Menaces informatiques et pratiques de sécurité en France

Édition 2012

- Les entreprises de plus de 200 salariés
- Les collectivités territoriales
- Les particuliers Internautes

Club de la Sécurité de l'Information Français

Remerciements

Le CLUSIF remercie les personnes qui ont constitué le Comité d'Experts ayant participé à cette étude.

NOM	ENTITÉ
M. BUNOUST Nicolas	CONSEIL GENERAL DE LOIRE ATLANTIQUE
Mme BUTEL Annie	BNP PARIBAS
M. CALEFF Olivier	DEVOTEAM
M. CAPRONI Nicolas	CEIS
M. CHIOFALO Thierry	BOLLORE LOGISTICS
M. CONSTANT Paul	CLUSIF
Mme COURTECUISSE Hélène	LISIS CONSEIL
Mme COUTURIER Marion	SOLUCOM
Mme COUWEZ Marie-Agnès	OPEN
M. DEPAUL Jonathan	IMPRIMERIE NATIONALE
M. FOUCAULT Jacques	TIBCO
M. FREYSSINET Éric	GENDARMERIE NATIONALE / STRJD
M. GIORIA Sébastien	FR CONSULTANTS
M. GOONMETER Nuvin	ACCENTURE
M. GRÉMY Jean-Marc	CABESTAN CONSULTANTS
M. GUÉRIN Olivier	CLUSIF
Mme GUIGNARD Martine	IMPRIMERIE NATIONALE
M. HAMON Bruno	MIRCA
M. HENNIART Thierry	RÉGION NORD PAS DE CALAIS
M. HUA Zeh-Ty	ACCENTURE
M. LE CHEVALIER Rémy	LCS CONSEIL
Mme LOUIS-SIDNEY Barbara	CEIS
M. MARIE Fabrice	CONSEIL GENERAL DES COTES D'ARMOR
M. MENESTRET Benjamin	ACCENTURE
M. MINASSIAN Vazrik	ADENIUM
M. MOURER Lionel	PROVADYS
M. PAUL Damien	ACCENTURE
M. PEJSACHOWICZ Lazaro	CNAMTS
M. RAVINET Sylvan	GAMBADE
M. ROULE Jean-Louis	CLUSIF
Mme TRAN Sophie	ACCENTURE
M. VANDEPUTTE Pascal	CONSEIL RÉGIONAL DU CENTRE
M. VANHESSCHE Patrick	AXYNERGIE

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

Enquête statistique réalisée pour le CLUSIF par le cabinet GMV Conseil et Harris Interactive.

Avant-propos

Il me revient cette année, pour la première fois, l'honneur de préfacer cette édition 2012 de notre rapport MIPS, acronyme qui commence à être bien connu mais aussi très attendu par les différents acteurs de la sécurité des Systèmes d'Information.

Cette attente nous a toujours surpris, autant notre regretté Pascal LOINTIER que moi-même qui était à l'époque son vice-président. Parce que, dans les faits, c'est peut-être le rapport le moins « impressionnant » de l'année : le nombre d'identités volées y sera toujours inférieur à la population mondiale et les outils qui sont largement déployés seront ceux qui ont été conçus il y a un certain temps et atteint un certain point de maturité.

Bien sûr, un des répondants à l'enquête a pu y répondre à la sortie d'un de nos délicieux cocktails et indiquer qu'il a mis en place *worldwide* le *Cyberfair7 V5*, mais notre Comité d'Experts l'aura surement détecté et l'aura indiqué dans les commentaires qui accompagnent les chiffres (nous ne modifions jamais les chiffres sortis de l'enquête !).

De plus, nos vieux démons comme la perte de services essentiels ou les erreurs de programmation occupent toujours une place privilégiée alors qu'ils semblent être disparus de beaucoup d'autres rapports.

Mais alors, quel intérêt ?

Celui de restituer, dans l'esprit d'échange égalitaire propre au Clusif, des chiffres réels, qui - les répondants savent - ne seront utilisés que pour fournir la photographie la plus exacte des atteintes à la sécurité subies par nos Systèmes d'Information ainsi que des pratiques mises en place pour y faire face.

Et, comble de luxe, ces chiffres sont commentés et mis en perspective par un Comité d'Experts prestigieux, composé par des membres du Club mais aussi des personnalités externes. De plus, les comparaisons avec les rapports précédents et le focus sur certains domaines d'activité (Territoriaux cette année) illustrent l'évolution et mettent en perspective la problématique de la SSI.

Je finirai juste sur l'utilité que chacun de vous peut trouver dans cet ouvrage et, pour ceci, je n'ai rien à ajouter à ce que Pascal avait écrit il y a deux ans :

“

- *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 laisse à Lionel MOURER, en même temps cerveau, chef d'orchestre et cheville ouvrière de ce rapport la tâche de remercier l'excellent travail de ceux qui l'ont accompagné.

Lazaro PEJSACHOWICZ
Président du CLUSIF

Synthèse de l'étude

Au travers de l'édition 2012 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 (351 ont répondu) et des collectivités territoriales (205 ont répondu) interrogées. Par ailleurs, elle se veut relativement exhaustive, puisque cette année, elle passe en revue l'ensemble des 11 thèmes de la norme ISO 27002, relative à la sécurité des Systèmes d'Information.

Enfin, cette année comme en 2008 et 2010, 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... » dans un contexte financier et organisationnel toujours très contraint

La mise en place d'une « organisation » et de « structures » de la SSI (Responsable de la Sécurité des Systèmes d'Information (RSSI ou RSI), Correspondant Informatique et Libertés (CIL), Politique de Sécurité des Systèmes d'Information (PSSI ou PSI), charte, etc.) continue à se mettre en œuvre, mais la mise en application concrète de ces « politiques » ne décolle toujours pas réellement !…

Côté budget, on constate une légère reprise, pondérée par le fait que le poste le plus augmenté est la mise en place de solution, avec 37 %. Pour beaucoup, la sécurité reste une histoire de mise en place de solutions techniques.

Le nombre d'entreprises ayant formalisé leur PSI est demeuré inchangé en deux ans (63 %). Les normes de sécurité poursuivent leur influence grandissante sur la PSI des entreprises, passant de 55 % en 2010 à 75 % en 2012.

La fonction de RSSI est de plus en plus clairement identifiée et attribuée au sein des entreprises (54 %, vs 49 % en 2010 et 37 % en 2008), ce qui va dans le sens de l'histoire. Enfin, à présent, 100 % des entreprises ont en permanence une « équipe sécurité », marquant l'importance du sujet et cela en quatre ans seulement (43 % n'en n'avaient pas en 2010) !

Point positif : il y a une forte progression des analyses de risques (54 % totale ou partielle vs 38 % en 2010) !

L'accès nomade aux ressources de l'entreprise est de plus en plus généralisé. La maturité des solutions technologiques de connexions, de contrôle des postes nomades et des informations qui transitent permettent un meilleur contrôle des risques associés.

Les PDA, tablettes et smartphones 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.

L'utilisation de la messagerie instantanée (MSN, Skype, etc., non fournie par l'entreprise) et des réseaux sociaux est aujourd'hui majoritairement interdite par les politiques de sécurité dans les entreprises.

Seules 12 % des entreprises ont placé leur SI sous infogérance et quand c'est le cas, plus d'une sur trois ne met pas en place d'indicateurs de sécurité !…

De même, après plusieurs années d'augmentation régulière, la formalisation des procédures opérationnelles de mise à jour des correctifs de sécurité (patch management) est, en 2012, en régression (59 % vs 64 % en 2010).

Ces deux dernières années marquent un palier dans la gestion des incidents de sécurité par les entreprises. En 2012, 53 % (+1 point vs 2010) d'entre elles ont une cellule (dédiée ou partagée) à la gestion de ces incidents de sécurité.

Les types d'incidents rencontrés par les entreprises connaissent des taux beaucoup plus faibles que les années précédentes :

- forte baisse des erreurs d'utilisation (17 %, -29 points vs 2010),
- les infections par virus restent toujours la première source d'incidents d'origine malveillante pour les entreprises (13,7 incidents de sécurité dus à des virus sur l'année 2011).

Un peu moins d'un tiers des entreprises ne prennent pas en compte la continuité d'activité. Ceci reste relativement stable au regard des résultats de l'étude réalisée en 2010. Sans surprise l'indisponibilité des 'systèmes informatiques' représente le scénario le plus couvert (59 %).

À 88 % (idem 2010), les entreprises se déclarent en conformité avec les obligations de la CNIL.

Sur une période de deux ans, deux tiers des entreprises interrogées ont réalisé au moins un audit ou contrôle de sécurité du Système d'Information par an (chiffres globalement équivalents à ceux de 2010).

Une large proportion d'entreprises (79 %) ne mesure pas régulièrement son niveau de sécurité liée à l'information (pas de tableau de bord de la sécurité de l'information).

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

Quels sont les facteurs déclenchant de vos projets sécurité ? À cette question, les collectivités auraient probablement répondus à l'unisson : la règlementation suivie de près par les impacts des incidents de sécurité. Preuve en est, les obligations de santé publique et de service minimum relatives à la pandémie de 2009 ont déclenché de nombreux projets et impliqués des ressources importantes. Une conséquence directe : l'accès à distance au Système d'Information. Seulement voilà, qui dit accès distant dit sécurité et plus particulièrement confidentialité.

Toujours sur le périmètre de la confidentialité, les exigences de la CNIL et les programmes de contrôle associés ont amené les collectivités à maintenir voir augmenter les ressources engagées. Il semble qu'une partie des intentions de 2008 se soient concrétisées, puisque nous constatons aujourd'hui 39 % de Correspondants Informatique et Libertés (CIL) nommés ou prévus (décision prise) par rapport à 37 % en 2008.

Un autre enseignement de cette étude fait apparaître des pratiques inégales entre les différents profils de collectivités. Les Conseils Généraux et les Conseils Régionaux font preuve d'une plus grande mise en œuvre des pratiques de sécurité. Il en est de même pour les métropoles qui ont pour la plupart structurées leur activité sécurité alors que les communautés ou les mairies de taille moyennes, par manque de ressources ou de connaissances, sont dans une approche plus empirique de ces pratiques.

Quels vont être les impacts de la rigueur budgétaire sur la sécurité ? Tous les interlocuteurs s'interrogent pour répondre à l'objectif de rationalisation. Porter l'effort sur les actifs les plus critiques de la collectivité ? C'est probablement la bonne réponse. Mais pour y arriver, celles-ci vont devoir renforcer la tendance en matière d'analyse de risque, seul dispositif permettant d'appliquer le principe de proportionnalité et de répondre à l'objectif de rationalisation.

Quelques éléments chiffrés :

- les statistiques de sinistralité sont globalement en net recul : conséquences des nouvelles mesures ou manque de traçabilité ? Les pertes de services essentiels (27 % vs 44 % en 2008), les infections virales (27 % vs 44 % en 2008) et les pannes d'origine interne (24 % vs 40 % en 2008) représentent toujours les principales causes de sinistralité,
- plus d'une Collectivité sur deux (54 %) ne dispose d'aucun processus de gestion de la continuité d'activité,
- 40 % de collectivités mènent un audit au moins une fois par an, alors que 56 % n'en mènent pas du tout (idem 2008). Les audits réalisés traitent plus souvent des aspects techniques que des aspects organisationnels,
- l'utilisation de tableau de bord n'a pas progressé depuis la dernière enquête. Ainsi, seule une collectivité sur 10 annonce avoir mis en place des outils de ce type.

Données personnelles, vie privée, réseaux sociaux, Cloud, mobilité et BYOD : les internautes commenceraient-ils à changer de comportement, auraient-ils enfin intégrés les nouveaux usages et les menaces ?

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

De son côté, le taux d'équipement en informatique continue à augmenter dans les foyers et l'ordinateur reste l'outil principal pour se connecter sur Internet, avec toutefois le raccordement d'un nombre croissant d'équipements sur Internet dont les télévisions et les consoles de jeux de salon.

Le wifi se généralise comme mode d'accès au réseau local et l'on note de nouvelles tendances dans les usages informatiques au sein des foyers, avec l'arrivée des tablettes et l'utilisation de services de Cloud Computing pour le stockage de données.

Par ailleurs, les deux tiers des internautes se connectent aussi sur Internet en dehors du domicile avec leur équipement mobile.

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… Mais 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…

Les tablettes apparaissent bien comme plus exposées aux risques que les ordinateurs.

Peu de problèmes de sécurité sont remontés par les internautes, et lorsque c'est toutefois le cas, il s'agit plus d'accidents de sécurité (fausse manipulation, panne matérielle), que d'incidents liés à des charges virales ou des piratages… Il est toutefois légitime de se demander si les internautes sont réellement conscients des problèmes qui se produisent et s'ils en font une analyse.

Côté usage, l'ordinateur familial sert aussi bien à des activités professionnelles et vice-versa (point constaté également dans le thème « Entreprises »).

Le paiement en ligne n'est pas encore rentré dans les mœurs depuis un smartphone ou une tablette, mais il est plus fréquent depuis un ordinateur, avec une vigilance accrue.

Les internautes expriment d'ailleurs clairement certains des facteurs les confortant dans leur démarche de paiement en ligne, tels que : le chiffrement des données des transactions, la renommée du site ou sa marque, la confirmation par un moyen tiers (e-mail, SMS), la possibilité d'utiliser des moyens de paiements spécifiques à Internet (e-carte). En revanche, un agrément par des organismes indépendants ou la localisation du site sont moins importants.

En termes de « moyens de protection », les solutions de protection gratuites sont toujours plébiscitées, les outils à couvertures multiples (anti-malware, anti-spam, anti-phishing, etc.) ne sont malheureusement pas aussi populaires que les outils à périmètre unitaire (anti-virus seul, etc.) ce qui peut conduire à un faux sentiment de sécurité.

Certaines actions considérées par les spécialistes de la sécurité comme des pré-requis, telle les sauvegarde ou l'application des correctifs, ne sont pas correctement prises en comptes et réalisées par les internautes.

En revanche, 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 est largement mise en œuvre.

Globalement les comportements s'améliorent, les mots de passe et le verrouillage d'écran étant surtout mis en œuvre… lorsqu'il s'agit d'une configuration par défaut de l'éditeur ou du constructeur.

Il y a un très net décalage entre les efforts faits en matière de sécurité par les internautes sur leurs équipements, selon qu'il s'agisse d'ordinateurs – outils plutôt « pas trop mal » gérés - ou des équipements

mobiles comme les smartphones et les tablettes pour lesquels l'existence d'outils de sécurisation sont peu, voire pas, connus.

Quant à l'utilisation de la messagerie, les aspects de confidentialité et de chiffrement ne sont quasiment pas rentrés dans les mœurs 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…

Même si la menace faiblit globalement, 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 !

Dans un écosystème numérique où les frontières entre l'entreprise, ses clients, ses partenaires, ses fournisseurs et ses propres collaborateurs sont de plus en plus floues, il est plus que jamais nécessaire de positionner le cadre de la sécurité du Système d'Information.

Les résultats de cette étude serviront, le cas échéant, de levier pour convaincre une direction concernée mais pas encore impliquée. Ils serviront également à apprécier les pratiques au regard du marché.

Alors, « au boulot » ! Pour les entreprises ou collectivités qui n'ont encore « rien fait », il est plus que jamais nécessaire de positionner le « cadre de la SSI ». Pour celles qui l'ont mis en place, reste à mettre en œuvre et jusqu'au bout des pratiques concrètes, ancrées dans les processus de la gestion de l'information. Ceci leur permettra de sécuriser leur capital informationnel et cela à la hauteur de leurs enjeux !

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 »

Sommaire

Liste des figures

LES ENTREPRISES

LES COLLECTIVITES TERRITORIALES

LES INTERNAUTES

Méthodologie

L'enquête du CLUSIF sur les menaces informatiques et les pratiques de sécurité en France en 2012 a été réalisée au cours de début janvier à mi-mars 2012, 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 : 351 entreprises de cette catégorie ont répondu à cette enquête,
- les collectivités territoriales : 205 d'entres-elles ont accepté de répondre,
- les particuliers internautes : 1 000 individus, issus du panel d'internautes de l'institut spécialisé Harris Interactive, 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 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 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 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, collectivité territoriale 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 2012 de son enquête, le CLUSIF souhaitait interroger un échantillon d'entreprises identique à celui interrogé en 2008 et 2010, mais regroupé différemment. En effet, cette année, le type « Services – Finance » a été découpé en deux catégories distinctes (du fait de niveaux de maturité en SSI assez différents) et les types « Industrie » et « BTP » ont été regroupés. Les autres types d'entreprises ont été conservés tels quels afin de pouvoir comparer les progrès ou les éventuelles régressions. Ainsi, la cible est constituée des entreprises de plus de 200 salariés des secteurs d'activité suivants :

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

351 entreprises ont répondu à la sollicitation du CLUSIF (entretien de 25 minutes en moyenne), avec un taux d'acceptation d'environ 10 % (identique à 2010) : sur 100 entreprises contactées, seulement 10 ont accepté de répondre à nos questions, ce qui a impliqué d'appeler environ 3 500 entreprises !

L'échantillon est construit selon la méthode des quotas avec 2 critères – l'effectif et le secteur d'activité des entreprises – pour obtenir les résultats les plus représentatifs de la population des entreprises.

Cet échantillon est ensuite redressé sur l'effectif et le secteur d'activité pour se rapprocher de la réalité des entreprises françaises, sur la base des données INSEE.

Entreprise Taille / Secteur	200-499 salariés	500-999 salariés	1 000 et plus	Total	Total en %		Données INSEE
Banque - Assurance	16	7	20	**43**	**12,3%**	→	**7%**
Commerce	22	4	18	**44**	**12,5%**	→	**15%**
Industrie - BTP	86	27	21	**134**	**38,2%**	→	**39%**
Services	42	13	31	**86**	**24,5%**	→	**27%**
Transport – Télécoms	18	5	21	**44**	**12,5%**	→	**12%**
Total	**184**	**56**	**111**	**351**	**100,0%**		**100%**
Total en %	**52,4%**	**16,0%**	**31,6%**	**100,0%**		↑ Redressement	
Redressement →	↓	↓	↓				
Données INSEE	**77%**	**17%**	**6%**	**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 23 % (29 % en 2010) des entreprises interrogées, mais plus de 45 % dans les plus de 1 000 salariés (40 % en 2010).

Toutes tailles et secteurs confondus, les personnes sondées sont à plus de 82 % des DSI (Directeur des Systèmes d'Information), des Directeurs ou Responsables informatiques ou des RSSI (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, 81 % d'entre elles jugent lourde de conséquences une indisponibilité de moins de 24h de leurs outils informatiques (avec un maximum de 91 % pour le secteur de la Banque – Assurance).

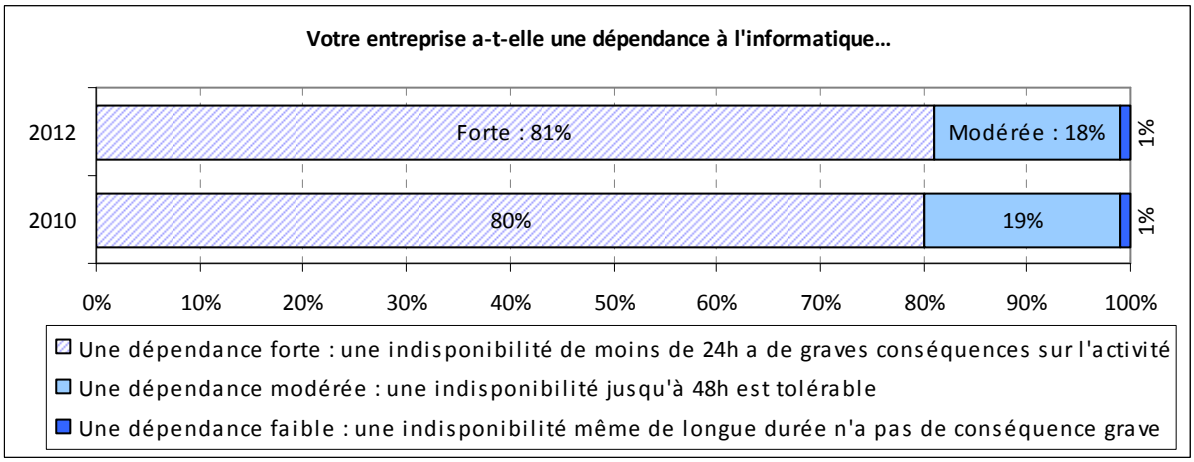

Figure 1 - Dépendance des entreprises à l'informatique

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

Un budget informatique moyen à 1,6 million €

Le budget informatique annuel moyen est de 1,6 million d'euros. Seuls 42 % des sondés ont répondu à cette question, ils étaient 51 % en 2010.

On constate que 64 % ont un budget inférieur à 1 million d'euro (58 % en 2010), 18 % entre 1 et 2 millions (20 % en 2010), 13 % entre 2 et 5 millions (15 % en 2010) et enfin 5 % au-dessus de 5 millions jusqu'à un maximum de 40 millions (7 % en 2010 avec un maximum de 20 millions).

Un budget sécurité dont le périmètre est toujours mal cerné

Les RSSI ont encore du mal à cerner le budget qui leur est attribué par rapport au budget informatique total. Ce flou augmente encore cette année par rapport à 2010, 36 % cette année contre 30 % en 2010.

Lorsque le budget est clairement identifié, la répartition est hétérogène.

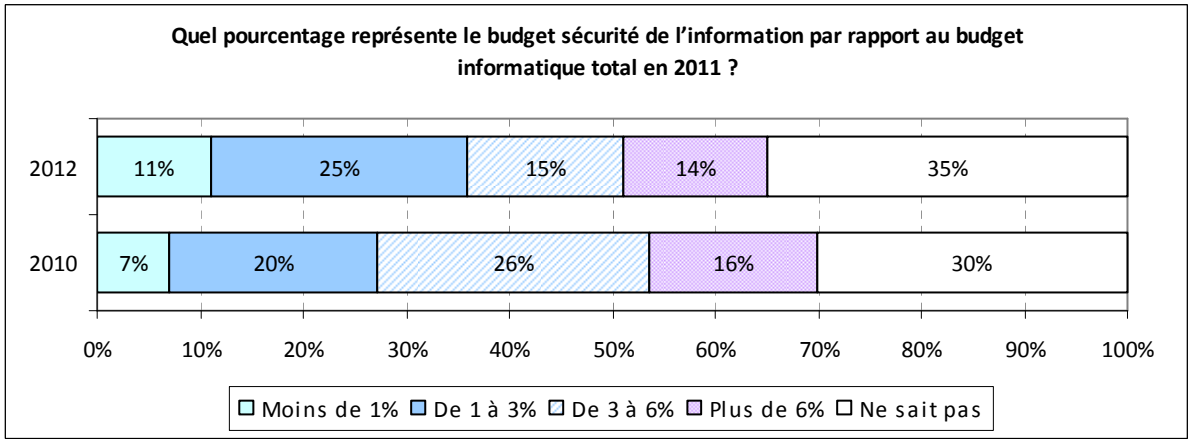

Figure 2 - Part du budget informatique alloué à la sécurité dans les entreprises

Une légère reprise des budgets sécurité

Globalement, le pourcentage des budgets « constants » augmente (64 % contre 48 % en 2010) tandis que 22 % des budgets sont en augmentation.

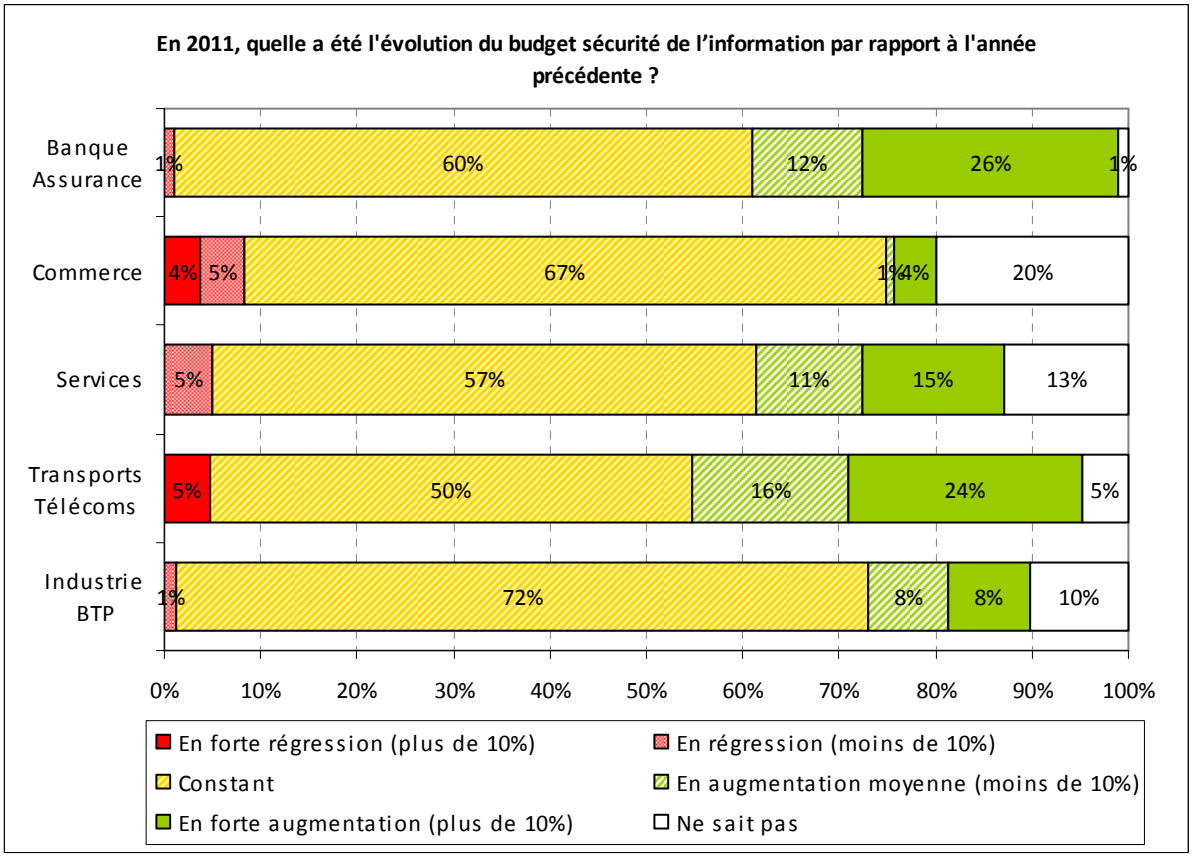

Figure 3 - Évolution du budget sécurité selon les secteurs d'activités

Toutefois, on constate que le poste ayant eu la plus grosse augmentation est la mise en place de solution, avec 37 %. Ainsi, la sécurité semble avant tout correspondre à la mise en place de réponses techniques.

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 %, -11 points vs 2010) : le manque de budget,
- 2ème raison citée (29 %, -1 point vs 2010) : les contraintes organisationnelles,
- 3ème raison citée (21 %, +7 points vs 2010) : le manque de personnel qualifié,
- 4ème raison citée (18 %, -6 points vs 2010) : la réticence de la hiérarchie, des services ou des utilisateurs,
- 5ème raison citée (14 %, +1 point vs 2010) : le manque de connaissance.

Les deux freins principaux restent comme en 2010 le manque de moyens budgétaires et les contraintes organisationnelles, avec toutefois une baisse par rapport à 2010. C'est un signe positif, particulièrement important pour le premier critère (manque de budget).

Au chapitre des bonnes nouvelles, la réticence de la Direction des Systèmes d'Information reste hors du top 5 (2 % seulement, contre 3 % en 2010).

Enfin, le manque de personnel qualifié remonte d'un cran, signe d'une continuelle agitation du marché de l'emploi dans le secteur de la SSI, démontré par ailleurs et de manière persistante, par le nombre important d'offres d'emplois…

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 demeuré inchangé en deux ans (63 %). De plus, cette politique est globalement à jour dans la mesure où 82 % des entreprises interrogées l'ont actualisée 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 (-1 point vs 2010).

Accélération de l'implication de la Direction Générale… au déficit de la DSI et du RSSI !

Les Directions des Systèmes d'Information sont nettement moins impliquées dans l'élaboration de la PSI (60 % en 2012 vs 80 % en 2010), et l'implication des RSSI passe de près de 50 % à un tiers. Il semble que cette perte d'implication se fasse au profit de celle de la Direction Générale, qui semble se saisir de ce dossier avec une implication pour 71 % des entreprises au lieu de 55 % en 2010.

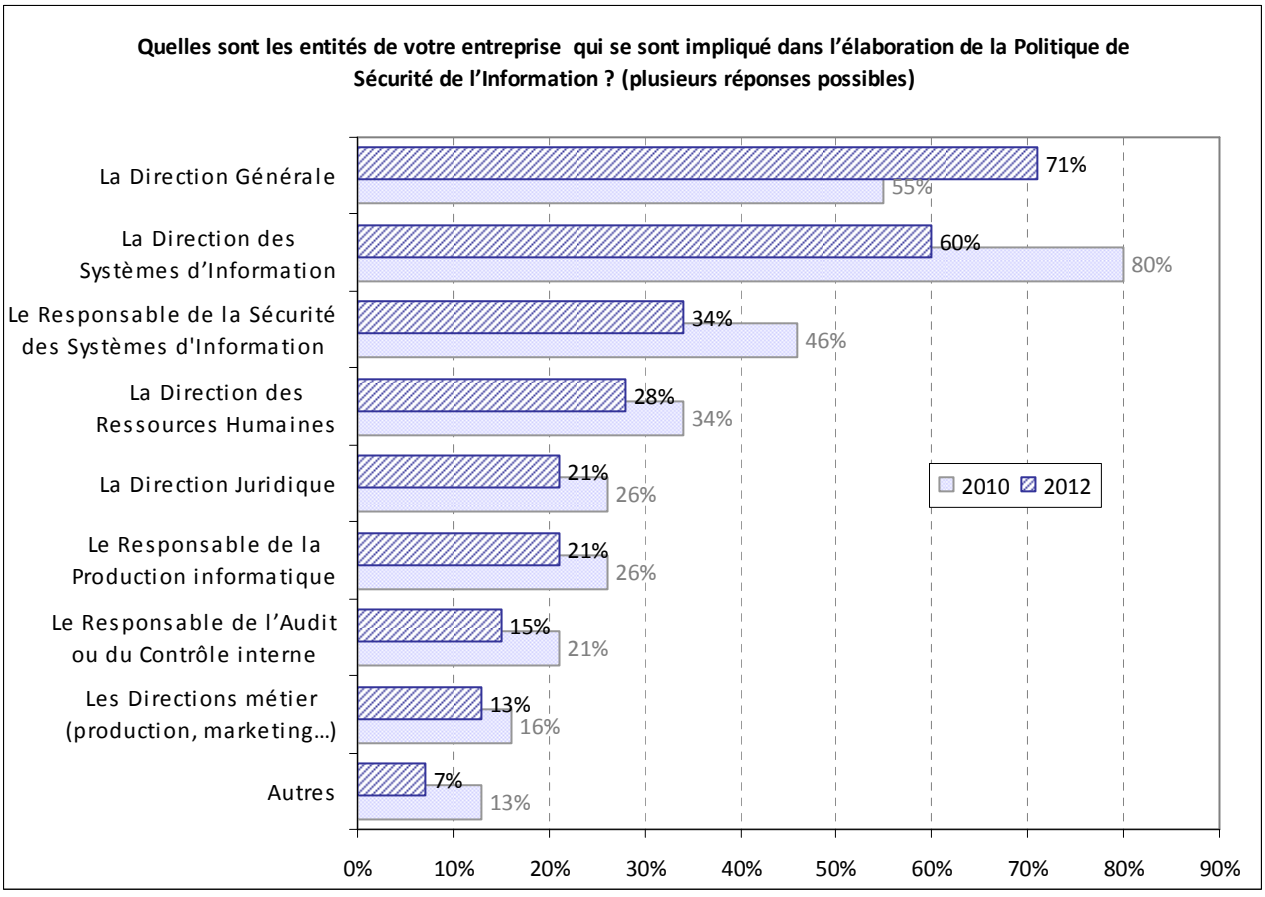

Figure 4 - Implication des différentes entités à la PSI

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

Aussi, suite à une question nouvelle posée en 2012, on constate l'arrivée des référentiels internes comme étant une base de la construction de la Politique de Sécurité de l'Information de l'entreprise pour plus de 20 % d'entre elles. L'influence de ces référentiels internes pourrait être liée à la montée en puissance en France des exigences portées par les impératifs de contrôle interne.

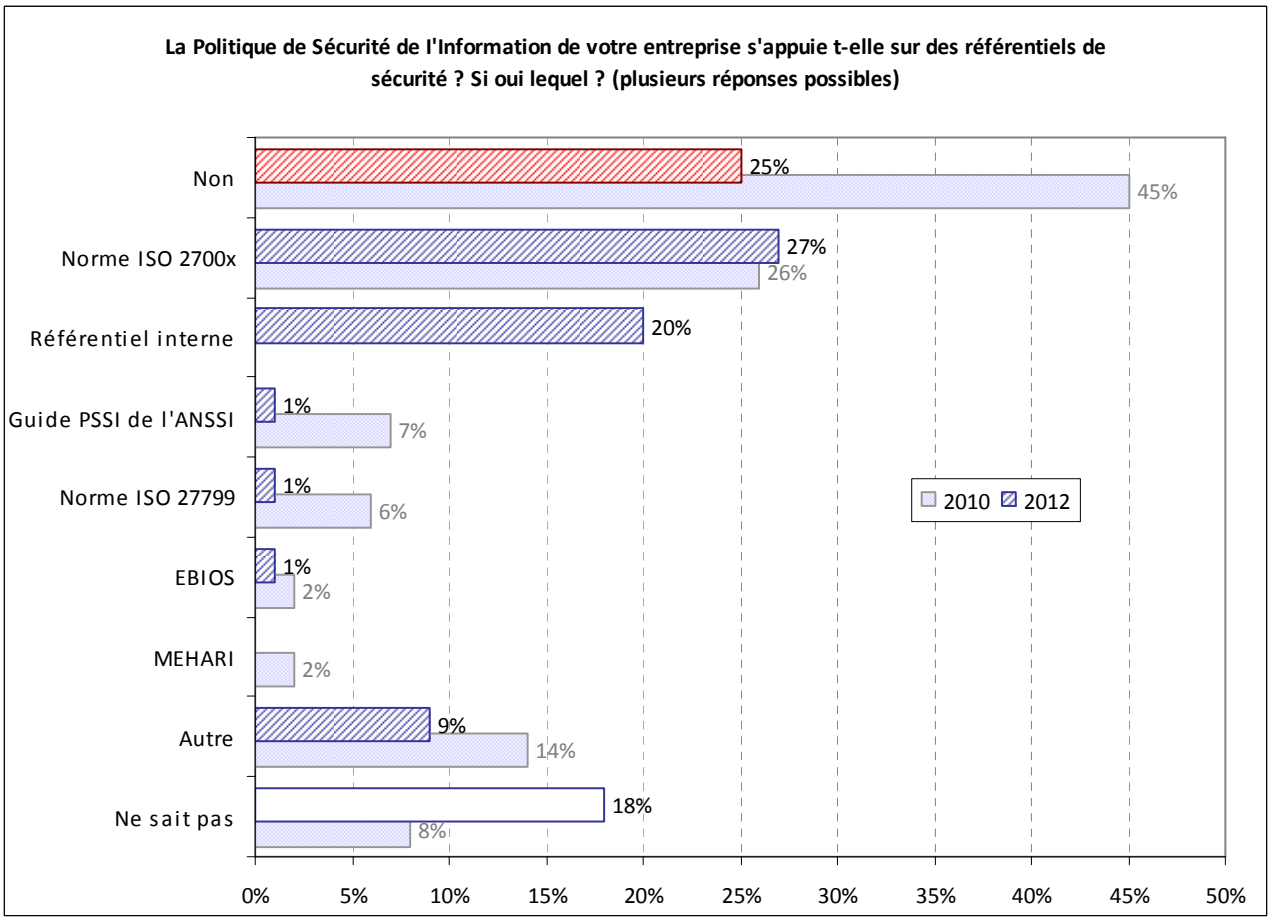

Figure 5 – Référentiels utilisés pour la formalisation de la PSI

Enfin, plusieurs référentiels apparaissent désormais d'usage marginal, tels que le guide PSSI de l'ANSSI, l'ISO 27799 pour le domaine de l'informatique de santé et MEHARI (cette dernière restant avant tout une méthode 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 Système d'Information dans 74 % des entreprises.

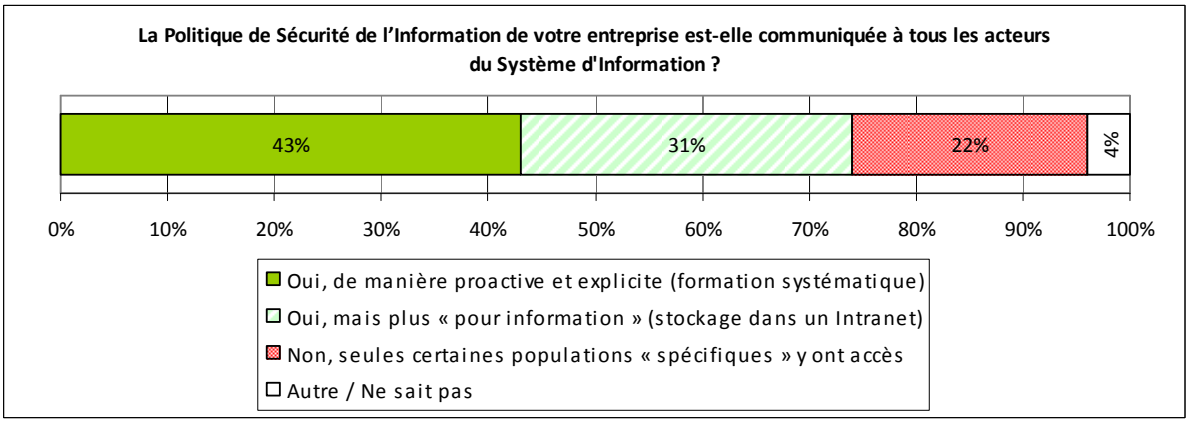

Figure 6 – Diffusion de la PSI au sein des entreprises

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.

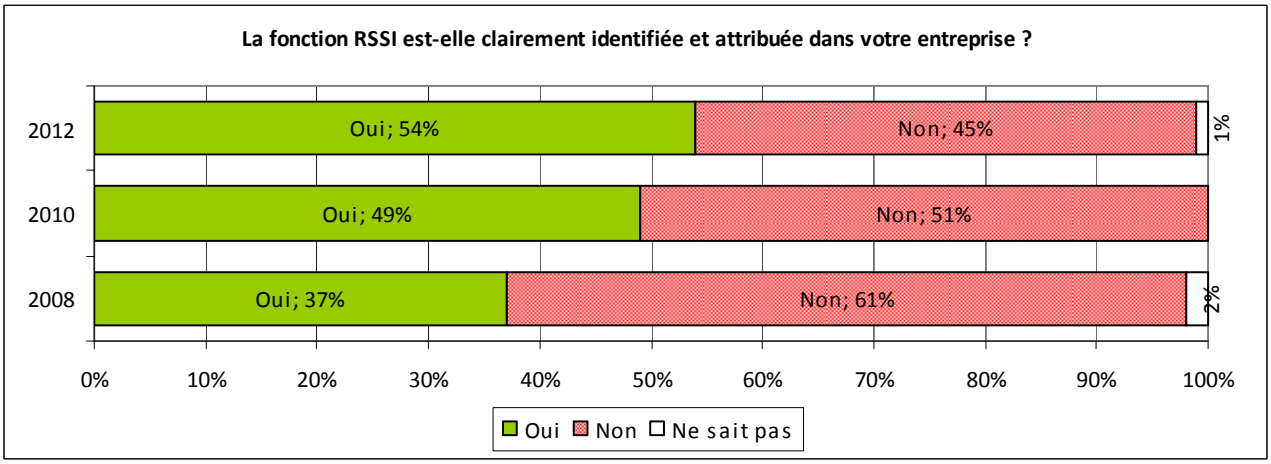

Figure 7 - Attribution de la fonction RSSI

Et 63 % des RSSI sont dédiés à cette tâche à temps plein (vs 49 % en 2010) et lorsque le RSSI n'existe pas, cette mission reste fortement attachée à la Direction des Systèmes d'Information.

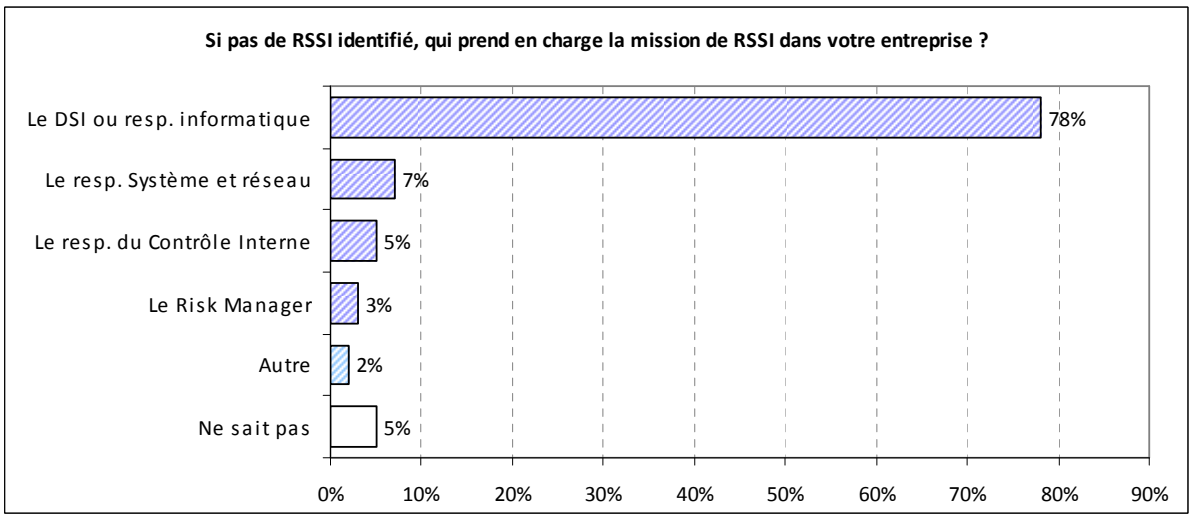

Figure 8 - Prise en charge de la fonction RSSI, lorsqu'il n'existe pas de RSSI

Un rattachement encore en perpétuelle évolution…

Le RSI ou RSSI est soit rattaché à la DSI (47 %), soit à la Direction Administrative et Financière (DAF) (10 %) ou directement à la Direction Générale pour près du tiers (32 %) des entreprises interviewées, encore en recul par rapport à 2010 (-2 %). Ceci peut s'expliquer par les arrivées plus nombreuses de RSSI au sein d'entreprises de tailles moyennes ayant un niveau de maturité en Sécurité des SI encore faible.

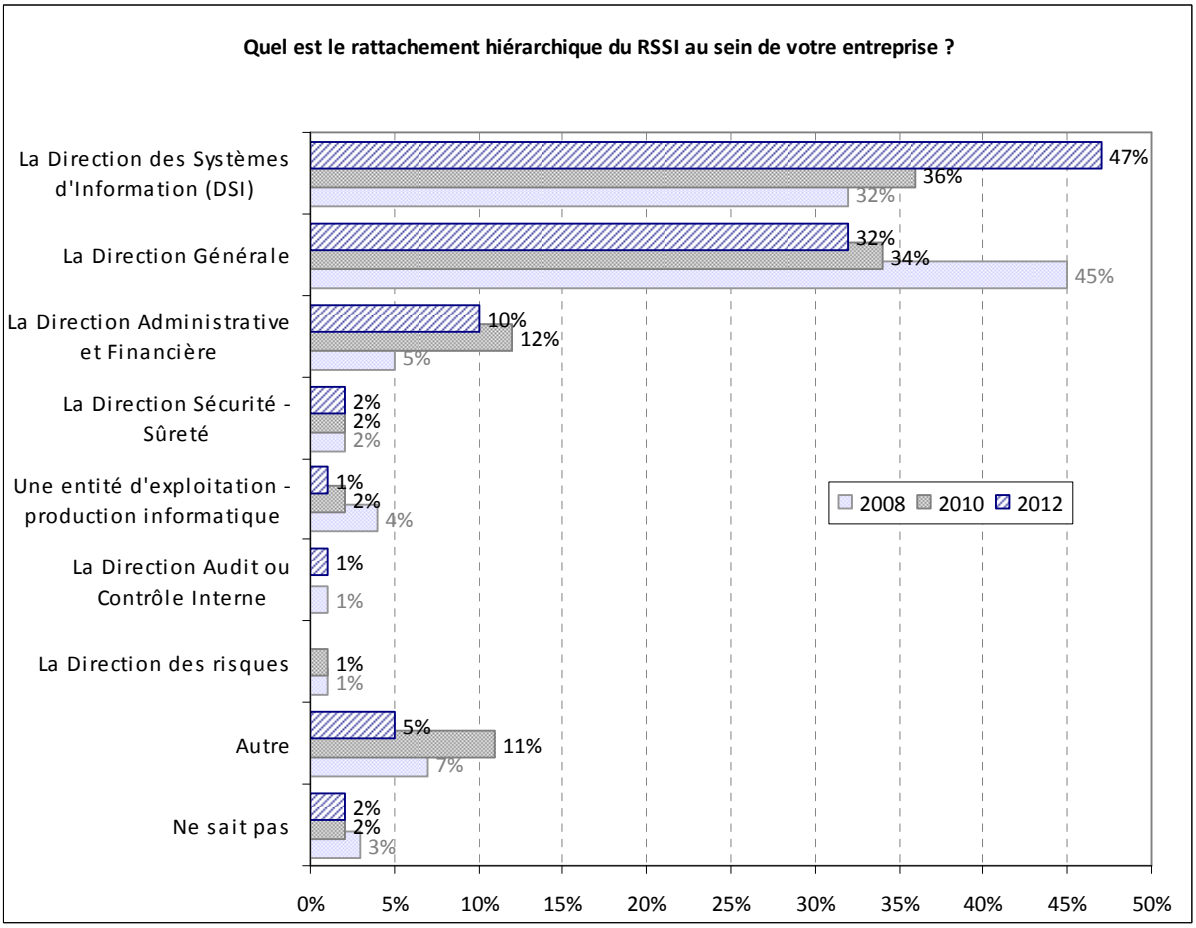

Figure 9 - Rattachement hiérarchique du RSSI au sein de l'entreprise

Globalement, la répartition des tâches du RSSI n'a pas évolué par rapport à 2010.

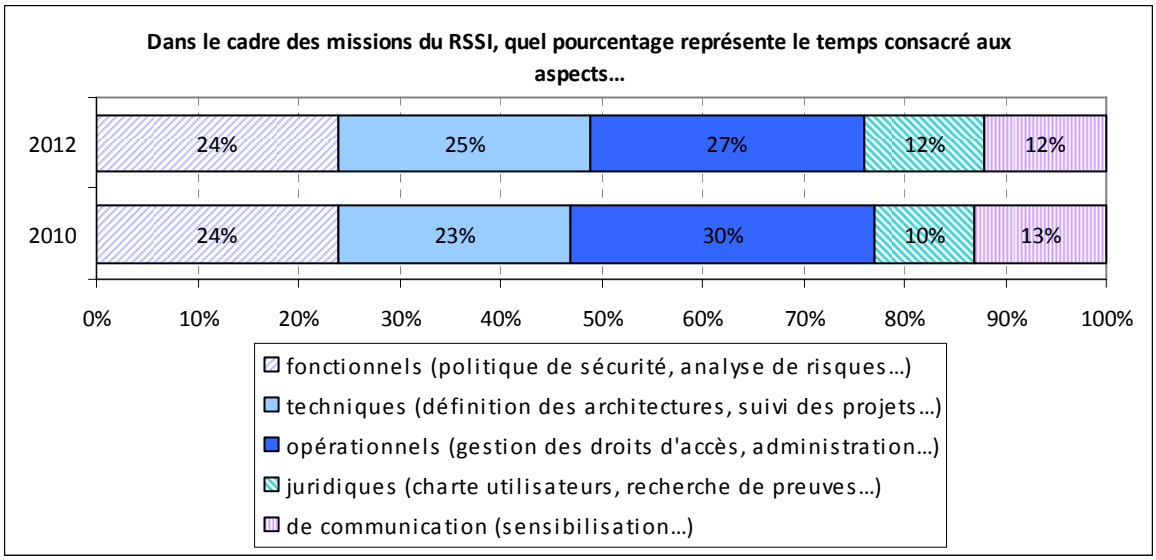

Figure 10 - Répartition des missions du RSSI

Enfin, à présent, 100 % des entreprises ont en permanence une équipe sécurité, marquant l'importance du sujet. Toutefois, dans 72 % des cas, le RSSI (ou son équivalent) est encore un homme ou une femme seul(e) ou en binôme seulement !

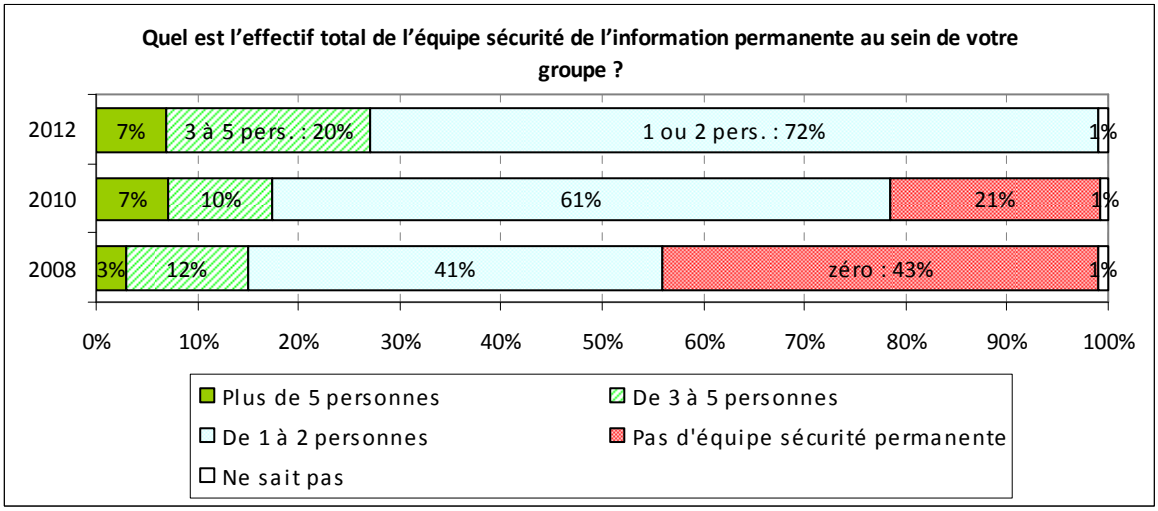

Figure 11 - Effectif total de l'équipe sécurité permanente au sein de l'entreprise

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

Inventaire et classification des informations : stabilité depuis deux ans

Le nombre d'entreprises réalisant l'inventaire de leur patrimoine informationnel et/ou la classification des informations est quasiment identique à celui de 2010. Assez souvent ces deux thèmes sont traités simultanément, ce que reflètent bien les résultats de l'enquête.

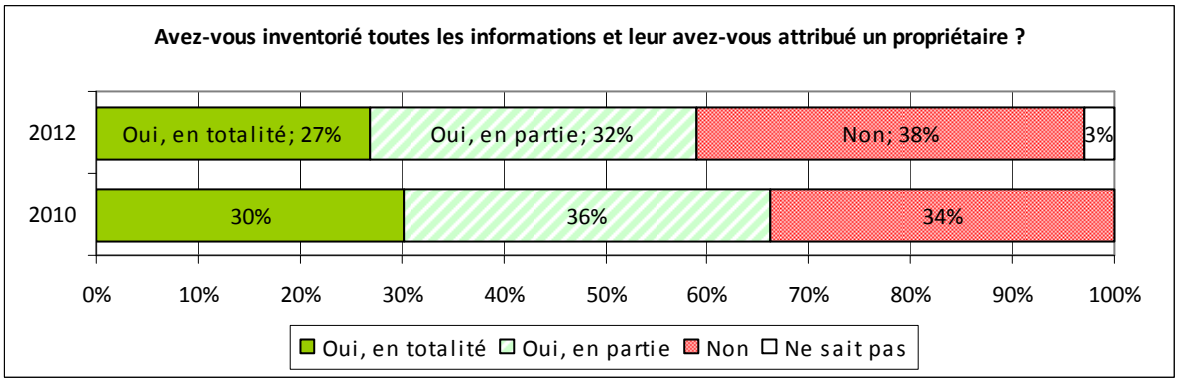

Figure 12 – Inventaire et attribution d'un propriétaire des informations de l'entreprise

Comme l'objectif de la classification est de définir les informations et/ou processus les plus sensibles, avec leurs supports, ces entreprises ont conscience du patrimoine qui participe à leur pérennité. Elles ont, à priori, les éléments discriminants pour faire le choix des mesures de sécurité les mieux adaptées. Le nombre de niveaux de sensibilité des informations est majoritairement fixé à 3, pour 43 % des entreprises.

Pour les 38 % 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, 28 % des sociétés de plus de 1 000 salariés n'ont engagé aucune démarche de classification de leurs informations.

Mais au-delà, si l'on considère qu'une classification partielle laisse « des trous dans la raquette », cela signifie que 75 % des entreprises ne peuvent dire avec précision sur quel périmètre il est indispensable de déployer des outils en priorité, 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 responsables sécurité utilisent des arguments suffisamment convaincants dans leur communication vis-à-vis du décideur budgétaire ?

L'analyse des risques en forte progression…

Les résultats de cette année montrent une forte progression des analyses de risques avec une inversion positive de la répartition par rapport à 2010.

Toutefois, seulement 19 % de ces analyses prennent en compte le périmètre complet de l'entreprise et pas uniquement celui des systèmes informatiques. La Banque-Assurance et les Services se positionnent en première position, avec 22 % d'analyse sur l'ensemble du périmètre de l'entreprise.

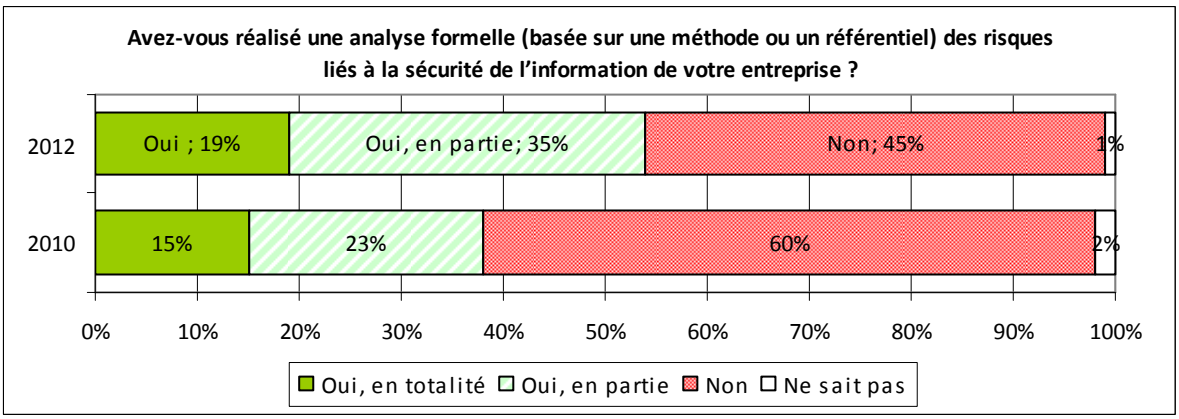

Figure 13 – Utilisation d'une méthode ou un référentiel pour réaliser l'analyse des risques

La boucle d'amélioration de la sécurité se met en place peu à peu avec la mise en œuvre d'un plan d'actions correctif consécutif à l'analyse de risques. Ainsi, 40 % des entreprises ayant réalisé une analyse de risque, totale ou partielle, ont défini et mis en œuvre un plan d'actions complet d'amélioration de la sécurité suite au rapport.

En revanche, 19 % des entreprises ne font rien suite à cette analyse. Dans ce cas, quel est l'objectif recherché ? S'agit-il de répondre à une demande de la direction, une loi, un règlement ? C'est une piste possible car les directions d'audit interne ou les directions informatiques insistent de plus en plus pour obtenir un document d'approche de management par les risques, quels que soient les métiers de l'entreprise. Par ailleurs, il arrive aussi que les ressources humaines soient insuffisantes, en nombre ou en compétence, pour réaliser les actions nécessaires.

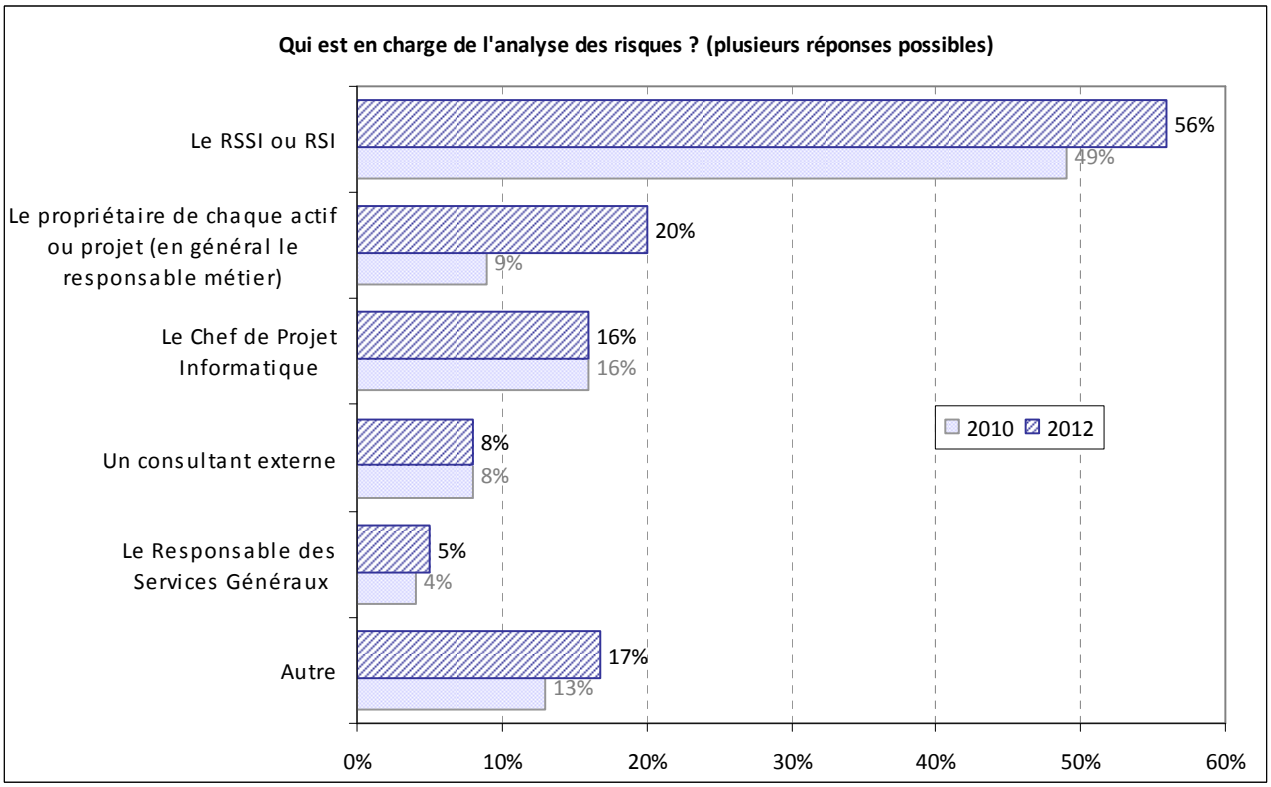

Figure 14 – Personne(s) en charge de l'analyse des risques

Les propriétaires des actifs sont nettement plus impliqués dans les analyses de risques qu'en 2010. On peut même noter que dans les entreprises de 500 à 999 salariés, ils sont 30 % à prendre en charge cette

mission. C'est un point positif, car c'est bien le propriétaire de l'information qui connaît le mieux les processus de son métier et les risques qu'il redoute.

Dans les entreprises de plus de 1 000 salariés, 67 % des RSSI sont en charge de ce sujet. Ces analyses sont réalisées pour 27 % d'entre elles en se basant sur les indications de la norme internationale ISO 27005 et pour 32 % sur d'autres méthodes, hors les méthodes spécifiques sécurité EBIOS (7 %) et MEHARI (5 %).

Thème 8 : Sécurité liée aux Ressources Humaines

Les chartes d'usage ou d'utilisation du SI mieux adoptées

Les deux dernières années n'ont pas entraîné une forte augmentation des rédactions de chartes d'usage ou d'utilisation du SI : +8 % (soit 6 points de mieux) des entreprises entre 2010 et 2012 disposent d'une charte finale ou en cours d'élaboration. De même qu'en 2010, l'effet de taille a son importance : la charte est présente dans 89 % des entreprises de plus de 1 000 personnes. En queue de peloton, le secteur du Commerce avec seulement 56 % de chartes formalisées.

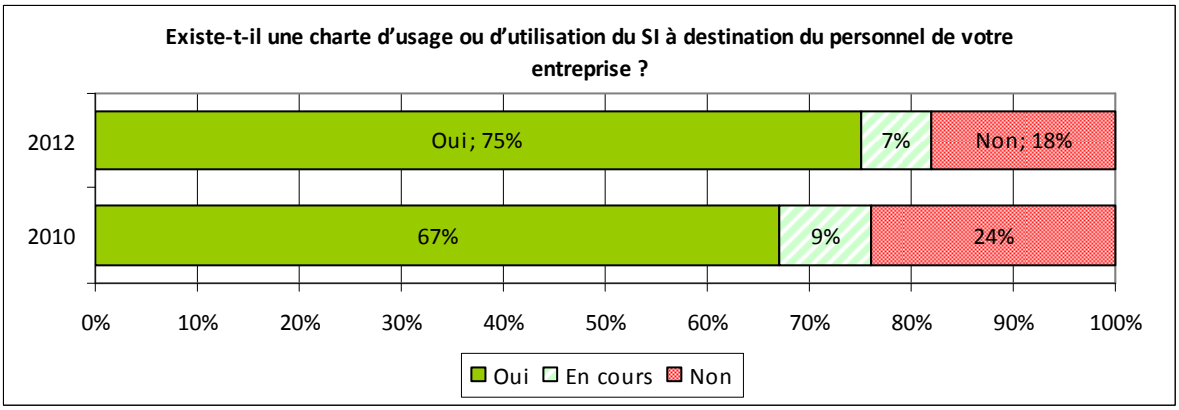

Figure 15 - Existence d'une charte d'usage ou d'utilisation du SI

Une telle charte ayant pour objectif principal de fixer les règles d'utilisation, de sécurité et les bonnes pratiques à respecter par les utilisateurs, il est primordial qu'elle soit approuvée par les instances représentatives du personnel, ce qui est le cas de plus de 91 % des entreprises (contre 84 % en 2010). En effet, les moyens de surveillance, analyse et contrôles mis en œuvre par l'entreprise, dans le respect de la législation, sont détaillés dans ce type de document.

Neuf entreprises sur dix la communiquent à l'ensemble des utilisateurs et 56 % la font signer par leurs salariés, ce qui représente une augmentation de 16 points par rapport à 2010.

Pas plus de programmes de sensibilisation…

Les programmes de sensibilisation à la sécurité de l'information sont toujours peu répandus dans les entreprises : près de deux tiers (57 % pas du tout et 8 % en cours) déclarent n'avoir déployé aucune action de communication. Cependant, ici encore, les chiffres montrent que la taille et le secteur d'activité ont un impact sur le niveau de déploiement. Ainsi, 49 % des entreprises de plus de 1 000 personnes en disposent et 45 % des entreprises en Banque/Assurance.

Quant à l'efficacité des programmes de sensibilisation existants, elle n'est mesurée que par 31 % des entreprises. Une complexité fréquemment rencontrée par les RSSI, qui les pénalise dans le lancement de tels projets, tant il est parfois difficile d'en montrer l'efficacité à leur Direction !

… mais plus de moyens quand ils existent !

Les moyens les plus utilisés dans le cadre des programmes de sensibilisation sont inchangés en 2012 : la publication / diffusion d'informations via différents supports (Intranet, mailing, affiches, etc.) et les formations périodiques de tout le personnel sont citées par une entreprise sur deux environ. En revanche, une tendance claire apparaît par rapport à 2010 : les programmes de sensibilisation, quand ils existent, s'étoffent. En effet, le recours aux différents outils est en augmentation dans tous les cas (51 % de

publications vs 19 % en 2010, 44 % de sensibilisation périodique vs 16 %, 26 % de sensibilisation de populations spécifiques vs 16 %).

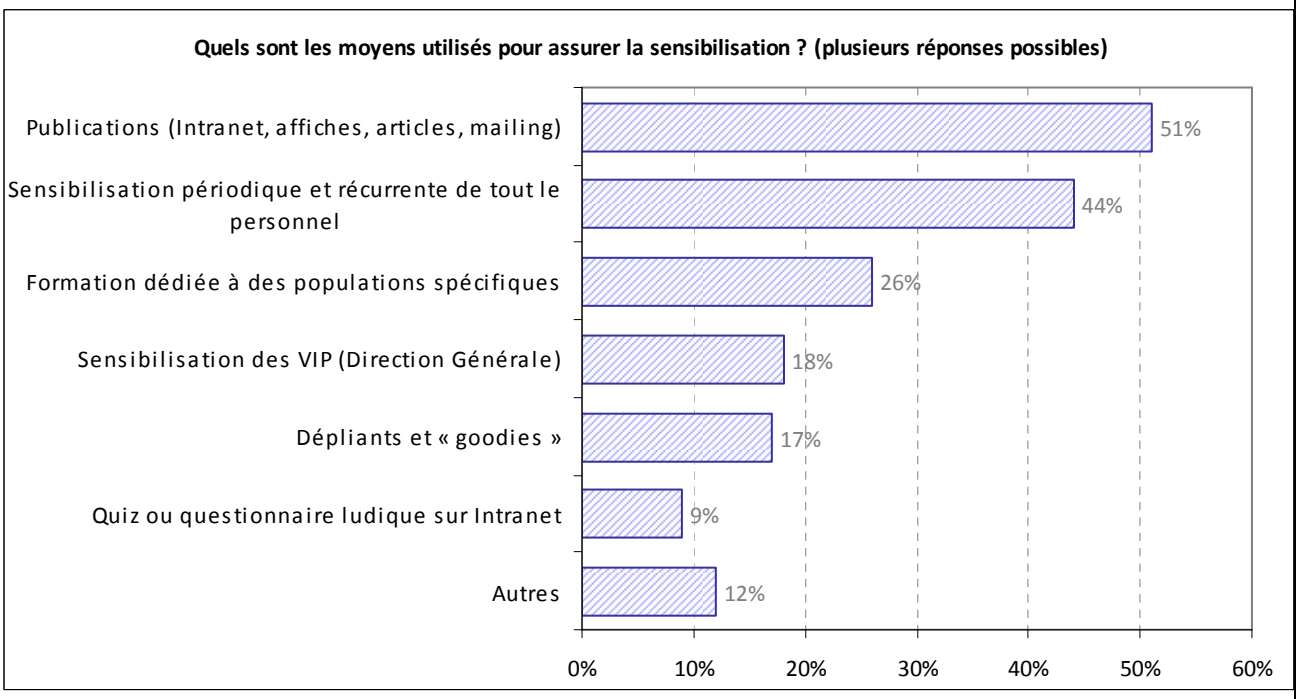

Figure 16 – Moyens de sensibilisation à la sécurité de l'information

Des procédures de gestion des accès liées au mouvement des collaborateurs

78 % des entreprises interrogées déclarent disposer d'une procédure qui fixe les règles de suppression des droits d'accès et de restitution du matériel lors du départ ou de la mutation des collaborateurs.

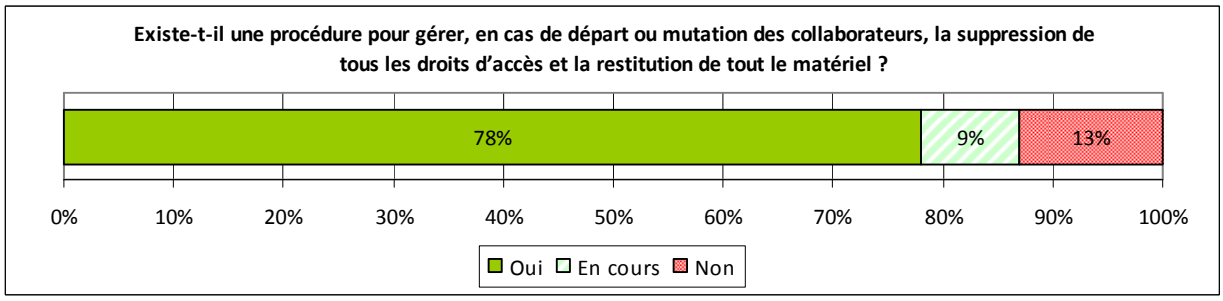

Figure 17 – Existence d'une procédure de suppression des accès et de restitution du matériel

Attention cependant à l'interprétation de ce chiffre : l'existence d'une procédure n'indique pas dans quelle mesure celle-ci est appliquée sachant que l'une des difficultés ici, avant même d'envisager la suppression des droits d'accès, est d'avoir une vue exhaustive sur ceux possédés par un utilisateur. Et c'est bien souvent là que le bât blesse dans le quotidien des entreprises !

Thème 9 : Sécurité Physique

Sécurité physique : peut mieux faire

L'enquête 2012 s'est focalisée, en sécurité physique, sur la prise en compte du cycle de vie des supports papier dans la classification des données.

Qui dans son entreprise n'a jamais trouvé un document sensible oublié au photocopieur, jeté à la poubelle ou laissé sur un bureau accessible à chacun ? Autre exemple, le rapport d'audit confidentiel, chiffré s'il est échangé par messagerie, restreint dans sa diffusion électronique, puis… imprimé pour travailler plus facilement, et finalement, encore, oublié quelque part…

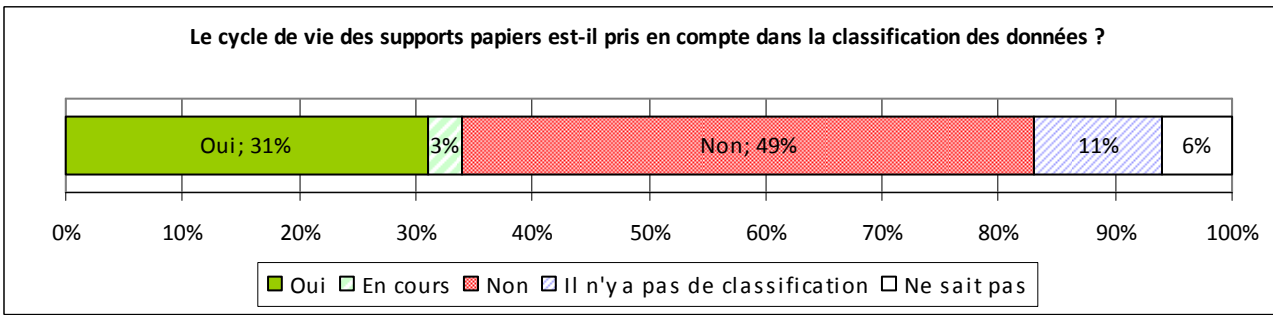

Figure 18 – Prise en compte du cycle de vie des supports papiers dans la classification des données

Les réponses positives recueillies dans ce thème sont cohérentes avec celles de la gestion des biens, pour les entreprises qui ont réalisé une évaluation du besoin de protection.

Pour 49 % des entreprises, avec une pointe à 58 % dans le secteur des Services, ces supports ne sont pas intégrés dans la classification. Le score grimpe à 60 % si l'on ajoute celles qui ne pratiquent pas du tout la classification de leurs données et supports.

On le voit, la route est encore longue dans la mise en œuvre, et surtout le contrôle, de bonnes pratiques qui doivent être rappelées régulièrement aux salariés, surtout si les informations manipulées sont sensibles : documents sous clé ou bureau fermé, même pour une courte absence, indication sur chaque document du niveau de sensibilité et/ou de diffusion, utilisation de broyeurs papiers pour la destruction.

Thème 10 : Gestion des opérations et des communications

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

L'évolution de nouvelles technologies connectées au SI se stabilise, il y a peu d'innovations (accès distant, wifi, smartphones, VoIP). Cependant, l'adoption de ces moyens de communication continue d'évoluer.

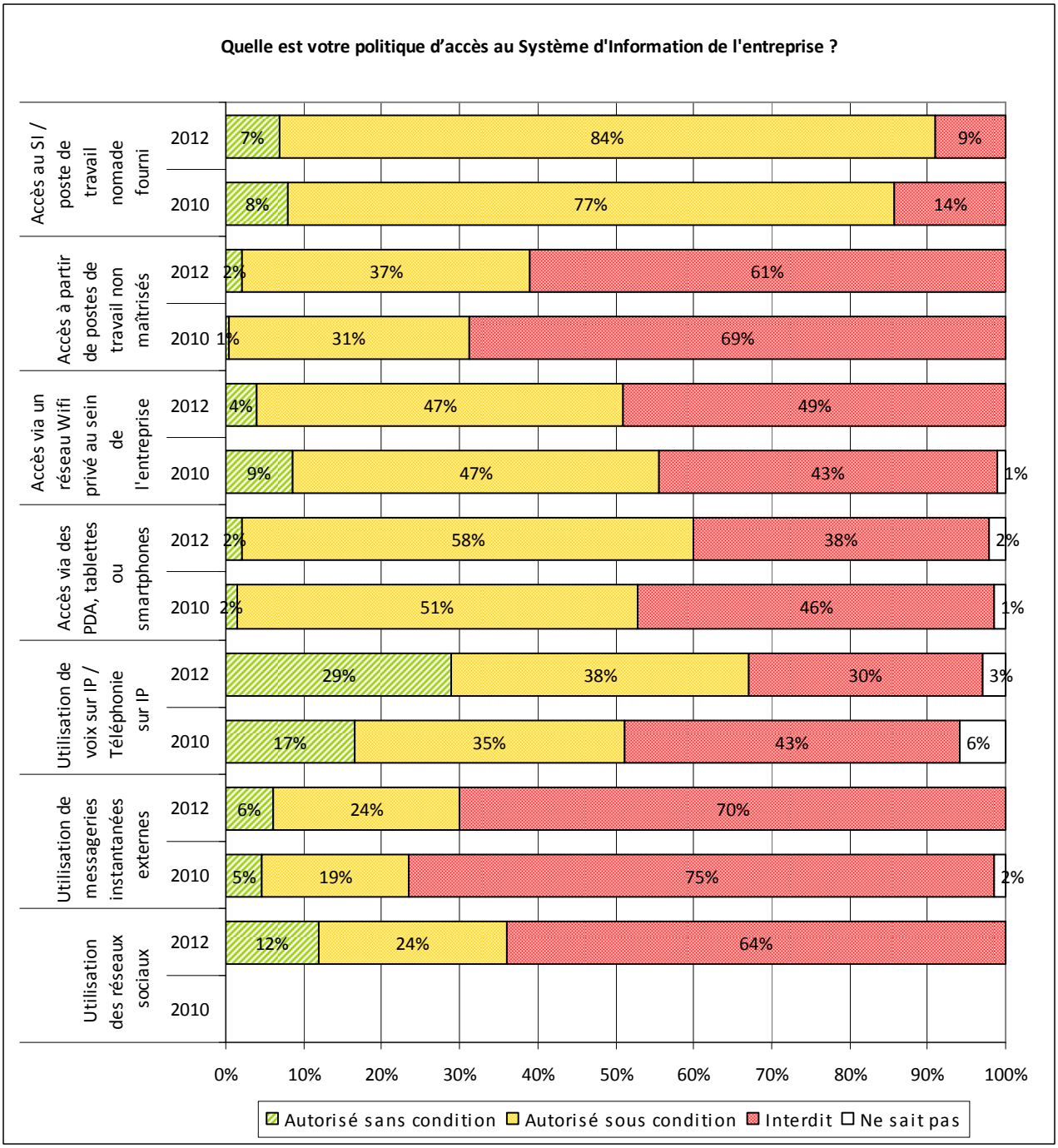

Figure 19 – Accès au Système d'Information de l'entreprise

Un accroissement du nomadisme

L'accès nomade aux ressources de l'entreprise est de plus en plus généralisé. La maturité des solutions technologiques de connexion, de contrôle des postes nomades et des informations qui transitent permettent un meilleur contrôle des risques associés. C'est également vrai pour l'accès au SI depuis un poste de travail non maîtrisé (accès publique, ordinateur personnel) qui est de plus en plus autorisé.

Cependant, les informations accessibles par cette méthode sont, en général, plus limitées, les vulnérabilités et menaces engendrées par ce type d'accès étant plus difficiles à maîtriser.

L'utilisation du wifi privé en entreprise diminue. L'explication peut se trouver dans les faiblesses démontrées des différentes solutions de sécurisation standard du wifi ces dernières années.

Les PDA, tablettes et smartphones 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. Ils doivent être considérés comme un moyen à part entière d'accès aux ressources du SI, au même titre que les ordinateurs portables. Les applications accédées sont cependant plus limitées : accès aux mails, à l'annuaire d'entreprise. Les menaces identifiées sont identiques à celles de 2010 : politique de PIN ou mot de passe faible, vol ou perte d'informations confidentielles, installation d'applications comportant du code malveillant, etc.

Le déploiement de la VoIP toujours en hausse.

La maturité et la diversité des solutions proposées aujourd'hui sur le marché font de la VoIP et ToIP des technologies incontournables de l'entreprise. De plus, leur déploiement continue de constituer dans l'esprit des entreprises une source d'économie importante, notamment dans le cas de grandes entreprises réparties sur plusieurs continents ou pour des utilisateurs nomades. On observe donc une progression significative de la prise en compte de ces technologies dans la politique de sécurité.

La messagerie instantanée et des réseaux sociaux peu autorisés.

L'utilisation de la messagerie instantanée non fournie par l'entreprise (MSN, Skype, etc.) et des réseaux sociaux est aujourd'hui majoritairement interdite par les politiques de sécurité. Les problématiques de sécurités liées à ces technologies sont nombreuses : confidentialité, chiffrement des échanges, journalisation des conversations, transmission des virus, fuite d'information. Bien que les menaces puissent être contrôlées par des dispositifs de sécurité de dernière génération (filtrage protocolaire, antivirus, DLP, etc.) elles sont souvent identifiées comme étant à l'origine du manque de productivité des utilisateurs.

❖ Technologies de protection et de gestion des vulnérabilités

Cette année, le choix a été fait de ne pas positionner les firewalls réseaux : en effet, les études précédentes montrent une mise en place systématique. De même, les antivirus/antispywares, les pare-feu personnels et les outils de chiffrement des données locales ont été découpés en 2 catégories : une pour les PC portables et l'autre pour les PDA, smartphones et tablettes.

De fait, cette seconde catégorie est aujourd'hui « mal » servie, bien que les PDA, smartphones et tablettes soit de plus en plus présents, et ce directement via l'entreprise ou amené par les utilisateurs eux-mêmes, au travers du BYOD…

Côté sécurité réseau, les IDS et IPS ont vu leur usage croître de 35 % et 50 % (+16 points pour les IDS et +19 points pour les IPS) depuis la dernière étude, portant le taux d'équipement des entreprises à respectivement 62 % et 56 %. Ces équipements permettant de détecter et de bloquer les attaques (des vers par exemple) en écoutant le réseau peuvent être de très bons compléments à un firewall de périmètre.

Toujours sur le réseau, le NAC (Network Access Control) qui existe depuis quelques années progresse lentement (6 points de mieux depuis 2010). Il faut dire que si la fonction apportée (contrôler l'accès « physique » au réseau) est très intéressante dans le contexte de la sécurité périmétrique, la mise en place reste délicate.

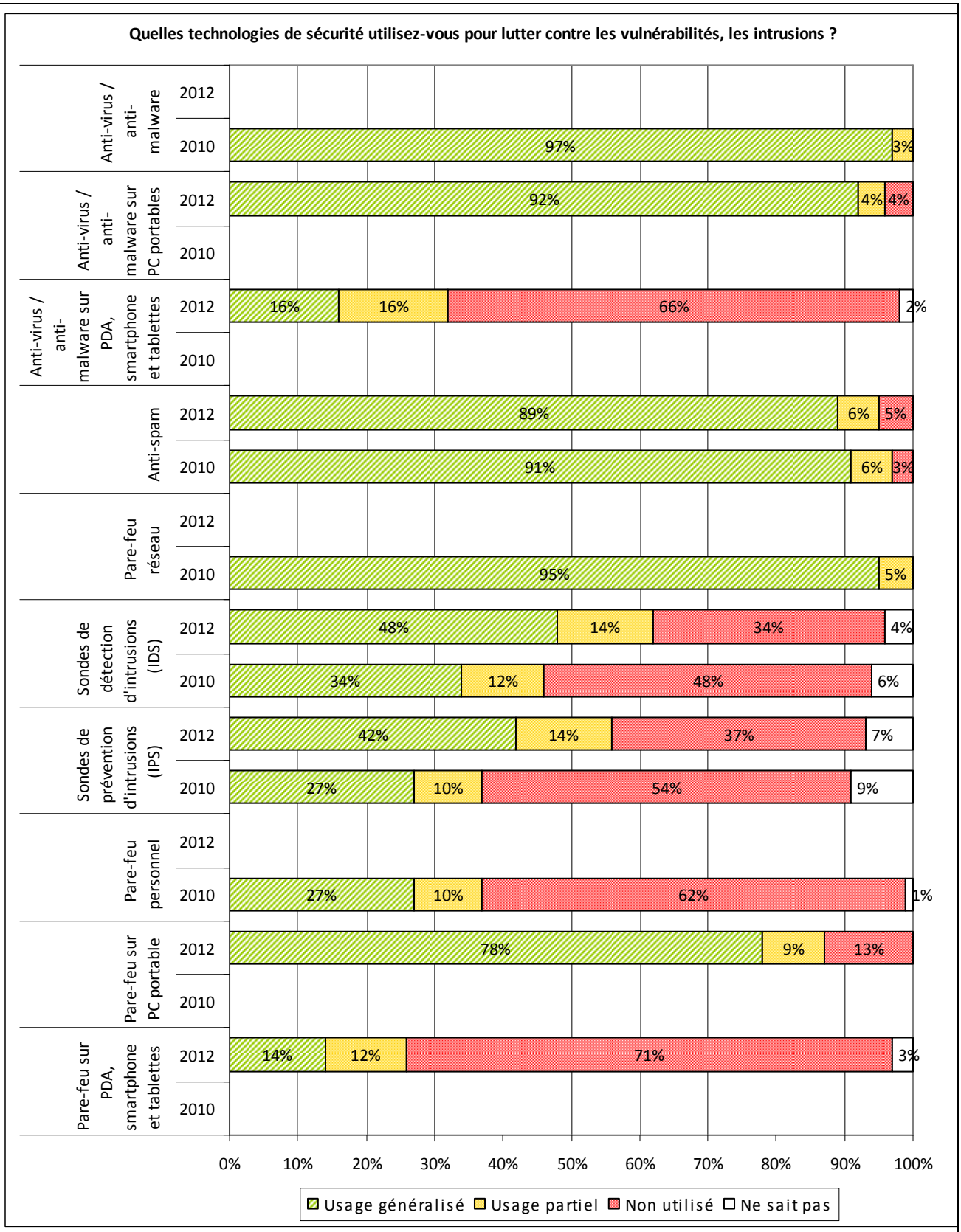

Figure 20 - Technologies de sécurité / lutte antivirale, anti-intrusion, gestion des vulnérabilités (1/2)

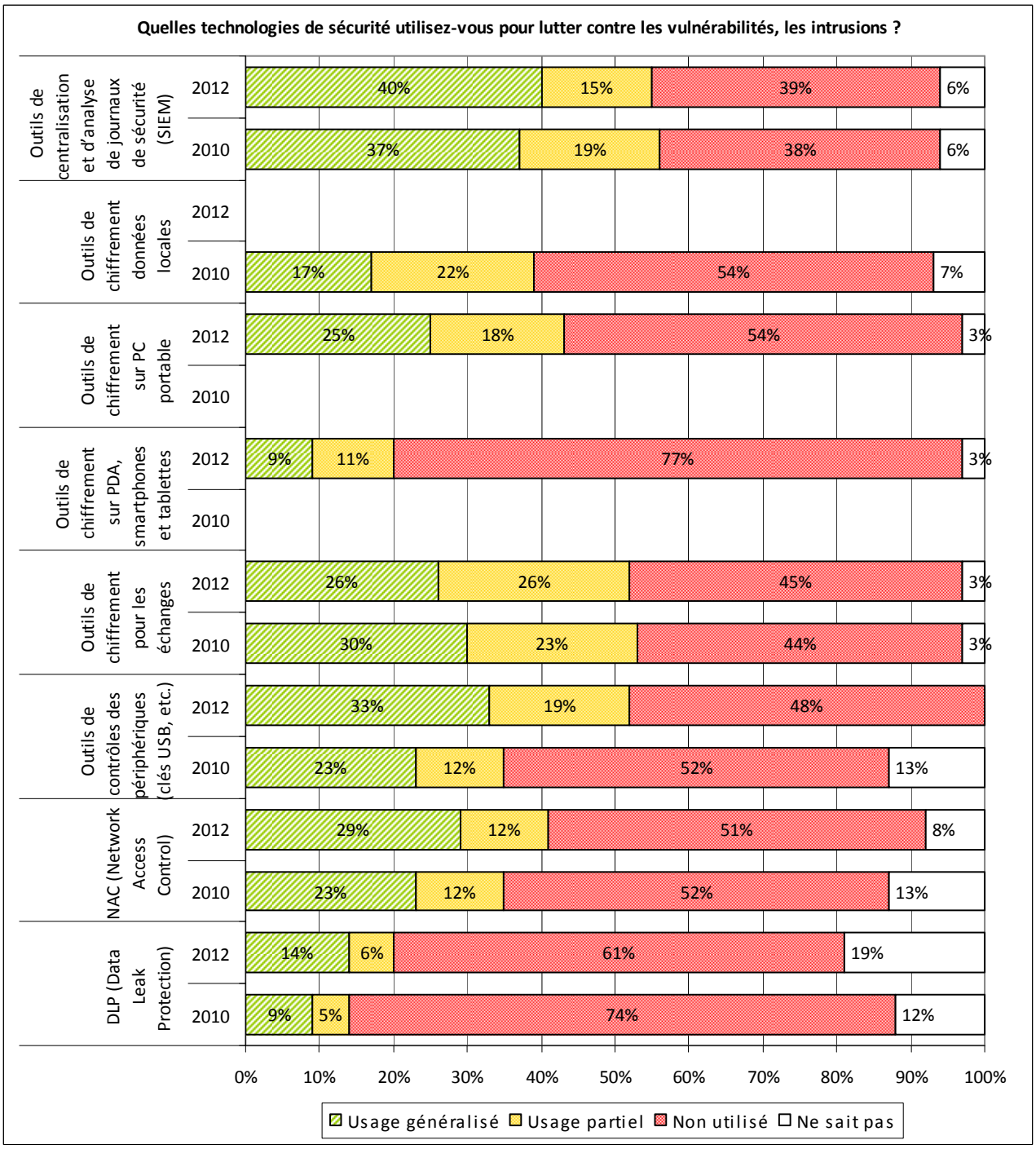

Figure 21 - Technologies de sécurité / lutte antivirale, anti-intrusion, gestion des vulnérabilités (2/2)

Les SIEM (Security Information and Event Management) permettent de savoir ce qui se passe sur le réseau de l'entreprise en rationalisant les journaux d'un grand nombre d'équipements. Ils correspondent donc à un besoin de contrôle *a posteriori*, qui peut répondre à une problématique juridique, technique, de supervision (alertes) ou de planification (par le biais des rapports à long terme). Les SIEM restent des produits difficiles à mettre en place et on voit que, malgré l'intérêt des ces technologies, le taux d'équipement tend à n'augmenter que très peu pour atteindre 55 % des entreprises dont 15 % l'ayant déployé sur un périmètre restreint.

Le contrôle des périphériques permet de limiter à la fois les risques d'infection virale (par clé USB par exemple) et les fuites de données. Ces solutions restent problématiques à mettre en place du fait de la limitation fonctionnelle qu'elles imposent car l'usage des périphériques amovibles fait aujourd'hui partie intégrante de la façon de travailler dans de nombreuses organisations. Le taux d'équipement constaté

montre d'ailleurs une relative stagnation avec une légère augmentation du total d'entreprises équipées (50 %) mais une baisse de celles en faisant un usage généralisé (33 % contre 37 % lors de la dernière étude).

Dernière technologie sur le marché, le DLP (Data Leak Protection) est conçu pour contrôler le flux de données aux frontières de l'entreprise et, plus précisément, se prémunir contre la fuite d'informations. Le niveau d'équipement reste encore faible (20 %, +6 points par rapport à 2010), mais il faut dire que la technologie est encore récente et que les produits adressant l'ensemble des portes de sortie du périmètre de l'entreprise (passerelles mail et Web, postes de travail, supports amovibles, etc.) sont encore rares.

❖ Infogérance

Il semble que les entreprises soient encore frileuses à l'idée de déléguer la gestion d'une partie de leur SI à une autre société. Entre 2010 et 2012, la part d'externalisation des SI des entreprises n'a pas beaucoup progressé, passant de 10 % à 12 %.

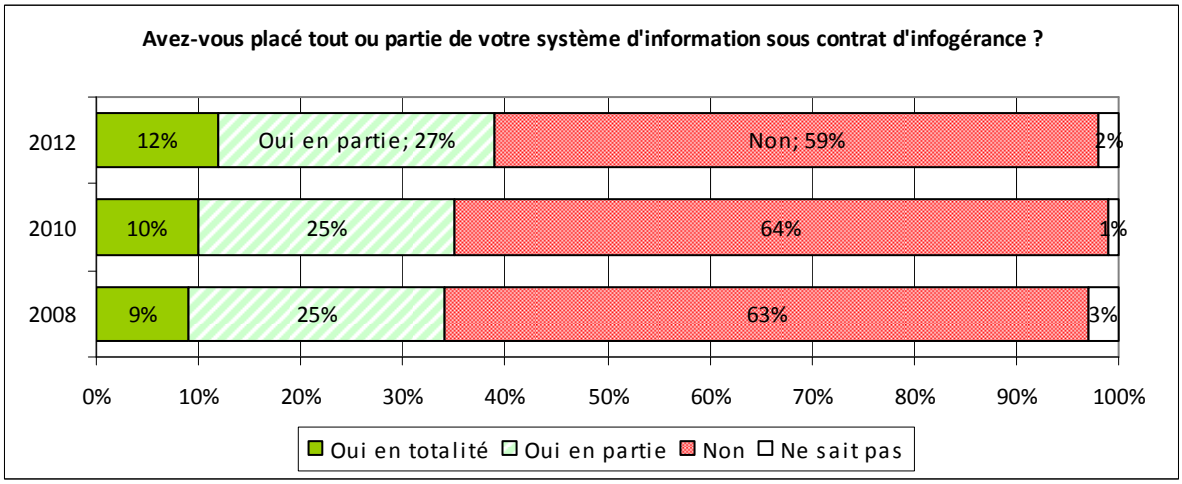

Figure 22 – Part des SI sous contrat d'infogérance

Parmi les entreprises qui ont externalisé tout ou partie de leur SI, le suivi par des indicateurs de sécurité n'a pas progressé non plus, pire, il a régressé (59 % vs 66 % en 2010). Même constat pour les audits des SI infogérés : on passe de 28 % en 2010 à 31 % seulement en 2012.

Cela pourrait-il s'expliquer par les renouvellements de contrats pour les mêmes prestataires, en qui les entreprises ont déjà confiance ou serait-ce plus simplement lié à des problèmes de budgets ?

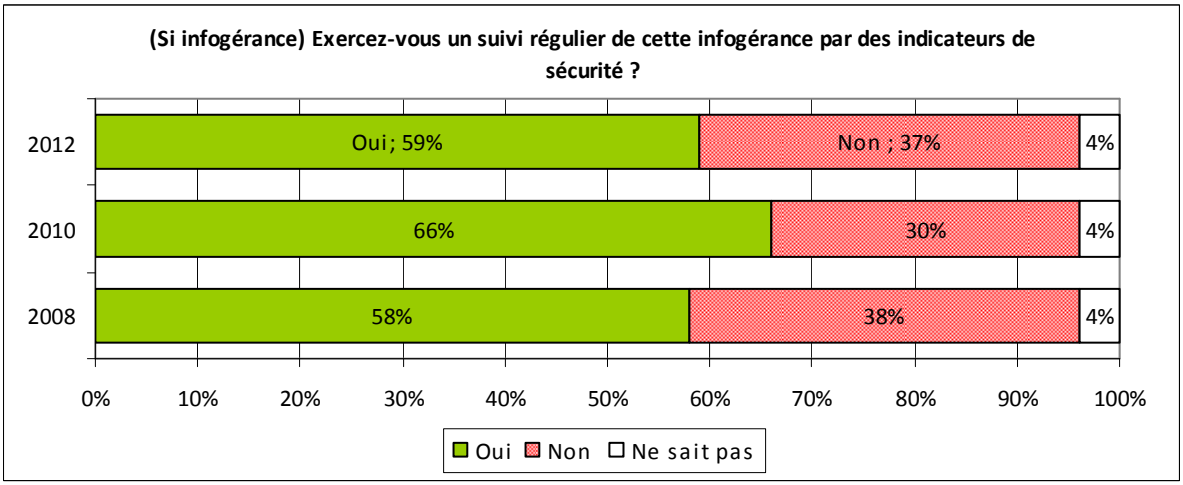

Figure 23 - Suivi de l'infogérance par des indicateurs de sécurité

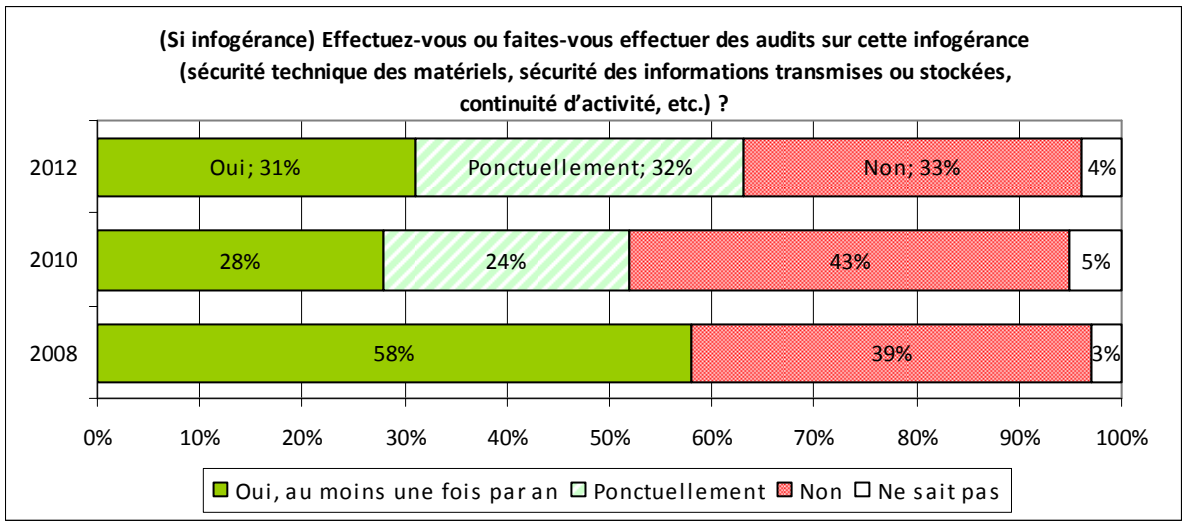

Figure 24 – Réalisation d'audit sur l'infogérance

Il semble que le Cloud Computing (informatique dans les nuages) ne soit pas encore un service très demandé : seules 14 % des entreprises l'utilisent. Il s'agit pour 66 % d'entre eux de Clouds privés, 20 % sont des Clouds publics et le reste sont hybrides.

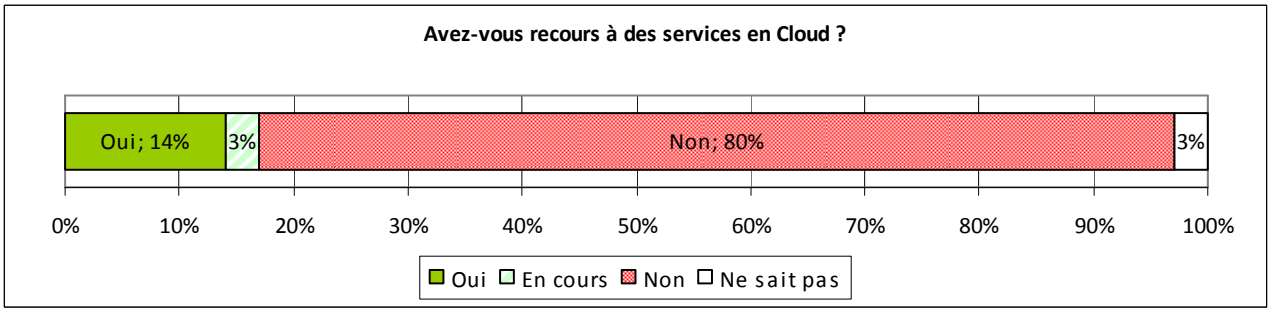

Figure 25 – Part du SI dans le Cloud Computing

La problématique de la sécurité des données (pas de contrôle direct et permanent sur le lieu physique d'hébergement, pas toujours de visibilité sur l'application des procédures de sécurité de l'entreprise, etc.) et des lois et réglementations (CNIL, RGS, etc.), sont aujourd'hui parmi les freins les plus présents quant à une utilisation du Cloud Computing plus élargie.

Thème 11 : Contrôle des accès logiques

Les moyens nécessaires aux contrôles d'accès pas encore au rendez-vous…

L'augmentation globale en matière d'utilisation et de gestion des technologies de contrôle d'accès en 2012 représente à peine 2 points de plus qu'en 2010.

La volonté de promouvoir les solutions SSO et Web SSO fait son chemin. De plus en plus de nouvelles solutions sont mises à disposition des entreprises et le marché est maintenant mature ; pourtant les implémentations ne sont pas encore au rendez-vous.

Les tendances de l'usage généralisé des technologies de contrôle d'accès logique pour 2012 sont présentées dans le tableau suivant.

Technologies de contrôle d'accès logique	Observations	Tendance 2012 vs 2010	
Le Provisionning (création / suppression automatique des comptes et droits)	Peu de confiance dans l'automatisation de la gestion des comptes	+1 pt	↗
Les Workflows d'approbation des habilitations	Pas de déploiement massif par les entreprises, difficulté d'harmoniser les modèles d'habilitation	+3 pt	↗
Les Modèles d'habilitation sur base de profils / rôle métier	La maîtrise des droits par rôle ou par profil métier est complexe à appliquer dans un schéma global d'habilitation car la dynamique actuelle des entreprises rend difficile une gestion centralisée de ces modèles	-1 pt	↘
Le Web SSO	La maturité et l'évolution des solutions commencent à mettre en confiance les entreprises	+3 pt	↗
Le SSO (Single Sign On)	Les solutions SSO intégrées aux applications déjà en place ne progressent plus, l'évolution va vers le Web SSO	-4 pt	↘
La Biométrie	Bien que les nouvelles technologies nous apportent plus de robustesse et de traçabilité pour le contrôle d'accès, une léthargie s'est instaurée dans les entreprises	0	↔
L'authentification par certificat électronique logiciel	Une progression notable montre l'intérêt d'utilisation des PKI ou IGC (Public Key Infrastructure ou Infrastructure de Gestion de Clés publiques) pour les applications en accès Web sécurisés	+7 pt	↗
L'authentification forte par certificat électronique sur support matériel (carte à puce ou clé à puce)	L'usage des supports matériels (clés USB, cartes à puce) est en augmentation, l'aspect pratique s'adapte parfaitement à une évolution de plus en plus présente vers le nomadisme	+4 pt	↗
L'authentification forte par calculette à mot de passe non rejouable	L'apport des technologies et des facilités de déploiement rendent la fonction OTP (One Time Password – mot de passe à usage unique) plus accessible pour les entreprises	+4 pt	↗

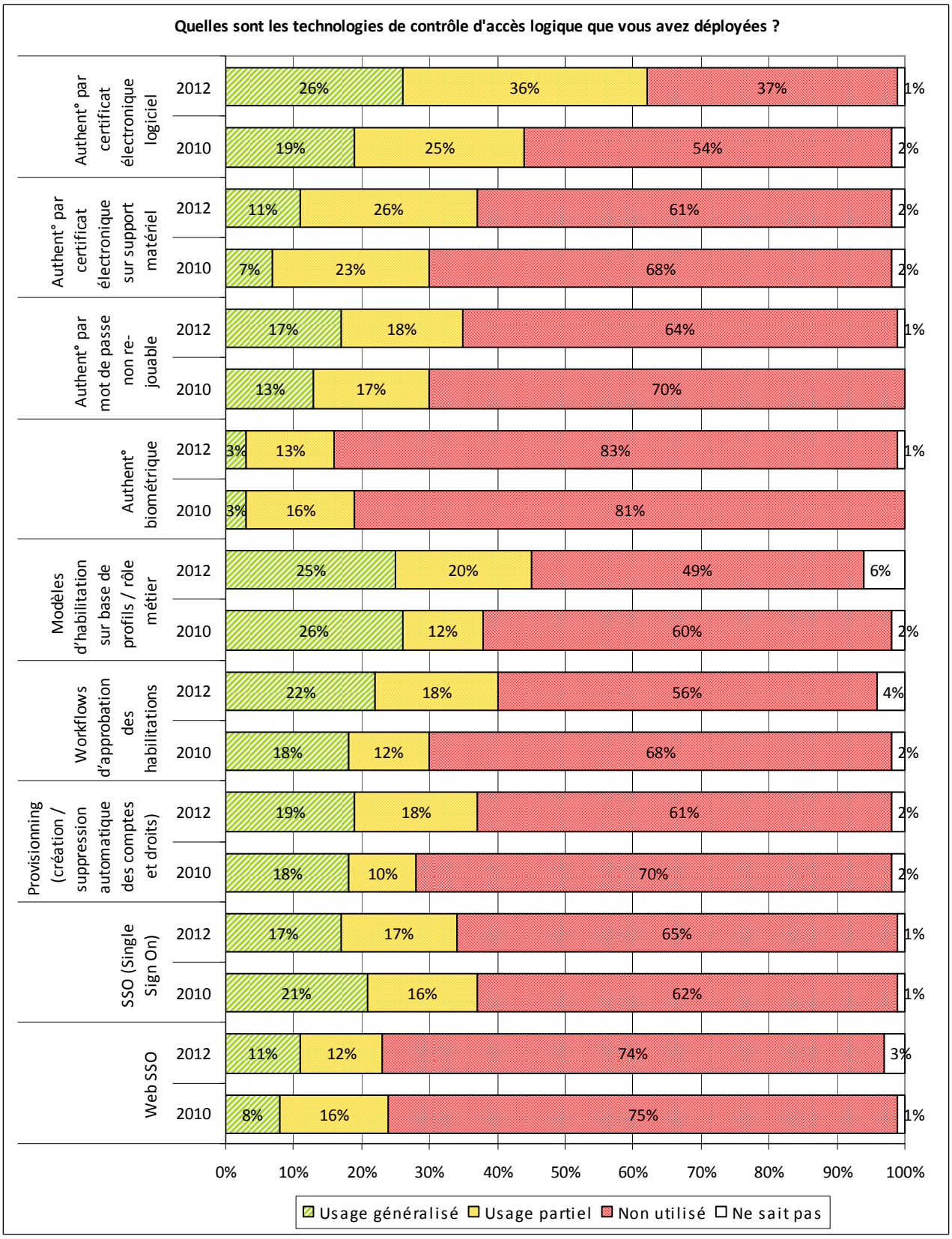

Figure 26 - Technologies de contrôle d'accès logique déployées en entreprise

…mais une gestion des comptes qui s'améliore nettement !

Les entreprises mettent en œuvre une véritable gestion des comptes utilisateurs à 64 %, au travers de procédures formelles de création, modification et suppression de comptes utilisateurs nominatifs. Ce chiffre monte même à 75 % dans la Banque/Assurance, preuve s'il en est de la maturité de ce secteur.

Toutefois, lorsque cette procédure existe, elle ne concerne pas les « administrateurs » dans 20 % des cas.

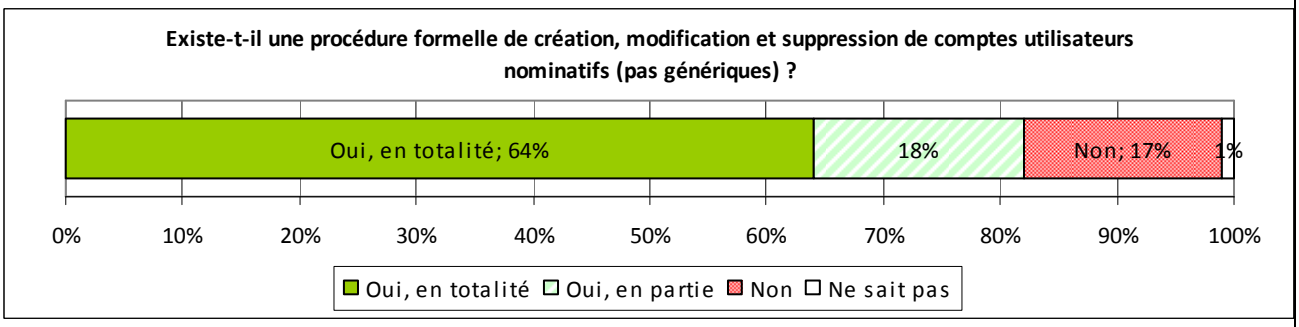

Figure 27 – Mise en place de procédures de gestion des comptes utilisateurs

Enfin, la mise en place de règles de constitution et de péremption des mots de passe régresse légèrement (80 % vs 82 % en 2010). Ici aussi, le bon élève est la Banque/Assurance, avec 93 %.

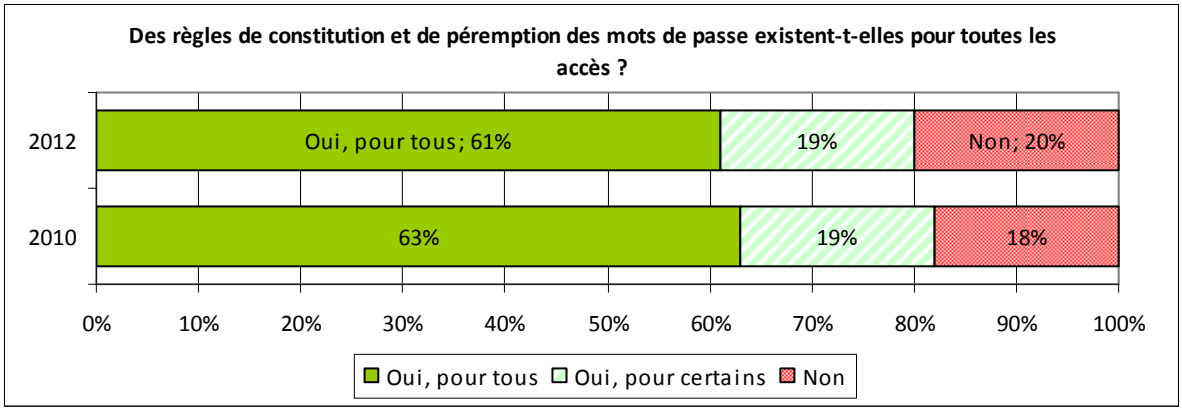

Figure 28 – Mise en place de règles de constitution et de péremption des mots de passe

Thème 12 : Acquisition, développement et maintenance

Veille et patch management en régression !…

Les applications, qu'elles soient directement développées en interne ou via des prestataires, voire acquises « sur étagère » (progiciels) se doivent d'être régulièrement surveillées du point de vue de 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, bien que n'évoluant pas ou peu dans les pratiques. Il reste quand même un bon tiers des entreprises qui n'assure aucune veille !

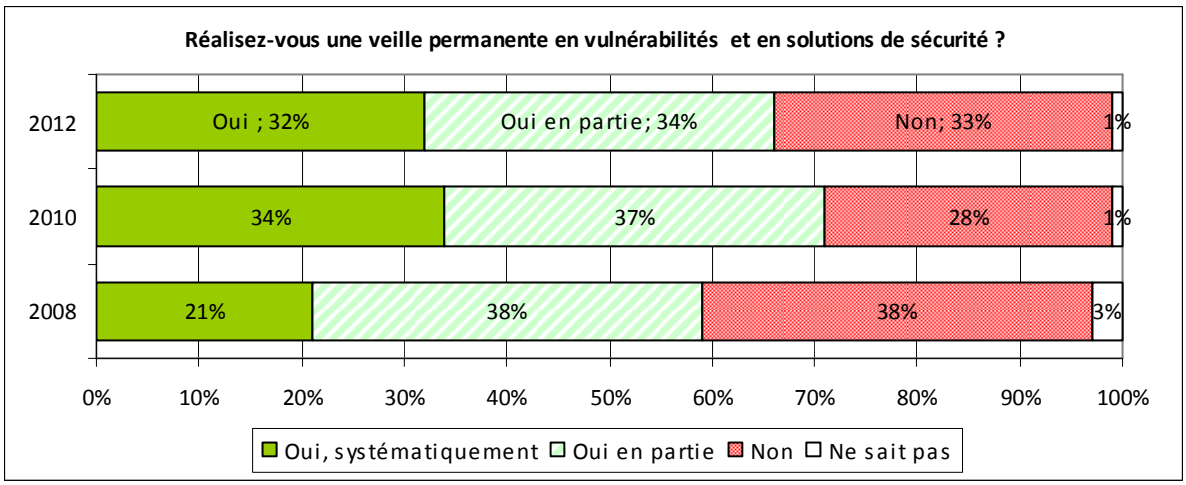

Figure 29 – Veille en vulnérabilités et en solutions de sécurité

De même, après plusieurs années d'augmentation régulière, la formalisation des procédures opérationnelles de mise à jour est, en 2012, en régression.

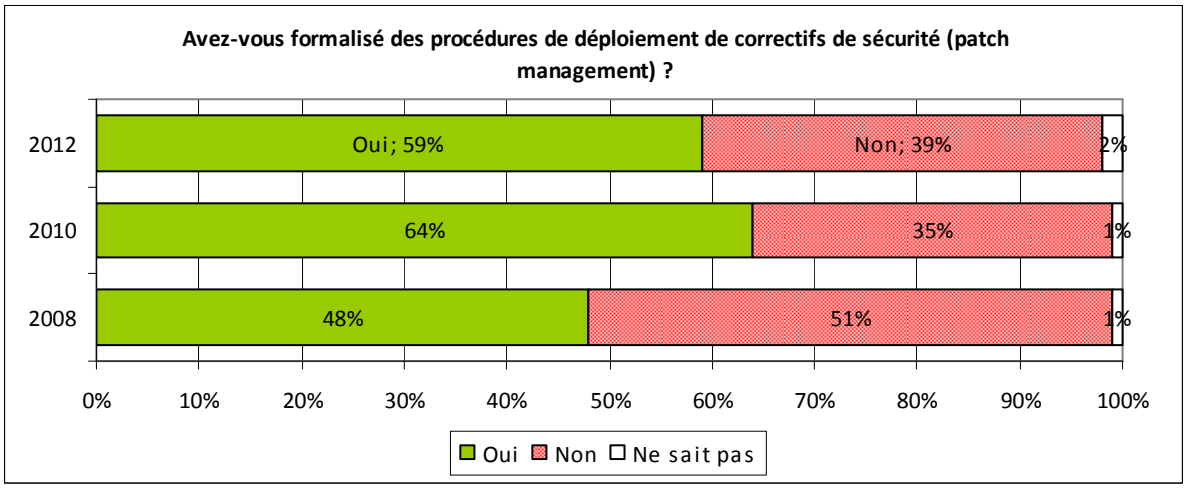

Figure 30 - Formalisation des procédures de déploiement de correctifs de sécurité

Par ailleurs, le délai nécessaire pour déployer les correctifs en cas de menace grave reste majoritairement « dans la journée » (58 %, +3 points vs 2010), puis 'dans l'heure' (21 %, -3 points vs 2010).

Concernant les développements, peu de sociétés (20 %, idem 2010) déclarent mettre en œuvre des cycles de développements sécurisés. Parmi les entreprises ayant mis en place un cycle sécurisé, 43 % utilisent SDLC (+3 % vs 2010), 41 % appliquent des « bonnes pratiques pragmatiques », le reste se répartit sur diverses méthodes « formelles » (INCAS, OWASP CLASP, Cigital DSL, etc.).

Thème 13 : Gestion des incidents – Sinistralité

Pas de réel progrès dans la gestion des incidents de sécurité…

Ces deux dernières années marquent un palier dans la gestion des incidents de sécurité par les entreprises. En 2012, 53 % (+1 point vs 2010) d'entre elles ont une cellule (dédiée ou partagée) à la gestion de ces incidents de sécurité.

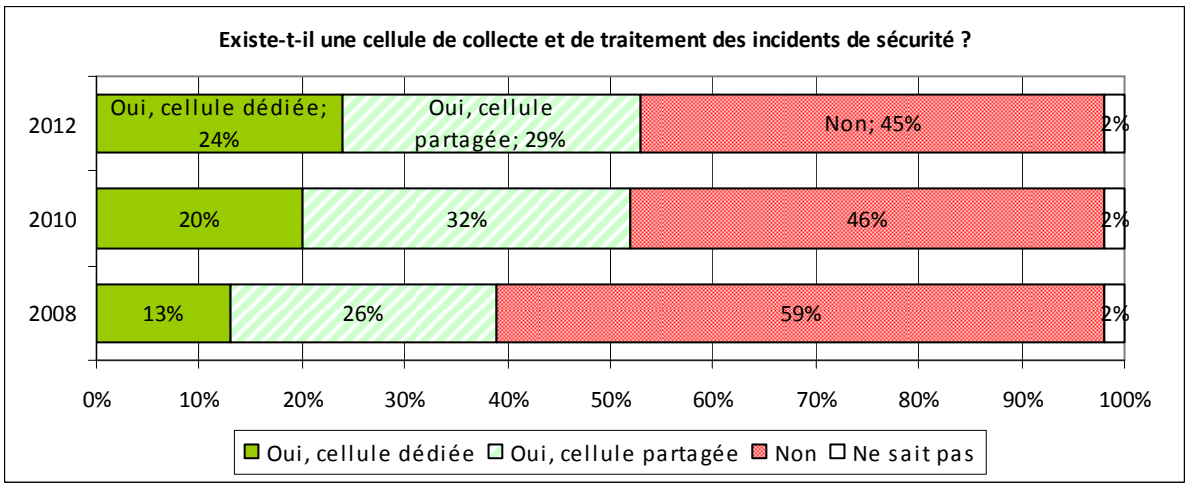

Figure 31 – Existence d'une cellule de collecte et de traitement des incidents de sécurité

On note toutefois une progression, inégale selon les secteurs, du nombre de cellules dédiées (24 % en 2012, +4 points vs 2010).

… et toujours aussi peu de dépôts de plaintes !

Une toujours (très) faible proportion d'entreprises se tourne vers le dépôt de plainte (6 %, -1 point vs 2010). En effet, rien n'oblige aujourd'hui une entreprise à déposer plainte suite à un incident de sécurité et, d'autre part, celui-ci comporte un risque d'atteinte à l'image.

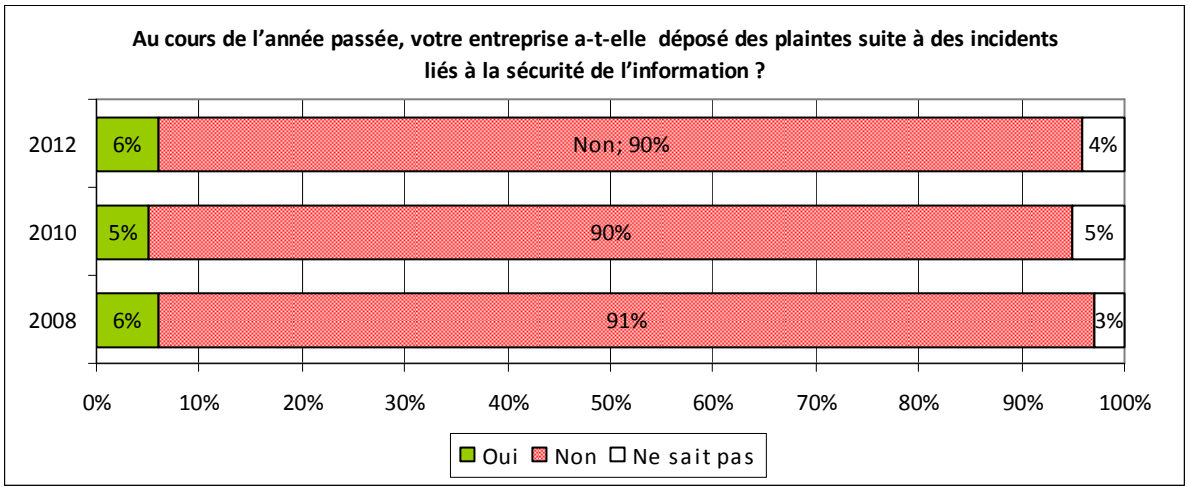

Figure 32 – Dépôts de plaintes suite à des incidents liés à la sécurité de l'information

Une perception manifestement différente des incidents rencontrés

Les types d'incidents rencontrés par les entreprises connaissent des taux beaucoup plus faibles que les années précédentes. Il est vraisemblable que leur perception ait évolué sur ces sujets (bien que leur organisation dans la gestion des incidents n'ait pas beaucoup changé). L'ordre d'importance des différentes catégories d'incidents a ainsi peu évolué, même si on note une forte baisse des erreurs d'utilisation (17 %, -29 points soit -63 % vs 2010) proportionnellement aux autres catégories.

Les infections par virus restent toujours la première source d'incidents d'origine malveillante pour les entreprises (13,7 incidents de sécurité dû à des virus), loin devant les vols ou disparition de matériel (3,7).

Du côté des incidents d'origine non malveillante, on retrouve les erreurs d'utilisation (7,1), suivies des erreurs de conception (5,9).

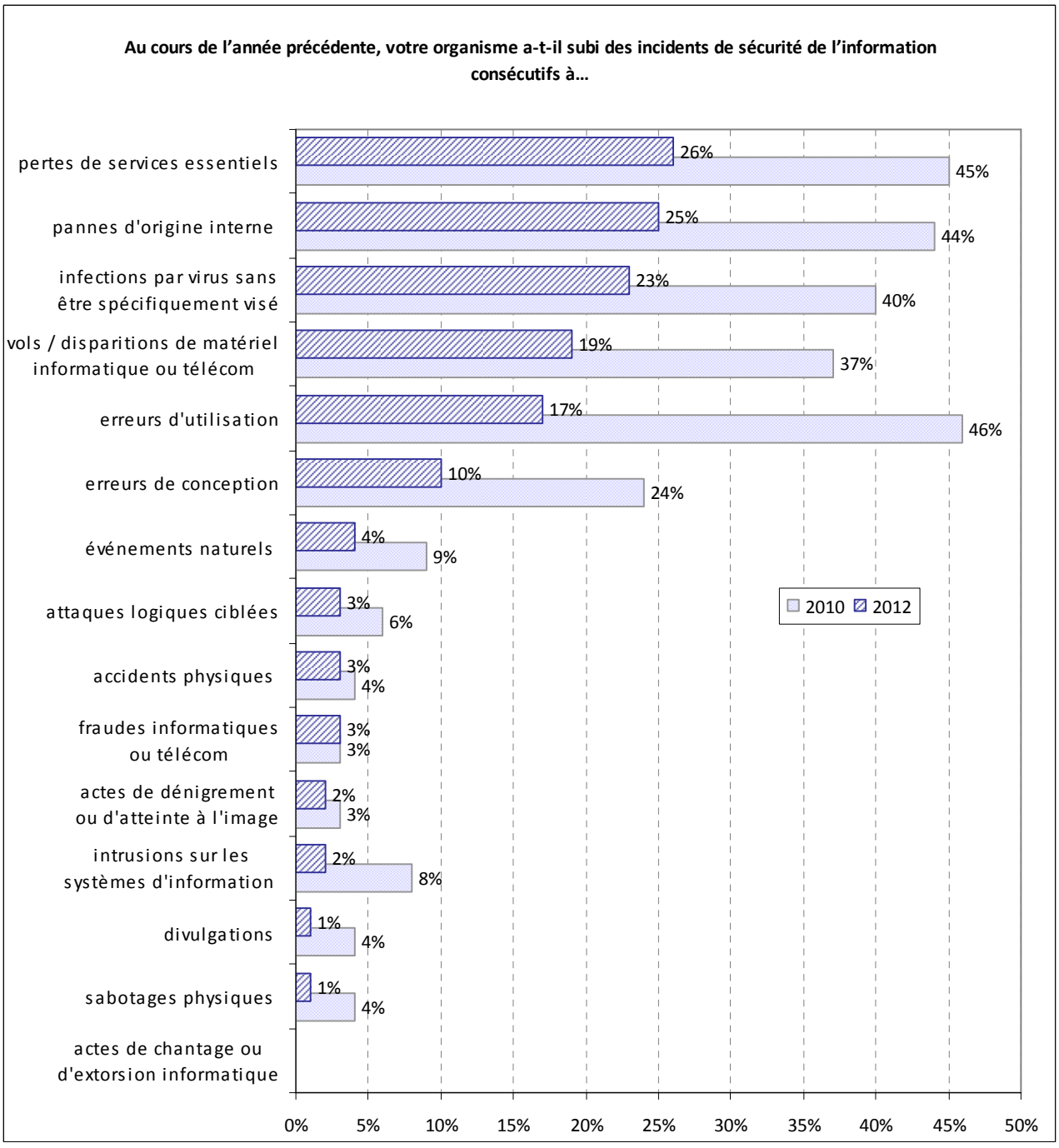

Figure 33 - Typologie des incidents de sécurité

Un impact financier toujours peu pris en compte

Enfin, l'impact financier des incidents est toujours aussi peu souvent évalué : 14 % (-2 points vs 2010) l'évaluent « systématiquement » et 25 % (idem 2010) « parfois ». Si l'on enlève les 5 % qui « ne savent pas », il reste donc 55 % des entreprises qui n'évaluent jamais cet impact.

Les RSSI devraient y réfléchir, afin de les aider dans la capacité à « vendre » la SSI à leurs Directions Générales.

Thème 14 : Gestion de la continuité d'activité

Intérêt pour les scénarii d'indisponibilité de leurs fournisseurs essentiels

Un peu moins d'un tiers des entreprises ne prennent pas en compte la continuité d'activité. Ceci reste relativement stable au regard des résultats de l'étude réalisée en 2010.

Sans surprise, l'indisponibilité des « systèmes informatiques » représente le scénario le plus couvert (59 %). Il est intéressant de noter que moins d'une entreprise sur deux prend en considération le scénario d'indisponibilité de ses locaux pourtant jugé comme un scénario traditionnel.

Cette année, notre enquête s'intéresse à l'indisponibilité des collaborateurs. 38 % couvrent ce scénario (grippe, grève, etc.) et démontrent une prise de conscience qui sera à suivre dans les prochaines années.

L'indisponibilité d'un fournisseur essentiel est aussi une nouveauté de cette étude. Il fait apparaitre qu'un quart des interviewés prend en compte désormais ce scénario. Il semble donc que les entreprises commencent à contrôler que leurs prestataires jugés « essentiels » disposent eux-mêmes de processus de continuité d'activité.

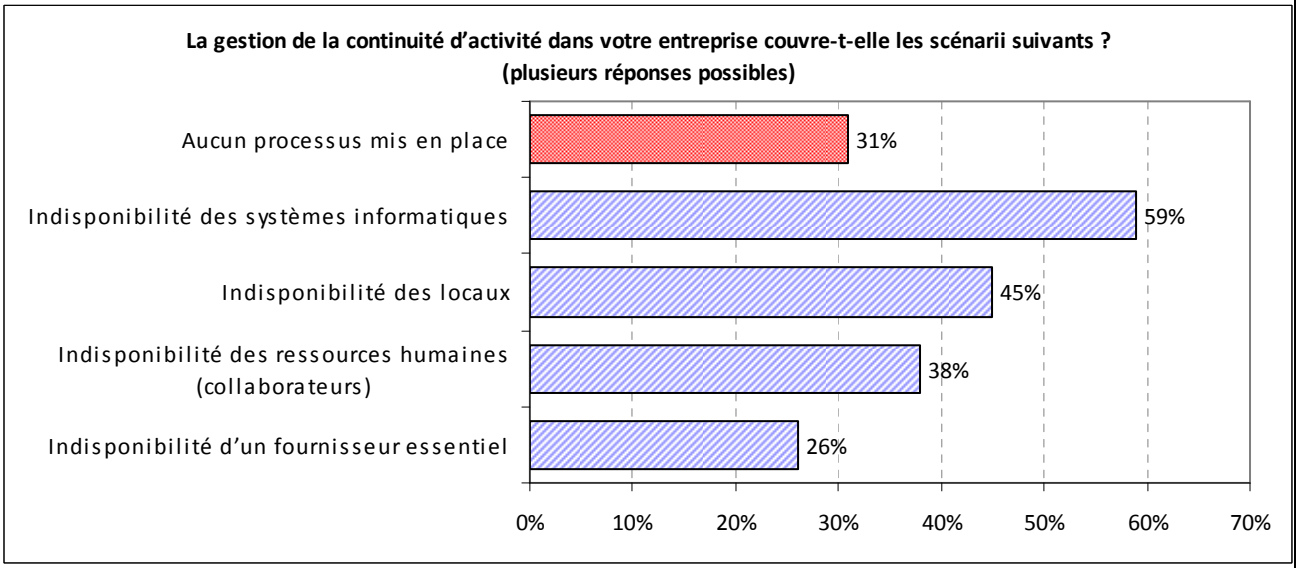

Figure 34 - Scénarii couverts par la gestion de la continuité d'activité

Forte progression de la prise en compte des exigences métiers

La question formulée dans l'étude 2012 sur l'évaluation des exigences métiers des entreprises dans le cadre d'un BIA (Bilan d'Impact sur l'Activité) présente des résultats en forte hausse par rapport aux résultats de 2010. En effet, on note une forte progression de 23 à 52 % des entreprises qui ont évalué leurs exigences métiers (les 52 % incluant les 9 % de celles qui affirment être en train de le faire).

Les résultats présentés semblent plus cohérents que ceux de 2010 au regard des scénarios de couvertures et prouvent que les entreprises commencent à adresser la gestion de la continuité d'activité avec l'aide d'un BIA.

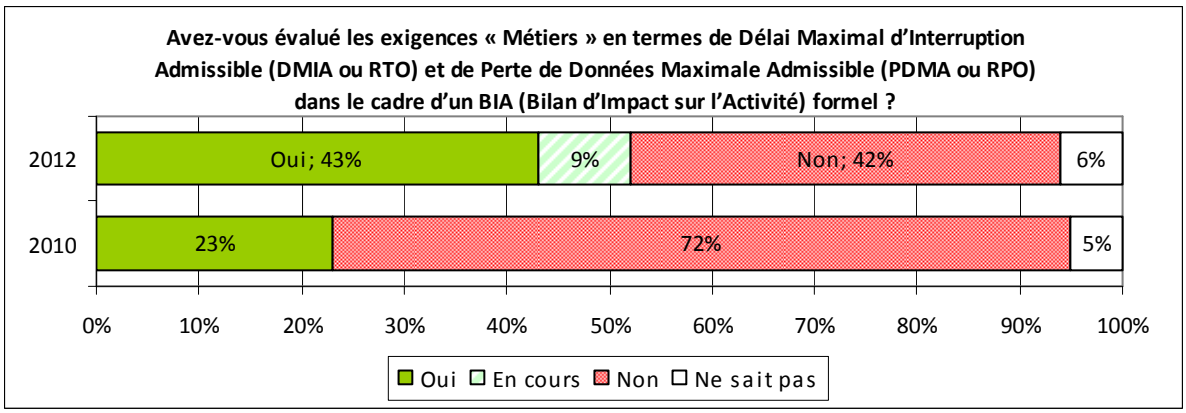

Figure 35 - Réalisation d'un BIA formel pour évaluer les impacts « Métiers »

Une insuffisance au niveau des tests qui perdure ….

La dissociation effectuée volontairement cette année entre Tests Utilisateur et Tests Informatique montre des résultats sensiblement équivalents.

Il subsiste encore 12 % de personnes qui ne savent pas répondre à la question sur le test utilisateur. Plus surprenant, 9 % ne savent pas non plus répondre sur le volet informatique.

Près de 40 % des entreprises ne testent jamais ou moins d'une fois par an leur PCA que ce soit sur le volet Utilisateur ou celui de l'Informatique.

Or, un PCA non testé (ou insuffisamment testé) donne l'illusion d'une couverture mais en cas d'activation, il aura peu de chance d'atteindre les objectifs fixés.

Seulement 11 % des entreprises effectuent des tests plusieurs fois chaque année. Espérons que dans les années à venir ce dernier pourcentage évoluera à la hausse. Rappelons en effet que seuls les tests permettent de s'assurer que les processus de continuité d'activité mis en place sont opérationnels.

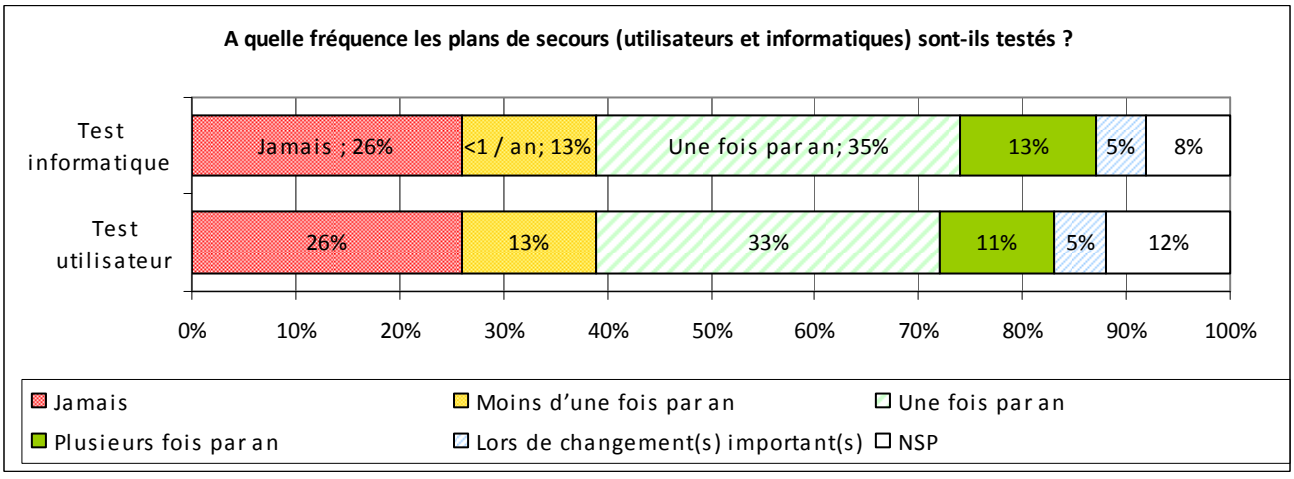

Figure 36 - Fréquence des tests de secours

Encore des efforts à faire en gestion de crise

Près de la moitié des entreprises (46 %) n'ont pas de processus formalisé de gestion de crise ! 42 % considèrent disposer d'une cellule de crise opérationnelle (CCO) et seulement 38 % d'entre elles d'une cellule de crise décisionnelle (CCD). Le répondant a-t-il bien interprété la différence entre ces deux cellules bien distinctes l'une de l'autre ?

Pour rappel : la CCO fait l'état des lieux, active, coordonne, contrôle la bonne exécution des tâches du PCA, centralise les informations, analyse et traite les imprévus, réalise les synthèses d'avancement et

recommandations d'ajustements stratégiques à destination de la CCD. Celle-ci, quant à elle, gère l'arbitrage des décisions stratégiques, la gestion des imprévus et la coordination de la communication.

L'autre point surprenant des réponses concerne le faible équipement en salle de gestion de crise comme en processus d'escalade (outils). Dans les années à venir, les entreprises vont devoir prendre conscience de la nécessité de disposer d'une gestion de crise et, de plus, de s'équiper de moyens afférents pour une meilleure efficacité.

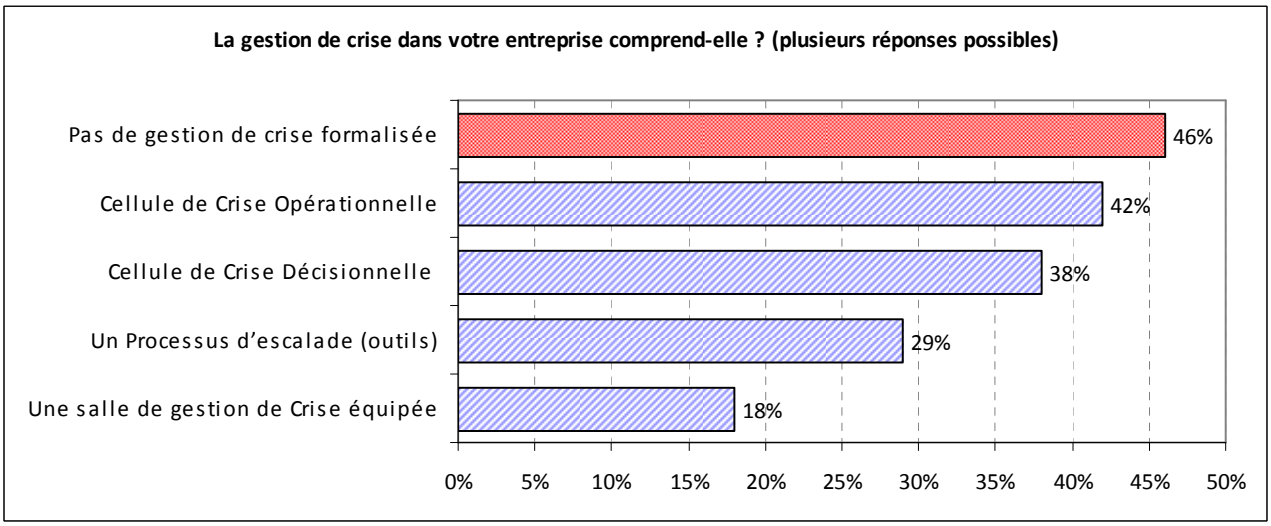

Figure 37 - Contenu des processus de gestion de crise

Thème 15 : Conformité

Ce thème aborde les éléments liés à la conformité sous 3 aspects :

- la conformité avec la loi « Informatique et Libertés »,
- l'audit des Systèmes d'Information,
- l'utilisation de tableau de bord.

❖ Conformité avec la loi « Informatique et Libertés »

À 88 % (idem 2010), les entreprises se déclarent en conformité avec les obligations de la CNIL. Ces bons résultats méritent néanmoins d'être nuancés par la relative faible proportion d'entreprises ayant désigné un Correspondant Informatique et Liberté (CIL) tel que défini par la CNIL.

En effet, même s'il est remarquable de noter que les chiffres progressent de 31 % par rapport à 2010 (+10 points), moins de la moitié des entreprises a désigné un CIL (pour 42 % d'entre elles). Nul doute que l'augmentation du nombre de contrôles par la CNIL pour apprécier l'efficacité du CIL a porté ses fruits, toutefois, des progrès sont encore possibles.

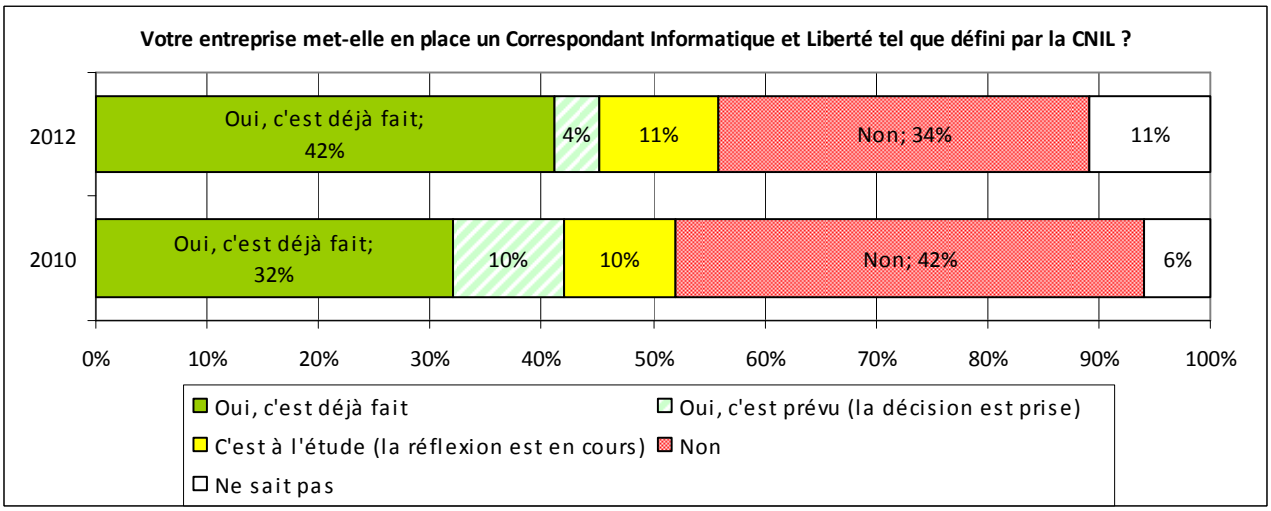

Figure 38 – Existence d'un Correspondant Informatique et Liberté

Côté secteurs d'activité, la Banque/Assurance est largement en tête avec 63 %, suivie du Commerce (48 %), alors que l'Industrie-BTP ferme la marche avec 34 %.

❖ Les audits

Sur une période de deux ans, deux tiers des entreprises interrogées ont réalisé au moins un audit ou contrôle de sécurité du Système d'Information par an (chiffres globalement équivalents à ceux de 2010).

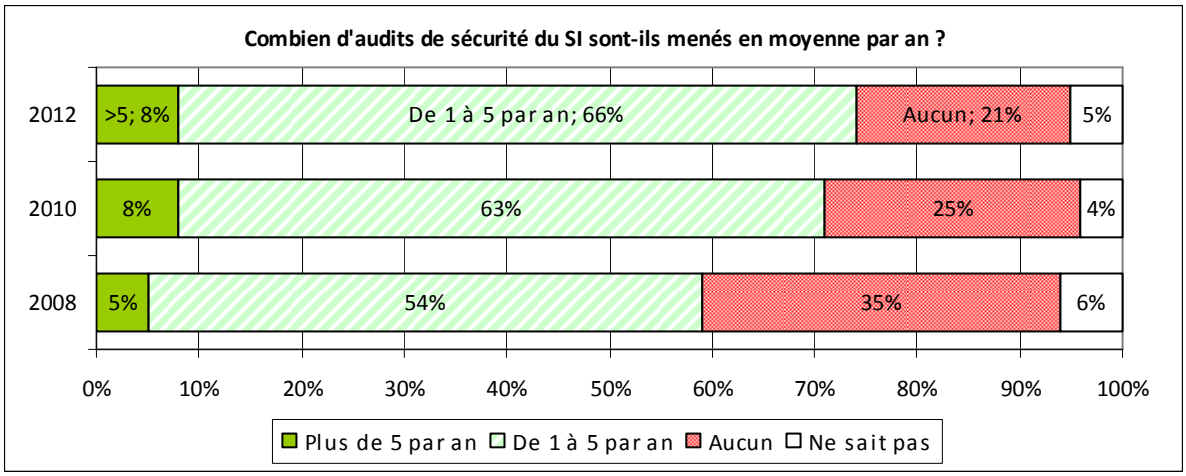

Figure 39 – Nombre d'audits de sécurité du SI réalisé en moyenne par an

Ces audits sont déclenchés principalement par respect de la PSSI (pour 45 % des entreprises sondées). De même, la conformité avec des exigences contractuelles ou règlementaires (dans 39 % des cas), ou le contrôle de tiers (assurances, clients), sont des sources de motivations pour mener des audits. Par ailleurs, il est à noter que par rapport à 2010, les entreprises déclenchent moins d'audits en réaction à un incident (30 % en 2010 vs 14 % en 2012). Les audits font partie intégrante du processus de management de la sécurité des Système d'Information.

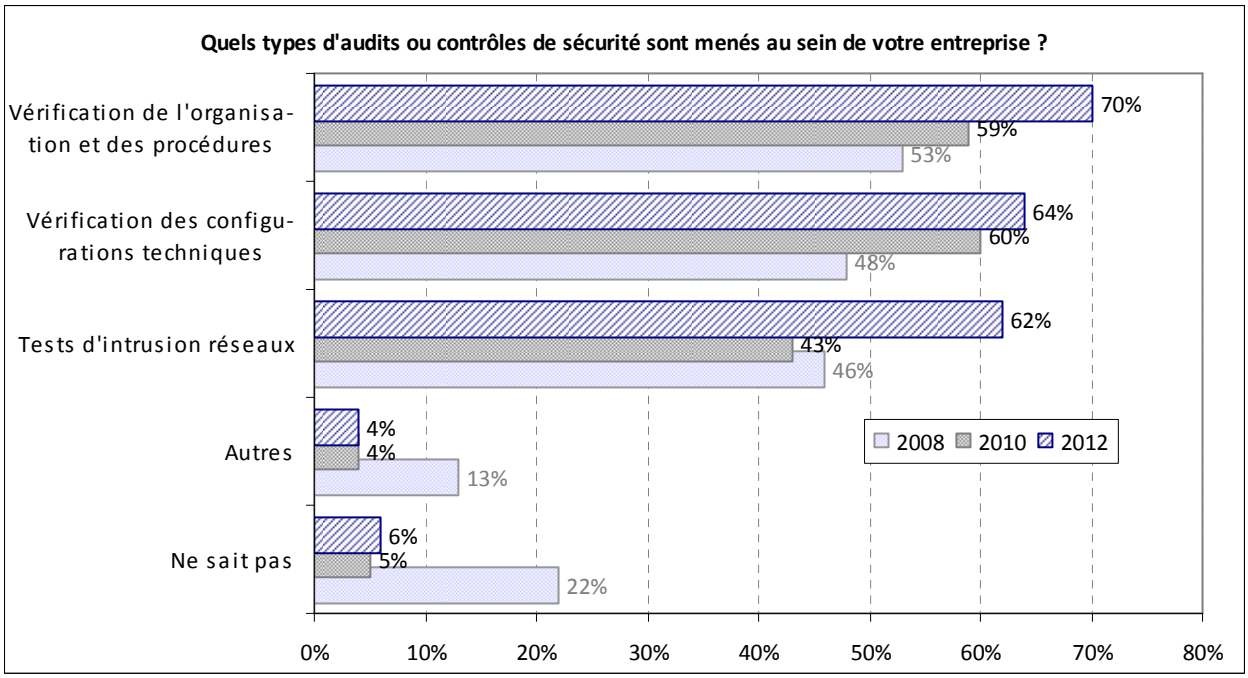

Figure 40 - Types d'audits ou contrôles de sécurité réalisés

Pour la première fois, les audits et contrôles orientés par les aspects organisationnels de la SSI arrivent en tête.

❖ Les tableaux de bord de sécurité

Une large proportion d'entreprises (79 %) ne mesure pas régulièrement son niveau de sécurité liée à l'information.

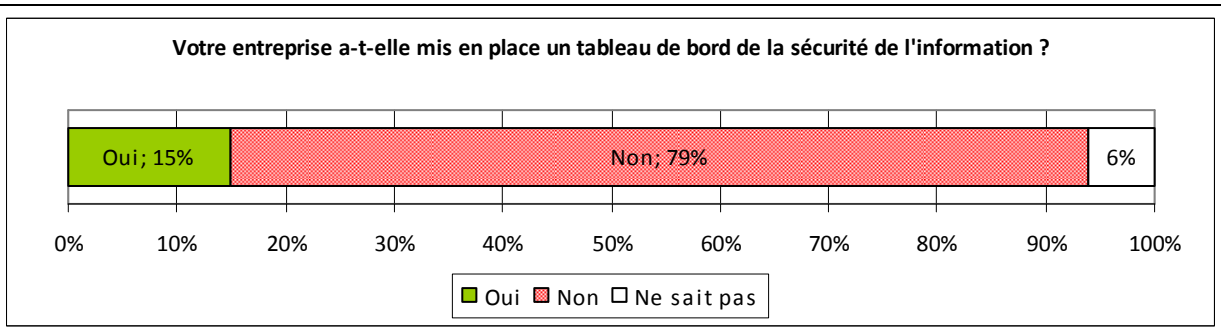

Figure 41 - Mise en place de tableaux de bord de la sécurité de l'information

Les tableaux de bords sont en premier lieu destinés aux opérationnels, puis au RSSI et enfin aux Directions Générales. Ces dernières sont finalement les moins bien informées en matière de sécurité de l'information : il y a là une source d'amélioration pour les RSSI.

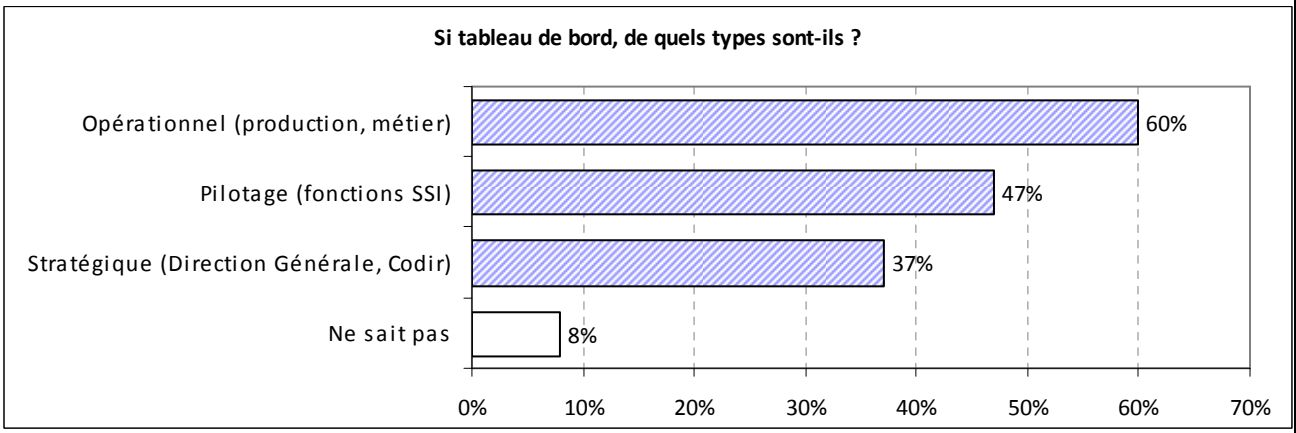

Figure 42 – Mise en place de tableaux de bord de la sécurité de l'information

Les indicateurs inclus dans le tableau de bord évoluent ! Bien entendu, les aspects techniques restent présents (nombre d'incidents sur une période, vulnérabilités détectées, etc.) mais les thèmes organisationnels sont également bien représentés malgré unerégression par rapport à 2010) :

- conformité avec la politique de sécurité,
- impacts directs et indirects des incidents de sécurité,
- conformité avec les normes,
- évaluation des risques métier,
- etc.

C'est le signe d'une certaine maturité, pour les 15 % d'entreprises qui formalisent des tableaux de bord.

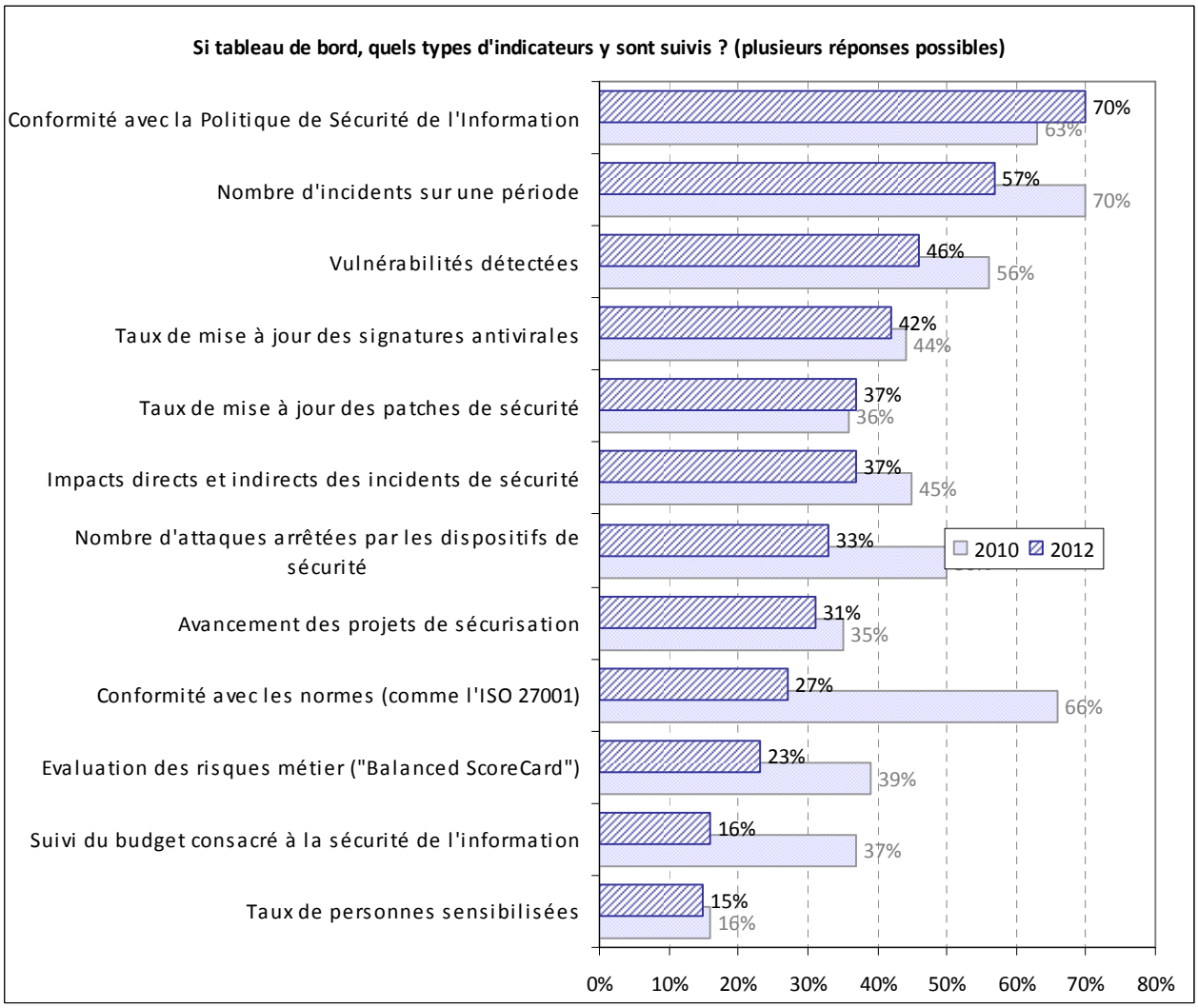

Figure 43 - Indicateurs suivis dans le tableau de bord de la sécurité

Collectivités territoriales

- 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 Collectivités Territoriales

Présentation de l'échantillon

Une analyse globale qui doit être relativisée par des disparités de pratiques entre les différents profils de collectivités

Cette année, le CLUSIF s'est intéressé aux collectivités territoriales. La cible de l'enquête 2008 a été reprise afin de pouvoir comparer les progrès ou les éventuelles régressions. La cible est constituée des collectivités suivantes :

- Communautés de communes de plus de 10 000 habitants,
- Communes de plus de 30 000 habitants,
- Communautés urbaines et d'agglomération,
- Conseils Généraux,
- Conseils Régionaux.

Sur plus de 800 collectivités de France métropolitaine interrogées, 205 ont répondu à la sollicitation du CLUSIF, soit un taux d'acceptation d'environ 25 %. Ce résultat est satisfaisant et nous permet de considérer que l'échantillon de la cible est représentatif.

	Echantillon CLUSIF	**%**	redressement	**Données nationales**
Commune de plus de 30 000 habitants	60	29 %	⇨	16 %
Conseils Généraux	21	10 %	⇨	6 %
Conseils Régionaux	7	3 %	⇨	1 %
Communautés urbaines et d'agglomération	34	17 %	⇨	14 %
Communautés de communes de plus de 10 000 habitants	83	40 %	⇨	62 %
Total	**205**	**100 %**	⇨	**100 %**

Au sein de chaque collectivité, nous avons cherché à interroger en priorité le **Responsable de la Sécurité des Systèmes d'Information** (RSSI). Celui-ci a répondu pour 16 % en moyenne, ce qui s'explique en partie par le fait que les collectivités de taille moyenne n'ont pas encore de fonction RSSI clairement identifiée ou attribuée. En revanche, au sein des collectivités de taille importante comme les Conseils généraux, plus d'un répondant sur deux est le RSSI.

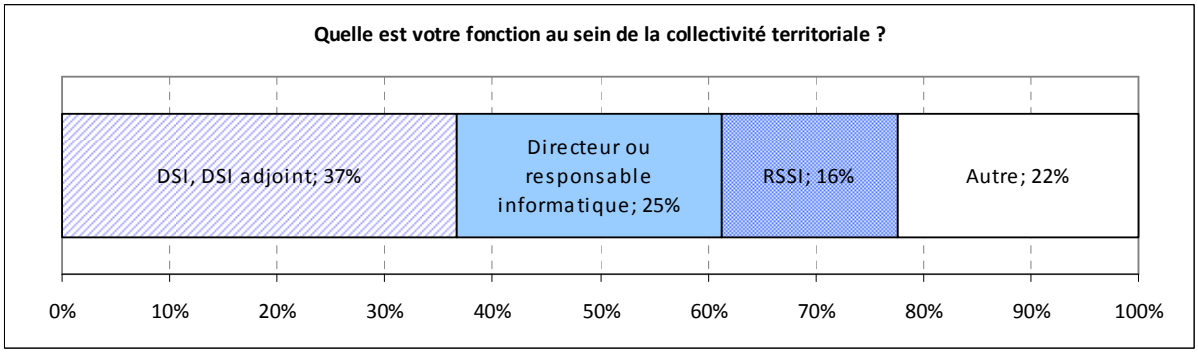

Figure 44 - Profil des interviewés

L'analyse détaillée des réponses fait apparaître des pratiques inégales entre les différents profils de collectivités. Les Conseils Généraux et Régionaux font preuve d'une plus grande mise en œuvre des pratiques de sécurité. Il en est de même pour les villes qui ont, pour la plupart, structuré leur activité sécurité. A contrario, les communautés d'agglomérations et de communes, entités encore assez jeunes, sont, par manque de ressources ou de connaissances, dans une approche plus empirique de ces pratiques.

Sentiment de dépendance à l'informatique

La même perception qu'en 2008

La mise en ligne d'informations pour le citoyen, l'augmentation du nombre de télé-services ou encore la mise en place progressive de PES –V2 pour la dématérialisation des flux comptables ne semblent pas avoir modifié la perception de la dépendance des collectivités à l'informatique.

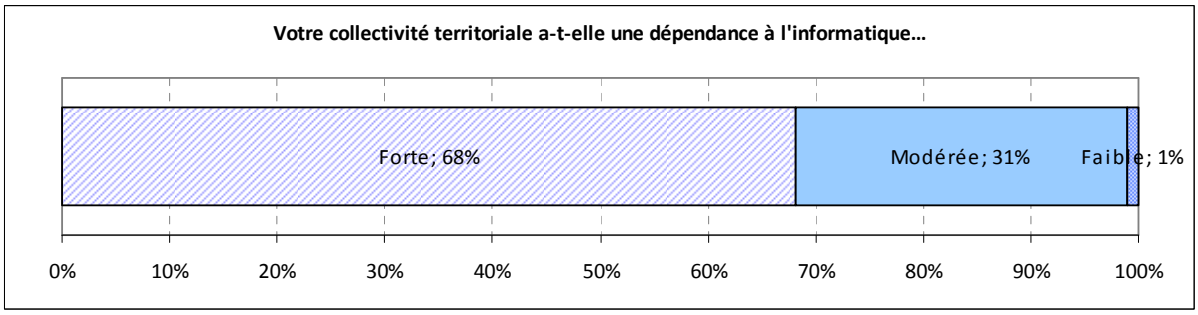

Figure 45 - Dépendance des collectivités territoriales à l'informatique

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

Des budgets en fonction de la taille et des services délivrés par la collectivité

En 2008, 50 % des collectivités avaient accepté de révéler le montant de leur budget informatique. Cette année, nous obtenons un taux de réponse de 79 %. Les budgets sont d'une grande disparité et varient selon la taille de la collectivité. D'une manière générale, ce sont les Conseils Généraux qui ont les plus gros budgets dépassant parfois assez nettement le seuil des 5 M€.

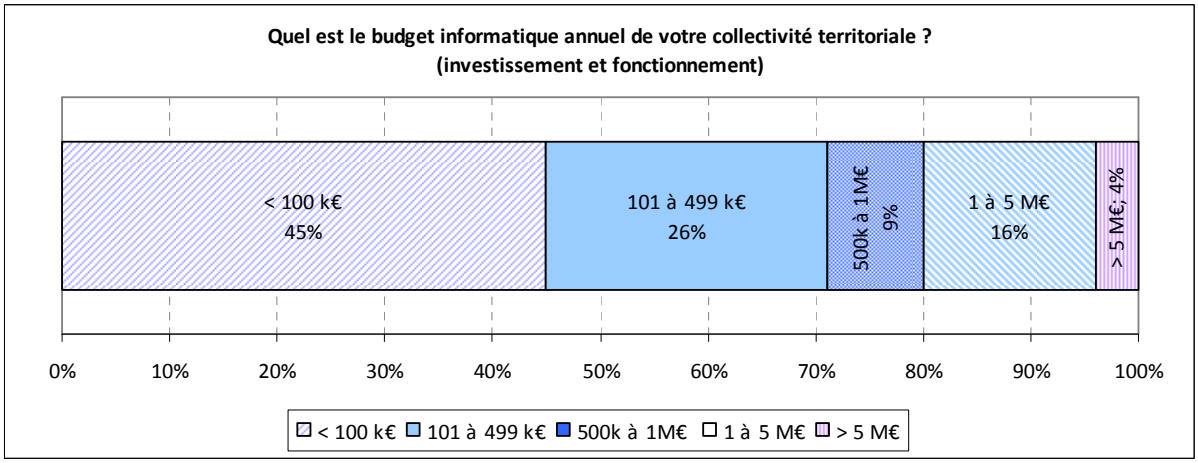

Figure 46 - Budgets informatiques annuels des collectivités territoriales

Un budget sécurité qui conserve les mêmes clés de proportionnalité qu'en 2008

Le budget sécurité est toujours difficile à évaluer. Par exemple; faut-il considérer que la solution de sauvegarde fait partie de ce budget, la réplication des données doit-elle être prise en compte ? Si 19 % des collectivités n'ont pas de ligne budgétaire précise pour la sécurité, les autres confirment que les clés de proportionnalité budgétaire n'ont pas beaucoup bougé depuis 2008.

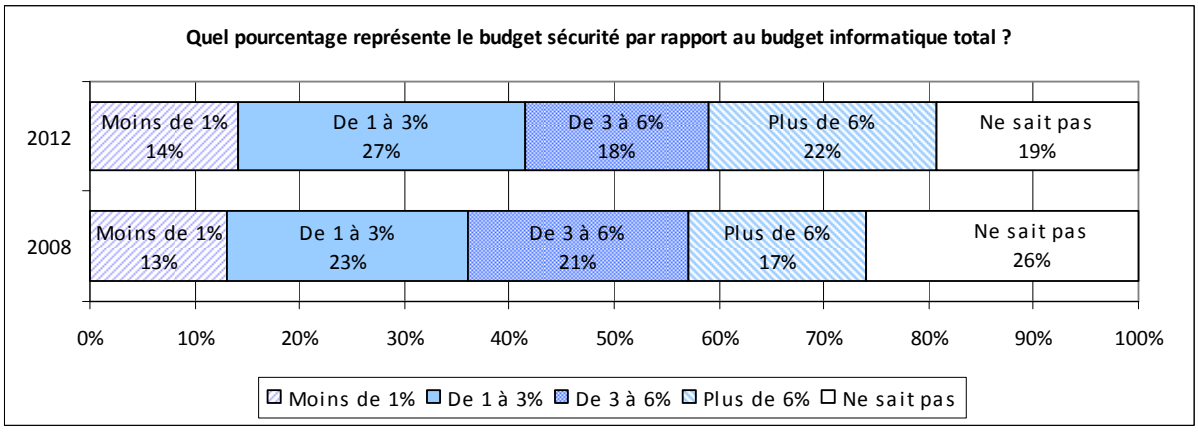

Figure 47 - Part du budget informatique consacré à la sécurité

La sécurité, un budget en légère reprise

Globalement, dans des proportions similaires à celles des entreprises, le pourcentage des budgets « constants » augmente (61 % contre 49 % en 2008) tandis que 29 % des budgets sont en augmentation.

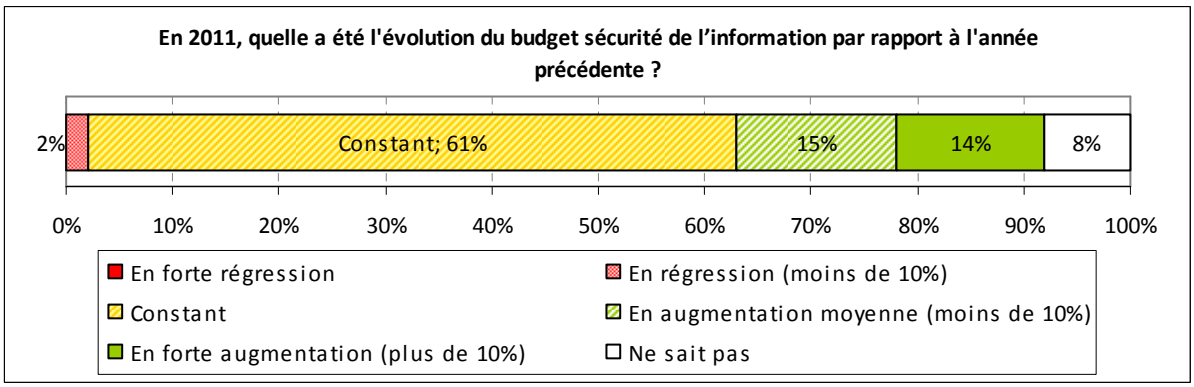

Figure 48 - Evolution du budget sécurité

Le poste budgétaire pour la mise en place de solutions augmente significativement

Lorsque l'on sait que les menaces viennent principalement de l'intérieur, il est satisfaisant de constater que le poste budgétaire formations/sensibilisations est en augmentation. La mise en place de solutions bénéficie en valeur absolue de la plus forte augmentation budgétaire. Les solutions qui répondent aux objectifs de disponibilité comme le renouvellement de la sauvegarde centralisée ou encore la mise en œuvre d'une salle secours informatique y sont probablement pour beaucoup.

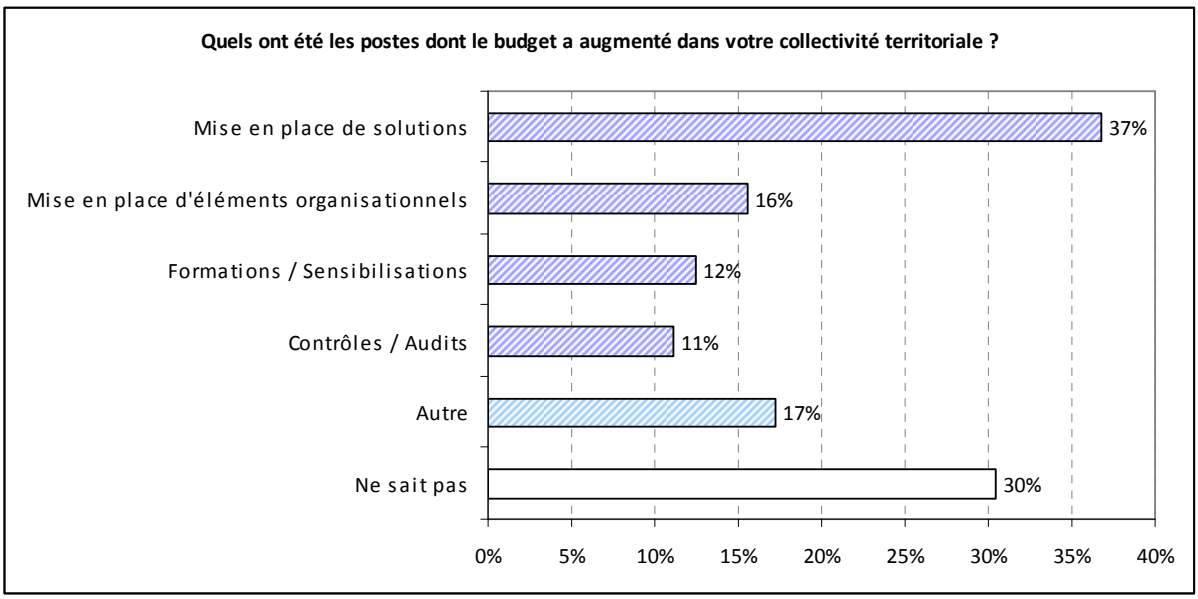

Figure 49 - Postes budgétaires en augmentation

Principal frein à la conduite des missions de sécurité, le manque de personnel qualifié

Alors qu'en 2008 le principal frein était le manque de budget, l'enquête de 2012 révèle que désormais c'est le manque de personnel qualifié qui freine la conduite des missions de sécurité (raison mentionnée par un tiers des collectivités). Cité en second, le manque de connaissances corrobore le point précédent, l'accès à la connaissance permettant d'améliorer la qualification de personnel.

Le manque de budget arrive ex-æquo en seconde position. Plus d'un RSSI sur quatre estime qu'il n'a pas suffisamment de moyens budgétaires pour conduire ses missions.

23 % des personnes interrogées se plaignent de contraintes organisationnelles. La transversalité de la fonction RSSI dans des organisations très verticales ne facilitant pas sa tâche. Enfin, la réticence des directions générales, des métiers et des utilisateurs aurait tendance à confirmer qu'un travail important de sensibilisation doit être fait pour avoir une plus grande adhésion de ces instances.

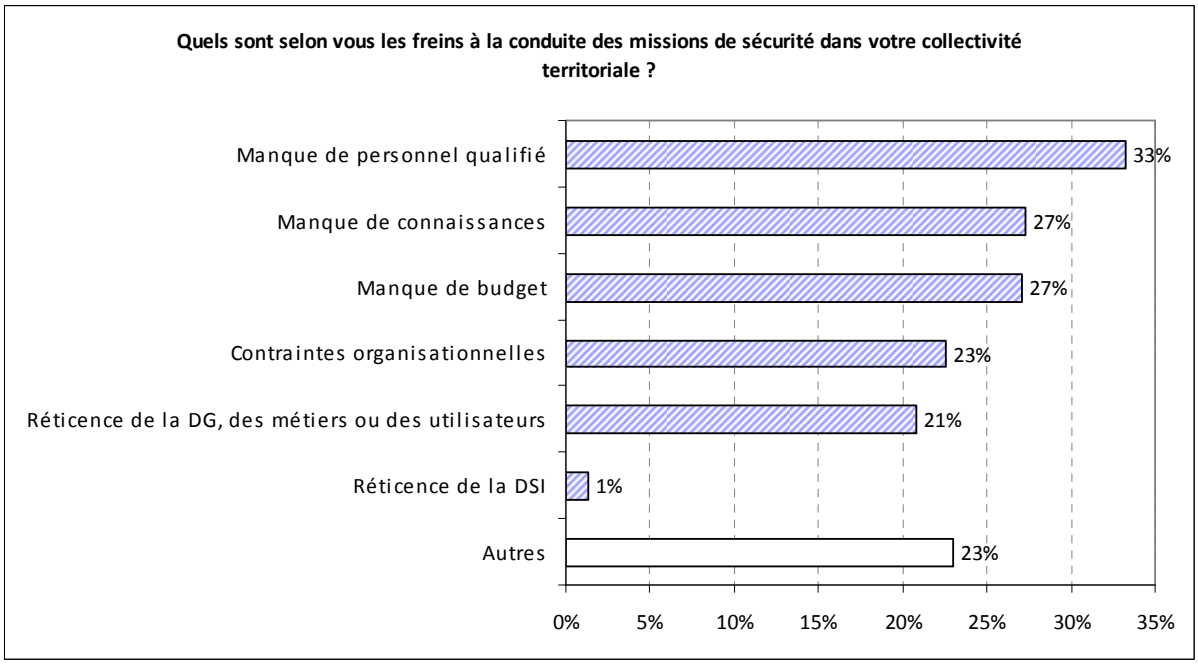

Figure 50 - Freins à la conduite des missions de sécurité

Thème 5 : Politique de sécurité de l'information

La formalisation de la politique de sécurité (PSI) n'évolue pas.

Au même titre que la dépendance perçue à l'informatique, les collectivités ne rattrapent pas leur retard dans la formalisation de leur PSI. Moins d'une collectivité sur 3 a formalisé sa PSI. Toutefois, le soutien de la hiérarchie est acquis dans 99 % des cas, soit une progression de 7 points par rapport à l'enquête de 2008. Pour pratiquement 8 collectivités sur 10, la PSI a été conçue ou mise à jour dans les 3 dernières années.

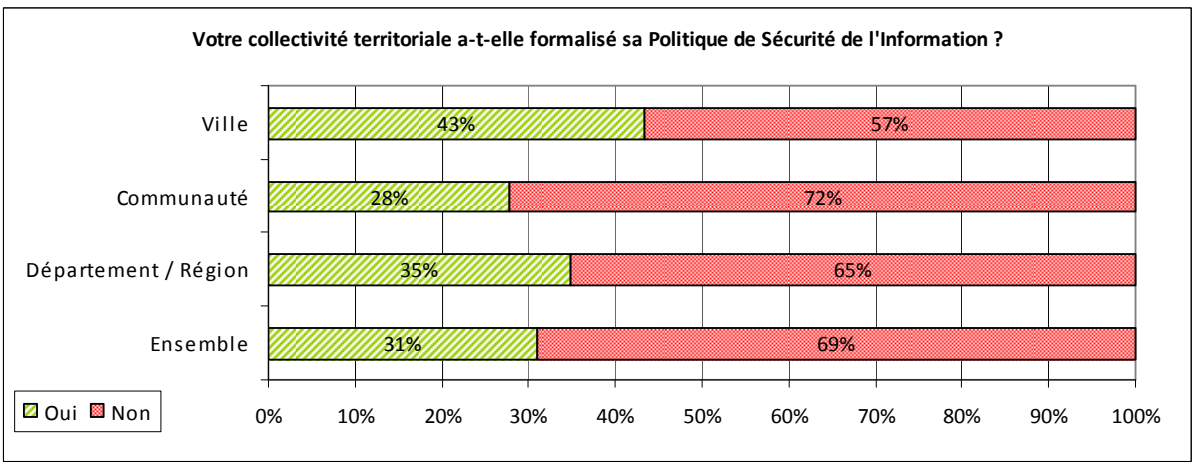

Figure 51 - Existence d'une politique de sécurité de l'information

Une Direction Générale concernée par la PSI

L'élaboration de la PSI implique majoritairement la Direction Générale des Services (80 %) en relation avec la Direction des Systèmes d'Information (57 %) et les équipes de production (23 %). La PSI voit également une forte progression de l'implication des élus et des directions métiers, même si cela reste minoritaire.

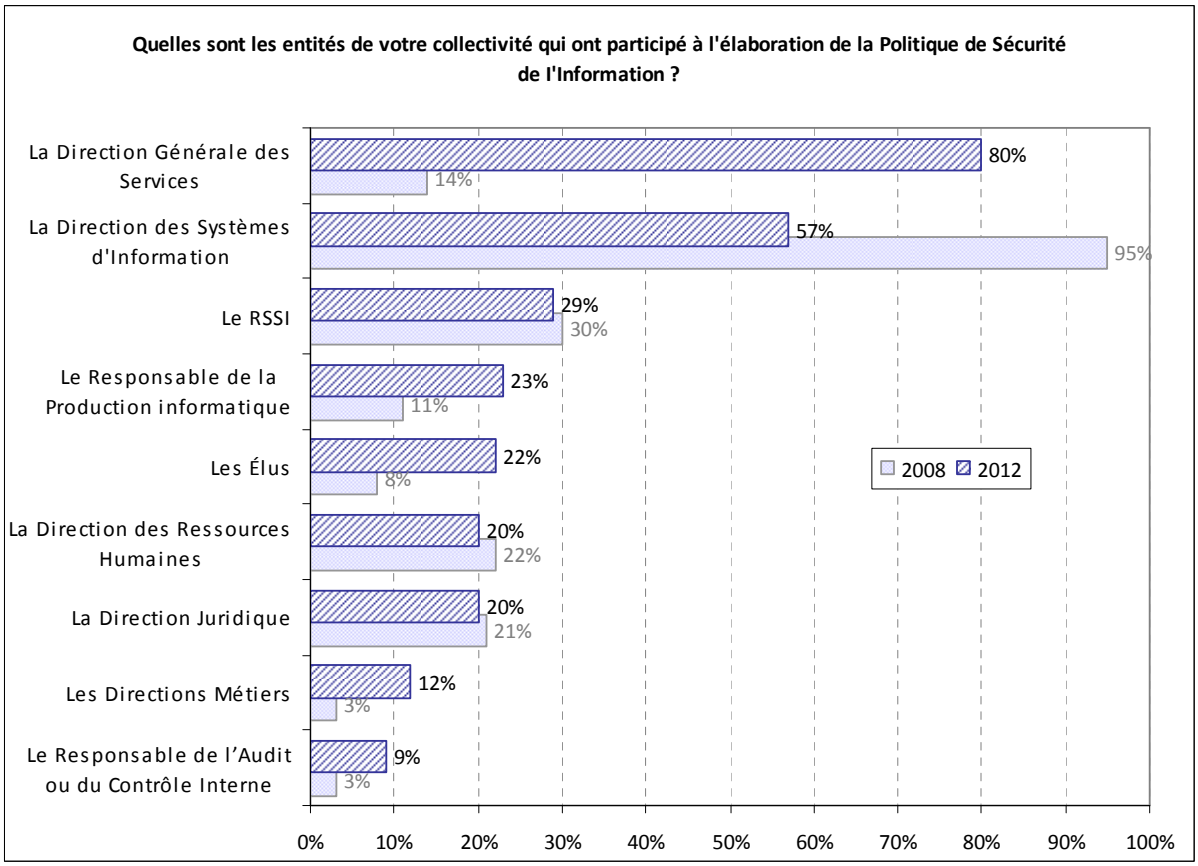

Figure 52 - Acteurs de la politique de sécurité de l'information

Une PSI qui voit son cadre méthodologique progresser

En 2008, 3 collectivités sur 5 ne s'appuyaient sur aucune « norme de sécurité » pour leur PSI. La situation en 2012 s'est inversée puisque 65 % d'entre elles utilisent une norme ou un référentiel.

Les départements et les régions plébiscitent l'ISO 2700x à 67 %. Globalement, le travail de l'ANSSI porte ses fruits auprès des collectivités puisque que le Guide PSSI et la méthode EBIOS associée sont citées 4 fois plus qu'en 2008.

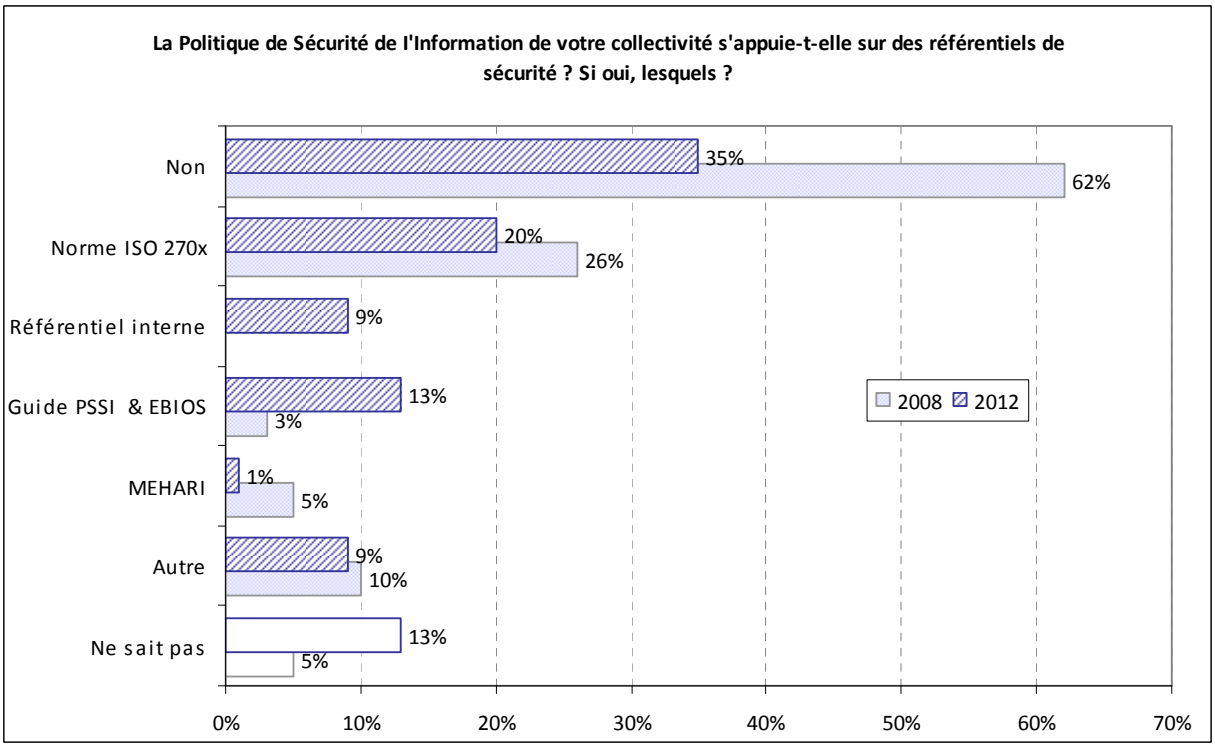

Figure 53 - Appui de la politique de sécurité de l'information des collectivités sur un référentiel de sécurité

Thème 6 : Organisation de la sécurité et moyens

Le RSSI : un poste métier en progression

La fonction de RSSI ou de RSI s'impose peu à peu dans le monde des collectivités territoriales : elle est clairement identifiée et attribuée dans 32 % des cas en 2012 contre 22 % en 2008. On note une présence plus forte d'un RSSI dans les Conseils Généraux et Régionaux.

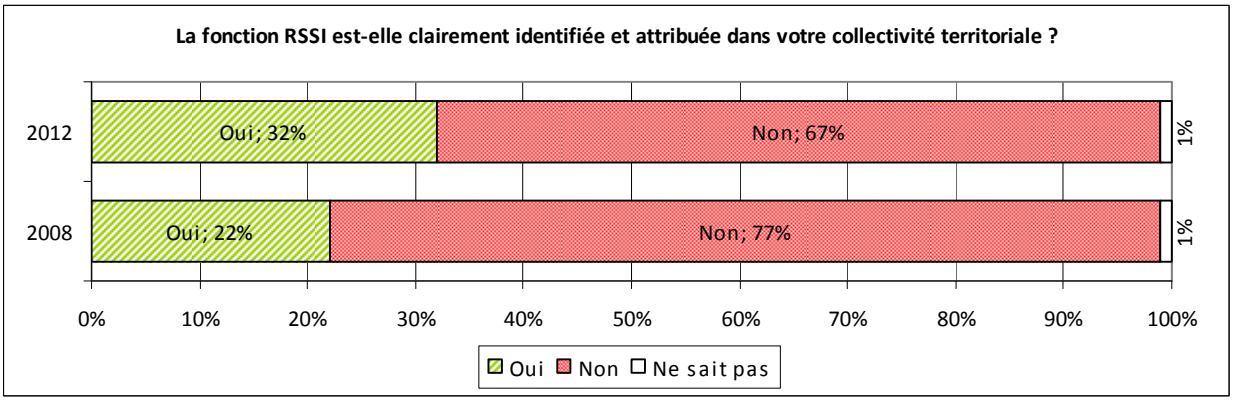

Figure 54 - Identification et attribution de la fonction RSSI

Le rôle de RSSI ou de RSI prend de plus en plus de poids : plus de 45 % des RSSI sont dédiés à cette tâche à temps plein en 2012, contre 32 % en 2008.

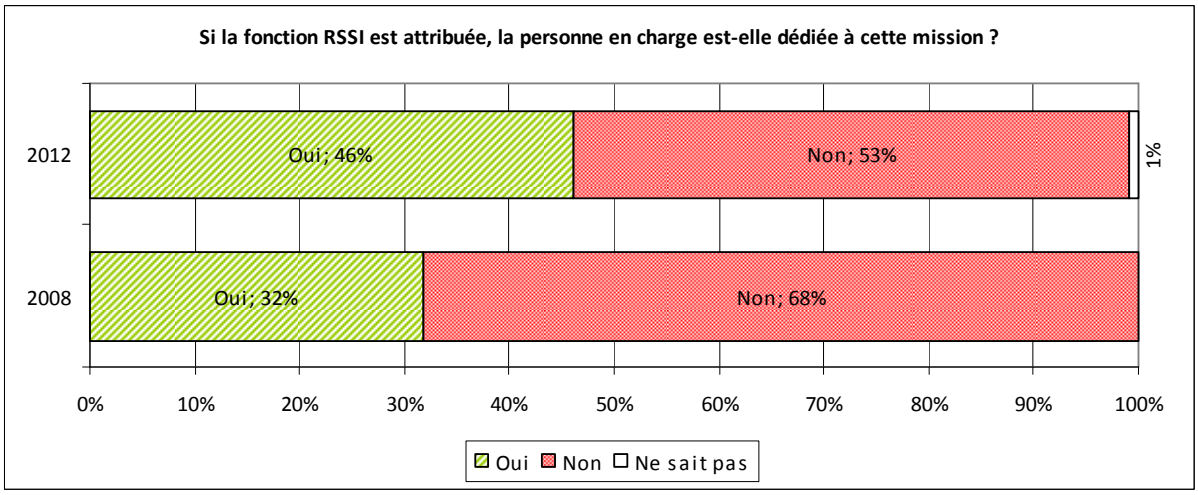

Figure 55 - Mutualisation des missions pour les RSSI identifiés dans les collectivités territoriales

Lorsque le RSSI n'existe pas, cette mission reste attribuée par défaut à la Direction des Systèmes d'Information ou à la Direction Informatique.

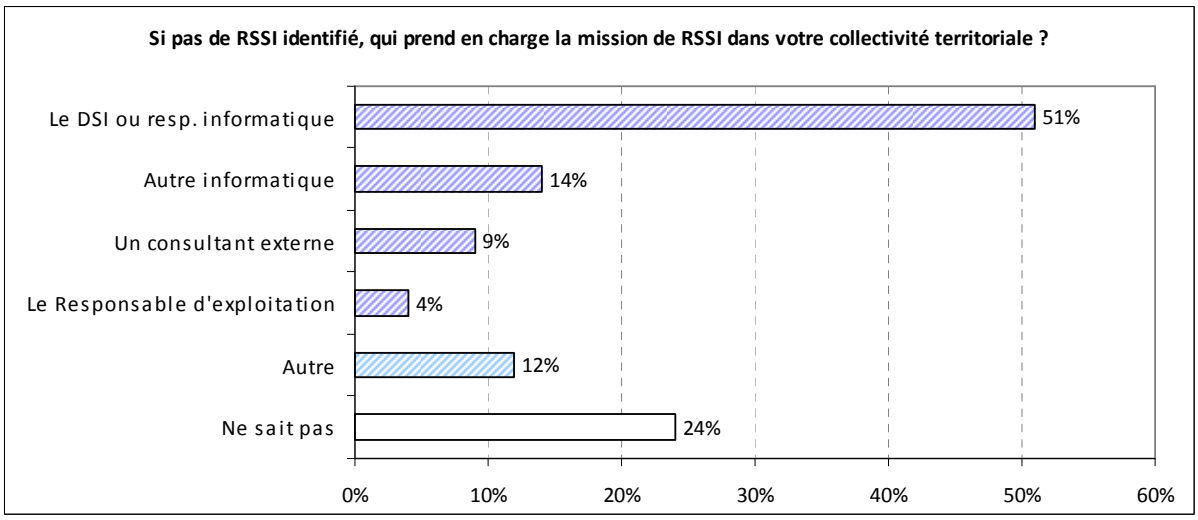

Figure 56 - Prise en charge de la fonction RSSI, lorsqu'il n'existe pas de RSSI

Le RSSI consacre désormais et en moyenne 12 % de son temps aux activités juridiques : déclaration CNIL et instruction de plaintes.

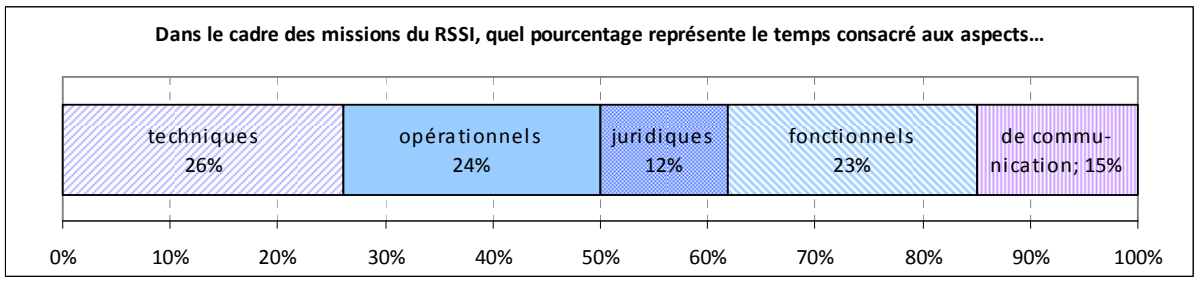

Figure 57 - Répartition des missions du RSSI

Thème 7 : Gestion des biens

Un manque d'outils pour la gestion des biens

On ne protège bien que ce que l'on connait bien ! Une bonne connaissance de ses actifs est essentielle. Nos interlocuteurs nous font part d'un manque d'outils pour la gestion des biens. Pour certaines collectivités, la réponse se trouverait dans les logiciels de cartographie.

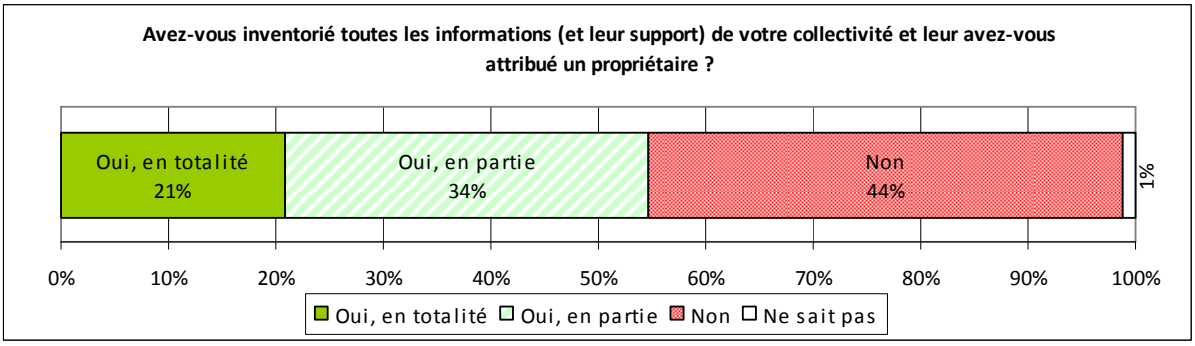

Figure 58 - Inventaire des informations dans les collectivités territoriales

60 % des collectivités n'ont pas classifié leurs informations. Est-ce par manque de méthode, par manque de temps ou est-ce lié à la difficulté de l'exercice ? Il n'empêche que cela se traduit probablement par des pratiques de sécurité identiques quelle que soit la valeur de l'actif. La classification présente pourtant un intérêt majeur, celui d'appliquer le principe de proportionnalité.

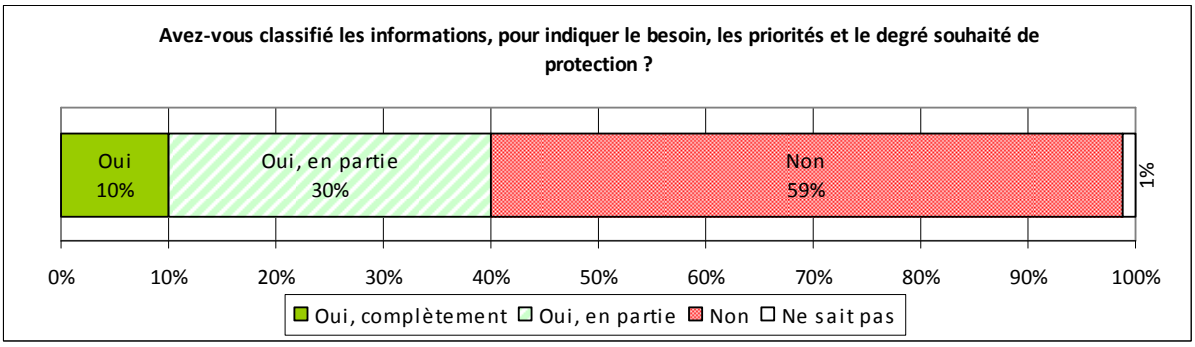

Figure 59 - Classification des informations dans les collectivités territoriales

La moitié des collectivités limitent à trois les niveaux de confidentialité. Cette classification facilite probablement l'application de règles de sécurité spécifiques et proportionnées pour garantir le secret médical dans les collectivités qui manipulent des données de santé.

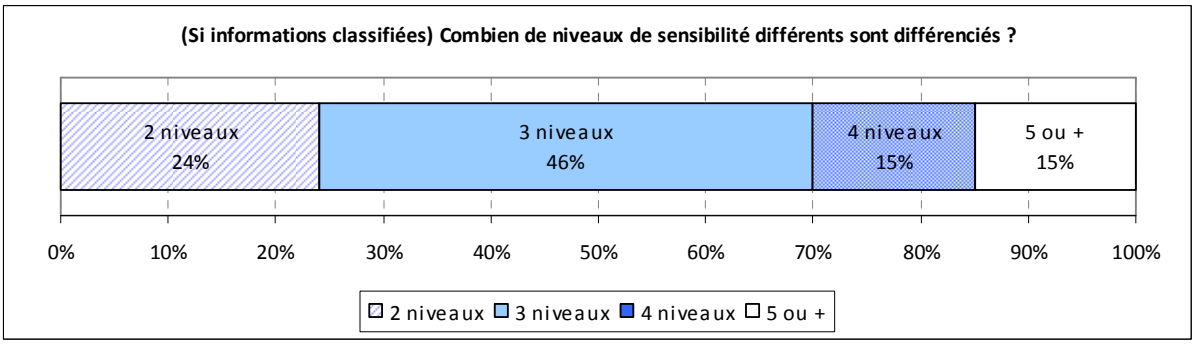

Figure 60 - Niveaux de sensibilité des informations dans les collectivités territoriales

La démarche d'analyse de risque serait en régression

L'analyse formelle des risques liés à la sécurité de l'information demeure une pratique limitée, en régression par rapport à 2008 (33 % en totalité ou en partie versus 42 %), voire confidentielle si l'on considère l'exhaustivité de la démarche.

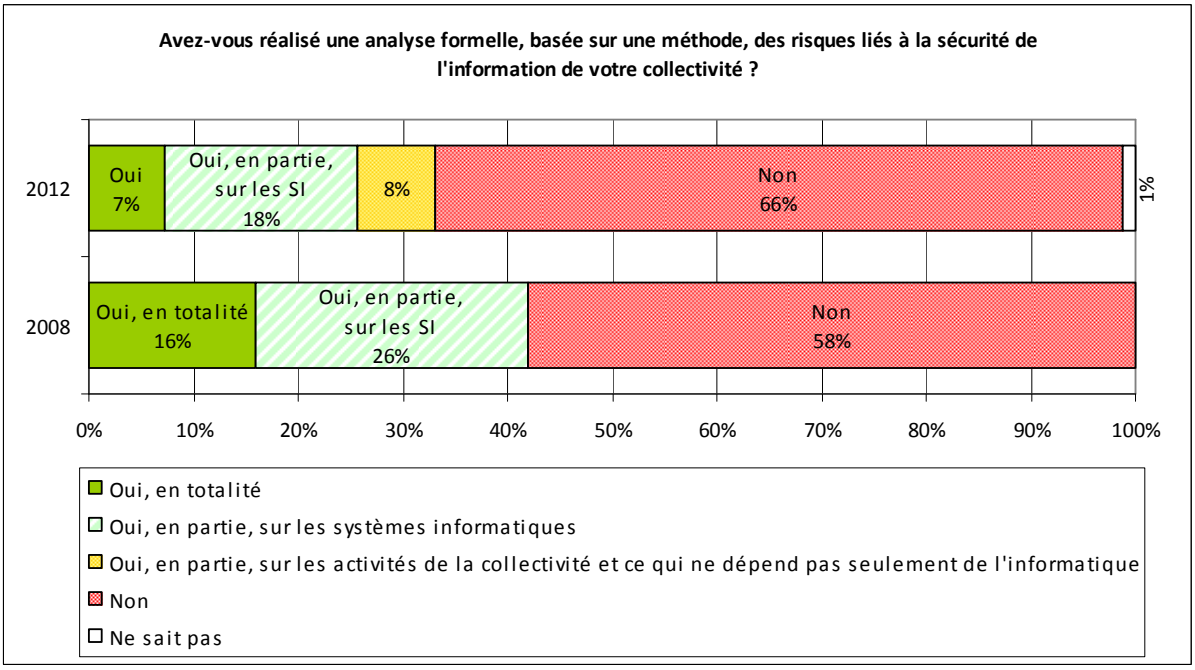

Figure 61 - Analyse formelle basée sur une méthode d'analyse des risques

La norme ISO 27005 ou une méthode « conforme ISO 27005 » sont données en référence dans un cas sur 2. Remarquons que la méthode EBIOS est plus souvent citée pour les Collectivités que pour les entreprises (17 % contre 7 %), probablement en raison de l'origine (secteur public) de cette méthode.

En revanche, le taux d'incertitude (« Autre » et « Ne sait pas ») ne permet guère d'autre conclusion, sauf peut-être qu'une partie des Collectivités utilise une méthode maison.

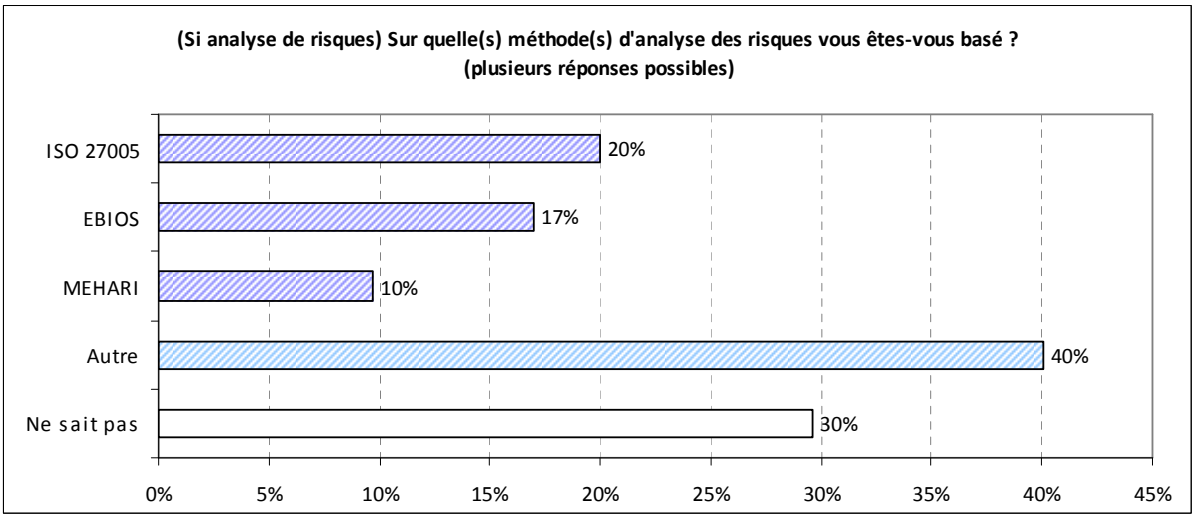

Figure 62 - Méthode utilisée dans les collectivités pour l'analyse de risques

Thème 8 : Sécurité des ressources humaines

La charte est soumise de manière quasi systématique au comité technique paritaire

La charte d'usage est souvent la première formalisation des règles de sécurité de l'établissement.

Cette pratique a peu évolué depuis 2008. L'arrivée du BYO (Bring Your Own Device) pourrait changer la donne. Les Communautés impactent fortement la moyenne nationale.

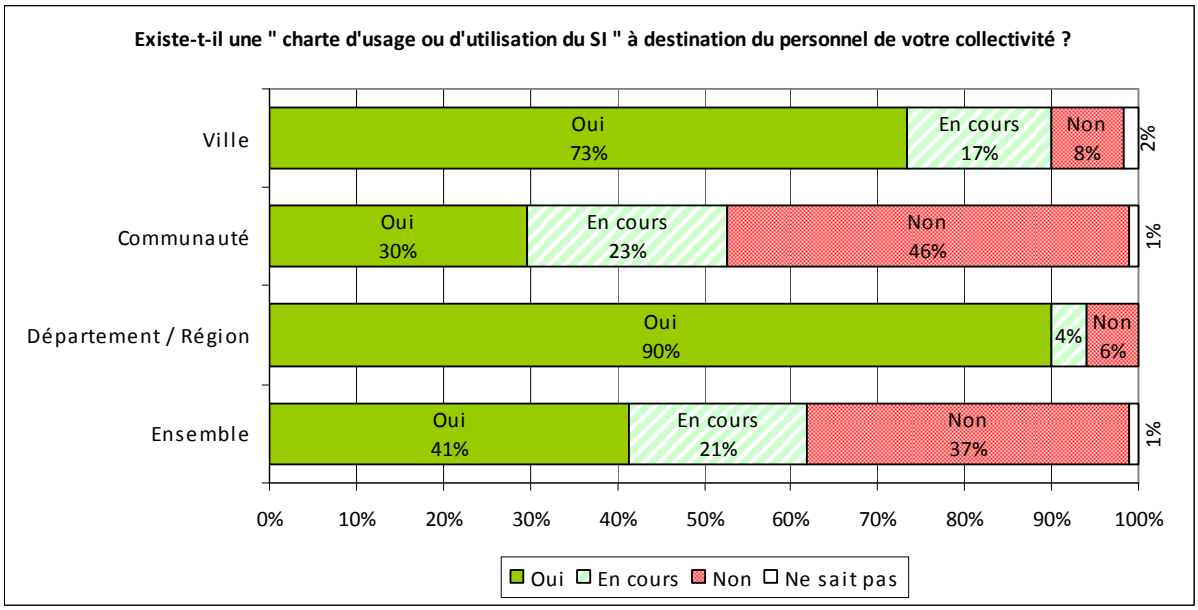

Figure 63 - Existence d'une charte d'usage selon le profil de la collectivité

Il faut toutefois noter une implication forte des instances représentatives. C'est un point réglementaire pris en compte pour rendre la charte effectivement applicable.

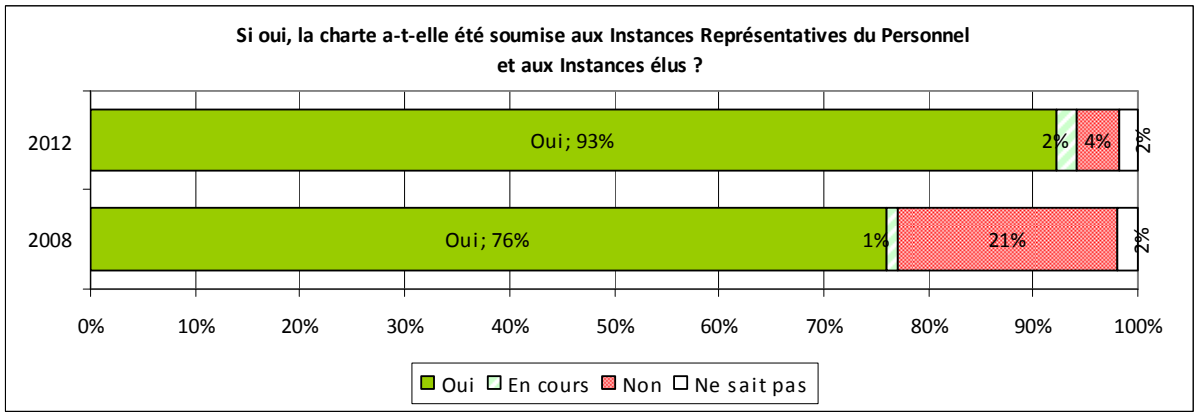

Figure 64 - Soumission de la charte aux instances représentatives du personnel

Dans 60 % des cas, la charte est officiellement signée par l'agent. Quelques collectivités estiment que cette pratique n'est pas justifiée : on ne signe pas le règlement intérieur et pour autant les règles qui y figurent engagent la responsabilité de la collectivité et de ses agents.

Pour les collectivités qui possèdent une charte, on enregistre une progression de 35 % (+25 points) dans la communication de son contenu.

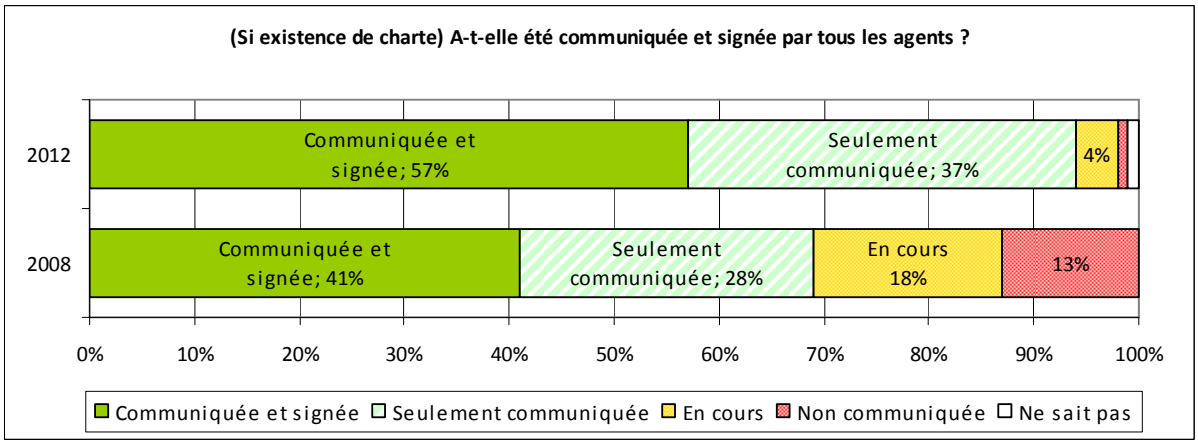

Figure 65 - Communication de la charte aux utilisateurs dans les collectivités

La sensibilisation des utilisateurs ne fait pas recette. La démarche semble s'essouffler puisque seules 17 % des collectivités ont lancé des actions dans ce domaine et 12 % en préparent. Soit à peu de chose près, la même proportion qu'il y a 4 ans.

D'une manière générale et lorsque la pratique existe, cette sensibilisation est très appréciée par les agents. Ils y voient un double intérêt : améliorer leurs pratiques pour leurs usages privés et professionnels.

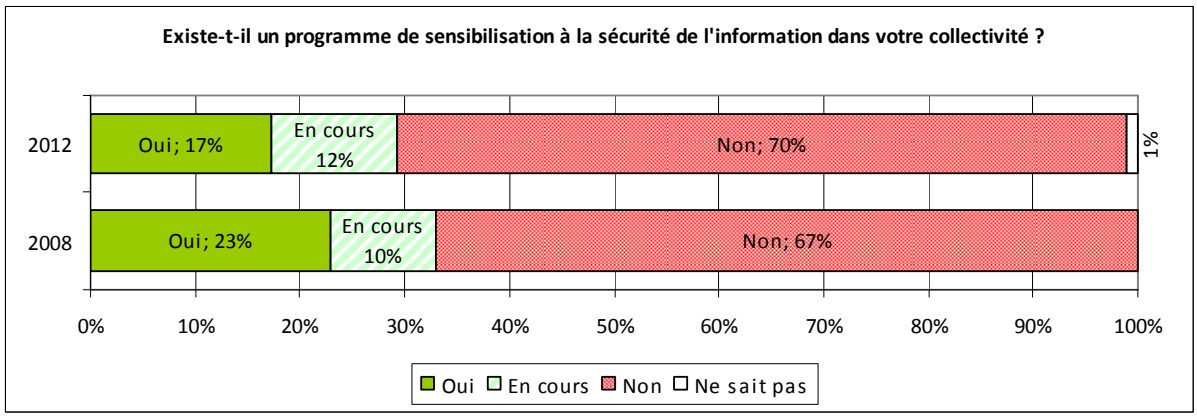

Figure 66 - Programme de sensibilisation à la sécurité dans les collectivités

Bien que la culture de l'évaluation ne soit pas ancrée dans les collectivités, l'impact de la sensibilisation est mesuré dans 1 cas sur 4, ce qui représente une évolution significative par rapport à la précédente enquête (1/10). L'approche de la sécurité des Systèmes d'Information par la sensibilisation des utilisateurs est intégrée dans le processus d'amélioration continue.

Les collectivités nous rapportent que ce n'est pas l'impact de la sensibilisation qui est mesuré prioritairement lors de ces programmes mais la satisfaction de l'agent. Néanmoins et parmi les vecteurs de mesure d'impacts, les collectivités nous font remarquer que le nombre de déclarations à la CNIL connait un léger pic après les séances de sensibilisation.

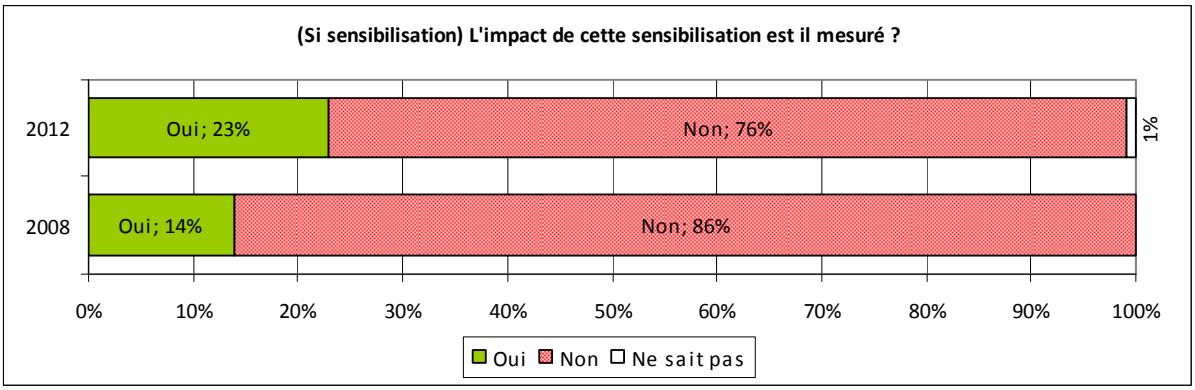

Figure 67 - Evaluation de l'impact de la sensibilisation

Partie intégrante de la sécurité liée aux ressources humaines, nous avons interrogé les collectivités sur leurs pratiques en matière de gestion des mouvements de personnel. Dans 60 % des collectivités, la gestion de la mobilité des agents (départ, mutation) est l'occasion de la remise à plat des droits d'accès aux Systèmes d'Information. D'une manière générale, il existe des procédures dont le périmètre est variable d'une collectivité à l'autre, mais beaucoup de nos interlocuteurs constatent que la DSI est rarement informée du départ de collaborateurs.

Pour pallier à cette déficience, certaines d'entre elles ont mis en place une procédure d'audit des comptes dormants.

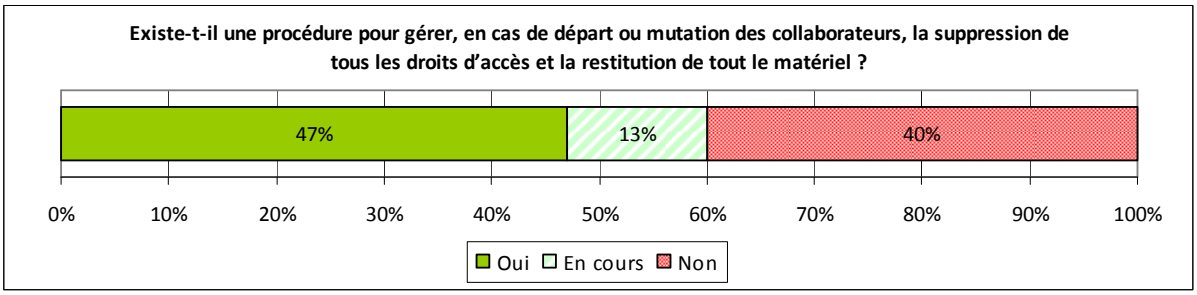

Figure 68 - Gestion des droits d'accès lors des départs

Thème 9 : Sécurité physique

La sécurité des supports papiers est à la discrétion des directions métiers

Cette année, l'enquête a porté sur les pratiques de sécurité des supports papiers. Dans la plus grande partie des collectivités, cette gestion est à la discrétion des directions métiers. Si les pratiques sont disparates d'une direction à une autre, d'une collectivité à une autre, l'instruction du 28 août 2009 de la Direction des Archives de France pourrait apporter une réponse d'harmonisation.

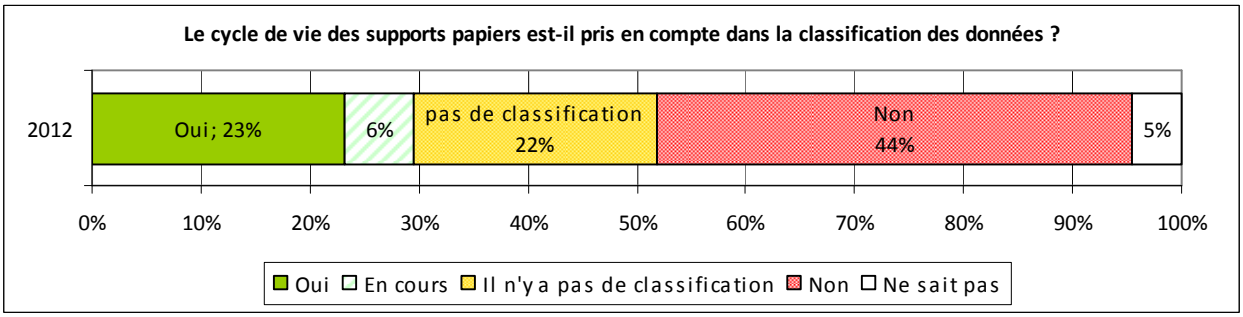

Figure 69 - Cycle de vie des supports papiers en fonction de la classification des données

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

Des collectivités qui ouvrent l'accès à leur Système d'Information.

Dans cette section, il est fait référence aux bonnes pratiques techniques mises en œuvre dans les organisations. Les technologies utilisées sont globalement les mêmes dans les collectivités que dans les entreprises, et les deux contextes seront mis en parallèle dans les lignes qui suivent. Il sera donc utile de se référer au chapitre correspondant de l'étude « Entreprises ».

Depuis la dernière enquête, les collectivités ont poursuivi la mise en œuvre des nouvelles technologies pour ouvrir les accès au Système d'Information en condition de mobilité. Nous constatons moins d'interdit et des droits et usages sont mieux encadrés.

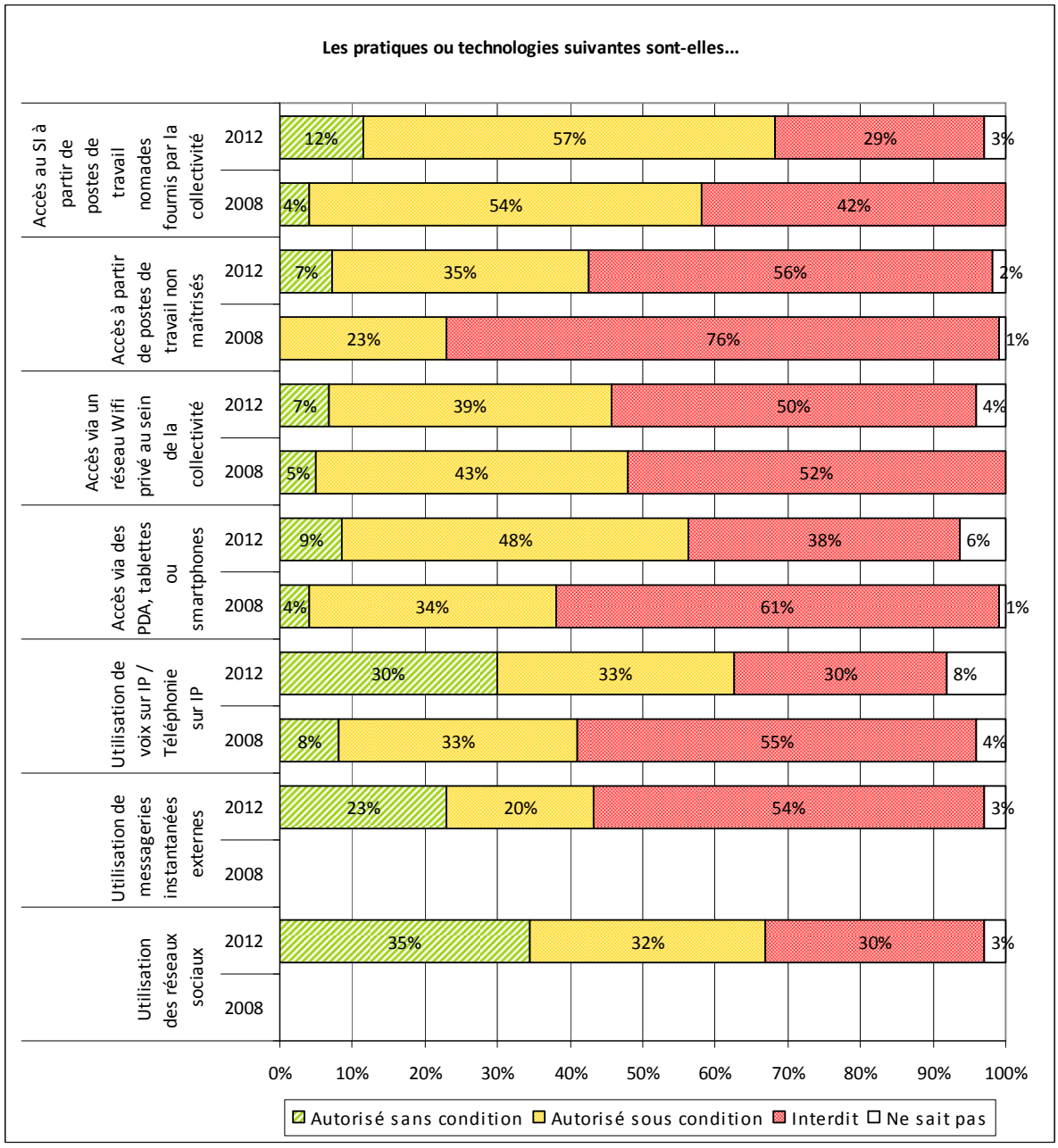

Figure 70 - Mobilité et accès au Système d'Information dans les collectivités

Tout comme l'accès au Système d'Information via des postes de travail non maîtrisés, l'usage des PDA et des smartphones est en assez forte progression. Les collectivités doivent faire face, comme les entreprises, au phénomène du BYOD. La téléphonie IP voit son utilisation sans condition augmenter significativement. Les collectivités ont-elles bien intégré les risques associés à cette technologie ?

L'enquête 2012 prend en compte l'utilisation des messageries instantanées et des réseaux sociaux. Les messageries instantanées externes sont interdites dans une collectivité sur 2 et encadrées dans 1 sur 3. Le droit d'utilisation des réseaux sociaux est plus disparate puisque les pratiques se répartissent uniformément entre l'interdiction et les autorisations avec ou sans condition. Si les collectivités utilisent les médias sociaux pour promouvoir leur communication et la démocratie participative, ont-elles pris la juste mesure des risques qu'elles encourent en n'encadrant pas davantage l'usage par l'ensemble de leurs agents ?

En synthèse, on observe que les Conseils Généraux et Régionaux et dans une moindre mesure les villes offrent plus de service de mobilité à leurs agents que la moyenne. Il apparaît également que la mise à disposition des moyens en mobilité est plus encadrée dans ces collectivités.

❖ Technologies de protection et de gestion des vulnérabilités

Les solutions largement adoptées : antivirus et anti-spam

Deux solutions techniques font aujourd'hui l'objet d'un usage systématique par l'ensemble des utilisateurs de Systèmes d'Information : les technologies d'antivirus (hors le cas particulier des terminaux mobiles de nouvelle génération) et d'anti spam. La généralisation de l'application de bonnes pratiques est en tout point comparable à celle qui est observée dans le monde des entreprises.

Figure 71 - Lutte antivirale, protection contre les intrusions et gestion des vulnérabilités

Encore plus que dans le monde de l'entreprise, la protection antivirus des terminaux mobiles de nouvelle génération (smartphones et tablettes) est un sujet en devenir puisque le taux d'équipement n'atteint que 18 % (dont 10 % sur périmètre restreint).

On peut d'ailleurs se poser la question de la percée réelle des tablettes et smartphones dans les Collectivités Territoriales, avec pour corollaire des questions telles que l'usage qui en est fait ou le taux de connexion réel au SI de l'organisation.

Ce faible niveau d'adoption se retrouve sur la technologie pare-feu (14 % des smartphones et tablettes équipés contre 26 % dans le monde de l'entreprise), alors que la mise en place de la technologie pare-feu sur les portables classiques est plus dans la moyenne avec 80 % d'équipement (ici aussi sans doute lié à la présence de cette technologie dans les suites « anti-virus » du marché).

Concernant le chiffrement, les smartphones et tablettes des collectivités ne sont pas mieux lotis que ceux des entreprises. Les portables classiques font, eux, l'objet d'une protection deux fois moins importante que dans les entreprises (20 % contre 43 %), peut-être est ce dû à une présence moindre de données confidentielles sur ces postes de travail, ou bien à une prise de conscience encore rare du niveau de confidentialité des données présentes sur les ordinateurs personnels.

Le contrôle des périphériques de stockage amovibles

Le nombre de collectivités effectuant le contrôle des périphériques de stockage amovibles (36 %) est comparable à celui rencontré pour les entreprises. Ce taux relativement faible s'explique souvent par les freins à l'adoption pour les utilisateurs pour lesquels les clés USB sont des outils d'échange particulièrement utiles. Il est important de noter que cette pratique (l'échange de données) est en train de se déplacer vers des services de type « stockage dans le Cloud », avec des problématiques identiques à celles rencontrées sur les périphériques amovibles.

La sécurité des réseaux

IDS et IPS font l'objet d'un niveau d'équipement bien plus faible que celui rencontré dans les entreprises. Les collectivités sont plus nombreuses à baser la sécurité de leur réseau sur les seuls firewalls. Pourtant, les collectivités déploient autant de réseaux étendus que les entreprises, réseaux sur lesquels des fonctionnalités IPS trouvent toute leur justification en proposant de limiter des « attaques » potentielles sans pour autant opposer de limitations fonctionnelles aux utilisateurs. Il apparaît donc que celles-ci sont moins nombreuses que les entreprises à avoir fait le choix de cette compartimentation.

L'exploitation des fichiers de journalisation

Le niveau d'adoption des outils de gestion de log est comparable à celui rencontré dans le monde des entreprises.

Le NAC et le DLP, des technologies fonctionnellement ambitieuses

Le NAC (contrôle d'accès au niveau réseau) et le DLP (contrôle de la fuite des données) font l'objet d'une adoption faible en entreprise et sont encore moins utilisés dans les collectivités. Les uns comme les autres sont confrontés à la complexité de mise en place de ces solutions, tant sur les plans fonctionnel que technique. Ce qui n'enlève rien à la pertinence de ces technologies, que ce soit pour contrôler l'accès au réseau ou le mouvement des informations de l'entreprise, par exemple au travers de périphériques de stockage amovibles.

❖ L'infogérance

Plus de recours à l'infogérance

Les raisons sont nombreuses et les collectivités citent les objectifs de disponibilité 24/7/365 pour certaines applications, la difficulté de maintenir une polyvalence sur l'intégralité du catalogue applicatif, la complexité des technologies qui nécessitent des savoir-faire externes et enfin la rationalisation de la DSI avec l'externalisation des applications ressources humaines et finance.

Parmi les collectivités qui ont recours à l'infogérance, nous remarquons une forte proportion de Communautés de communes. Il s'agit sans doute pour elles de pallier pour partie à un manque de compétences internes.

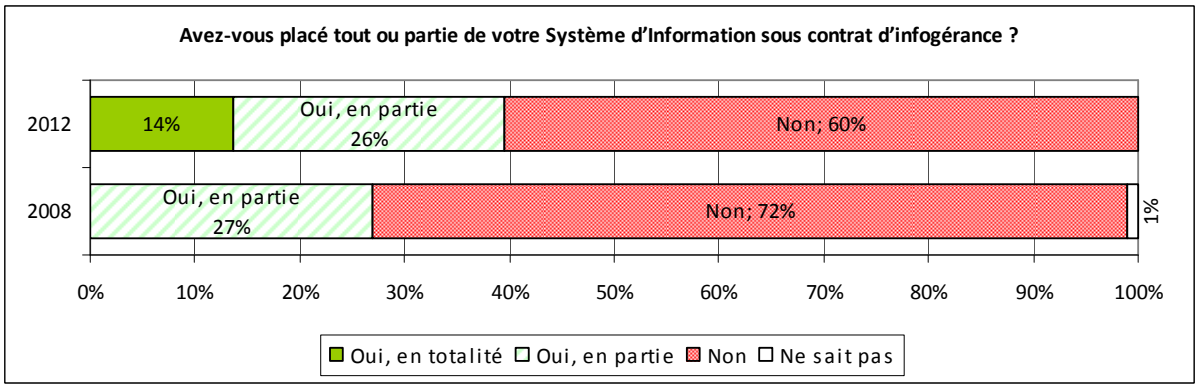

Figure 72 - Part des Systèmes d'Information de collectivités sous contrat d'infogérance

L'augmentation des services infogérés a entraîné une augmentation de la maturité et des pratiques de sécurité vis-à-vis des tiers. Désormais, 50 % des collectivités suivent cette infogérance par des indicateurs de sécurité.

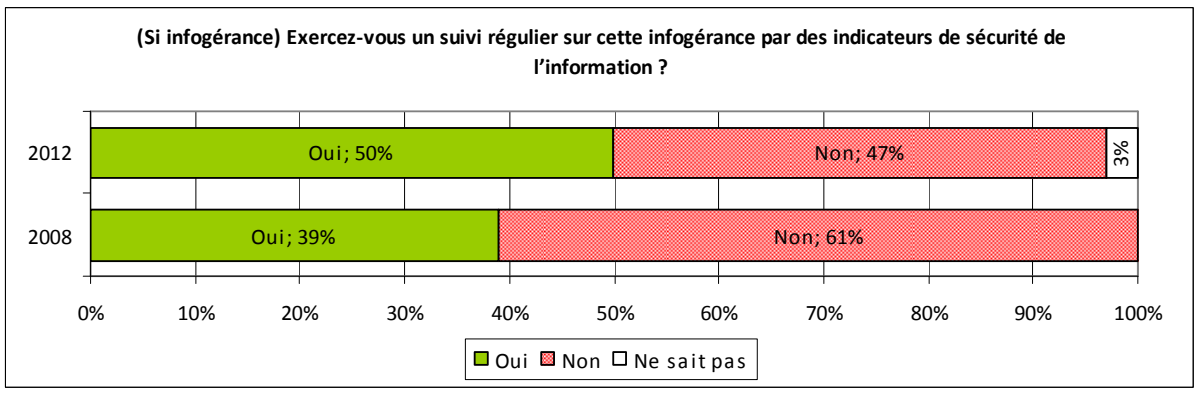

Figure 73 - Suivi de l'infogérance par des indicateurs de sécurité

Les services infogérés sont de plus en plus audités. Néanmoins, lorsque les choix et la gestion de certains services infogérés échappent au périmètre de la DSI, celle-ci déplore le fait de ne pas pouvoir faire de tests de vulnérabilités.

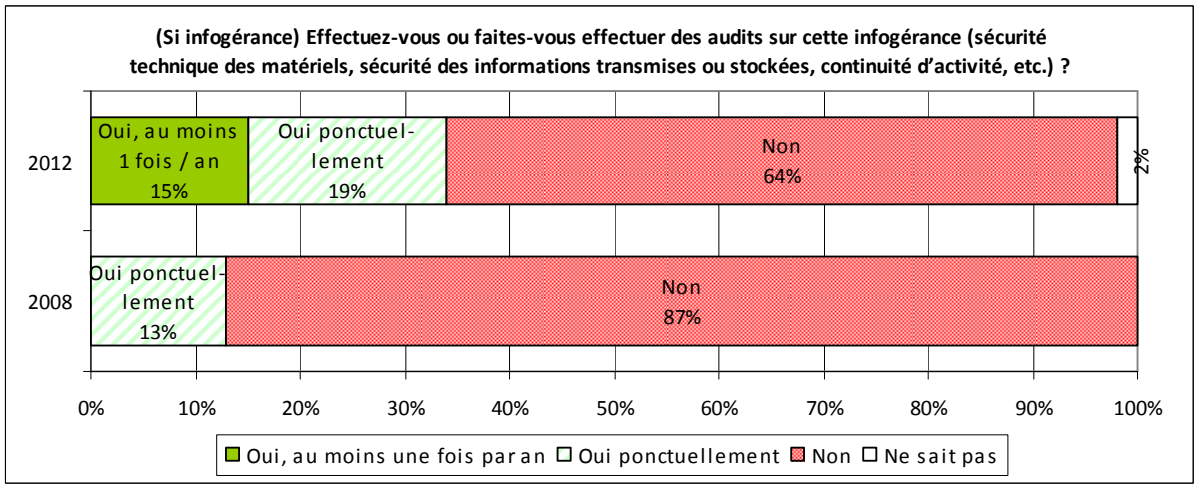

Figure 74 - Réalisation d'audits sur l'infogérance

Pour cette édition, notre questionnaire s'est intéressé au monde du Cloud (« informatique dans le nuage »). Si la démarche existe, elle est parfois subie (service de stockage en ligne grand public) et pas forcément maîtrisée. La « mise en Cloud » n'est pas sans conséquence sur les budgets puisque dans ce cas, la collectivité ne récupère pas la TVA.

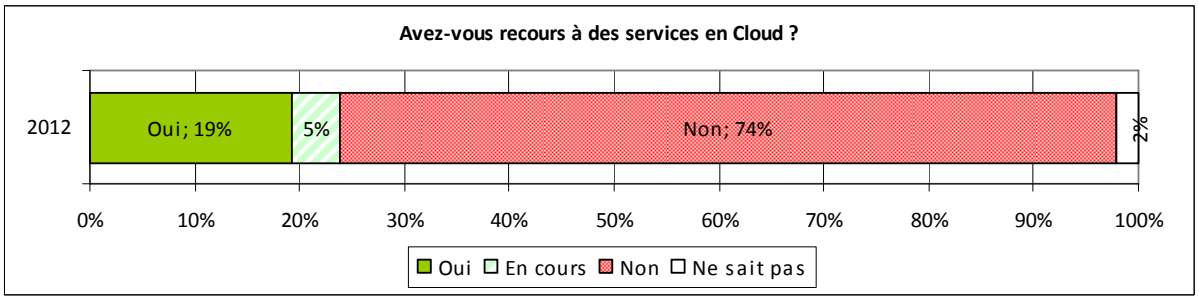

Figure 75 - Recours au cloud computing dans les collectivités

Il s'agirait avant tout de Cloud privé. Pour les services de Cloud public, les collectivités nous citent les services SMS, les échanges de fichiers mais aussi les transports scolaires. La mise à disposition de données publiques au travers du Cloud, l'Open Data, est en bonne voie mais la démarche est peu structurée.

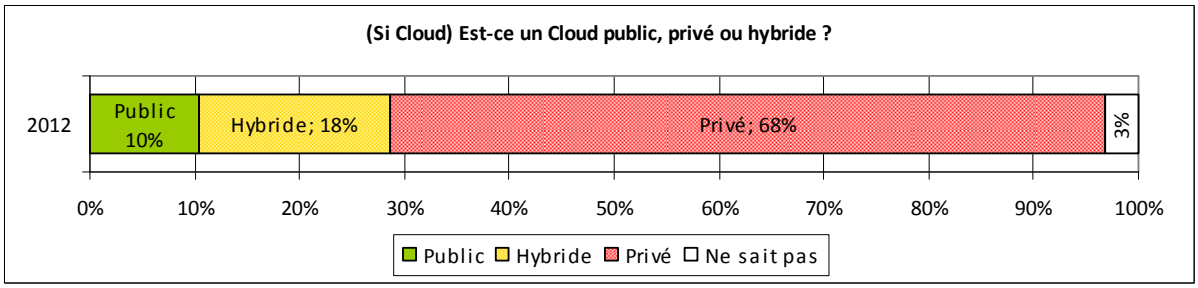

Figure 76 - Cloud public, privé ou hybride dans les collectivités

Thème 11 : Contrôle d'accès

Nette progression de l'authentification par certificat numérique

Le contrôle des accès logiques est abordé sous trois dimensions : les moyens d'authentification forte, la manière de gérer et mettre en œuvre les droits d'accès des utilisateurs, les systèmes de contrôle d'accès centralisés et d'authentification unique.

Afin de comparer avec la situation 2008 qui n'avait pas la même échelle, les propositions de 2008 ont été regroupées en : « largement utilisé » pour « usage généralisé » et « expérimenté ou envisagé » pour « usage partiel ».

Alors que l'authentification forte par certificat électronique sur support matériel marque le pas, nous notons un regain d'intérêt pour l'authentification par certificat électronique logiciel – peut être en lien avec les obligations légales – Marchés publiques, HELIOS, ACTES, etc. Cette tendance est plus marquée dans les villes, les départements et les régions.

L'authentification forte par calculette effectue également une belle progression. C'est plutôt dans les agglomérations et les villes où son utilisation à tendance à se généraliser

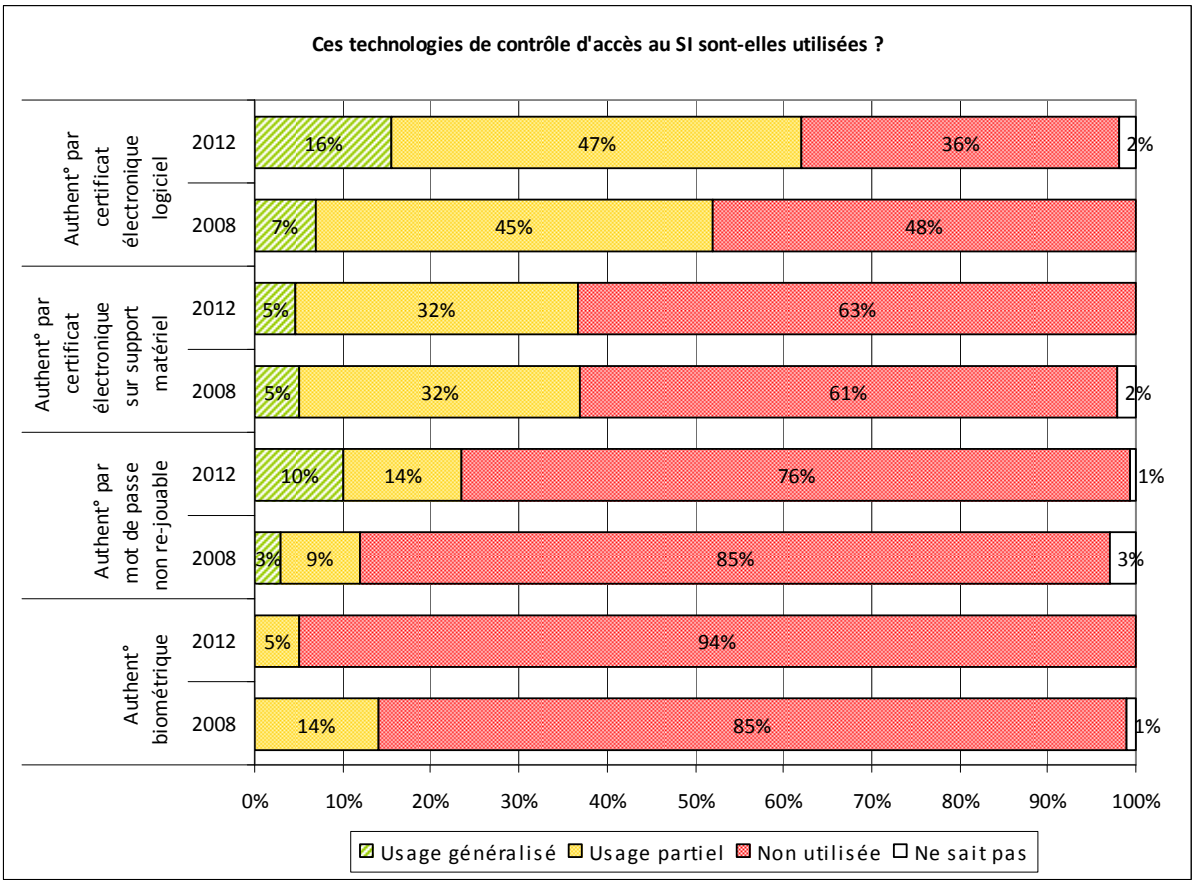

Figure 77 - Technologies de contrôle d'accès au SI utilisées dans les collectivités

Contrôle d'accès centralisé

Les systèmes de contrôle WebSSO et SSO maintiennent leur progression dans les collectivités. Ici encore, les villes, les Conseils Généraux et Régionaux utilisent complètement ou partiellement ces technologies dans 4 à 5 cas sur 10 pour le SSO et dans 3 à 4 cas sur 10 pour le WebSSO.

Les intercommunalités sont plutôt frileuses. Elles n'utilisent ces technologies que dans 1 (WebSSO) à 2 (SSO) cas sur 10.

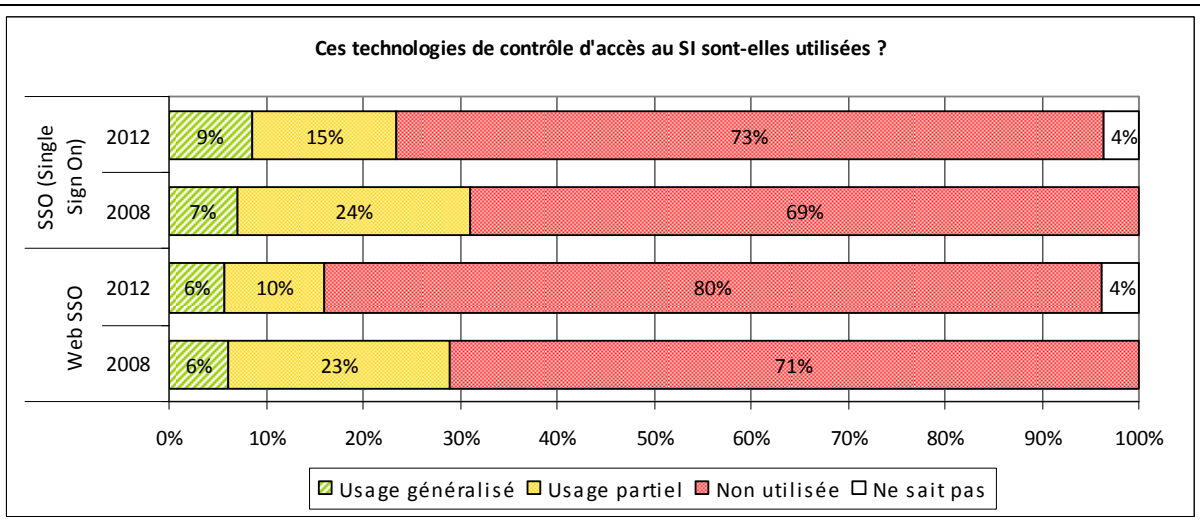

Figure 78 - Technologies de contrôle d'accès centralisé

Gestion des habilitations : un manque d'intérêt

A peine 3 collectivités sur 10 ont mis en place une gestion des droits par rôle ou profil métier. Ici encore, il y a une assez grande disparité. C'est une mairie sur 2 et plus de 3 Conseils Généraux et Régionaux sur 10 qui ont mis en place ces outils, contre 1 sur 4 pour les intercommunalités.

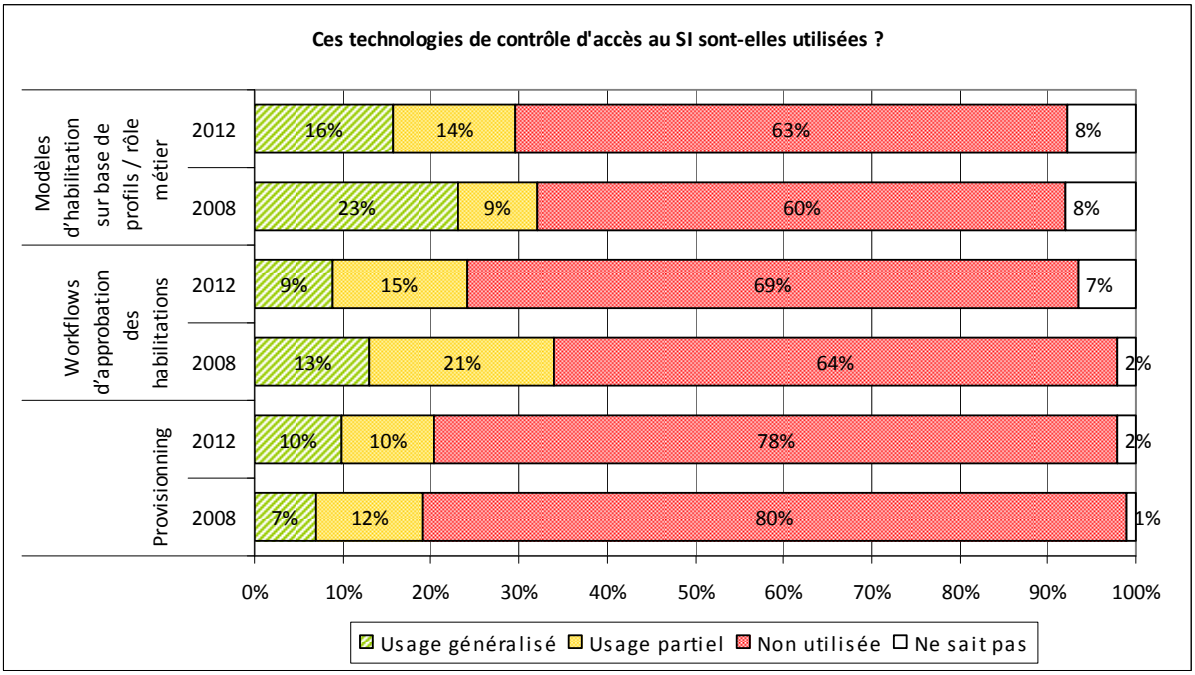

Figure 79 - Gestion des habilitations dans les collectivités

Logiquement, la mise en place d'un workflow de validation des habilitations suit la même courbe, avec une différence par rapport à 2008 plus marquée (perte de 10 points) mais une répartition hétérogène – près d'un conseil général ou régional et d'une ville sur 2 en font un usage généralisé ou partiel.

Le provisionning est en faible croissance, principalement tiré par les Conseils Généraux et Régionaux qui l'utilise dans 50 % des cas. Cela peut s'expliquer du fait que ces collectivités ont du faire face depuis 2008 à l'arrivée importante de nouveaux agents suite aux transferts de compétences.

Ces outils s'accompagnent de procédure formelle de création, modification et suppression de comptes utilisateurs nominatifs dans 6 collectivités sur 10 et même dans 8 villes ou Conseils Généraux et Régionaux sur 10. Ces procédures s'appliquent à tous les comptes dans 60 % des cas y compris les comptes administrateurs.

Des règles de constitutions et de péremption des mots de passe existent dans 1 collectivité sur 2. Elles sont systématiques dans un cas sur 3. Ici encore, les villes, les Conseils Généraux et Régionaux se démarquent, puisque les règles sont systématiques dans une ville sur 2 et 6 Conseils Généraux et Régionaux sur 10.

Thème 12 : Acquisition, développement et maintenance du S.I

Que les solutions soient directement développées en interne ou via des prestataires, la sécurité fait partie intégrante de leur acquisition, leur développement et de leur maintenance.

Les vulnérabilités étant évolutives, il convient de mettre en place une veille et des processus de mise à jour particuliers.

Si la veille en vulnérabilités est toujours présente et empirique, il reste quand même un bon tiers des collectivités n'ayant pas de pratique particulière.

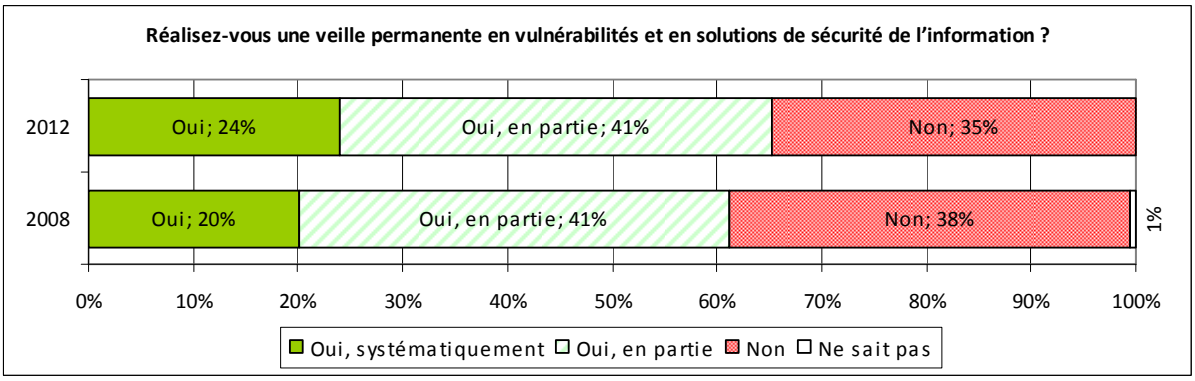

Figure 80 - Veille et gestion des vulnérabilités dans les collectivités

Un point étonnant, concerne la gestion des patchs où l'on note un net recul des pratiques.

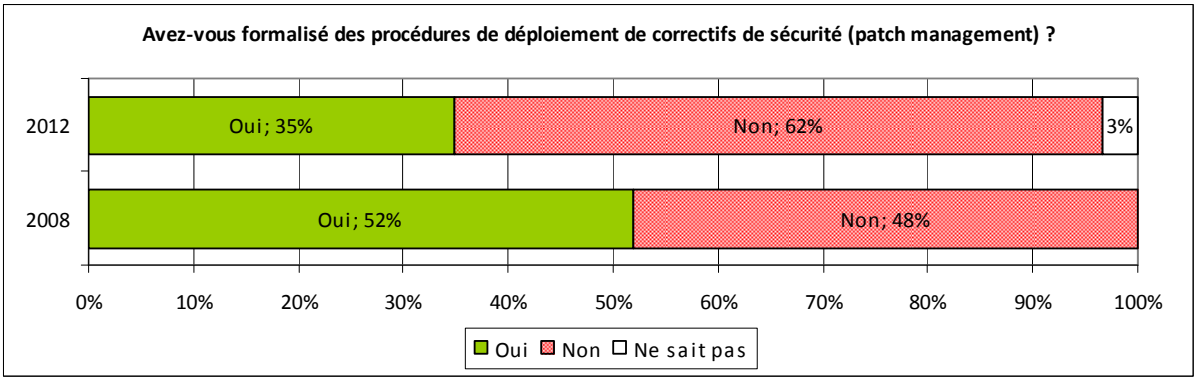

Figure 81 - Procédures formalisées de déploiement de correctifs de sécurité

Il est à noter malheureusement que ces politiques semblent influencer les collectivités sur leur réactivité lors de la découverte d'incidents. Là où, en 2008, nous avions plus des 2 tiers capables de réagir dans la journée sur un incident, nous avons maintenant une réactivité approchant les 50 % sur 3 jours.

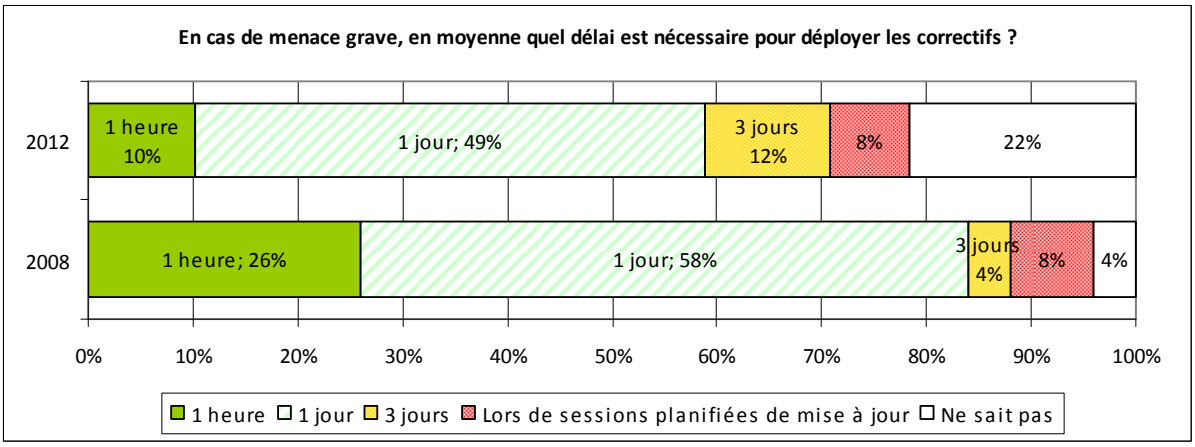

Figure 82 - Délai de déploiement des correctifs de sécurité

Concernant les développements, les collectivités déclarent pour 5 % d'entre-elles avoir mis en place des cycles de développements sécurisés

Thème 13 – Gestion des incidents de sécurité

Une progression dans la prise en compte des incidents par les collectivités

Les collectivités territoriales investissent dans une meilleure appréhension des incidents de sécurité, avec des cellules de traitement de mieux en mieux organisées. L'étude révèle une progression dans l'évaluation des impacts financiers des incidents.

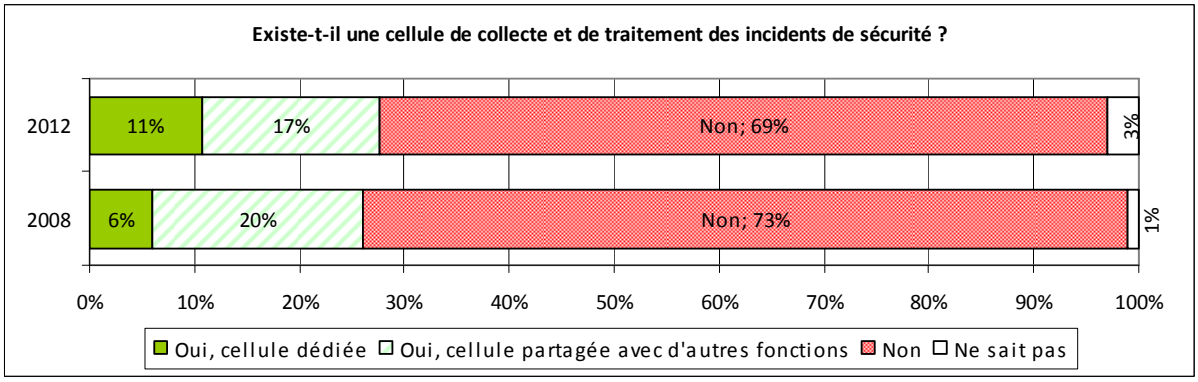

Figure 83 - Existence d'une cellule de collecte et de traitement des incidents de sécurité

Recul global de la sinistralité mais progression des infections par virus

Les statistiques de sinistralité sont en net recul : conséquences des nouvelles mesures ou manque de traçabilité ? Les pertes de services essentiels, les infections virales et les pannes d'origine interne représentent toujours les principales causes d'incidents de sécurité. Ceux liés aux fraudes, sabotages et intrusions représentent un total de 6 % des sinistres identifiés.

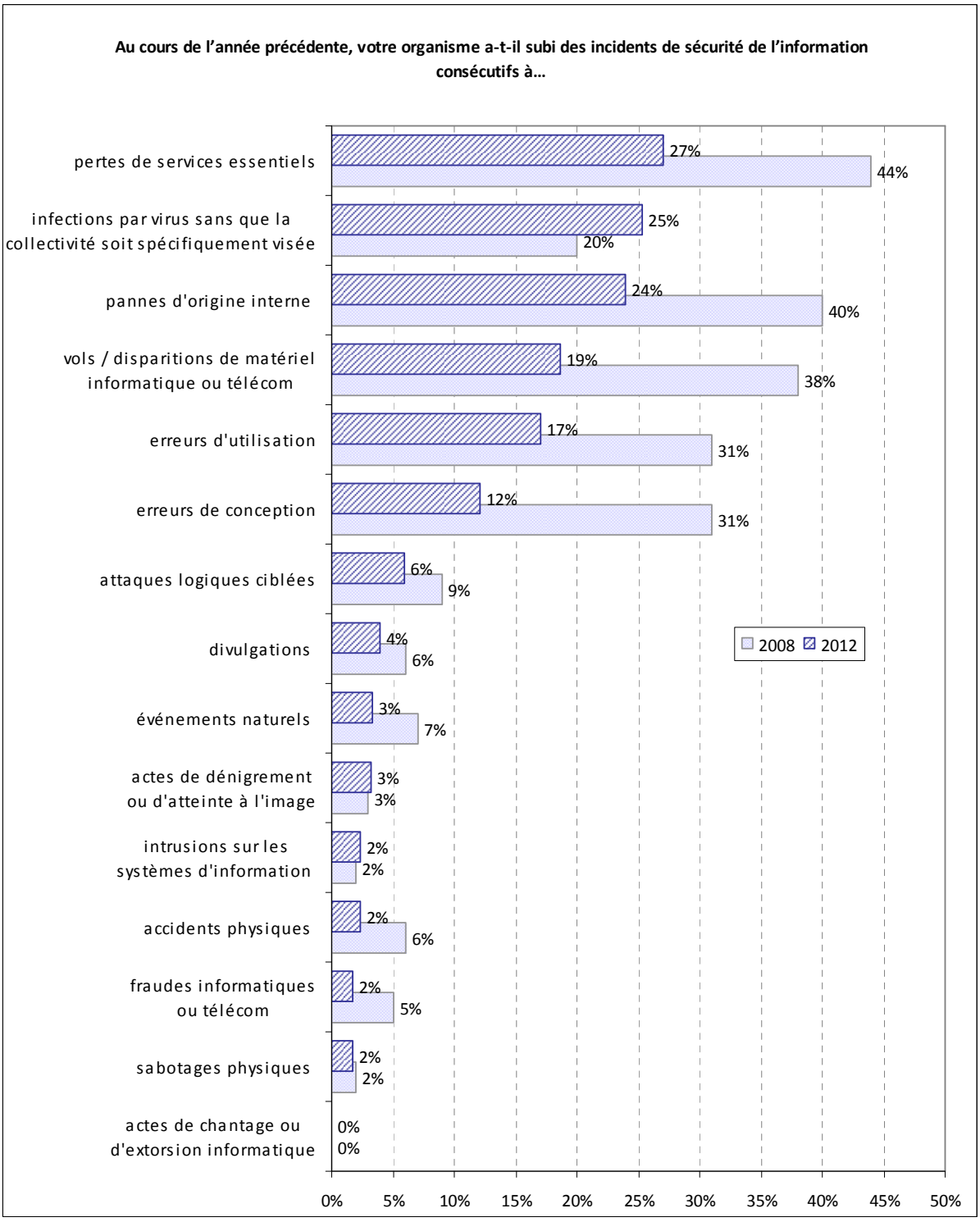

Figure 84 - Typologie des incidents de sécurité pour les collectivités

Thème 14 – Gestion de la continuité d'activité

L'enquête montre, qu'en matière de gestion de la continuité d'activité, les Collectivités sont très en retrait par rapport aux entreprises.

Pour preuve, plus d'une Collectivité sur 2 ne dispose d'aucun processus de gestion de la Continuité d'activité. Plus surprenant encore, sur l'aspect indisponibilité des systèmes informatiques, seulement 42 % d'entre-elles le prennent en compte.

Un quart des Collectivités considèrent les deux scénarios : locaux et agents.

Enfin, on peut se poser la question de ce que feraient les 87 % des Collectivités qui négligent le scénario d'une panne électrique ou d'un opérateur essentiel.

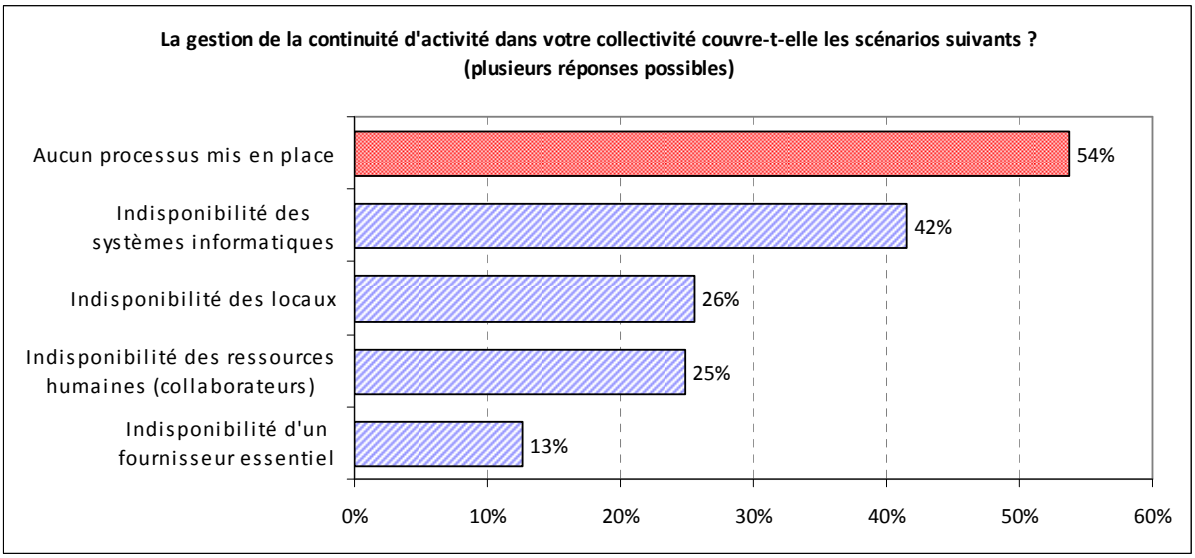

Figure 85 - Couverture des scénarios de gestion de la continuité dans les collectivités

Un quart des Collectivités ont déjà un Bilan d'Impact sur l'Activité. Ces résultats sont intéressants à double titre ; on note une forte prise en compte (90 %) de l'étape d'un BIA qui devrait se traduire par une amélioration de la couverture des scénarios dans les prochaines années.

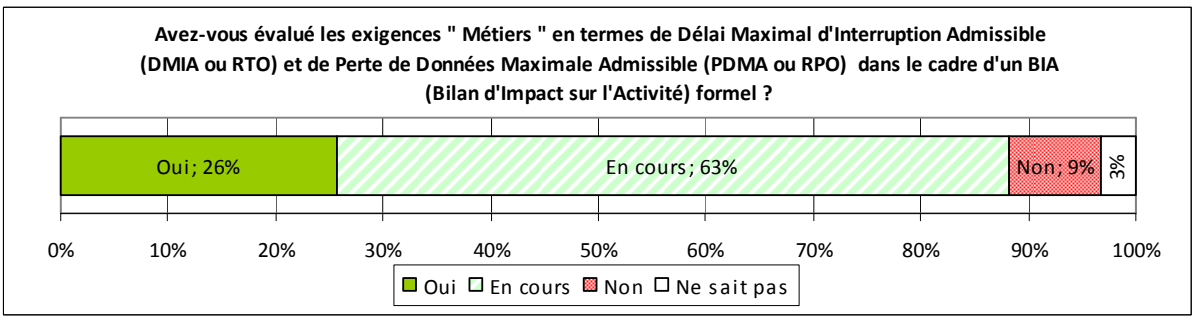

Figure 86 - Evaluation des exigences métiers dans le cadre du bilan d'impact sur l'activité

Plus de la moitié des collectivités ne teste pas son plan de continuité. Cette pratique est faiblement suivie par manque de ressources pour réaliser les tests. Si le processus du BIA se formalise, il devient nécessaire d'allouer des ressources pour le maintien en conditions opérationnelles du PCA.

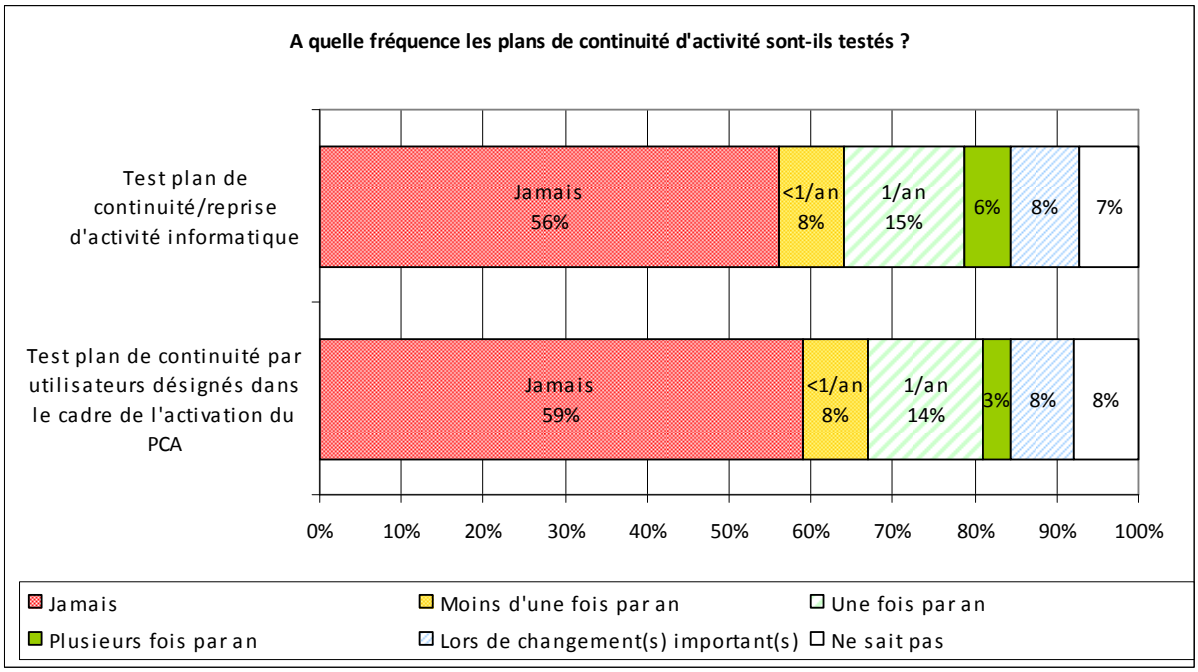

Figure 87 - Fréquence des tests des plans de continuité

Thème 15 Conformité

Ce thème aborde les éléments liés à la conformité sous 3 aspects :

- la conformité avec la loi « Informatique et Libertés »,
- l'audit des Systèmes d'Information,
- l'utilisation de tableau de bord.

❖ Conformité avec la loi « Informatique et Libertés »

Concernant la conformité aux obligations de la CNIL, une baisse de 8 points s'est opérée en 2012, par rapport à 2008. S'agit-il d'une prise de conscience plus aigüe des exigences de la CNIL ? Cela témoigne-t-il d'une plus grande « sensibilité », favorisée par les actions de contrôle menée par la CNIL ?

Probablement, et les exigences du RGS (Référentiel Général de Sécurité) ont vraisemblablement suscité un regard plus attentif à certaines exigences communes.

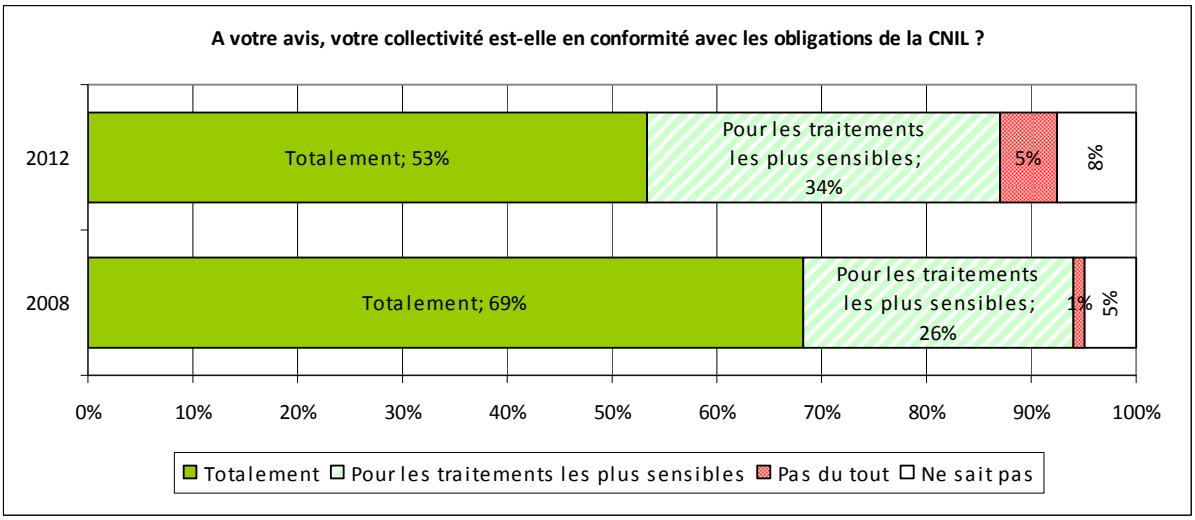

Figure 88 - Conformité CNIL des collectivités

Une partie des intentions de 2008 se sont concrétisées. Nous constatons aujourd'hui 39 % de Correspondants CNIL nommés ou prévus (décision prise) par rapport à 37 % en 2008. Cette évolution de 2 points masque une forte disparité entre les Communautés et les autres Collectivités.

Sur cet aspect également les Conseils Généraux et Régionaux sont en avance (44 % en place). Les Communes expriment une nette intention de satisfaire à cette exigence : 35 % de CIL sont nommés et 17% prévus et décidés.

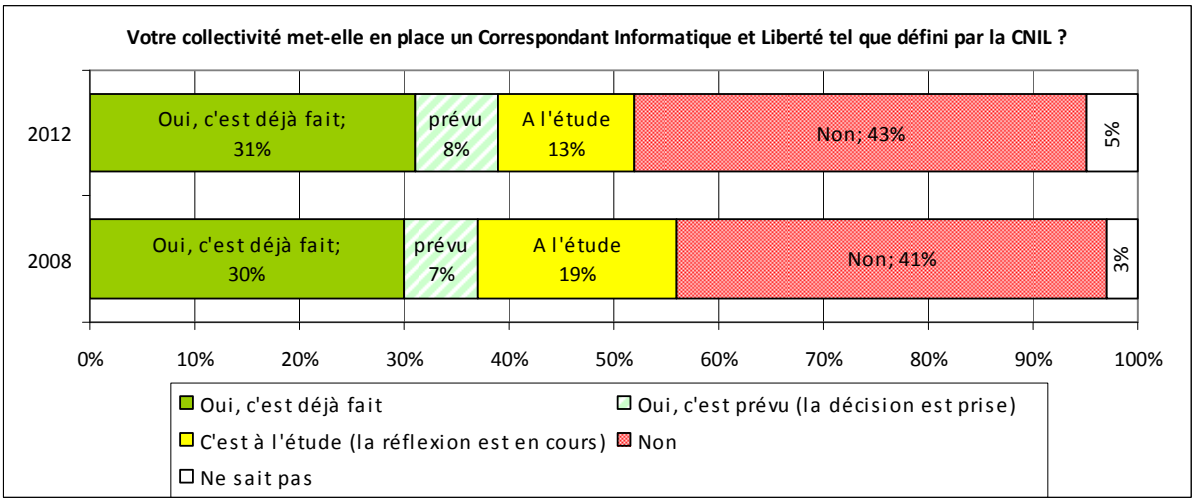

Figure 89 - Existence d'un Correspondant Informatique et Liberté dans les collectivités

Les Conseils Généraux et les Conseils Régionaux témoignent d'une plus grande connaissance de leurs obligations légales : 45 % ont répondu « oui ».

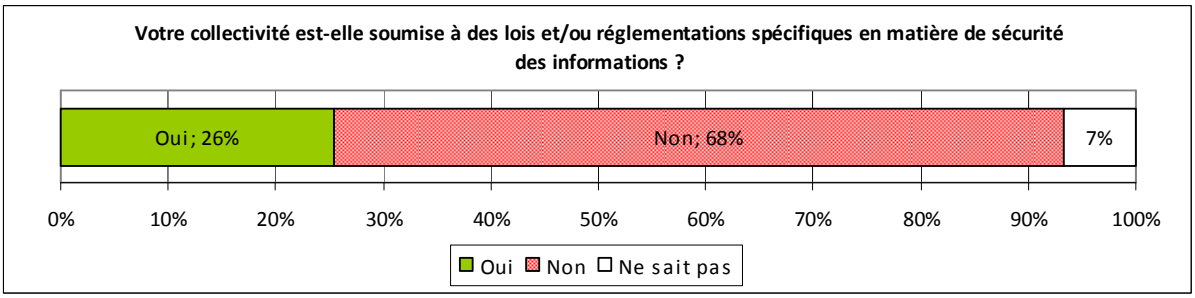

Figure 90 - Réglementations spécifiques en matière de sécurité de l'information

Malgré le décret paru en 2010 concernant le RGS (Référentiel Général de Sécurité), seulement 37 % des Collectivités déclarent avoir pris en compte les obligations de conformité pour 2013. Ici encore, les chiffres montrent une grande disparité entre collectivités puisque les Conseil Généraux et Régionaux sont en cours de conformité à 59 % et les villes à 62 %.

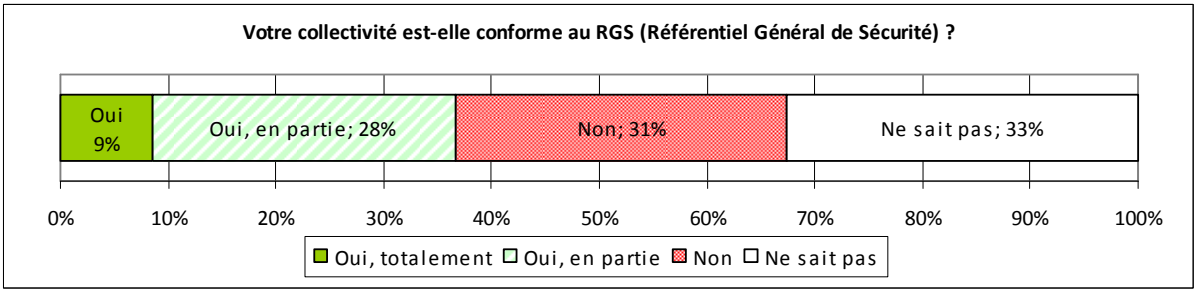

Figure 91 - Conformité des collectivités au RGS

❖ Les audits

Une pratique de l'audit qui ne s'améliore pas.

40 % de collectivités mènent un audit au moins une fois par an, alors que 56 % n'en mènent pas du tout. Ces chiffres sont les mêmes que lors de la dernière enquête.

Les audits réalisés traitent plus souvent des aspects techniques que des aspects organisationnels. Si les chiffres sont deux fois plus importants qu'il y a 4 ans, la proportion entre les différents types d'audit est stable.

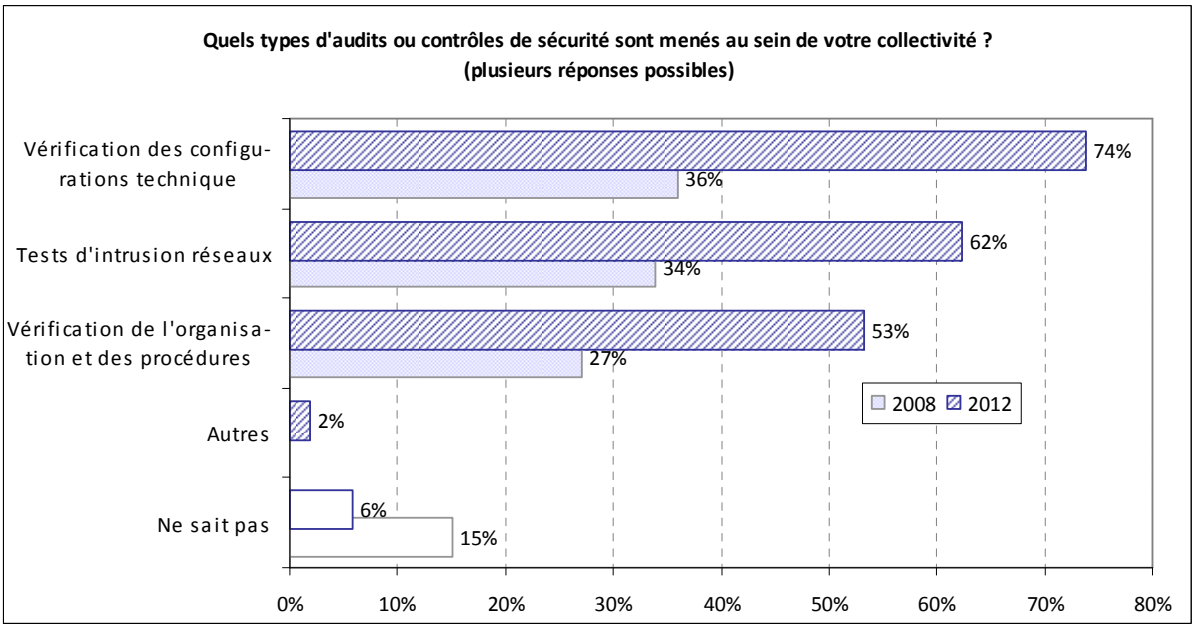

Figure 92 - Types d'audits ou de contrôles de sécurité réalisés

Ces audits sont une fois sur 2 motivés par la politique de sécurité ou des exigences contractuelles ou réglementaires. Les exigences du RGS se font sentir sur les projets « sensibles ». Les incidents déclenchent un audit deux fois plus qu'il y a 4 ans.

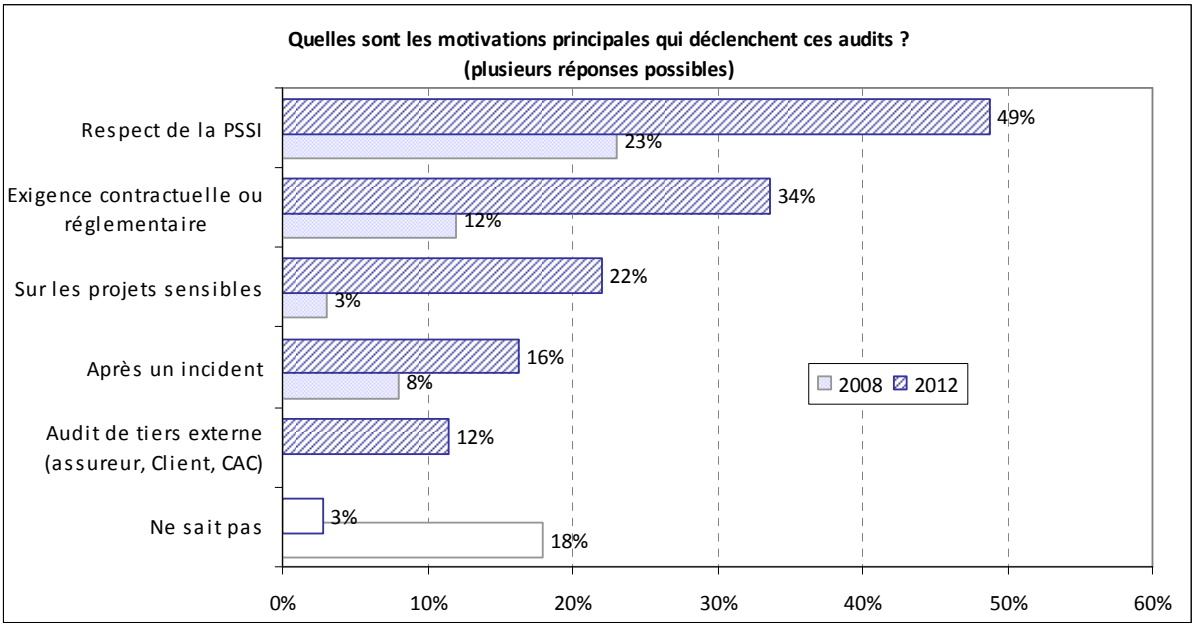

Figure 93 - Motivations pour la réalisation des audits

❖ Les tableaux de bord de sécurité

L'utilisation de tableau de bord n'a pas progressé depuis la dernière enquête. Ainsi, seule 1 collectivité sur 10 annonce avoir mis en place des outils de ce type. Il s'agit alors majoritairement des tableaux de bord opérationnels (74 % des cas), à des fins de pilotage de la fonction sécurité (40 %) et dans les intercommunalités et CG/CR de tableaux de bord stratégiques à destination de la Direction Générale ou des élus (40 %).

Bien que la population concernée soit faible (1 collectivité sur 10) et qu'il soit délicat d'en tirer une conclusion globale, il apparaît intéressant de présenter les types d'indicateurs mis en œuvre.

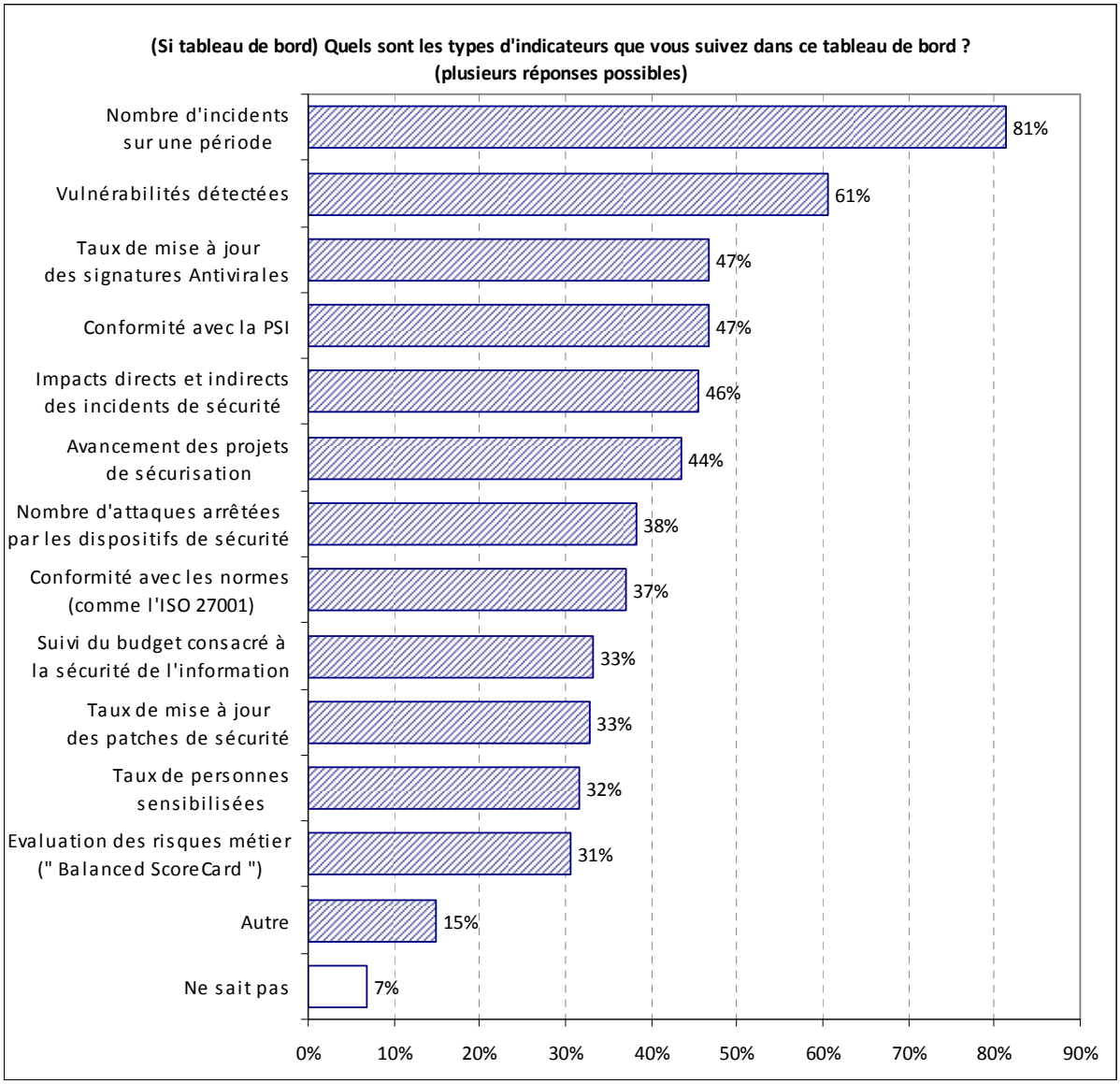

Figure 94 - Indicateurs suivis dans le tableau de bord

Internautes

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

Les internautes

Présentation de l'échantillon

Pour la troisième fois consécutive, le CLUSIF enquête sur les pratiques et les comportements des particuliers autour d'Internet à partir de leurs équipements personnels. Cette nouvelle étude a été réalisée début 2012 à partir d'un échantillon de 1000 personnes.

Comme pour les études précédentes, les opérations et les traitements statistiques des données ont été effectués par le cabinet spécialisé GMV Conseil qui s'est appuyé sur un panel d'internautes géré par Harris Interactive.

L'échantillon a été constitué de façon à représenter le plus précisément possible la réalité des internautes français à partir des données socioprofessionnelles dont dispose le cabinet.

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

Partie I – Profil des Internautes et inventaire informatique

En 2010, la précédente enquête montrait que la moitié des foyers interrogés ne possédait qu'un seul ordinateur familial, aujourd'hui le nombre d'unités par foyer a fortement augmenté.

Le nombre des foyers possédant trois ordinateurs ou plus est ainsi passé de 21 % à 27 %, avec une stabilisation du pourcentage des foyers en possédant deux. Les pourcentages des foyers possédant 1 ou 2 ordinateurs familiaux sont très proches maintenant et se répartissent de manière identique dans chaque classe d'âge.

On constate surtout une arrivée en masse des autres équipements :

- près de 50 % des foyers sont équipés d'un ou deux smartphones, près de 60 % chez les moins de 35 ans,
- dans environ 11 % des cas, les foyers possèdent au moins une tablette, pour toutes les tranches d'âge au dessus de 25 ans.

On arrive globalement à un nombre moyen d'équipements par foyer de 1,7 unité (ordinateur, smartphone, tablette).

Malgré cette diversité d'équipements, la très grande majorité des internautes (96 %) se connecte à Internet avec l'ordinateur familial.

Au domicile, les deux tiers des accès sont effectués au travers d'une connexion sans fil (wifi). Quant au mode de raccordement lui-même, c'est au travers d'une liaison haut débit (ADSL, câble ou fibre optique) pour près de 90 % des foyers.

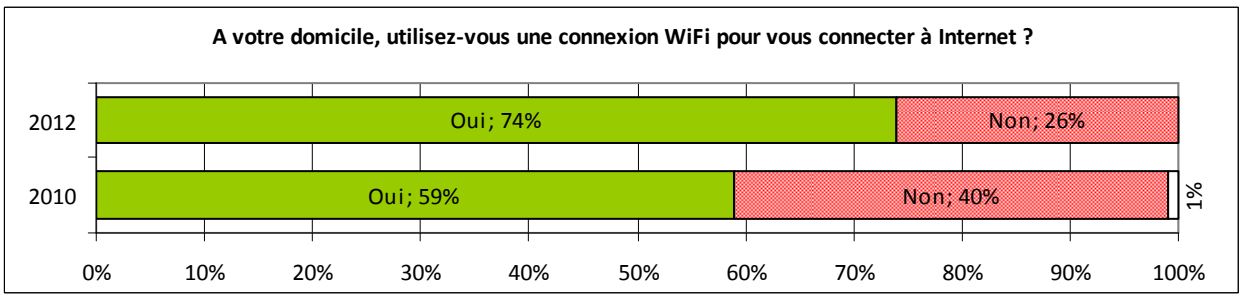

Figure 95 - Utilisation du Wifi

Toujours dans la sphère personnelle, les foyers qui possèdent des écrans de télévision et des consoles de jeux qui communiquent, les connectent effectivement à Internet à respectivement 35 % et 26 %. Viennent ensuite avec des pourcentages beaucoup plus faibles, la voiture, l'électroménager…

En dehors du domicile, 46 % des internautes se connectent très régulièrement à Internet.

Les services de stockage dans le nuage sont encore peu utilisés (16 % des foyers), la majorité s'en servant pour stocker des données personnelles (11 % des foyers).

Les équipements personnels (ordinateur, tablette ou smartphone) sont utilisés dans 42 % des foyers pour traiter des données liées à l'activité professionnelles (hors conversation téléphonique) sachant que seul 85 % de l'échantillon des internautes est concerné par le sujet.

Partie II – Perception et sensibilité aux menaces et aux risques

Une prise de conscience accrue des risques liés à Internet

La prise de conscience des Internautes quant aux risques liés à l'accès Internet depuis leur ordinateur est plus nette qu'il y a deux ans : ils sont maintenant 15 % contre 10 % à considérer qu'il n'y a aucun risque, et 30 % contre 23 % à considérer que les risques sont « importants » ou « très importants ». Certains, bien conscients des risques, ont fait l'effort d'augmenter leurs moyens de protection, de façon à diminuer le niveau de risque.

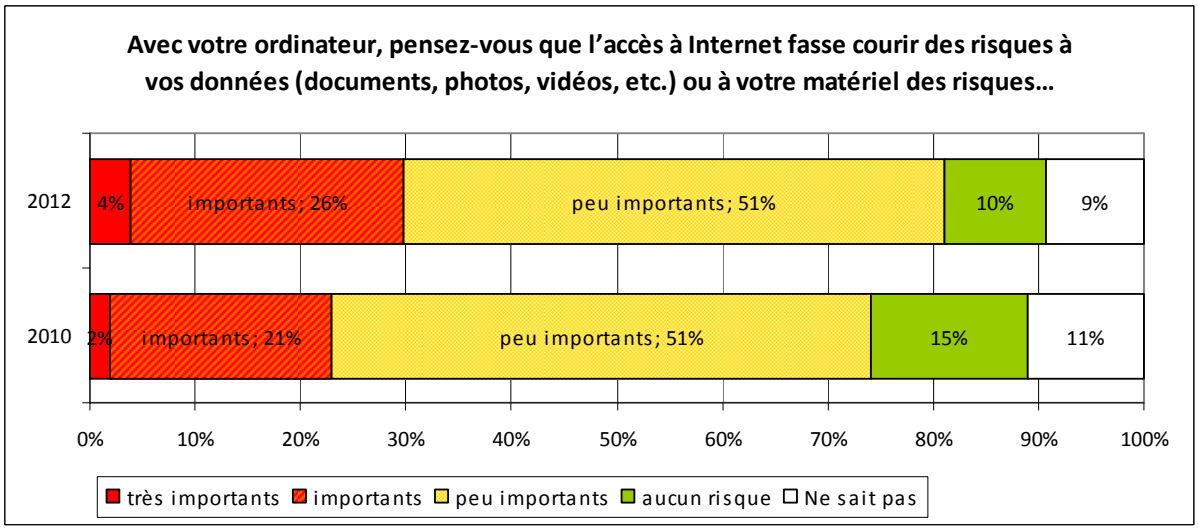

Figure 96 - Prise de conscience des risques

Pour les smartphones et les tablettes, le risque est perçu comme étant plus fort que sur les ordinateurs personnels

L'accès depuis un smartphone ou une tablette est perçu comme étant « un peu plus » ou « beaucoup plus » risqué pour 26 % des internautes, tandis que 31 % pensent que le niveau de risque est le même que sur un ordinateur.

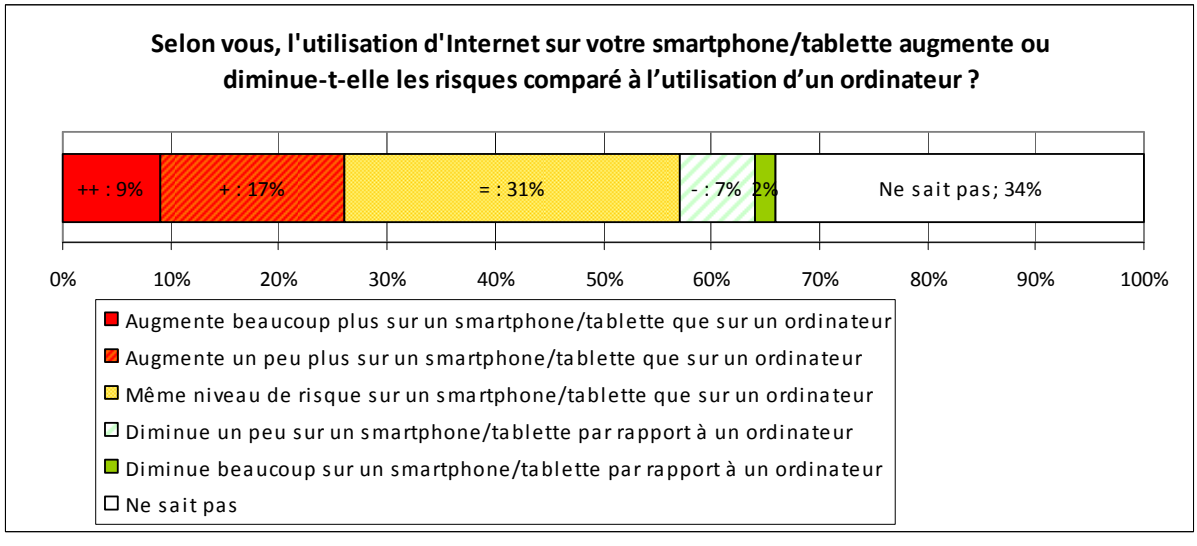

Figure 97 - Perception des risques sur smartphone et tablette par rapport à un ordinateur

La perception des risques auxquels les smartphones et tablettes sont exposés est élevée : 40 % des internautes pensent même qu'elle est en hausse, et autant pensent qu'elle est stable. L'utilisation de ces équipements apparaît globalement comme plus à risque que pour des ordinateurs personnels pour lesquels la perception, bien qu'en hausse nette depuis deux ans (de 20 à 32 %) reste inférieure.

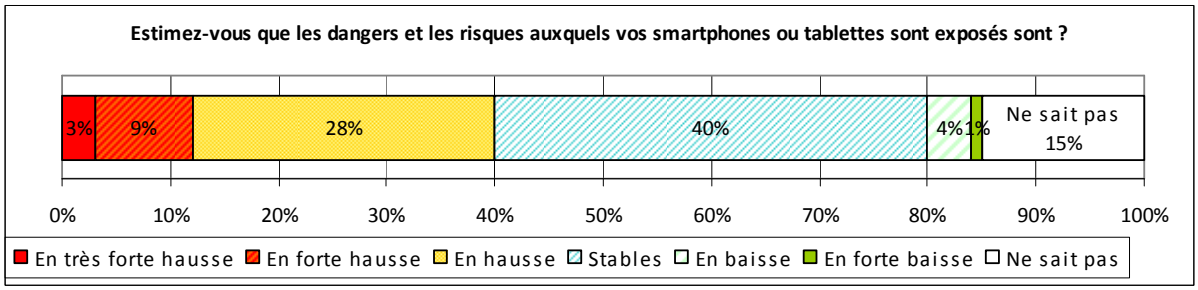

Figure 98 - Perception de l'évolution des risques pour smartphone et tablette

Vie privée sur Internet : des écarts générationnels marqués

Le degré de sensibilité aux dangers relatifs à leur vie privée sur Internet est variable : 19 % des internautes considèrent qu'elle est fortement en danger sur Internet contre 16 % lors de la précédente étude. Parmi eux, la génération Y des 15-24 ans apparait fortement sensibilisée : ils sont 27 % à percevoir un fort danger alors que les autres tranches d'âge sont moins de 20 % à le penser.

En revanche, 29 % des internautes considèrent désormais que leur vie privée n'est « pas du tout » ou « pas vraiment » en danger alors qu'ils n'étaient que 24 % il y a deux ans. Parmi eux, les 35-49 ans apparaissent comme percevant le moins les risques.

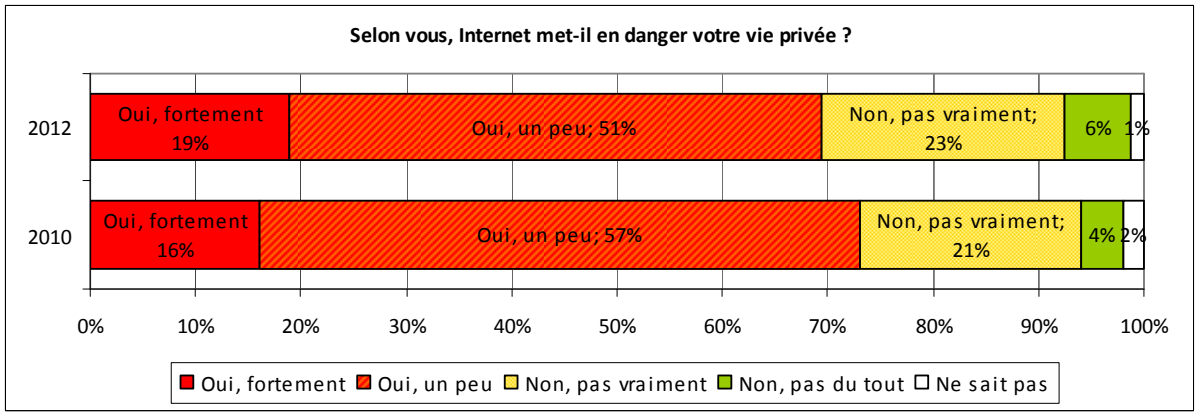

Figure 99 - Perception du risque par rapport à la vie privée

Stockage dans le nuage : un nouvel usage encore peu répandu

Dans l'ensemble, la moitié des internautes ne se prononce pas sur les risques liés à l'utilisation de service de stockage d'information dans le nuage. Parmi les internautes utilisateurs, 15 % sont plus confiants que dans un stockage local, contre 35 % qui pensent que les risques sont plus élevés dans le nuage et 32 % qui considèrent que le niveau de risque est équivalent.

Mineurs et Internet : un risque dont les internautes sont largement conscients

Le questionnaire s'enrichit cette année d'une question relative à la perception du danger que peut représenter Internet pour les mineurs.

On ne peut que se réjouir de ce qu'une grande majorité des internautes (77 %) considèrent qu'Internet représente un danger pour les mineurs, tous types de supports confondus (que ce soit sur un ordinateur, une tablette ou un smartphone).

La mobilité ne semble pas être perçue comme un facteur déterminant ou amplifiant le danger : seuls 7 % des internautes ont estimé qu'Internet représente un danger pour les mineurs, « surtout avec une tablette ou un smartphone ».

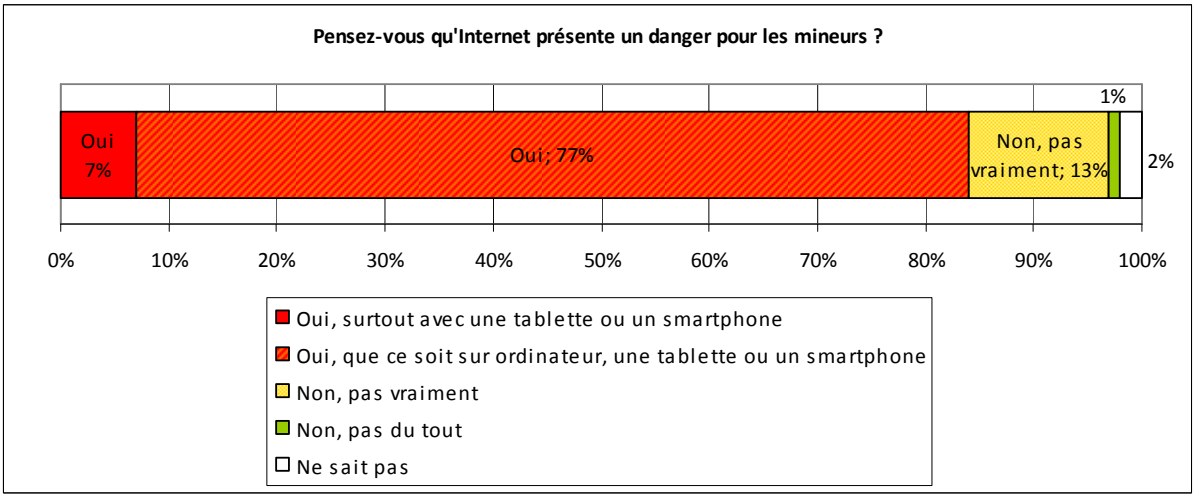

Figure 100 - Perception du danger d'Internet pour les mineurs

Les internautes ont majoritairement (84 %) conscience du danger que peut représenter Internet pour les mineurs.

Toutefois, ces bons chiffres sont à relativiser avec la proportion, encore importante, d'internautes qui considèrent qu'Internet ne représente « pas vraiment » ou « pas du tout » un danger pour les mineurs (14 %).

Le vol de données, un danger sous-estimé par les internautes ?

Seuls 34 % des internautes déclarent avoir perdu des données sur leur ordinateur au cours des 24 derniers mois. Plus précisément, seuls 3 % auraient perdu des données suite à un piratage, et pour 7 % d'entre eux, ce serait lié à une activité virale.

Ces résultats sont faibles face à l'accroissement observé par ailleurs du nombre de piratages et de corruption d'ordinateurs.

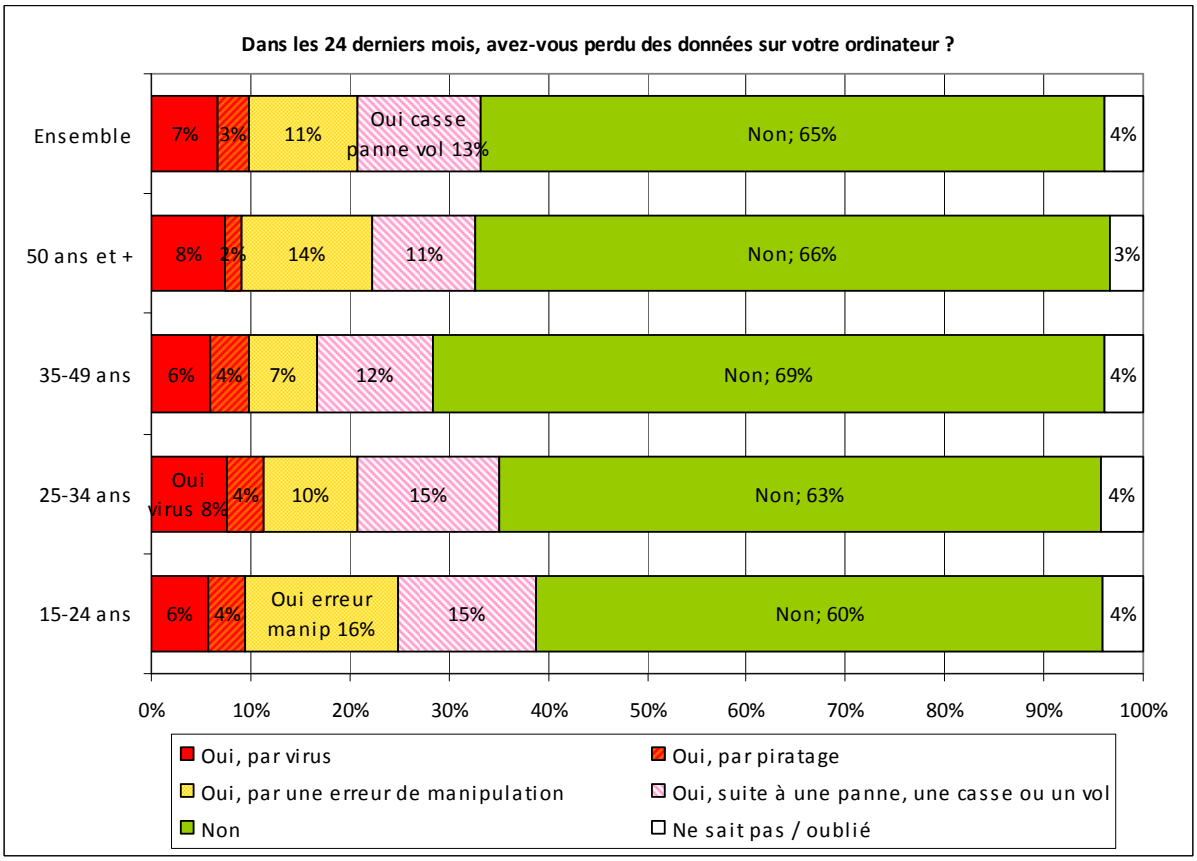

Figure 101 - Perte de données sur les ordinateurs

Ainsi, 65 % des internautes déclarent n'avoir subi aucune perte de données sur leur ordinateur durant ces 24 derniers mois.

Il est cependant difficile de distinguer les internautes n'ayant pas conscience des pertes de données subies (à leur insu) de ceux n'ayant effectivement pas subi de perte de données ! Ce résultat est à mettre en perspective avec la nature discrète et furtive, du piratage ou de l'activité d'un virus ou d'un malware, qui sont en conséquence rarement détectés.

Il confirme également la tendance observée dans l'étude 2010, selon laquelle la perception du risque d'intrusion par les internautes était en baisse.

L'erreur de manipulation et la panne sont quant à elles plus facilement perçues et signalées par les internautes. Ainsi, 11 % d'entre eux déclarent avoir subi une perte de données sur leur ordinateur suite à une erreur de manipulation et 13 % suite à une panne, une casse ou un vol.

Contre toute attente, l'âge n'influence que peu, voire pas, la perception de la menace en la matière.

Ainsi, et contrairement aux idées reçues, les « jeunes » et les « digital natives » (dans la tranche des 15-24 ans et des 25-34 ans) ne paraissent pas plus au fait d'éventuelles pertes de données faisant suite à des piratages ou à la présence de virus, que les plus « âgés » (35-49 ans et 50 ans et plus) !

Les chiffres sont en effet très homogènes : à titre d'exemple, tant les 15-24 ans que les plus de 50 ans sont entre 60 et 70 % à déclarer n'avoir connu aucune perte de données ; et seuls 6 % des 15-24 ans déclarent en avoir connu une sur leur ordinateur au cours des 24 derniers mois, contre 8 % pour les 50 ans et plus.

Une confiance maîtrisée ?

Au palmarès des situations susceptibles d'augmenter le plus fortement les risques, on trouve par ordre décroissant :

- l'absence d'anti-virus sur son ordinateur : pour 88 % des internautes, contre 91 % il y a deux ans.

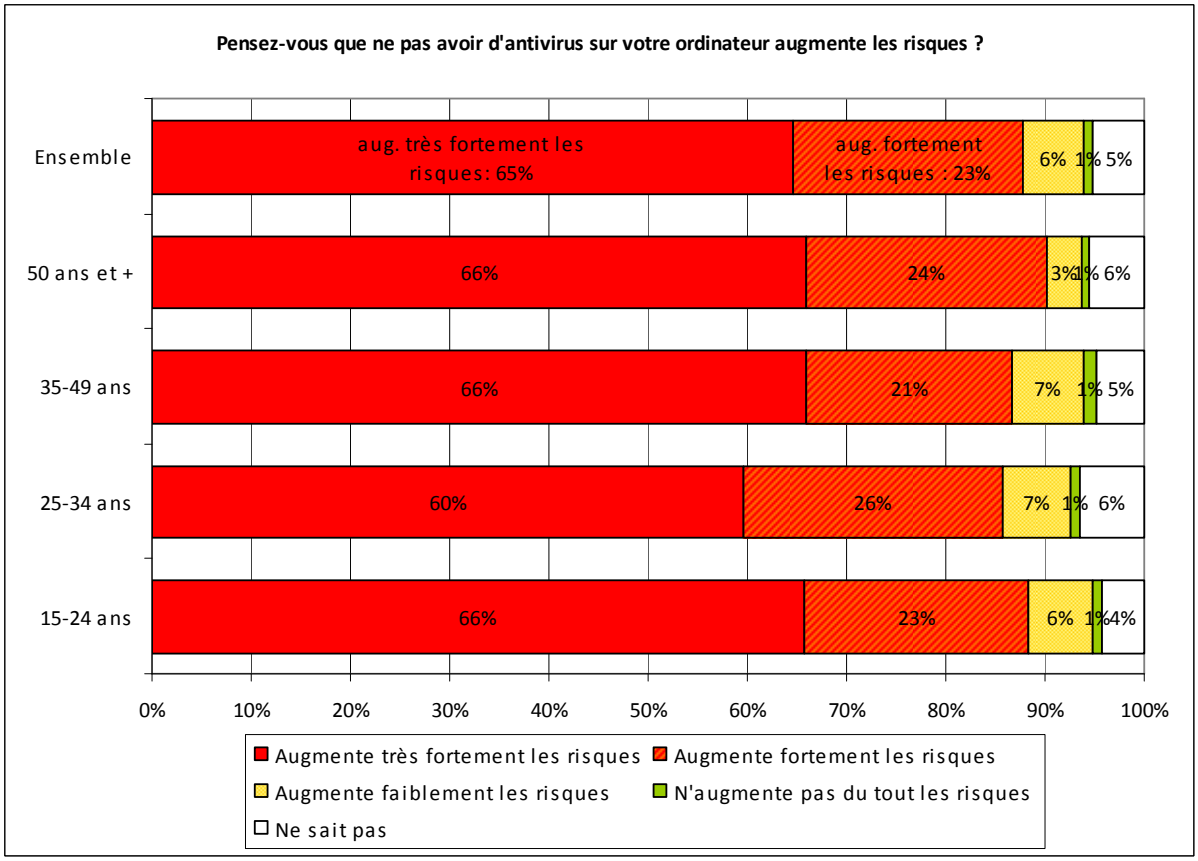

Figure 102 - Perception du risque « absence d'antivirus sur l'ordinateur »

- la divulgation de ses coordonnées personnelles sur des sites Internet : pour 80 % des internautes, sachant toutefois que 52 % des internautes font des achats en ligne par internet « souvent » à « très souvent », et 36 % « parfois »,
- l'absence de firewall (pare-feu) : pour 79 % des internautes,
- un anti-virus mais qui n'est pas à jour : pour 75 % des internautes, c'est-à-dire, un anti-virus qui n'est pas efficace contre les menaces récentes. A noter que les 15-24 ans sont beaucoup moins méfiants que les plus de 50 ans,
- le choix de mots de passe trop simples : pour 71 % des internautes,
- l'absence de sauvegardes des fichiers : pour 70 % des internautes, … qui se trouveront donc fort dépourvus lorsque la perte sera venue …

Plus de la moitié des internautes considèrent qu'il y a de nombreuses autres situations susceptibles d'augmenter les risques :

- pour les mots de passe : avoir le même sur plusieurs sites Internet ou ne pas en avoir sur son smartphone,
- télécharger des logiciels ou des bonus gratuits (24 % des internautes disent le faire « souvent » à « très souvent »), des utilitaires, des smileys, des fonds d'écran, des barres de navigation, des codes de contournement pour des jeux, des musiques ou des films en peer-to-peer, etc.,
- ne pas bien s'y connaitre en informatique,

- ne pas avoir d'anti-spam sur son ordinateur, les 15-24 ans étant beaucoup plus confiants que les plus de 50 ans,
- faire des achats en ligne avec son smartphone : un tiers des internautes déclare le faire, ce qui nécessite généralement la saisie des coordonnées bancaires. On notera que les 15-24 ans sont plus confiants que les plus de 50 ans, même si au total 15 % des internautes estiment ne pas savoir si un antivirus est nécessaire à la sécurité de leurs smartphones ou de leurs tablettes !,
- ne pas avoir d'anti-virus sur son smartphone ou sa tablette !,
- ne pas faire de copie de sauvegarde des données de son smartphone, les 15-24 ans étant encore une fois moins conscients des risques que les plus de 50 ans.

Mais quelques incertitudes, ou une confiance indue

Ainsi, certains risques sont très mal connus des internautes, par exemple :

- la nécessité d'avoir un système d'exploitation à jour, et de le maintenir dans cet état : en moyenne 12 % ne le sait pas,
- le danger de télécharger des applications depuis son smartphone ou sa tablette : si en moyenne 19 % ne le sait pas, on retrouve l'écart générationnel inversé : 26 % pour les plus de 50 ans, mais seulement 9 % pour les 15-24 ans, sans qui sont plus familiarisés avec ces outils,
- le danger de télécharger des musiques ou des films en peer-to-peer (eMule, BitTorrents, etc.) : pour environ 17 % des plus de 35 ans,
- ne pas avoir de système de protection électrique pour son ordinateur, comme un onduleur.

Enfin, cette étude montre que les internautes pêchent par excès de confiance quand il s'agit de smartphones ou de tablettes : ils ne sont que 38 % à penser que le téléchargement d'applications mobiles, d'utilitaires, de jeux ou autres, peut en augmenter les risques ! Pour les 15-24 ans, qui sont pourtant gros consommateurs de ces téléchargements, seuls 24 % le pensent.

Il y a de quoi frémir, quand on connait tous les cas de piratages ou de vols de données survenus sur des smartphones à l'aide d'applications infectées par des malwares !

Les pirates ont décidément encore de beaux jours devant eux …

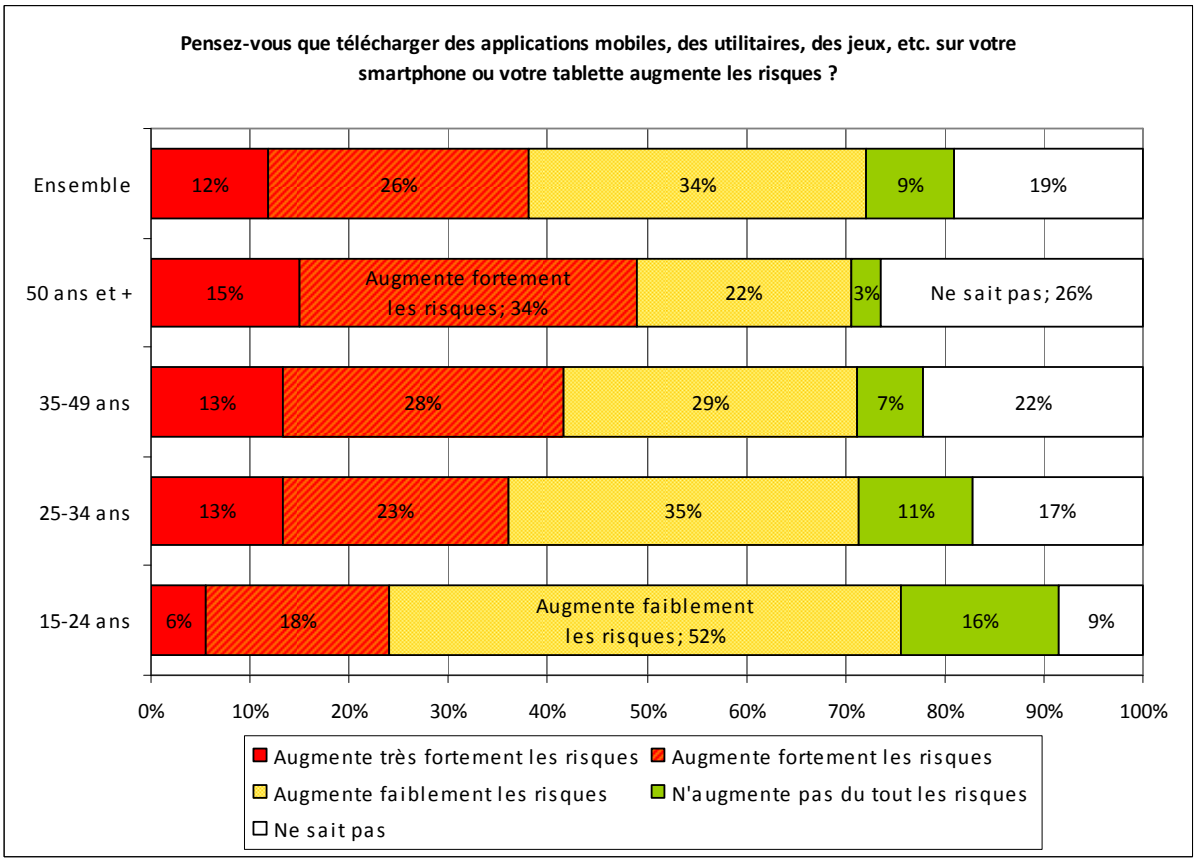

Figure 103 - Perception du risque lié au téléchargement d'applications sur smartphone et tablette

…Et si l'on considère que cette étude révèle qu'environ un tiers des internautes utilise leur ordinateur ou leur smartphone personnel pour des usages professionnels, il apparait évident que la sensibilisation des salariés aux principes de sécurisation et à l'application des règles qui en découlent sont nécessaires !

Partie III – Usages des internautes

Utilisation de l'ordinateur familial

L'enquête confirme bien que l'ordinateur familial est utilisé uniquement pour un usage privé par 68 % des internautes, 31 % faisant un usage mixte et 1 % un usage strictement professionnel. On note que l'usage personnel est pour toutes les tranches d'âge, supérieur à 50 % mais que l'usage mixte diminue avec l'âge pour une moyenne globale de 31 %.

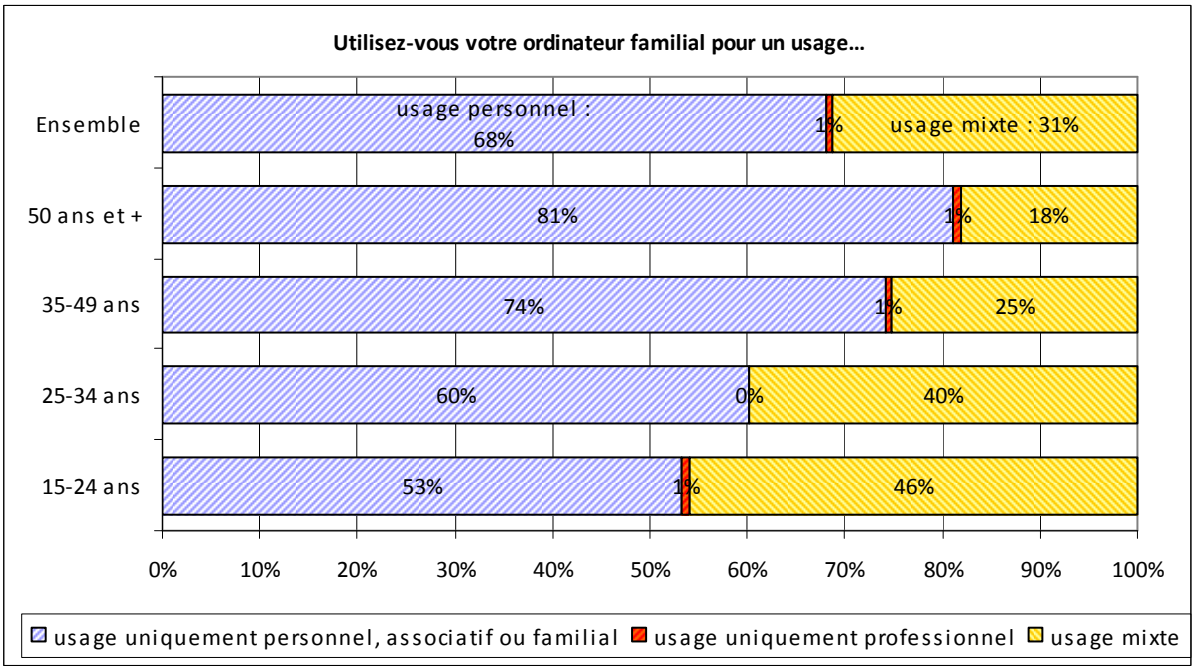

Figure 104 - Types d'usage de l'ordinateur familial

L'utilisation d'un ordinateur familial pour réaliser des travaux professionnels apparaît comme une solution de secours ou de confort.

Depuis l'enquête 2010, on note toutefois une augmentation de l'usage mixte dans la tranche d'âge 25-34 ans (+15 points) qui se situe aujourd'hui au même niveau que la tranche 15-24 ans.

Utilisation de smartphone et de tablette personnels

Les smartphones et tablettes personnels sont tout autant utilisé que l'ordinateur familial.

La population des 25-34 ans a une utilisation mixte plus importante que les autres tranches.

Le taux de non équipement est relativement homogène par tranche d'âge.

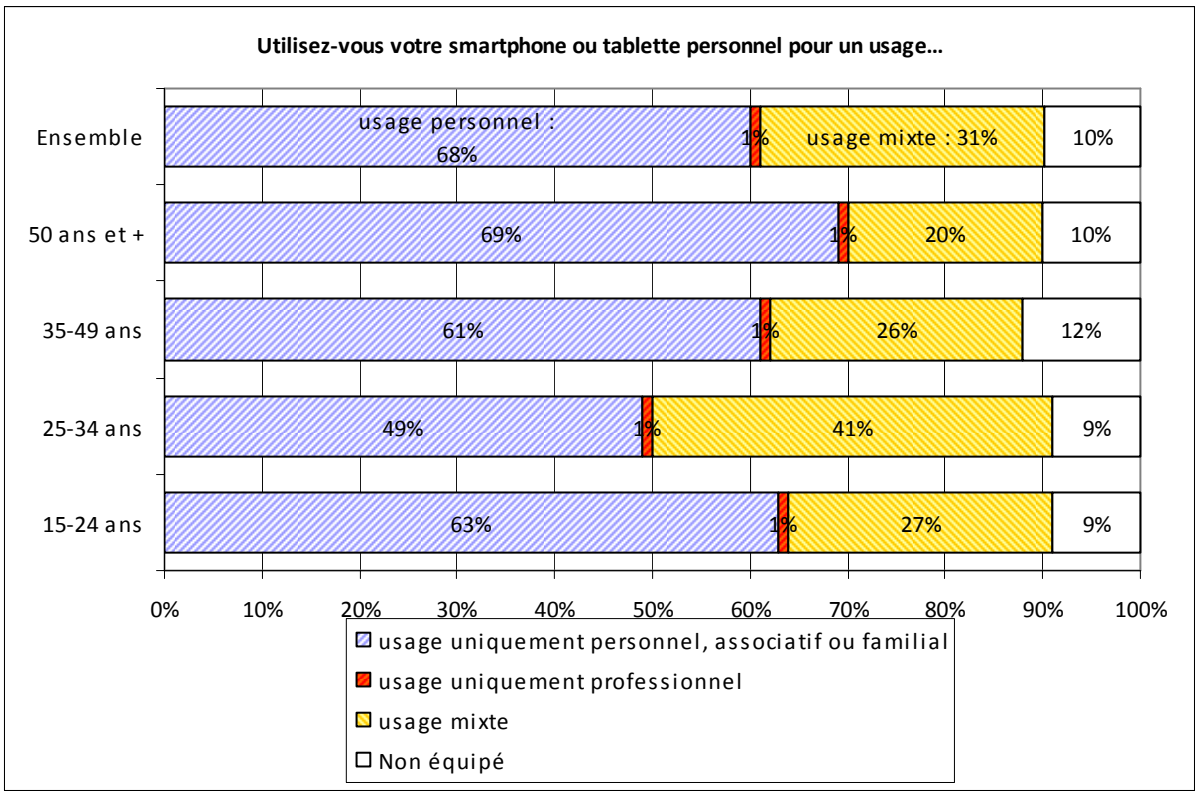

Figure 105 - Type d'utilisation des outils de mobilité personnels

L'utilisation d'un ordinateur professionnel

L'enquête montre que l'ordinateur professionnel est utilisé uniquement pour un usage professionnel par 34 % des internautes, 25 % en faisant un usage mixte, et même jusqu'à 38 % pour les 25-34 ans, et 7 % un usage non professionnel.

34 % des internautes n'utilisent pas d'ordinateurs dans le milieu professionnel. Ce taux était de 56 % en 2010, soit une augmentation d'équipement de 40 % !

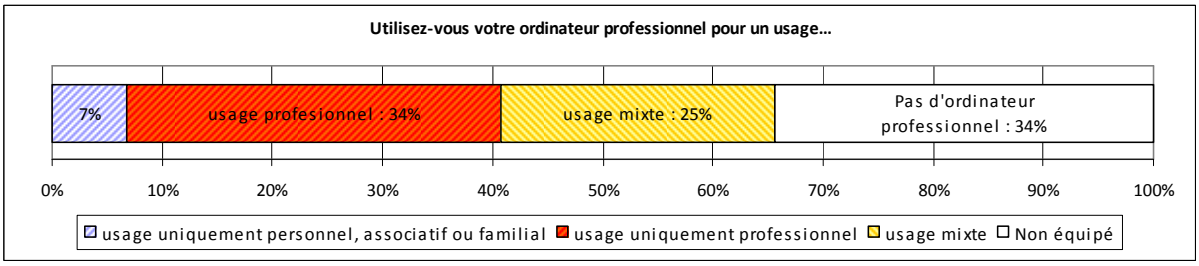

Figure 106 - Types d'usage de l'ordinateur professionnel (ensemble de la population)

Quand les internautes sont dotés d'ordinateurs professionnels, ils ne sont utilisés à usage exclusivement professionnel que dans 1 cas sur 2.

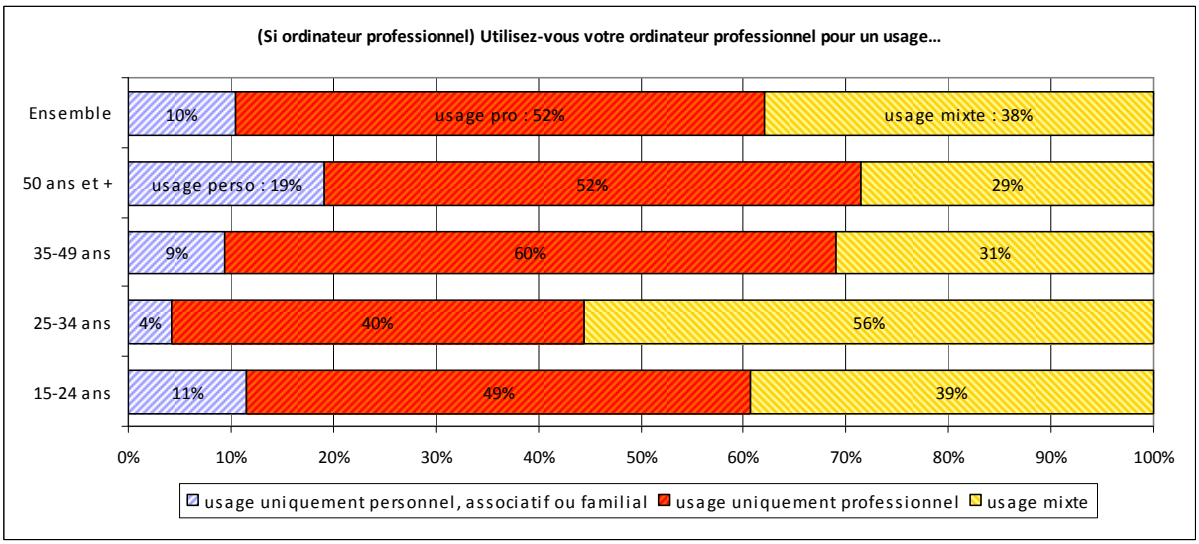

Figure 107 - Types d'usage de l'ordinateur professionnel (population équipée)

Utilisation d'un smartphone professionnel ou d'une tablette professionnelle

Quand les internautes en sont équipés (20 % des cas), le taux d'utilisation professionnel est de 35 %, mais l'utilisation à un usage uniquement personnel est de 20 % (sic) et mixte de 45 %.

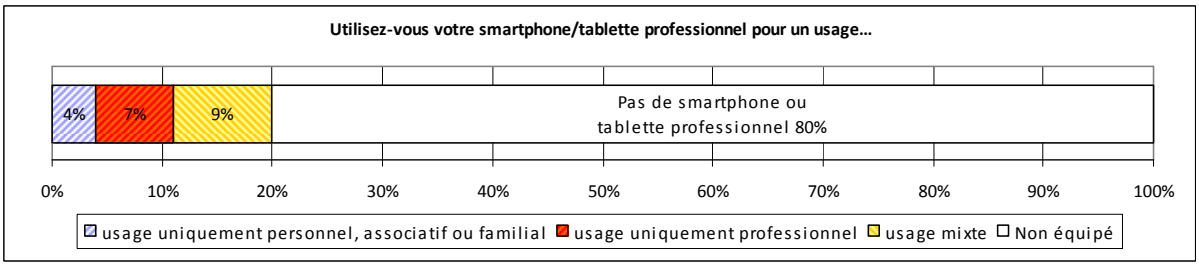

Figure 108 - Type d'utilisation des outils de mobilité professionnels

Usages sur Internet

Même si l'on constate un léger recul en 2 ans, Internet sert principalement aux internautes pour surfer (89 %) et envoyer des mails (90 %).

Depuis la dernière enquête, les internautes dialoguent moins par messagerie instantanée (62 % contre 74 %) mais utilisent plus les logiciels de téléphonie sur Internet (38 % contre 54 %). Ces derniers cas d'utilisation sont souvent l'affaire d'habitués.

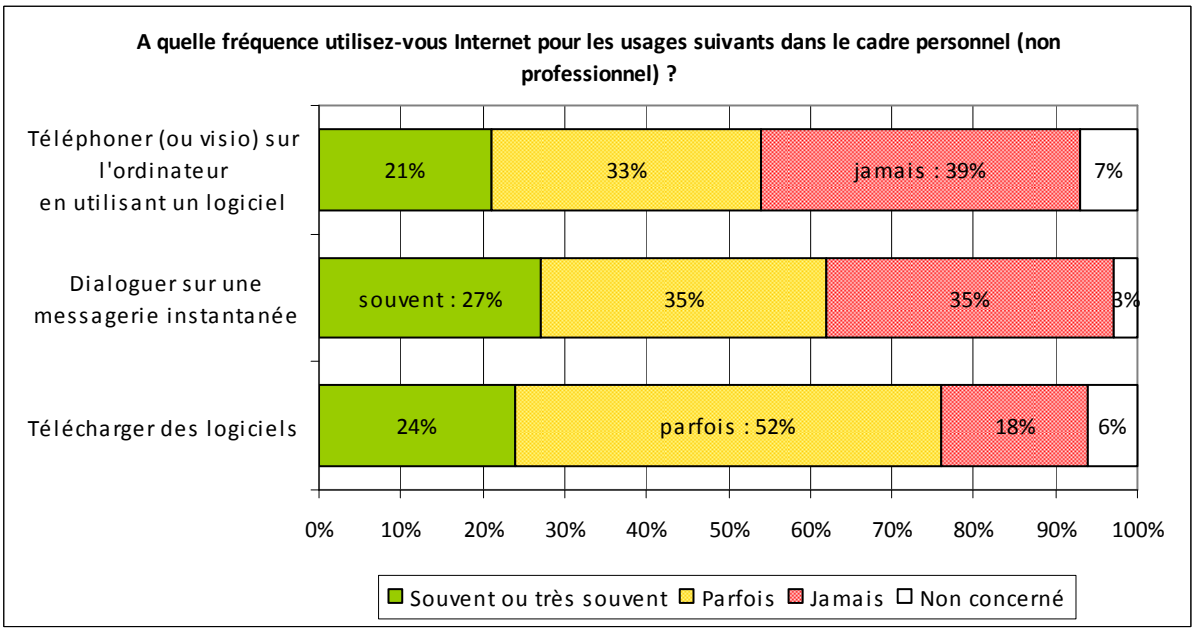

Figure 109 - Pratiques de téléchargement, de messagerie instantanée et téléphonie sur Internet

Le jeu multi-joueurs en ligne progresse de 30 % depuis la dernière enquête. C'est naturellement chez les 15-24 ans que le taux d'usage est le plus fort puisque seuls 37 % indiquent ne pas fréquenter ce type de site.

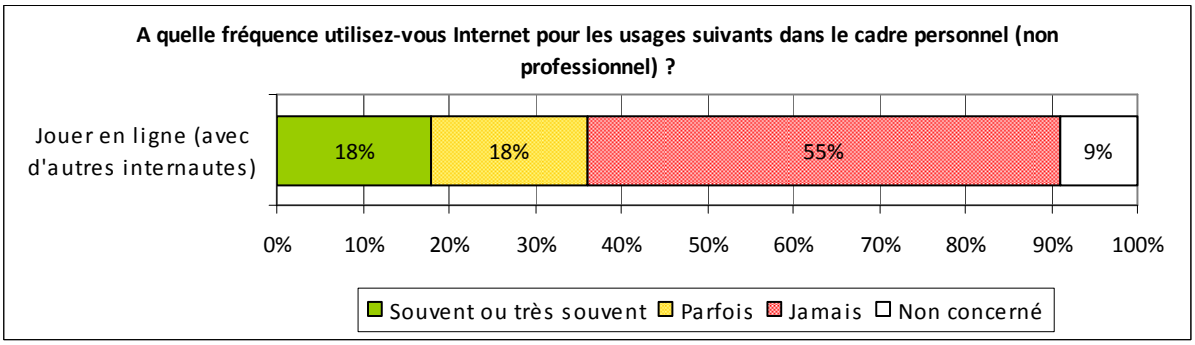

Figure 110 - Pratique de jeu en ligne sur Internet

Les internautes se tournent vers les réseaux sociaux. La tendance est tirée par les jeunes générations puisque les 15-24 ans sont 77 % à les fréquenter et 64 % chez les 25-34 ans.

Ceux sont les leaders du marché (Facebook, Google+,…) qui sont mis en avant. Twitter, qui a été identifié spécifiquement cette année, est utilisé par moins de 20 % des internautes, principalement chez les 15-24 ans. Les réseaux sociaux remplacent peu à peu la tenue d'un blog ou d'un site personnel (20 % contre 34 %). Les sites de rencontres voient leur fréquentation doubler, mais cela reste assez marginal, avec mois de 10 % des internautes qui déclarent les fréquenter.

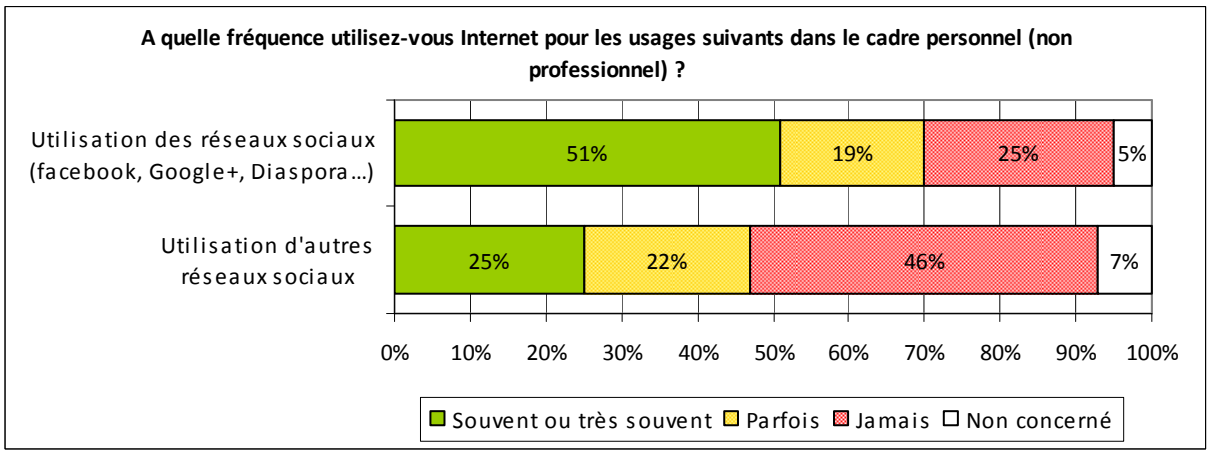

Figure 111 - Pratiques des réseaux sociaux

L'utilisation d'Internet pour les démarches administratives n'a pas progressé depuis la dernière enquête.

Les services de stockage en ligne sont utilisés par 16 % des internautes. On note toutefois que 25 % des internautes utilisent les services d'Apple (iCloud, iTunes…).

Les téléchargements de musique et de film sur des sites légaux est également en forte progression pour atteindre 36 % (+ 21 points) pour les films, 28 % (+12 points) pour la musique.

Ce sont principalement les 15-24 ans qui tirent la tendance : Ils sont 4 fois plus nombreux que les 50 ans et plus, et 2 fois plus que les 35-49 ans.

Les achats en ligne avec paiement sont effectués par 9 internautes sur 10. C'est même une activité fréquente ou très fréquente pour 50 % d'entre eux.

La proportion d'internautes qui se connectent à distance au réseau de leur entreprise n'a pas évolué. Toutefois, il y a 3 fois plus d'internautes qui déclarent ne pas être concernés (30 % en 2012, par rapport à 10 % en 2010).

Le paiement en ligne

Les internautes font de plus en plus confiance dans les solutions de paiement en ligne mais demandent des garanties. Ils sont moins réticents qu'en 2010 à acheter et à vendre sur Internet. Dans le cas du paiement en ligne, ce n'est ni le montant, ni la réputation du site qui motive ou non un achat. Les internautes réclament en nombre croissant un environnement qui les sécurise et qui soit adapté en faisant appel à des techniques telles que le chiffrement, le paiement sécurisé, ou les certificats.

On notera cependant que même s'il y a toujours des réticences pour effectuer des transactions en ligne, le niveau d'acceptation a considérablement augmenté depuis l'enquête de 2010 et que les internautes ont de plus en plus d'exigences de sécurité.

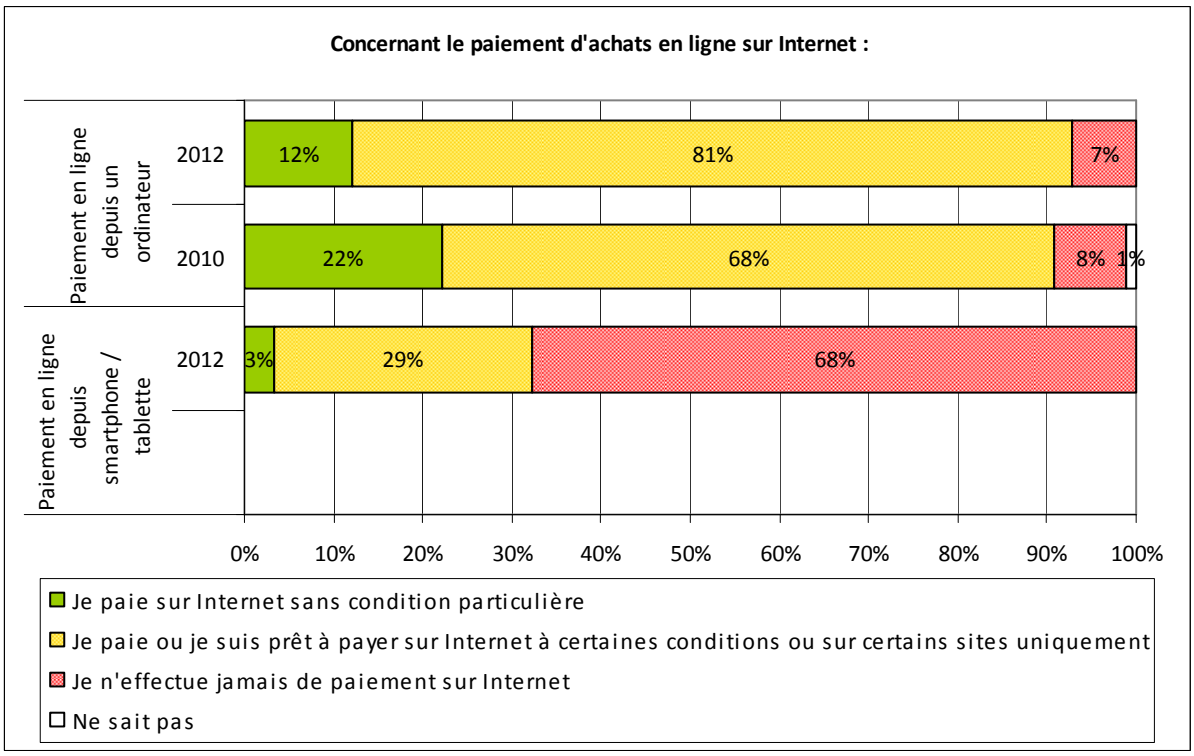

Figure 112 - Paiement sur Internet sur ordinateur et sur smartphone ou tablette

Le paiement sur Internet, mais depuis quels outils ?

Les internautes sont très réticents pour le paiement en ligne depuis un smartphone ou une tablette. Seules 3 % des internautes payent sans se poser de questions particulières.

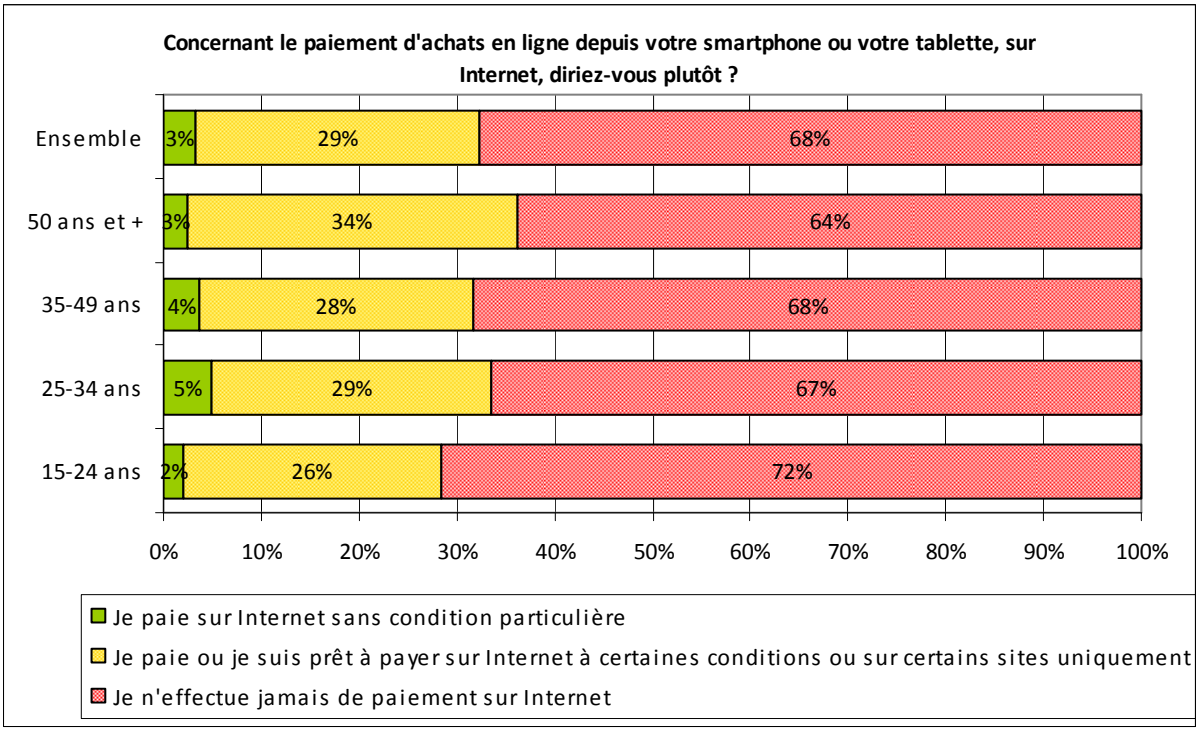

Figure 113 - Paiement sur Internet depuis smartphone / tablette selon l'âge

Un quart des internautes fait autant confiance à son ordinateur qu'à son smartphone pour les paiements en ligne. Ils sont 38 % à penser que l'ordinateur est plus sûr, presque autant que les indécis (36 %) qui ne peuvent pas, ou ne semblent pas pouvoir, faire un choix et les comparer en matière de sécurité.

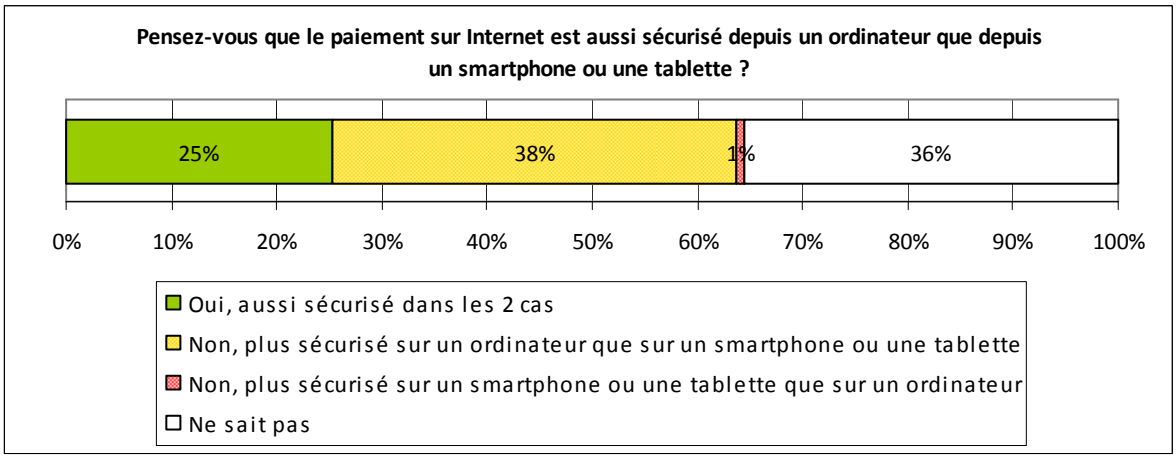

Figure 114 - Perception de la sécurité relative entre ordinateur et smartphone ou tablette

Paiement en ligne : quels pré-requis pour un sentiment de sécurité

On notera cependant que même s'il y a toujours des réticences pour les transactions en ligne, le niveau d'acceptation a considérablement augmenté depuis l'enquête de 2010 et que les internautes ont de plus en plus d'exigences de sécurité.

Comme évoqué précédemment, même s'il y a toujours des réticences pour effectuer des transactions en ligne, les internautes sont plus matures dans l'appréciation des conditions de sécurité.

En particulier, la gestion du paiement multi canal (par Internet et par SMS) et la fidélisation (enregistrement préalable des données bancaires) font leurs apparitions dans le panel des réponses.

Pour accepter de payer en ligne, un internaute demande en moyenne que 4 des conditions suivantes soient remplies : cf. Figure 115 ci-après.

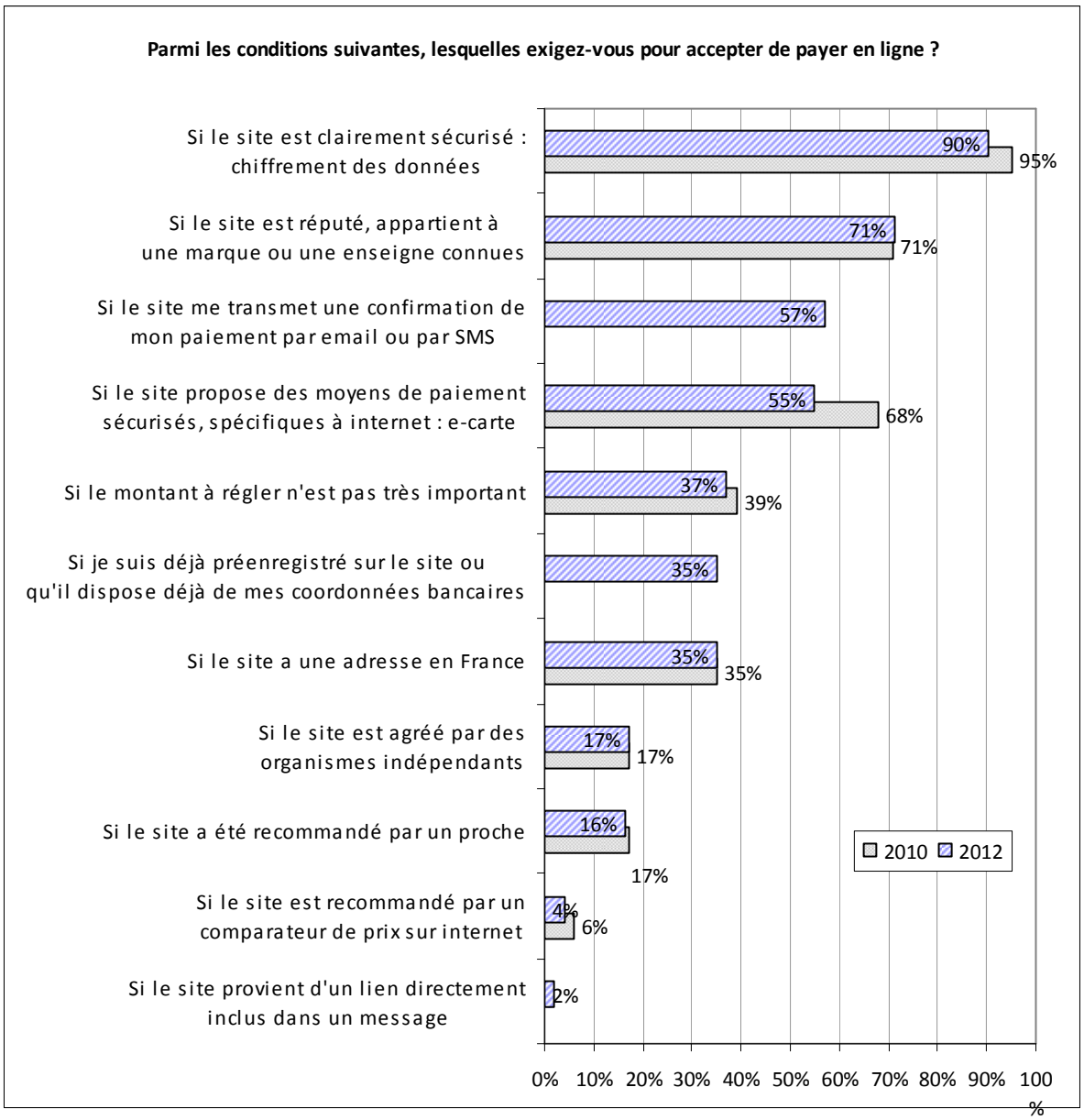

Figure 115 - Critères de confiance dans la sécurité pour les paiements en ligne

Les données personnelles

Les internautes remplissent assez facilement des formulaires en ligne qui leurs demandent leurs données personnelles, **dès lors qu'ils ont une confiance dans le site**.

Les 35-50 ans et plus sont légèrement plus réticents que le reste de la population.

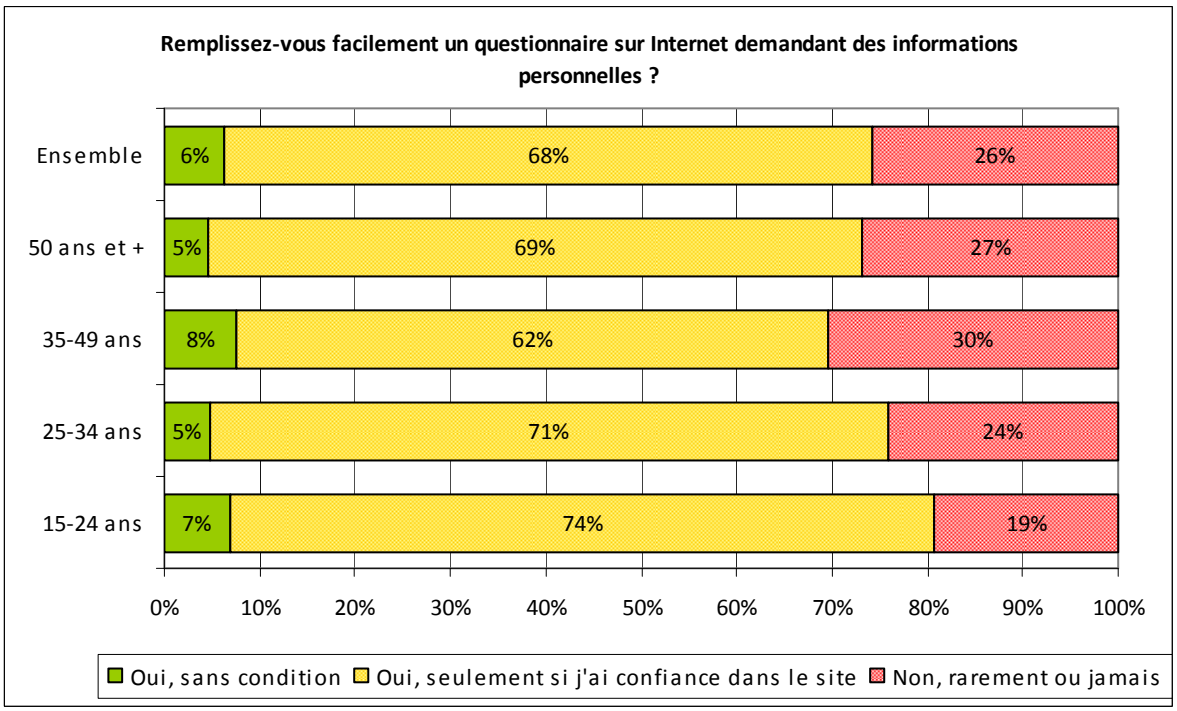

Figure 116 - Formulaires sur Internet et données personnelles

Partie IV – Moyens et comportements de sécurité

Logiciels de sécurité comme moyens de protection

Les suites logicielles de sécurité commerciales qui intègrent plusieurs modules de sécurisation (anti-virus, anti-spam, anti spyware, pare-feu) ne sont utilisées que par un tiers des internautes (31 % en 2012).

En matière d'antivirus, les internautes semblent plébisciter l'antivirus gratuit (65 %).

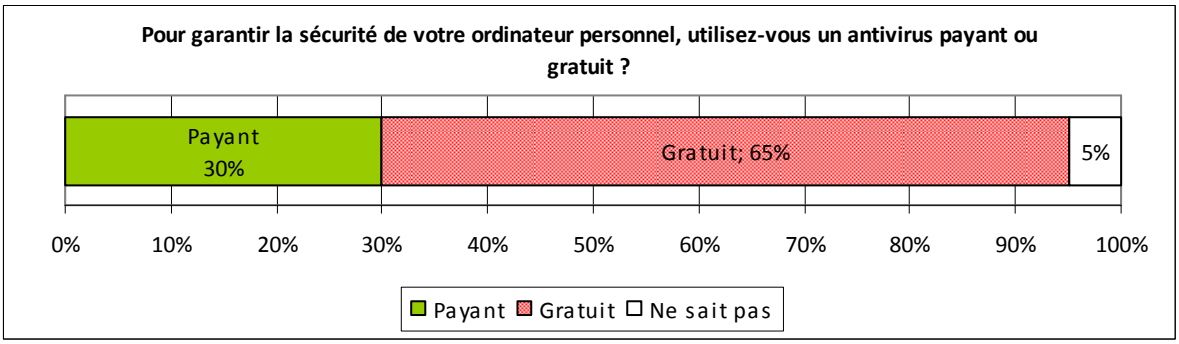

Figure 117 - Utilisation d'antivirus payant ou gratuit sur ordinateur

On note en 2012 une légère baisse de l'utilisation des solutions d'anti-spyware (de 65 % en 2010 à 61 % en 2012). On constate la même tendance à la baisse pour l'utilisation des logiciels d'anti-spam et des pare-feu (de 86 % en 2010 à 80 % en 2012).

Sécurité du Wifi

On note une stabilité depuis 2008 sur la sécurité du Wifi, avec environ 77 % des internautes qui déclarent sécuriser leur connexion Wifi.

Ce sont les 25-34 ans qui sont les plus sensibilisés aux risques liés à la non-sécurisation des réseaux Wifi (83 %), avec une progression de 10 points chez les plus de 50 ans (de 66 % en 2010 à 76 % en 2012).

Mise à jour automatique

Plus de 80 % des internautes déclarent utiliser les mécanismes de mise à jour automatisée des logiciels. Cette tendance peut s'expliquer par la volonté affichée par certains éditeurs de logiciels d'intégrer cette fonctionnalité **par défaut** dans leurs solutions.

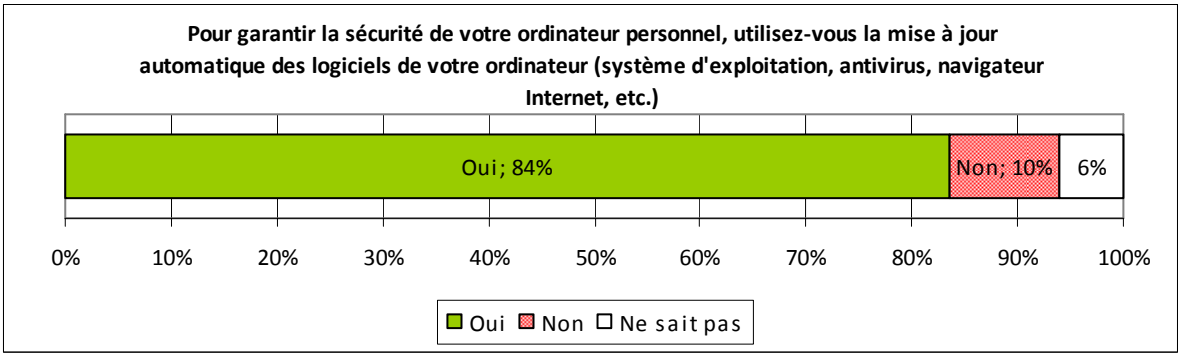

Figure 118 - Utilisation des mécanismes de mise à jour automatique sur ordinateur

Sauvegarde

Alors qu'entre 2008 et 2010 on pouvait se réjouir de voir que la sauvegarde était une pratique en forte augmentation, l'étude de cette année fait apparaître une forte baisse de l'utilisation des outils de sauvegardes des données personnelles (chute de 90 % en 2010 à 69 % en 2012).

Mots de passe de session

Cette année est heureusement marquée par une forte hausse de l'utilisation des mots de passe d'ouverture de session (59 %). Entre 2008 et 2010, cette pratique avait fortement diminué (passant de 47 % en 2008 à 5 % en 2010).

Protection électrique

Les dispositifs de protection électrique sont légèrement moins utilisés (24 % en 2012 contre 27 % en 2010). Ces dispositifs de protection de type onduleur sont une nouvelle fois plutôt utilisés par les plus âgés des utilisateurs (33 % des +50 ans contre 13 % des 15-24 ans).

Sécurité des e-mails et des pièces-jointes

Les internautes sont peu nombreux (13 %) à chiffrer leurs envois de courrier électronique.

Les systèmes de protection des pièces jointes envoyées par messagerie (chiffrement, mot de passe sur fichier, zip avec mot de passe) sont eux aussi que peu utilisés par les internautes sondés (20 %).

Les internautes ne semblent donc pas particulièrement sensibles aux risques liés aux fuites de données personnelles.

Biométrie

L'utilisation de la biométrie est en baisse depuis 2010 (6 % en 2012 contre 11 % en 2010), malgré la généralisation des lecteurs d'empreintes digitales sur les ordinateurs portables.

Système antivol d'ordinateur portable

L'utilisation de dispositifs antivol pour les ordinateurs portables n'est toujours pas un réflexe pour les utilisateurs. Seuls 8 % d'entre eux déclarent en utiliser.

Contrôle parental

L'utilisation des logiciels de contrôle parental est aussi en baisse (15 % en 2012 contre 34 % en 2010). Seulement un quart des internautes de la tranche 35-49 ans déclare avoir mis en place ce type de solution.

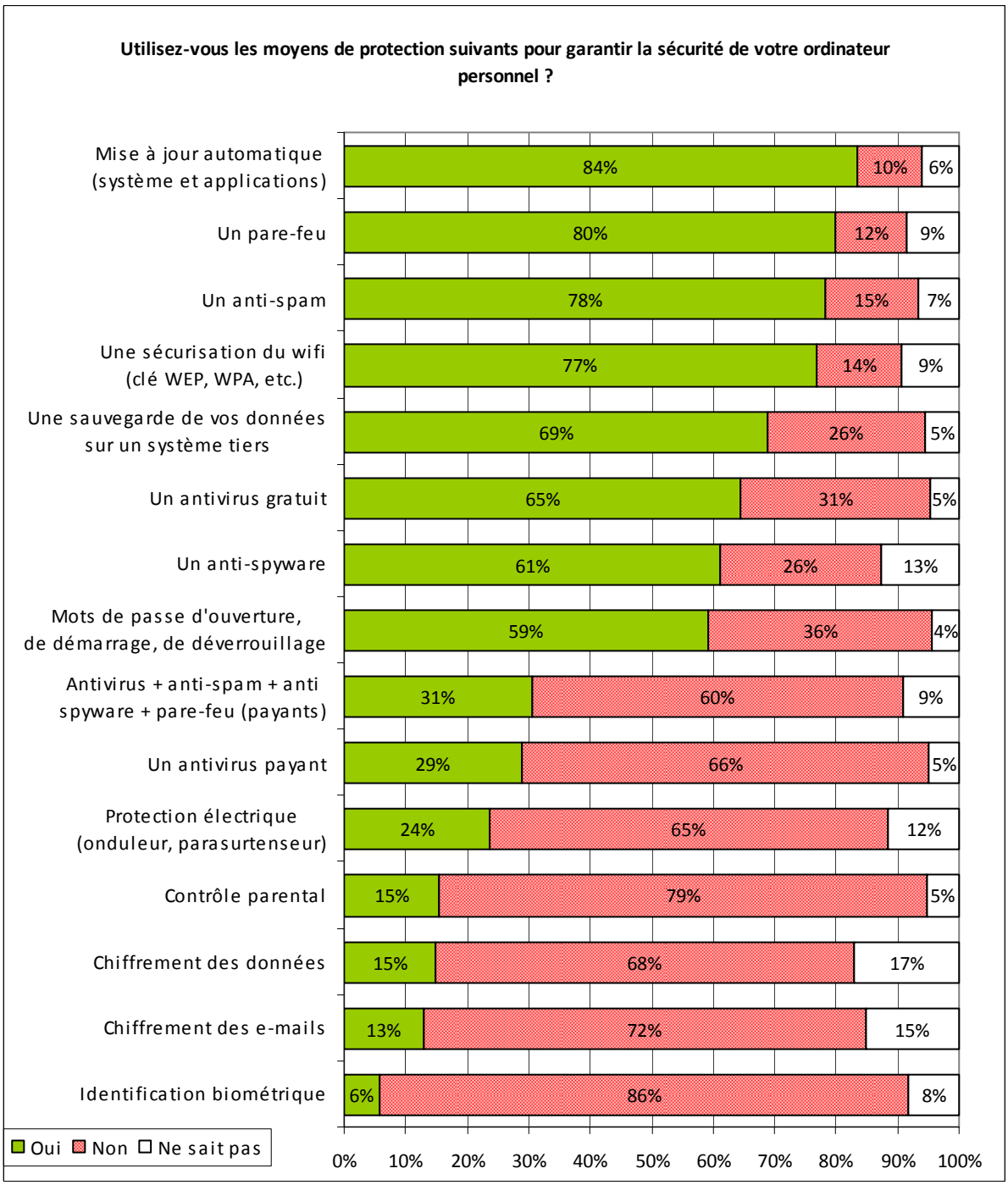

Figure 119 - Moyens de protections utilisés sur les ordinateurs personnels

Moyens et comportement des internautes sur les smartphone et tablettes

La préoccupation des internautes concernant la sécurité de leur smartphone est apparue depuis la précédente enquête.

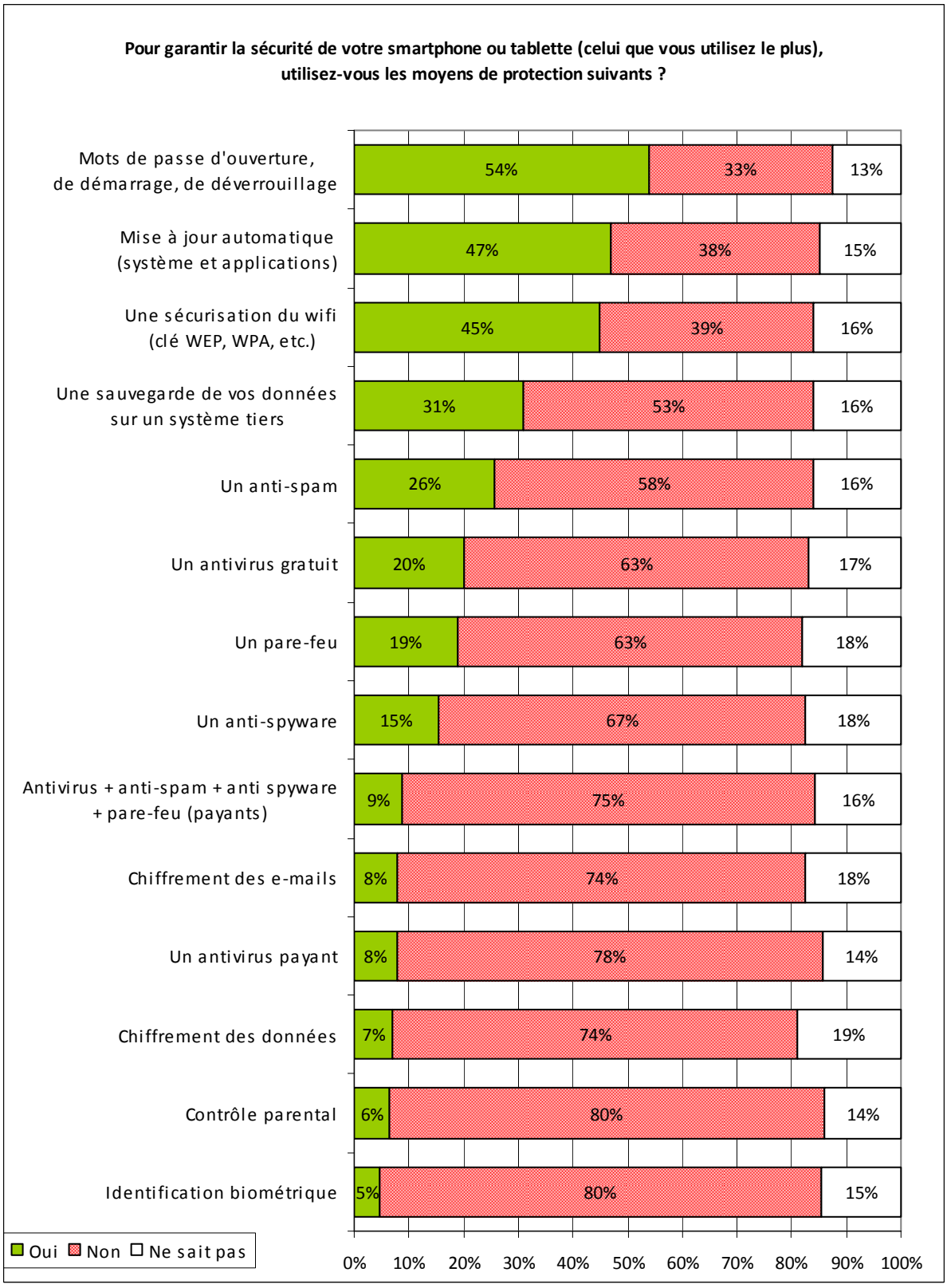

Figure 120 - Moyens de protections utilisés pour smartphone et tablette

On constate que globalement, 50 % des internautes utilisent au moins un moyen de sécuriser leur smartphone en privilégiant les moyens naturellement installés sur le smartphone lors de sa livraison. On ne sait donc pas si ces précautions relèvent d'une réelle sensibilisation à la sécurité de leur mobile ou si elle relève des habitudes acquises.

En effet, l'usage de moyens plus poussés comme le taux d'équipement en antivirus ou en pare-feu est seulement de moins de 20 %. 10 % des internautes reconnaissent qu'ils ne savent pas s'ils utilisent un quelconque moyen de protéger leur smartphones. La confiance qu'il semble mettre dans leur opérateur et dans la sécurité des configurations des smartphones, mais aussi la sécurité qui serait intégrée dans le réseau, tendraient ainsi à expliquer pourquoi ils ne se posent pas de question plus avant.

On constate aussi que les internautes de plus de 35 ans sont globalement plus concernés par la sécurité que les plus jeunes. Ce constat concerne tous les types de moyens de protection.

Enfin, seul un tiers des internautes sauvegardent les données de leur smartphone.

A peu près la moitié des internautes, quel que soit leur âge utilisent un mot de passe de session, la mise à jour automatique des logiciels du smartphone et la sécurisation de la connexion WIFI.

Les outils plus sophistiqués comme les anti-virus, anti-spyware et pare-feu concernent à peu près un tiers des plus de 35 ans et une part beaucoup plus réduite des plus jeunes.

Les mises à jour des systèmes et logiciels pour les ordinateurs…

Les mises à jour automatiques est activées pour près de 9 internautes sur 10. Ce choix, qui est généralement celui par défaut, permet d'éviter le pire.

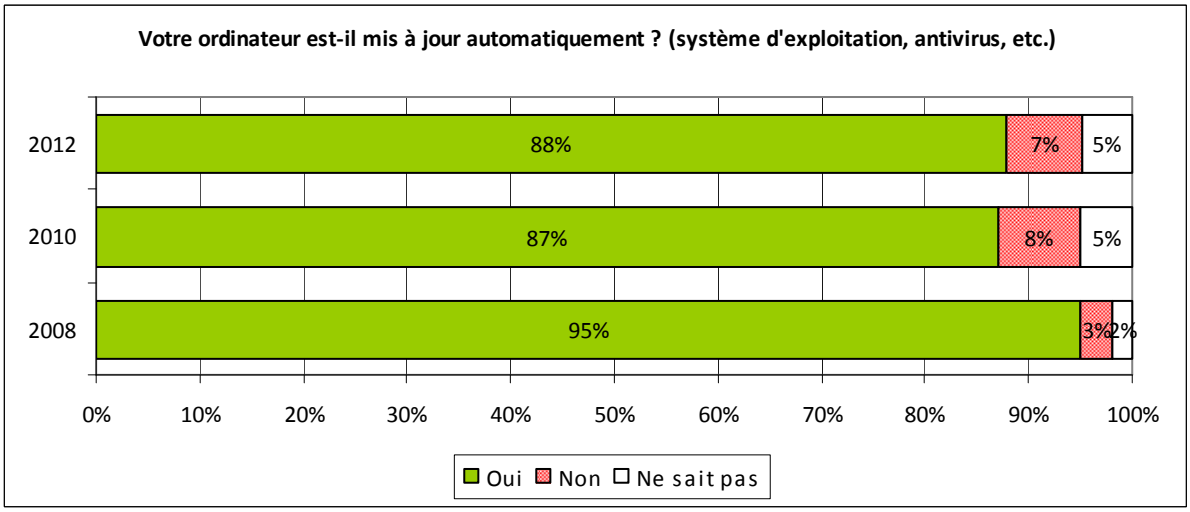

Figure 121 - Mise à jour des systèmes d'exploitation et des logiciels des ordinateurs

En effet, pour les internautes n'ayant pas de mises à jour automatiques, plus de la moitié ne font des mises à jour au mieux qu'une fois par mois.

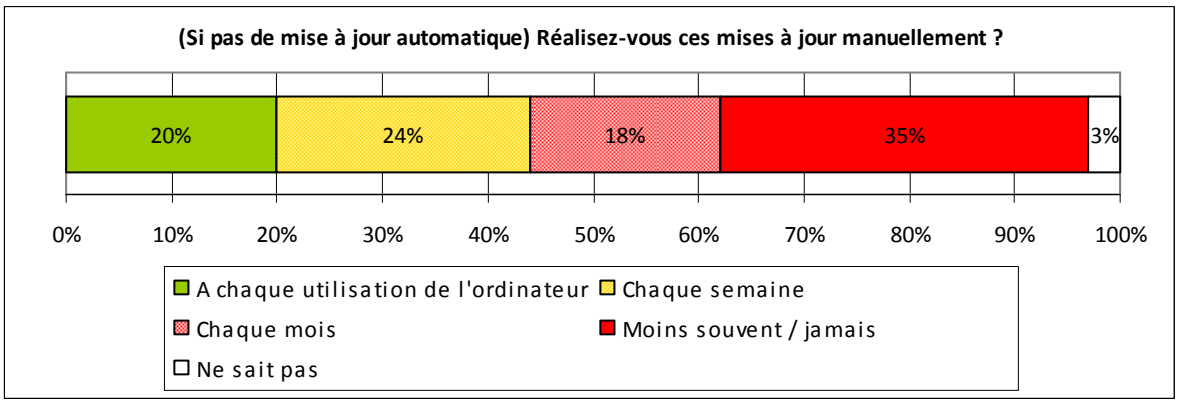

Figure 122 - Fréquence des mises à jour manuelles pour les ordinateurs

… Et pour les Smartphones

Concernant les smartphones la situation est nettement moins bonne car plus de la moitié des personnes ne mettent pas à jour leur smartphone régulièrement (moins d'une fois par mois).

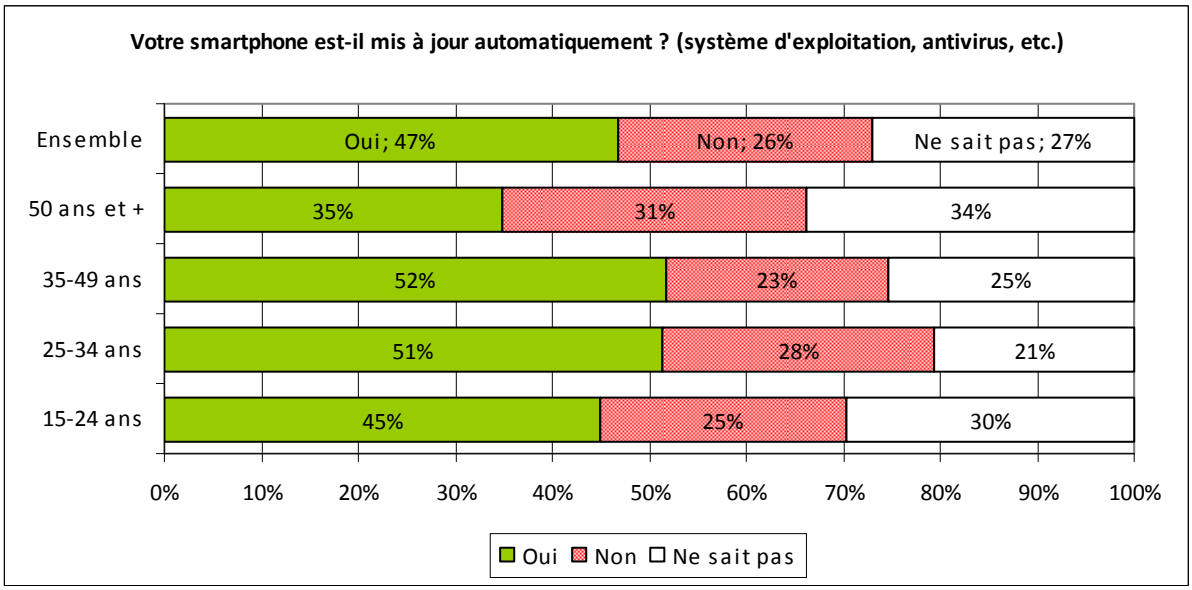

Figure 123 - Mise à jour des systèmes d'exploitation et des logiciels des smartphones

Les mises à jour ne sont pas pour autant réalisées manuellement car là encore 30 % des internautes le font moins d'une fois par mois et 31 % ne savent pas ou ne le font pas du tout.

Cette tendance pourrait s'expliquer par le fait que les internautes n'ont pas pris conscience qu'un smartphone est avant tout … un mini ordinateur.

Dommages sur l'ordinateur personnel

Dans l'ensemble, lorsqu'ils subissent un ou plusieurs dommages sur leur ordinateur personnel, les internautes préfèrent résoudre eux-mêmes les problèmes informatiques (56 %).

Ils ne sont que 22 % (en baisse de 6 points depuis 2010) à confier la réparation de l'ordinateur personnel à un professionnel, car ils préfèrent, dans 39 % des cas, faire appel à un tiers « bénévole » (famille, ami, etc.).

Le sentiment de confiance sur Internet

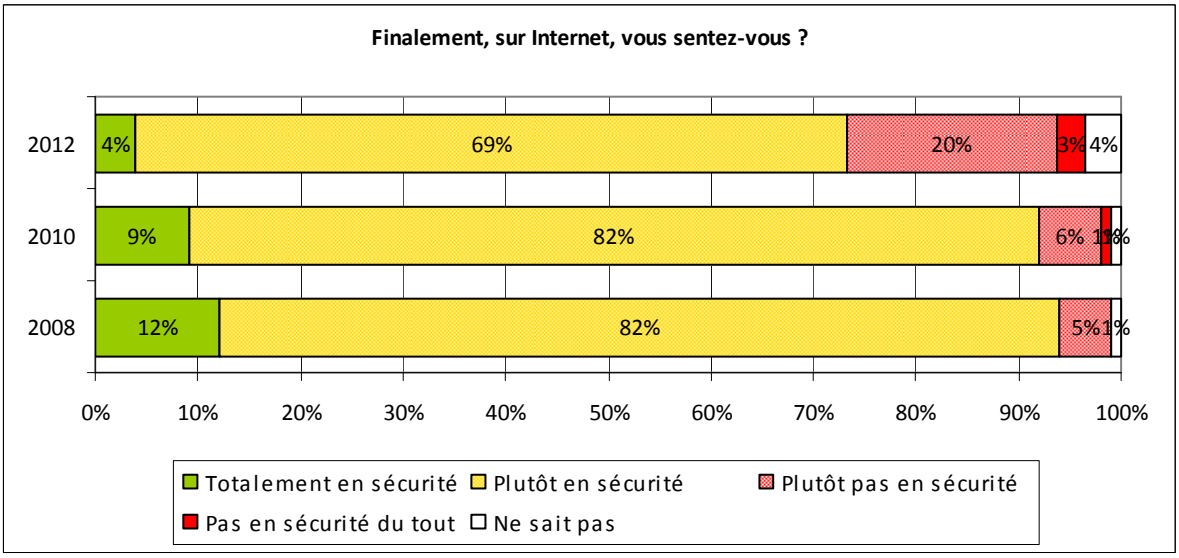

Figure 124 - Perception globale du contexte sécurité sur Internet

Les internautes se sentent en grande majorité (73 %) totalement ou plutôt en sécurité sur Internet. Cette tendance est toutefois en forte baisse depuis 2010, avec une baisse de 18 points.

En complément, on constate une forte hausse du sentiment d'insécurité sur Internet. Les internautes sont en effet en 2012 près de 23 % à se sentir plutôt pas et pas du tout en sécurité sur le Web.

Ces tendances restent vraies quelles que soient les catégories d'âge.

L'ESPRIT DE L'ÉCHANGE

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

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

Téléchargez les productions du CLUSIF sur

www.clusif.fr