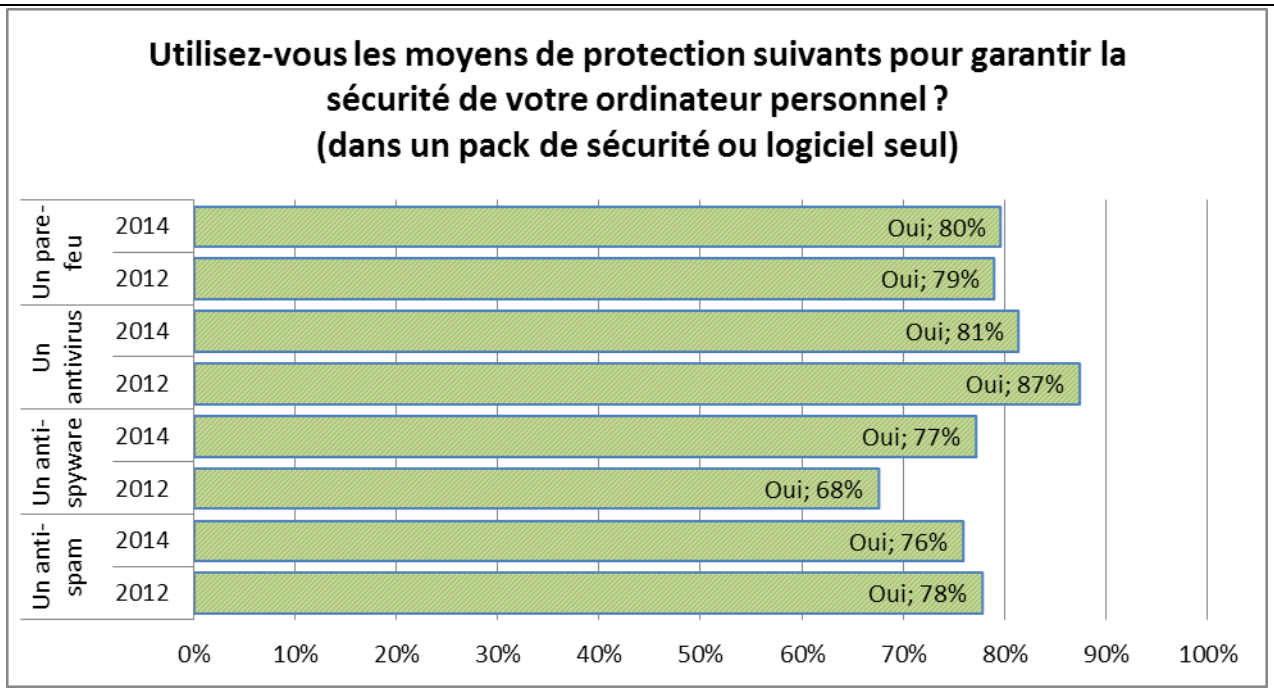

Figure 127 - Moyens de protection de l'ordinateur utilisés (2/2)

Cette année, il ressort de l'enquête que les internautes commencent à utiliser des moyens de protection électrique (onduleur ou parasurtenseur), seulement pour 33% d'entre eux.

Les dispositifs de contrôle parental, de protection des pièces jointes ainsi que le chiffrement de données sont en augmentation mais reste marginaux (en dessous des 20% d'utilisation). La complexité de mise en œuvre et l'objectif mal compris de ces solutions expliquent en partie ces mauvais scores.

De manière générale, l'internaute a augmenté son utilisation de systèmes et dispositifs de sécurité pour pérenniser son ordinateur personnel entre 7 à 10% ces deux dernières années.

La protection des smartphones et tablettes en progrès

En moyenne, une augmentation de plus de 20% par rapport à 2012 est constatée sur l'installation de logiciels de sécurité (anti-spyware, anti-spam, pare-feu) sur les appareils mobiles tels que les smartphones et les tablettes.

Les internautes utilisent les mêmes moyens de protection pour leur smartphone et/ou tablette que pour leur ordinateur portable : mots de passe, antivirus, mais dans des proportions moindres. En effet, seulement un internaute sur deux utilise un moyen de protection sur sa tablette ou son smartphone pour garantir la sécurité de ses données.

Tout comme pour les ordinateurs personnels, les dispositifs de contrôle parental, de protection des pièces jointes ainsi que le chiffrement de donnés sur les smartphones et les tablettes sont en légère augmentation mais reste marginaux (en dessous des 20% d'utilisation).

Dans l'ensemble, les internautes sont plus sensibilisés à la sécurité de leur ordinateur personnel qu'à celle de leur smartphone et/ou tablette.

Le sentiment de confiance sur Internet en baisse régulière depuis 6 ans

Les internautes, dans leur majorité encore, se sentent plutôt en sécurité lorsqu'ils utilisent Internet. 15% des 15-17 ans se sentent totalement plus rassurés sur Internet. Ce qui est 5% au-dessus de la moyenne des autres catégories des Internautes. Néanmoins ce sentiment de sécurité diminue avec les années. En effet, il y a deux ans 73% des internautes se sentaient rassurés sur Internet alors qu'actuellement seulement 66% des internautes se sentent rassurés sur Internet.

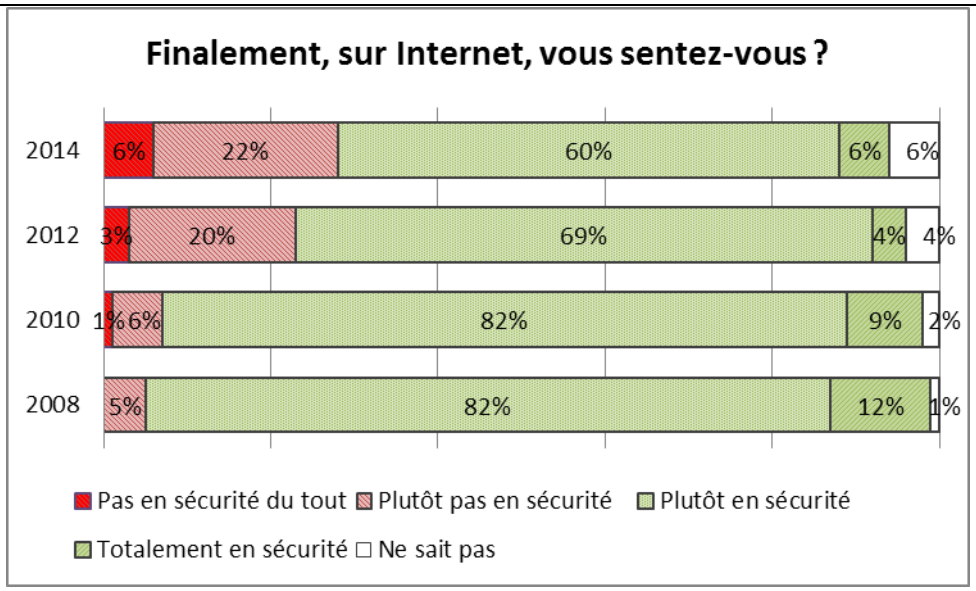

Figure 128 - Perception globale du contexte sécurité sur Internet

En complément, le sentiment d'insécurité lié à Internet augmente au cours des années quelle que soit la catégorie d'âge utilisant Internet.

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANCAIS

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

Téléchargez les productions du CLUSIF sur

www.clusif.fr