Menaces informatiques et pratiques de sécurité en France

Édition 2010

- Les entreprises de plus de 200 salariés
- Les hôpitaux
- 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. BESENVAL Stéphane	OZSSI ÎLE-DE-FRANCE
M. BOURCIER Stéphane	MINISTÈRE DE LA DÉFENSE
M. BOURSAT Jean-Marc	DEVOTEAM
M. BRUCKMANN Francis	FT ORANGE
M. BUTEL Annie	BNP PARIBAS
M. CALEFF Olivier	DEVOTEAM
M. CARTAU Cédric	CHU NANTES
M. CHIOFALO Thierry	BOLLORÉ LOGISTICS
M. CONSTANT Paul	CLUSIF
M. COURTECUISSE Hélène	LISIS CONSEIL
M. DOIDY Mathieu	ACCENTURE
M. FREYSSINET Éric	GENDARMERIE NATIONALE
M. GAZAY Emmanuel	ACCENTURE
M. GIORIA Sébastien	FR CONSULTANTS
M. GOONMETER Nuvin	ACCENTURE
M. GRONIER Loup	DEVOTEAM
M. GROSPEILLER Éric	MINISTÈRE DE LA SANTÉ
M. GUÉRIN Olivier	CLUSIF
M. HADOT Daniel	MINISTÈRES FINANCIERS
M. HAMON Bruno	SIDEXE
M. JOUAS Jean-Philippe	CLUSIF
M. LOINTIER Pascal	CHARTIS
M. MINASSIAN Vazrik	ADENIUM
M. MOURER Lionel	ESR CONSULTING
M. PEJSACHOWICZ Lazaro	CNAMTS
M. RICHY Paul	ORANGE
M. RITZ Jean-Philippe	OCLCTIC
M. ROSE Philippe	BEST PRACTICES SYSTÈMES D'INFORMATION
M. ROULE Jean-Louis	CLUSIF
M. VANHESSCHE Patrick	CONSULTANT EN SÉCURITÉ DES SI

Le CLUSIF remercie également vivement les représentants des entreprises et hôpitaux 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

Une politique de sécurité (de l'information) est à la fois une nécessité économique en raison de la dépendance croissante de nos activités aux informations numériques et parfois une nécessité réglementaire pour le respect d'une conformité. C'est pourquoi, l'emploi d'une méthode d'analyse de risques, telles que EBIOS ou MÉHARI, permet d'apprécier ses besoins intrinsèques de sécurité et d'ordonner les priorités de mise en œuvre de plans relatifs.

Mais la connaissance des faits, de la « réalité terrain », est tout aussi importante et c'est pour cela que les rapports du CLUSIF ont toujours suscité un intérêt de la part d'un lectorat de plus en plus important. Autrefois appelées les « statistiques du Clusif » et réalisées à partir de données du monde de l'assurance, ces rapports sont maintenant élaborés à partir d'une enquête nationale, par des professionnels, pour acquérir une photographie la plus représentative de l'échantillon ciblé : entreprise, administration, internaute… Le nombre croissant de téléchargements, le référencement dans des présentations en conférence et dans les formations, la traduction en anglais pour un accès international en sont d'autres témoignages.

La lecture et l'exploitation des données ainsi recueillies présentent des avantages quelle que soit la nature de votre activité :

- 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.

La lecture de ce rapport peut donc se faire en multicritères… et en fonction d'un besoin immédiat ou non, sachant que les données restent relativement pérennes ce qui justifie une livraison biennale.

Enfin, au nom de l'association et des futurs lecteurs, je tiens à remercier l'ensemble des contributeurs à ce rapport, professionnels membres de l'association, mais aussi les experts invités à collaborer à ce Groupe de Travail.

Pascal LOINTIER
Président du CLUSIF

Synthèse de l'étude

Au travers de l'édition 2010 de son enquête sur les menaces informatiques et les pratiques de sécurité (MIPS), le CLUSIF réalise, comme tous les 2 ans, un bilan approfondi des usages en matière de sécurité de l'information en France.

Cette enquête se veut être une référence de par la taille et la représentativité des échantillons d'entreprises (350 entreprises ont répondu) et d'hôpitaux (151 ont répondu) interrogés. 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, 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 : le travail continue… laborieusement !

Avec un sentiment de dépendance à l'informatique toujours en hausse, les entreprises continuent d'avancer dans la prise en compte de la Sécurité des Systèmes d'Information (SSI). Toutefois, les changements concrets se font à petits pas…

La prise en compte « théorique » de la SSI est de plus en plus visible, tant dans la formalisation de la Politique de Sécurité des Systèmes d'Information (PSSI) (73%, + 14% vs 2008), l'existence de charte SSI (67%, +17% vs 2008) que dans l'évolution du nombre de Responsables de la SSI (RSSI) (49%, + 12% vs 2008) ; avec toutefois une baisse quant à son rattachement à la Direction Générale (34%, - 11% vs 2008), certainement liée au fait que les RSSI « récents » proviennent souvent de la Direction des Systèmes d'Information (DSI). L'utilisation des « normes » est également en hausse.

On constate, depuis près de 4 ans maintenant, la mise en place d'une « organisation » et de « structures » de la SSI (RSSI, Correspondant Informatique et Libertés (CIL), PSSI, charte, etc.) sans que, toutefois, la mise en application concrète de ces « politiques » ne décolle réellement !… Les budgets restent très serrés, parfois inconnus, et encore souvent réservés à la mise en œuvre concrète de moyens techniques au détriment de la sensibilisation des utilisateurs (57% n'en font pas).

Nouvel entrant cette année dans notre enquête, le thème ISO 27002 numéro 9 (sécurité physique), nous montre que pour 41% des entreprises, le responsable des « données papier » n'est pas clairement identifié.

Peu de différences dans l'utilisation des technologies de sécurité, l'anti-virus, le pare-feu et l'anti-spam restent très largement en tête (respectivement 97%, 95% et 91%). Les IDS/IPS, technologies arrivées à maturité, progressent (34% et 27%, +11% vs 2008). Le chiffrement pour les utilisateurs évolue (17%, +7% vs 2008), mais reste à un niveau faible. Les technologies récentes (type NAC ou DLP) peinent à se déployer (respectivement 23% et 9%)…

Seul 10% des entreprises ont placé leur SI sous infogérance et quand c'est le cas, près d'une sur trois ne met pas en place d'indicateurs de sécurité !…

Côté contrôle d'accès, le SSO et le Web-SSO décollent enfin (respectivement 21% et 8%, +14% et +5% vs 2008), signe d'une meilleure prise en compte de la simplification d'accès des utilisateurs. Cerise sur le gâteau, ce mécanisme permet également une meilleure traçabilité.

Parmi les points positifs : la veille est de plus en plus réalisée, tant sur les vulnérabilités que sur les solutions de sécurité (34%, +13% vs 2008). Idem pour les procédures de déploiement de correctifs de sécurité ou patch management (64%, +16% vs 2008).

Autre point positif, un mieux sur la gestion des incidents, avec une quantité d'incidents identifiée en hausse (26% déclare ne pas avoir eu d'incident, -19% vs 2008), certainement dû à des mécanismes d'alerte plus pertinents, pour un niveau de dépôt de plainte quasi identique à 2008 (5%, -1%).

Reste que 33% (-7% vs 2008) des entreprises ne disposent toujours pas d'un plan de continuité d'activité pour traiter les crises majeures !…

Enfin, les aspects « conformité », pour lesquels des progrès restent à faire, au travers :

- des « obligations CNIL » : en légère progression (68% « conforment », 20% « conforment pour leurs traitements sensibles », respectivement +4% et +1% vs 2008),
- des audits de sécurité : 25% des entreprises n'en font toujours pas !…,
- du tableau de bord de la sécurité informatique : 34% seulement en dispose (malgré les +11%).

Hôpitaux : la sécurité est en marche !

Avec la parution au Journal Officiel le 29 novembre 2009 des arrêtés actant la dissolution du GIP-CPS (Groupement d'Intérêt Public - Carte de Professionnel de Santé) et l'élargissement du périmètre des missions de l'Agence des Systèmes d'Information Partagés de santé (ASIP), une nouvelle étape a été franchie dans la réforme de la gouvernance des systèmes d'information de santé. Sur la page d'accueil de son site internet, l'ASIP affirme : « Sécuriser les données de santé : une condition indispensable au développement du Dossier Médical Personnel (DMP) et de la télémédecine ».

Les directions informatiques des hôpitaux sont de plus en plus convaincues de la nécessité absolue du pilotage médical des projets et de la participation des soignants : la sécurité doit devenir une valeur à partager, d'où l'apparition dans les hôpitaux ou à un niveau régional de responsables sécurité des systèmes d'information (RSSI), qui cumulent souvent leur fonction avec celle de Correspondant Informatique et Libertés (CIL). La mise en conformité des établissements avec le décret confidentialité relève aussi de leurs compétences.

De huit membres en 2008, le club des RSSI hospitaliers est passé à une quinzaine en 2009. Les thèmes abordés sont notamment : l'identifiant patient (IP) et le problème des appareils biomédicaux.

Par ailleurs, dans le cadre du projet de loi Hôpital Santé Patients Territoires (HPST), il a été décidé de regrouper la MAINH (Mission nationale d'Appui à l'Investissement Hospitalier, la MEAH (Mission nationale d'Expertises et d'Audites Hospitaliers) et le GMSIH (Groupement pour la Modernisation des Systèmes d'Information de Santé) au sein d'une nouvelle entité : l'Agence Nationale d'Appui à la Performance des établissements de santé et médico-sociaux (ANAP).

La Sécurité apparaît maintenant souvent comme une préoccupation de la Gouvernance des hôpitaux (soutenue à 94% par la DG) : la montée en puissance des contraintes législatives et réglementaires n'est pas étrangère à cette tendance. L'élaboration de la Politique de Sécurité

et des plans d'action est de plus en plus liée à l'analyse de risques, basée principalement sur les directives du GMSIH (36%).

Depuis la dernière enquête en 2006, les hôpitaux ont adopté les chartes de sécurité (63%, +21% vs 2006) et mis en place des CIL (39%, +10%). Ils n'ont pas résisté au nomadisme, ni au développement des réseaux sans fil et de la téléphonie sur IP.

En progression, la détection des incidents de sécurité : l'augmentation des vols de matériels informatiques (44%) et de la perte de services essentiels (46%) est forte, en raison de l'augmentation de la pénétration des Systèmes d'Information dans les actes médicaux.

En retrait toujours : la sensibilisation générale des salariés à la sécurité de l'information (27%, +2% vs 2006), la mise en place de plans de continuité métiers (54% en tout ou partie, +18% vs 2006), les audits de sécurité (49% n'en font pas) et les tableaux de bord de suivi (7%, +1% vs 2006).

Même si à travers cette enquête MIPS 2010 on peut constater quelques réponses discordantes, probablement dues à la subjectivité de l'observation sur des domaines difficilement quantifiables, ou au fait que la sécurité est encore dépendante de la culture de chaque établissement, il apparaît clairement que les défis à relever par les hôpitaux dans les prochaines années sont encore importants et multiples !

Vers une maîtrise de la sécurité par les Internautes ?

D'une manière générale, la perception de la menace (spam, fishing, intrusion, virus, logiciel espion, etc.) résultant de la connexion à Internet est en très légère diminution par rapport à l'étude précédente (23% « risque important ou très important », vs 25% en 2008).

En revanche, le sentiment de danger concernant la protection de la vie privée augmente (73% « mise en danger de la vie privée - fortement ou un peu », vs 60% en 2008).

Concernant les usages, ils évoluent peu : 96% stockent et manipulent des photos ou des vidéos, 90% traitent des documents personnels (courriers, comptabilité, etc.), seuls 42% traitent des documents professionnels (-7% vs 2008).

Enfin, concernant le paiement d'achats en ligne, les blocages diminuent. En effet, 90% des internautes déclarent accepter de le faire : 68% sous conditions (utilisation de https : 99% de confiance, notoriété de l'enseigne accédée : 72% de confiance ou utilisation d'une e-card : 68% de confiance), et 22% sans condition…

Enfin et concernant les moyens et comportements de sécurité mis en œuvre, on observe que les ordinateurs sont peu protégés par des mots de passe (5%) ou des contrôles biométriques (11%), mais aussi que les mises à jour de sécurité semblent être déployées régulièrement (+90%), qu'il s'agisse de déploiement automatique ou manuel.

Les mesures de protection professionnelles sont très peu utilisées sur l'ordinateur familial : 80% n'utilisent pas de chiffrement, 88% n'ont pas d'antivol physique et 65% n'ont pas de protection de leur alimentation électrique

Au final, nous observons une banalisation de l'usage Internet, avec un sentiment de sécurité qui ne change pas grâce à une meilleure connaissance de l'outil informatique et de ses dangers. La menace semble se transférer vers une préoccupation plus importante concernant les données personnelles.

Pour conclure…

Pour autant, la menace ne faiblit pas et notre enquête montre de nouveau que les malveillances et les incidents de sécurité sont bien présents : attaques virales, vols de matériel, accroissement des problèmes de divulgation d'information et attaques logiques ciblées sont toujours au menu !

Passer des politiques de sécurité « parapluie », que l'on formalise pour se donner bonne conscience, vers des pratiques tangibles, véritablement ancrées dans les processus de gestion de l'information, reste l'enjeu pour les années à venir…

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

Méthodologie

L'enquête du CLUSIF sur les menaces informatiques et les pratiques de sécurité en France en 2010 a été réalisée au cours des mois de janvier et février 2010, en collaboration avec le cabinet spécialisé GMV Conseil, sur la base de questionnaires d'enquête élaborés par le CLUSIF. Trois cibles ont été retenues pour cette enquête :

- les entreprises de plus de 200 salariés : 350 entreprises de cette catégorie ont répondu à cette enquête,
- les hôpitaux : 151 hôpitaux ont accepté de répondre à cette enquête,
- 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 2010, 2008 et 2006. 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 2009, 2007 et 2005.

Enfin, le groupe d'experts tient également à préciser que toute enquête de ce type contient nécessairement des réponses discordantes dues à la subjectivité de l'observation sur des domaines difficilement quantifiables ou, dans le cas du domaine spécifique de la sécurité du SI, de la « culture » et de la maturité de chaque entreprise, hôpital 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 2010 de son enquête, le CLUSIF souhaitait interroger exactement le même échantillon d'entreprises que celui interrogé en 2006 et 2008 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 :

- Industrie,
- BTP,
- Commerce,
- Transport – Télécoms,
- Services – Finance.

350 entreprises ont répondu à la sollicitation du CLUSIF (entretien de 28 minutes en moyenne), avec un taux d'acceptation d'environ 10% (en hausse de 4% par rapport à 2008) : 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 / Type	200-499 salariés	500-999 salariés	1 000 et plus	Total	Total en %		Données INSEE
Industrie	68	36	39	**143**	**40,9%**	→	**42%**
BTP	8	7	8	**23**	**6,6%**	→	**6%**
Commerce	24	9	15	**48**	**13,7%**	→	**17%**
Transport – Télécoms	17	7	29	**53**	**15,1%**	→	**9%**
Services - Finance	20	16	47	**83**	**23,7%**	→	**27%**
Total	**137**	**75**	**138**	**350**	**100,0%**		**100%**
Total en %	**39,1%**	**21,4%**	**39,4%**			↑ Redressement	
Redressement →	↓	↓	↓				
Données INSEE	**65%**	**19%**	**16%**	**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 29% (21% en 2008) des entreprises interrogées, mais plus de 40% dans les plus de 1 000 salariés.

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

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, 73% d'entre elles jugent lourde de conséquences une indisponibilité de moins de 24h de leurs outils informatiques (avec un maximum de 83% pour le secteur du commerce).

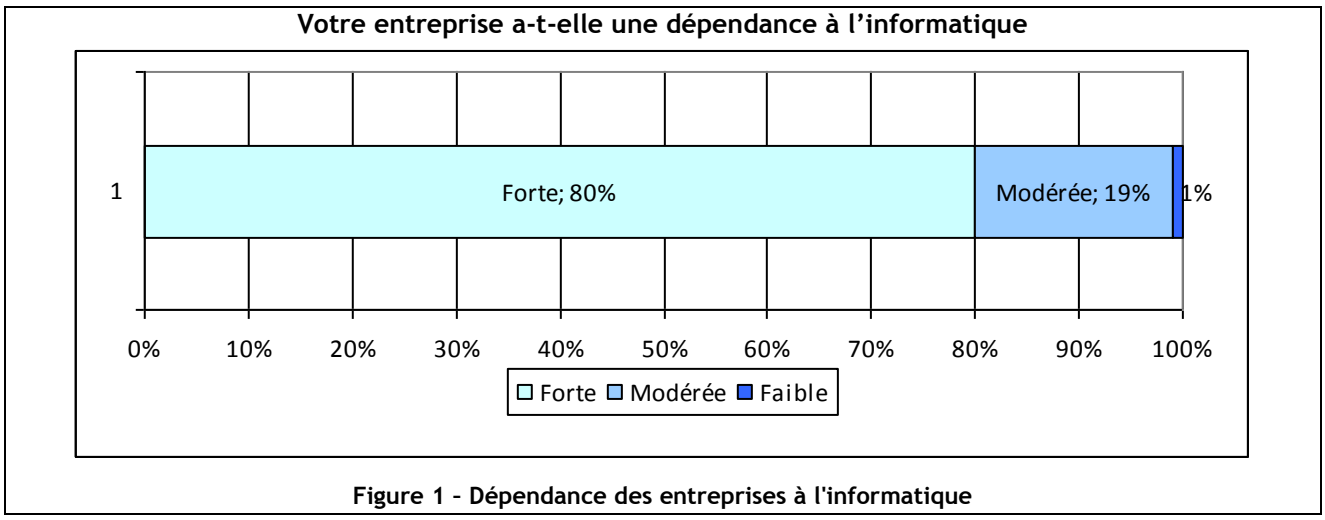

Figure 1 – Dépendance des entreprises à l'informatique

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

Un budget informatique moyen à 1,45 million €

Lorsqu'on les interroge sur leur budget informatique, 51% des entreprises répondent (soit 2 fois plus qu'en 2008). Ainsi, 58% ont un budget inférieur à 1 million d'euros, 20% compris entre 1 et 2 millions d'euros et 15% entre 2 et 5 millions d'euros. Enfin, 7% des budgets sont supérieurs à 5 millions d'euros pour un maximum de 20 millions d'euros.

Un budget sécurité dont le périmètre semble encore et toujours mal cerné

Plutôt que de les interroger sur un budget en valeur absolue, peu significatif s'il n'est pas très précisément corrélé avec les caractéristiques de taille et de métier de chaque répondant, nous avons interrogé les RSSI sur la part du budget informatique dédié à la sécurité de l'information.

Peu d'évolution entre les résultats des années précédentes et ceux que nous découvrons aujourd'hui.

Les responsables sécurité ont toujours des difficultés à se positionner puisque 30% d'entre eux (même chiffre qu'en 2008) avouent ne pas savoir quel poids leur budget représente dans le budget informatique. De plus, lorsque ce budget est clairement identifié par rapport au budget informatique, on ne peut que constater une grande hétérogénéité.

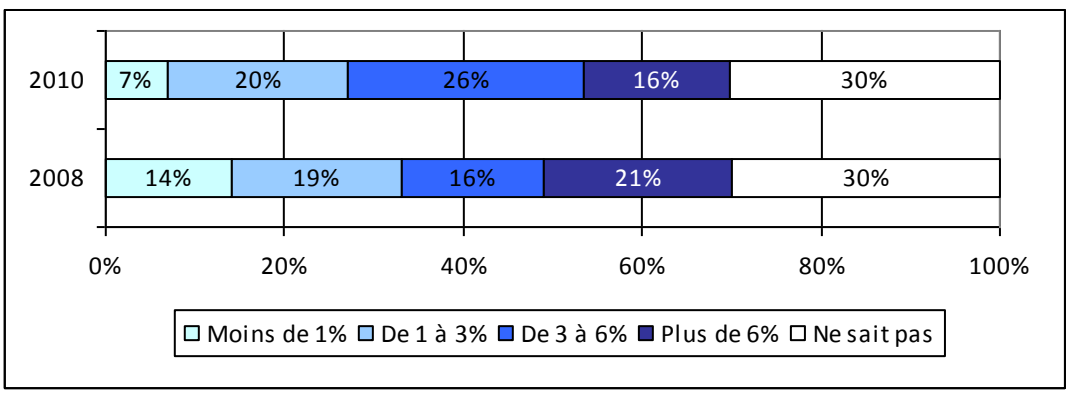

Figure 2 – Part du budget informatique alloué à la sécurité dans les entreprises

Une inquiétante stagnation des budgets sécurité

En terme d'évolution, il est intéressant de noter que ces budgets sont majoritairement constants et ce, quelle que soit la taille de l'entreprise. Ce sentiment de stagnation est heureusement relativisé par quelques augmentations : 61% des entreprises du secteur BTP et 43% des Transport et Télécoms ont augmenté leur budget cette année, parfois de manière très importante (15% des entreprises du BTP ont noté une augmentation de plus de 10% de leur budget).

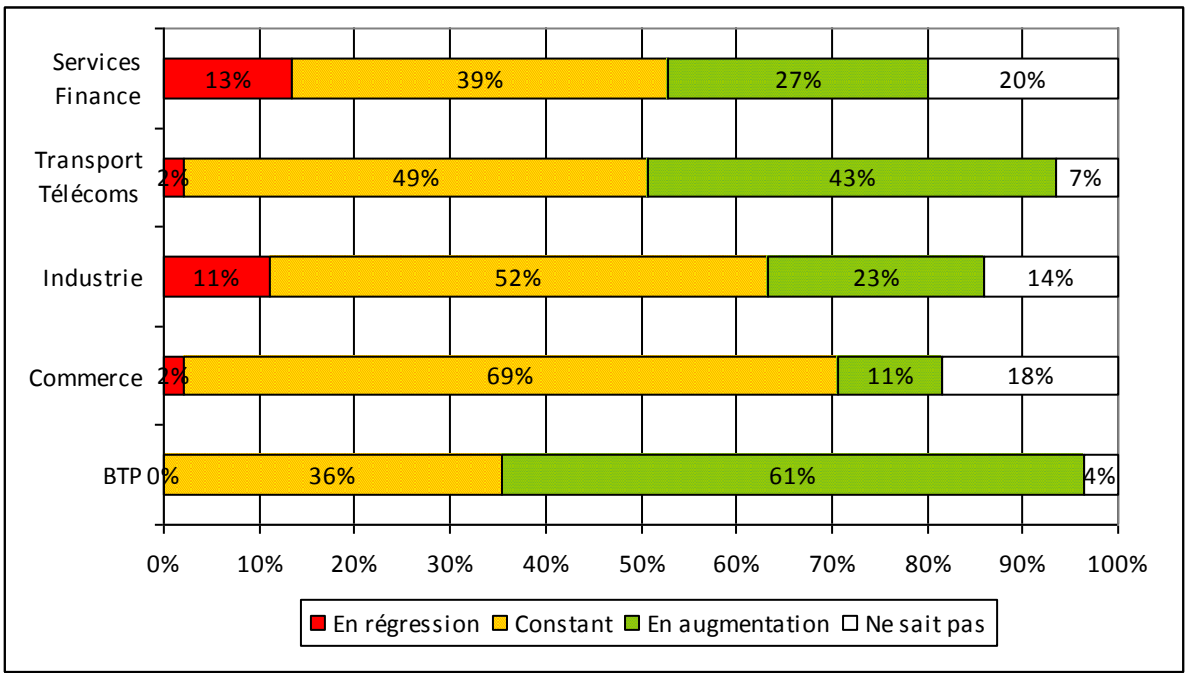

Figure 3 – Évolution du budget sécurité selon les secteurs d'activités

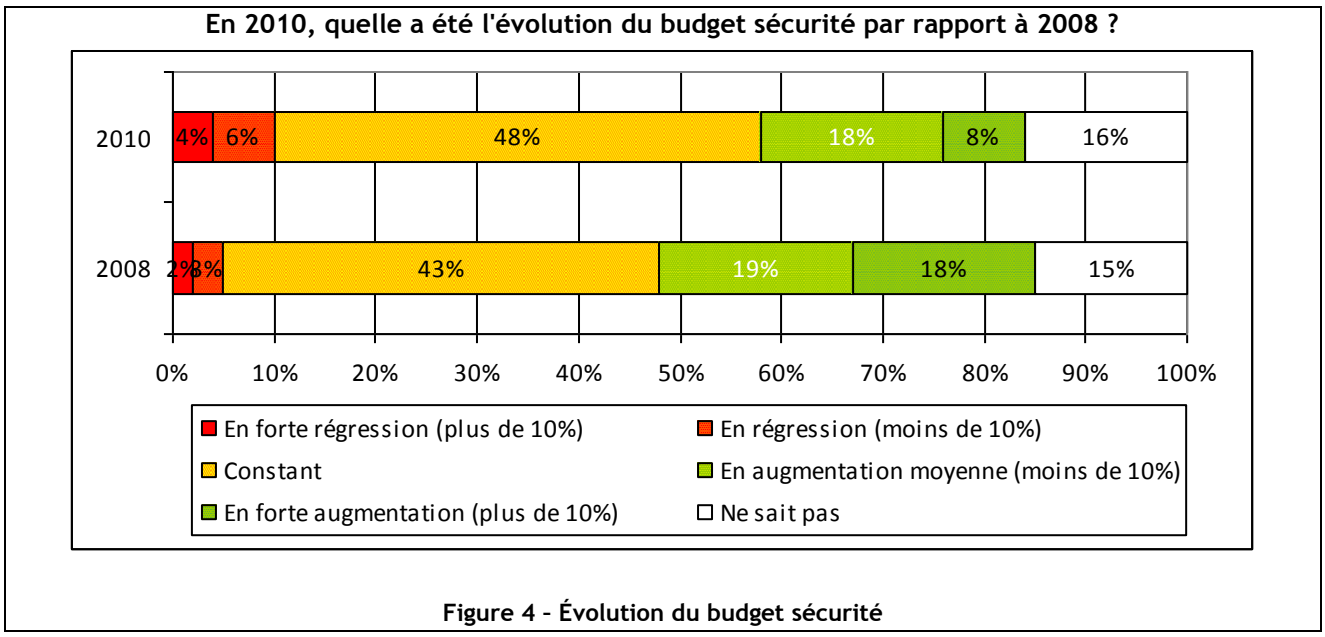

Figure 4 – Évolution du budget sécurité

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 (45%, +10% vs 2008) : le manque de budget,
- 2ème raison citée (30%, -6% vs 2008) : les contraintes organisationnelles,
- 3ème raison citée (24%, -3% vs 2008) : la réticence de la hiérarchie, des services ou des utilisateurs,
- 4ème raison citée (14%, -9% vs 2008) : le manque de personnel qualifié,
- 5ème raison citée (13%, hors top 5 en 2008) : le manque de connaissance.

Les deux freins principaux sont le manque de moyens budgétaires (+10% par rapport à 2008 : nous n'avons pas fini de nous alarmer…) et les contraintes organisationnelles.

Au chapitre des bonnes nouvelles, la réticence de la Direction des Systèmes d'Information sort du top 5 (3% seulement, contre 8% en 2008) et l'utilisateur du Système d'Information semble de moins en moins systématiquement perçu comme une gêne par les RSSI.

Le manque de personnel qualifié était le frein numéro 2 en 2006, 4ème en 2008, place qu'il occupe toujours, tout en perdant 9%. Ce résultat pourrait sembler satisfaisant si ce n'était que le détail des réponses montre un résultat moins convenable qu'il n'y paraît puisque plus d'un RSSI sur deux dénoncent ce manque de personnel comme frein majeur (choix 1 ou choix 2 des freins les plus importants). L'agitation forcenée du marché de l'emploi dans le secteur de la SSI et le toujours haut niveau du nombre d'offres restent d'ailleurs d'autres témoins de cette insatisfaction continue.

Thème 5 : Politique de sécurité

Une formalisation qui augmente toujours…

Le nombre d'entreprises ayant formalisé leur Politique de Sécurité de l'Information (PSI) a augmenté de près de 10% en deux ans. Aujourd'hui, près des deux tiers des entreprises ont formalisé leur PSI, alors qu'en 2008, un peu plus de la moitié l'avaient élaboré.

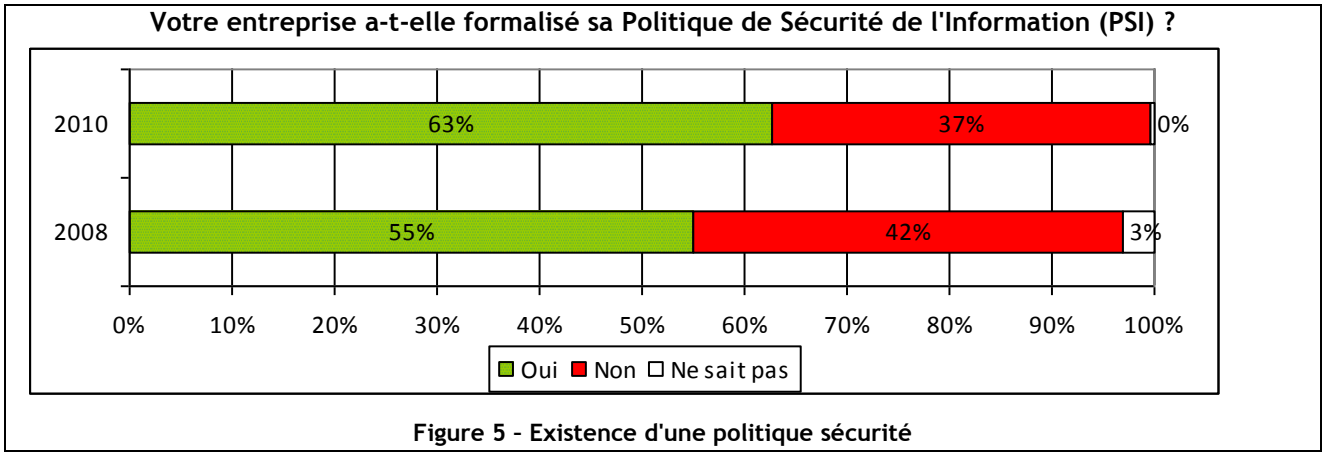

Figure 5 – Existence d'une politique sécurité

De plus, cette politique est à jour dans la mesure où 75% des entreprises interrogées l'ont actualisée il y a moins de deux ans. D'ailleurs la PSI des entreprises est massivement soutenue par la Direction Générale (73% en 2010, +14% vs 2008), qui a contribué pour plus de la moitié à son élaboration.

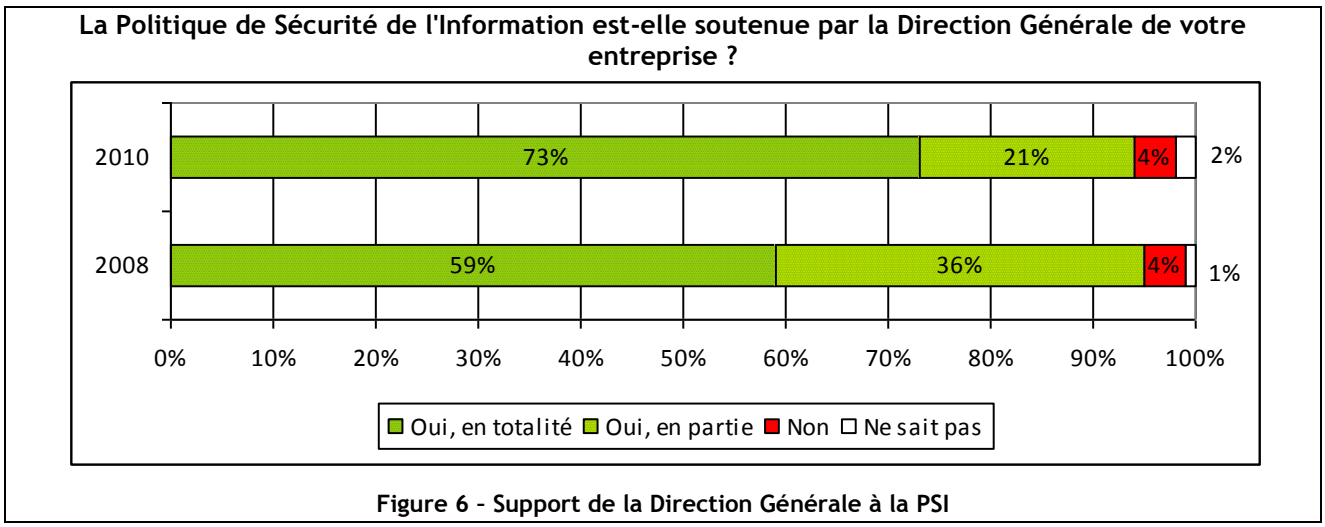

Figure 6 – Support de la Direction Générale à la PSI

En outre, même si environ un tiers des entreprises fondent leur Politique de Sécurité de l'Information (PSI) sur les normes ISO (27001, 27002, 27799), il convient de remarquer que près de la moitié des entreprises ne s'appuie sur aucune norme.

La Politique de Sécurité de l'Information (PSI) de votre entreprise s'appuie-t-elle sur des « normes » de sécurité ?

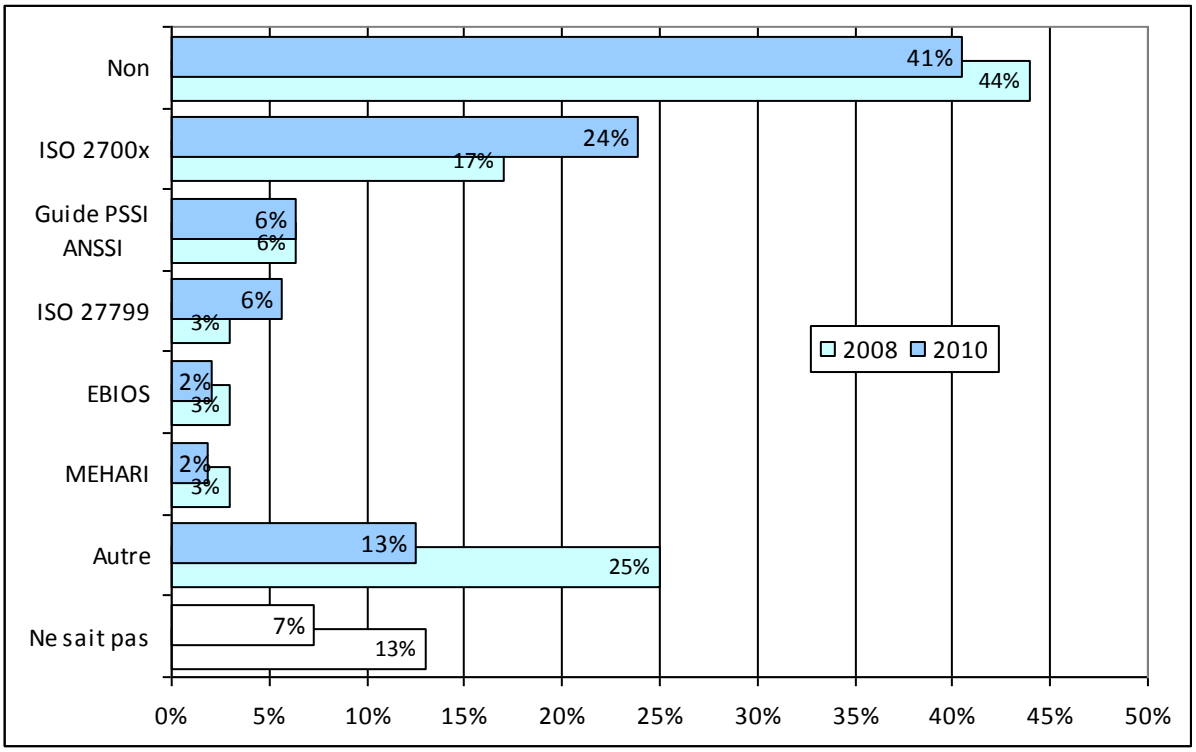

Figure 7 - Appui de la PSI entreprise sur une « norme » de sécurité

Thème 6 : Organisation de la sécurité et moyens

Une fonction RSSI qui prend de l'ampleur

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 marque un net progrès par rapport aux années précédentes. En effet, près de la moitié d'entre elles bénéficient de ses services, alors qu'en 2008, plus de 60% des organisations n'avaient pas pleinement identifié son rôle.

La fonction de Responsable de la Sécurité des Systèmes d'Information (RSSI) est-elle clairement identifiée et attribuée ?

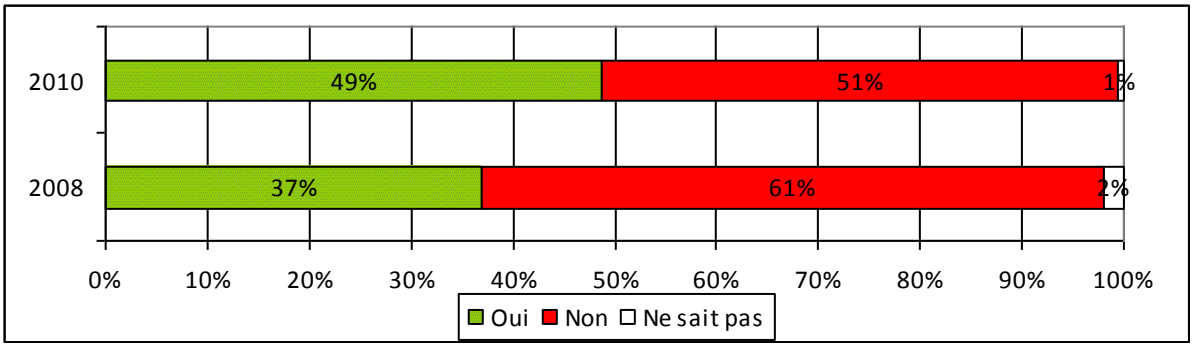

Figure 8 - Attribution de la fonction RSSI

Toutefois, seule la moitié des RSSI sont dédiés à cette tâche à temps plein et lorsque le RSSI n'existe pas, cette mission reste fortement attachée à la Direction des Systèmes d'Information ou Direction Informatique.

Lorsqu'il n'existe pas de RSSI, par quelle autre fonction la mission de RSSI est-elle prise en charge ?

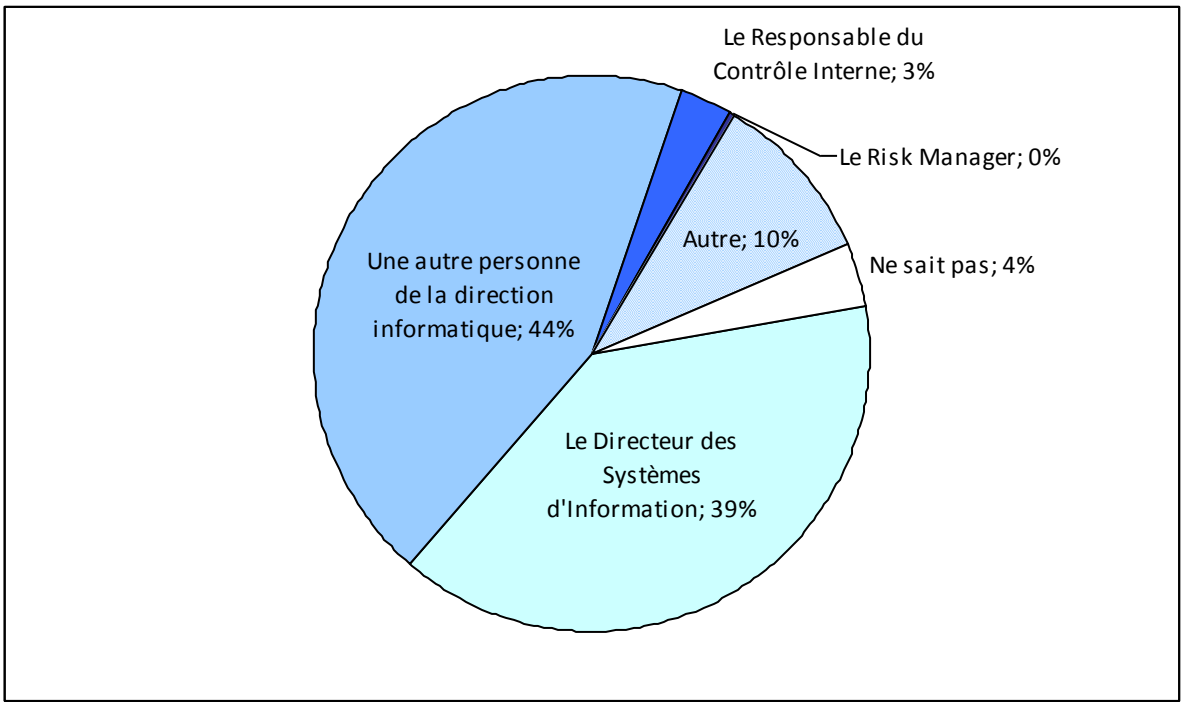

Figure 9 - Prise en charge de la fonction RSSI, lorsqu'il n'existe pas de RSSI

Un rattachement en perpétuelle évolution…

Le RSI ou RSSI est soit rattaché à la DSI (36%), soit à la Direction Administrative et Financière (DAF) (12%) ou directement à la Direction Générale pour près de la moitié (34%) des entreprises interviewées, en fort recul par rapport à 2008 (-11%). Ceci peut s'expliquer par l'arrivée plus nombreuse de RSSI au sein d'entreprises de tailles moyennes ayant un niveau de maturité en SSI encore faible.

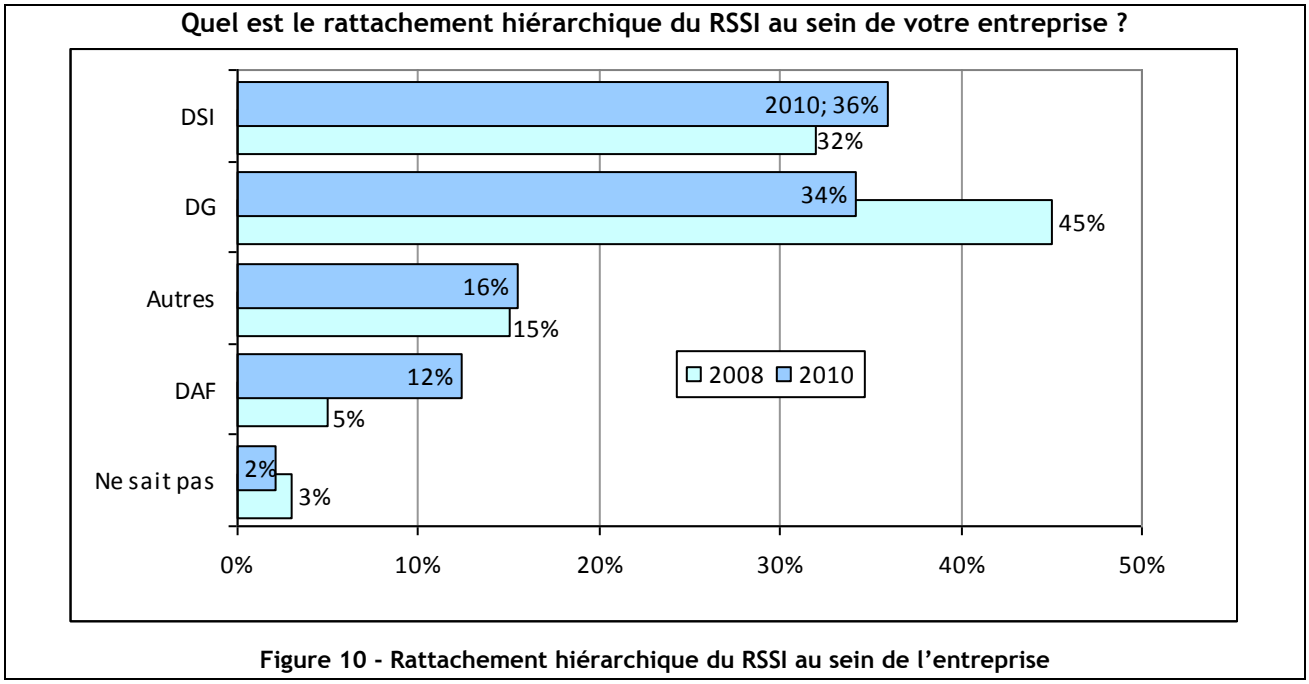

Figure 10 - Rattachement hiérarchique du RSSI au sein de l'entreprise

Le RSSI consacre en moyenne 50% de son temps aux aspects techniques et opérationnels (définition des architectures, suivi des projets, gestion des droits d'accès, etc.). Le temps restant est partagé à égalité entre les aspects fonctionnels (PSI, analyse des risques), et les aspects de communication (sensibilisation) et juridiques.

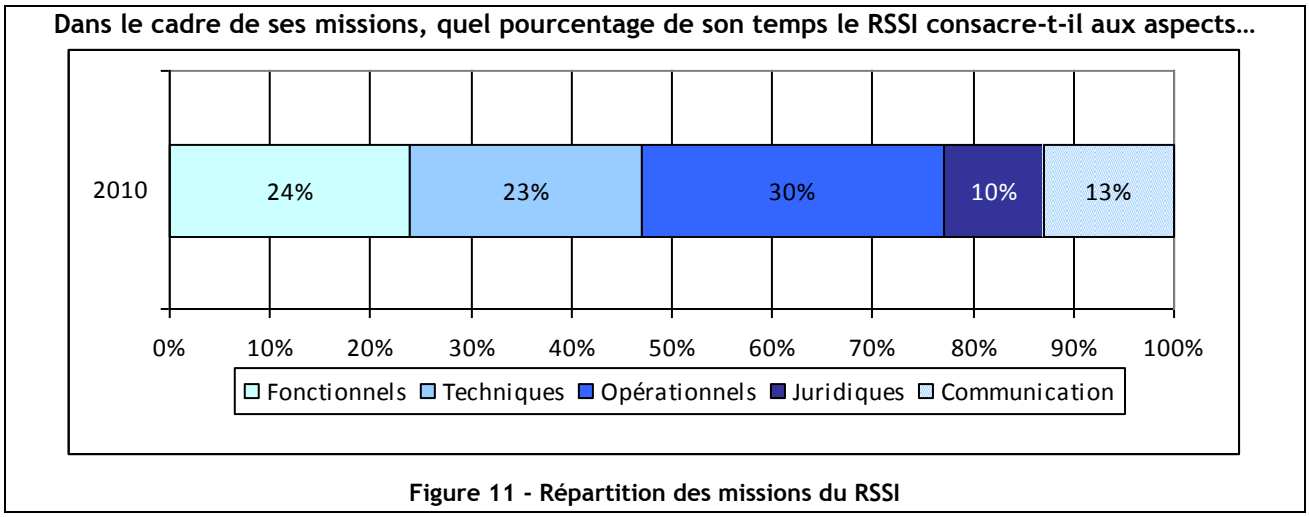

Figure 11 - Répartition des missions du RSSI

Enfin, à présent, près de 80% des entreprises ont en permanence une équipe sécurité, alors qu'il y a deux ans, seul près 57% des entreprises en bénéficiaient. Toutefois, dans 61% des cas, le RSSI est encore un homme ou une femme seul(e) ou en binôme seulement !…

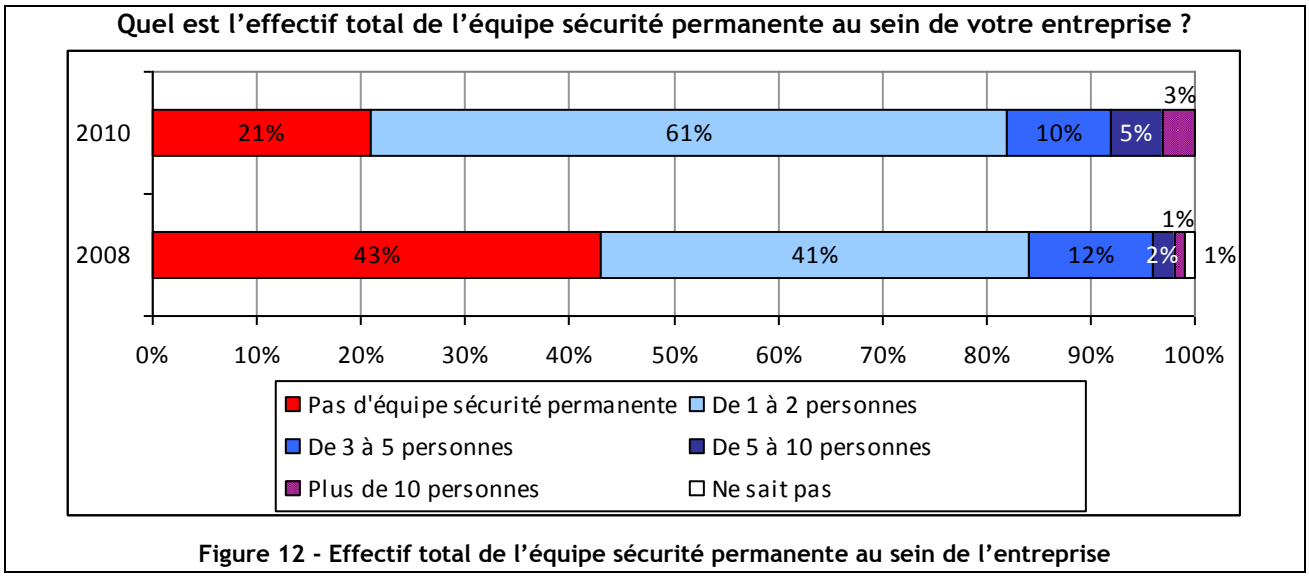

Figure 12 - Effectif total de l'équipe sécurité permanente au sein de l'entreprise

Les moyens humains affectés à la gestion des problèmes de sécurité de l'information apparaissent en retrait de ce qui pourrait être attendu au regard de la dépendance exprimée des entreprises vis-à-vis de leur Système d'Information.

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

Une notion d'inventaire encore peu ancrée dans la culture des entreprises

La notion d'inventaire des informations et de leurs supports n'est pas encore complètement ancrée dans la culture des entreprises. En effet, seulement 30% des entreprises ont réalisé un inventaire complet de leurs données et 4% l'ont fait sur des données qui ne dépendent pas uniquement de l'outil informatique. Sur les 66% restants, 32% ont effectué un inventaire partiel alors que 34% n'ont rien réalisé.

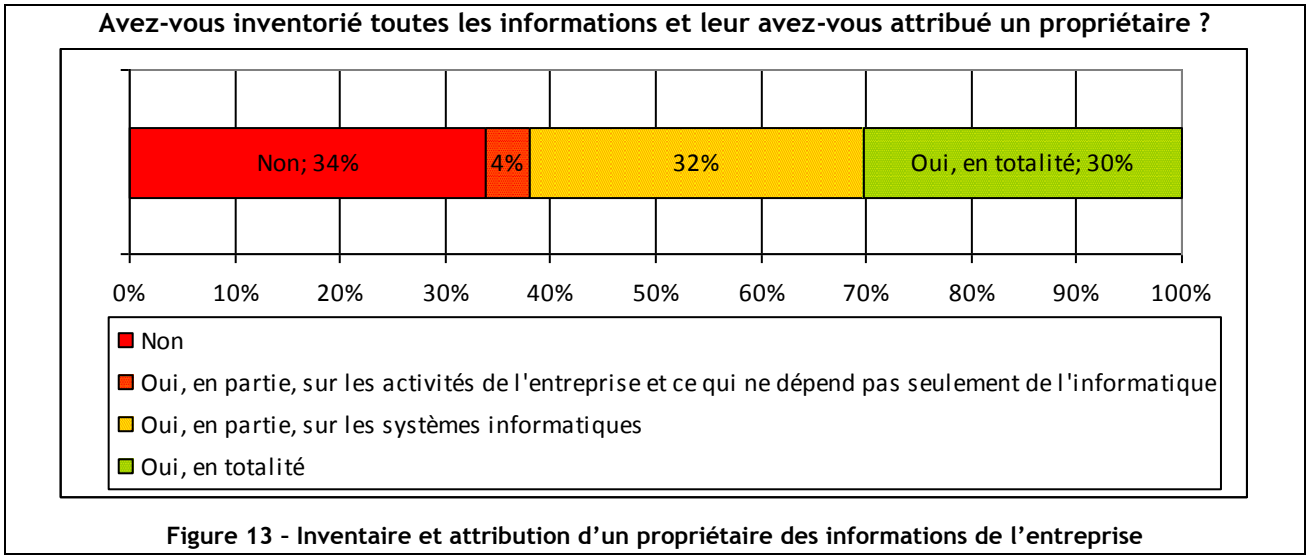

Figure 13 – Inventaire et attribution d'un propriétaire des informations de l'entreprise

Une fois l'inventaire réalisé, la question de la classification des informations se pose. 23% des entreprises ayant réalisé un inventaire annoncent avoir effectué une classification des informations ce qui signifie que seulement 7% des entreprises disposent de cette classification sur la totalité de leurs biens informationnels.

L'échelle des critères utilisée comporte, pour une majorité (42%) trois niveaux de sensibilité, alors que pour 26% une échelle à deux niveaux semble suffisante ; le reste utilisant une échelle à 4 niveaux, voire plus.

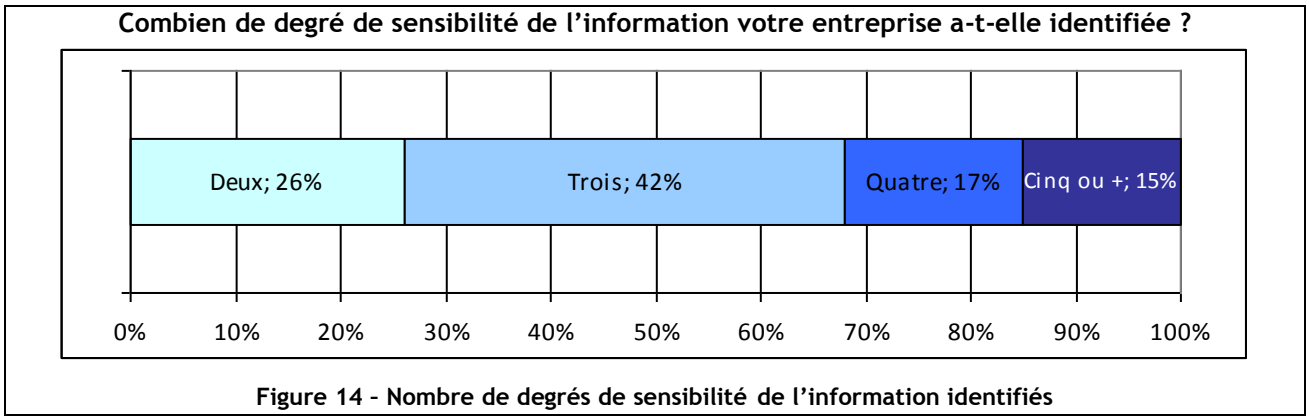

Figure 14 – Nombre de degrés de sensibilité de l'information identifiés

Cette information est intéressante car elle fait ressortir qu'une grande majorité (+ 50%) utilise une échelle disposant d'un nombre impair de niveaux, ce qui offre toujours la possibilité d'utiliser un niveau médian, donc non significatif…

Sans surprise, le critère de confidentialité des informations arrive en tête (88%) des critères employés devant la notion de disponibilité (69%). Pour autant, la confidentialité n'est qu'assez rarement traité au niveau attendu…

Une pratique de l'analyse de risque difficile à cerner…

Seulement 38% des entreprises réalisent des analyses de risques avec une méthode formelle, 20% le font sur une partie du Système d'Information et 3% sur des activités qui ne dépendent pas uniquement du Système d'Information.

Au final, 15% des entreprises réalisent une analyse de risques exhaustive sur l'ensemble de leur Système d'Information par le biais d'une méthode formelle (MEHARI, EBIOS, etc.).

Sur ces 38%, le nombre ayant entrepris un plan d'action suite à l'analyse de risque, reste quasi-identique entre 2008 et 2010, soit environ 90%. Ce qui change, c'est la proportion ayant réalisée ce plan sur l'ensemble du Système d'Information qui est passée de 41% en 2008 à 54% en 2010. À l'inverse, les entreprises n'ayant agi que sur une partie du SI, sont passées de 49% en 2008 à 35% en 2010. La prise en compte de la sécurité sur la globalité du SI effectue donc un net progrès comme les chiffres le laissent apparaître clairement.

Concernant la réalisation des analyses de risque, le RSSI trouve sa position de leader largement confortée en 2010, au détriment des propriétaires des actifs ou des projets et de la direction informatique. En 2008, 20% des analyses de risques étaient effectuées par des tiers mal identifiés ; en 2010, on s'aperçoit que les responsables des services généraux commencent à s'engager dans une démarche d'analyse de risques. Le débat n'est pas clos…

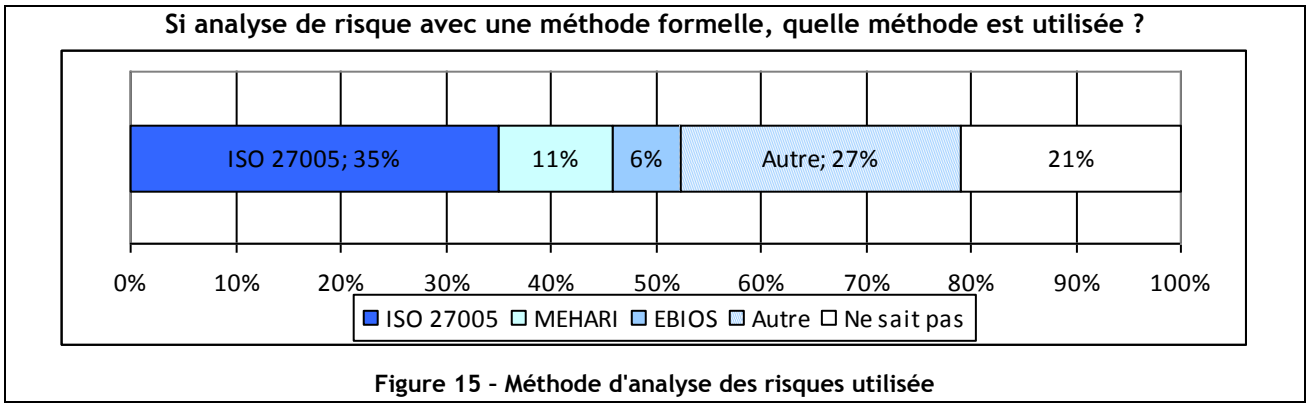

Figure 15 – Méthode d'analyse des risques utilisée

La norme ISO est-elle une méthode d'analyse de risque ?… Si l'on en croit les réponses à l'enquête, il semblerait que pour une majorité, la réponse soit « oui », car 36% des personnes interrogées reconnaissent l'avoir utilisée pour mener à bien une analyse de risque et 27% utilise une autre méthode.

Les méthodes formelles telles qu'EBIOS ou MEHARI ne recueillent qu'un score de 18% avec un avantage à MEHARI, certainement lié aux outils disponibles. Est-ce un problème de perception (lourdeur des méthodes), ou un manque de compétences, toujours est-il que presque un tiers des entreprises (27%) utilise une autre méthode, souvent propriétaire.

Thème 8 : Sécurité liée aux Ressources Humaines

Chartes de sécurité : augmentation sensible, toute taille d'entreprise confondue

La proportion d'entreprises qui déclarent disposer d'une charte sécurité a globalement fortement progressé (+15 à +20% selon leur taille) entre 2008 et 2010. Reste qu'un tiers des entreprises n'en dispose toujours pas. Pourtant, ce document contribue de manière importante à la sensibilisation des utilisateurs et à la réglementation de leurs pratiques.

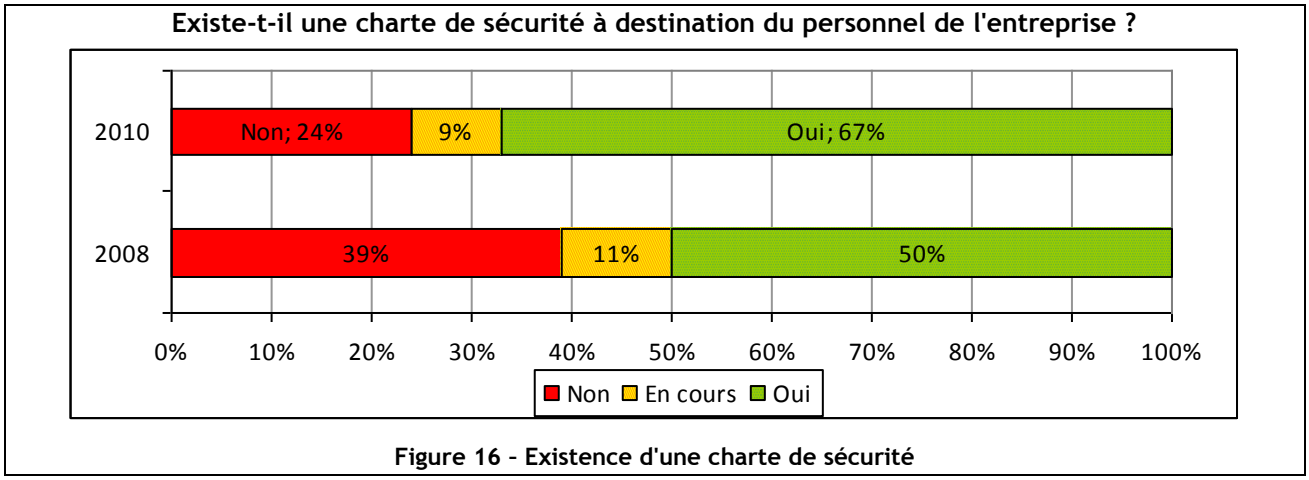

Figure 16 – Existence d'une charte de sécurité

Les entreprises de plus de 1000 personnes (avec près de 83%) ainsi que celles du secteur des services (40%) ont une longueur d'avance, signe d'une certaine maturité de la politique de sécurité et de moyens plus conséquents.

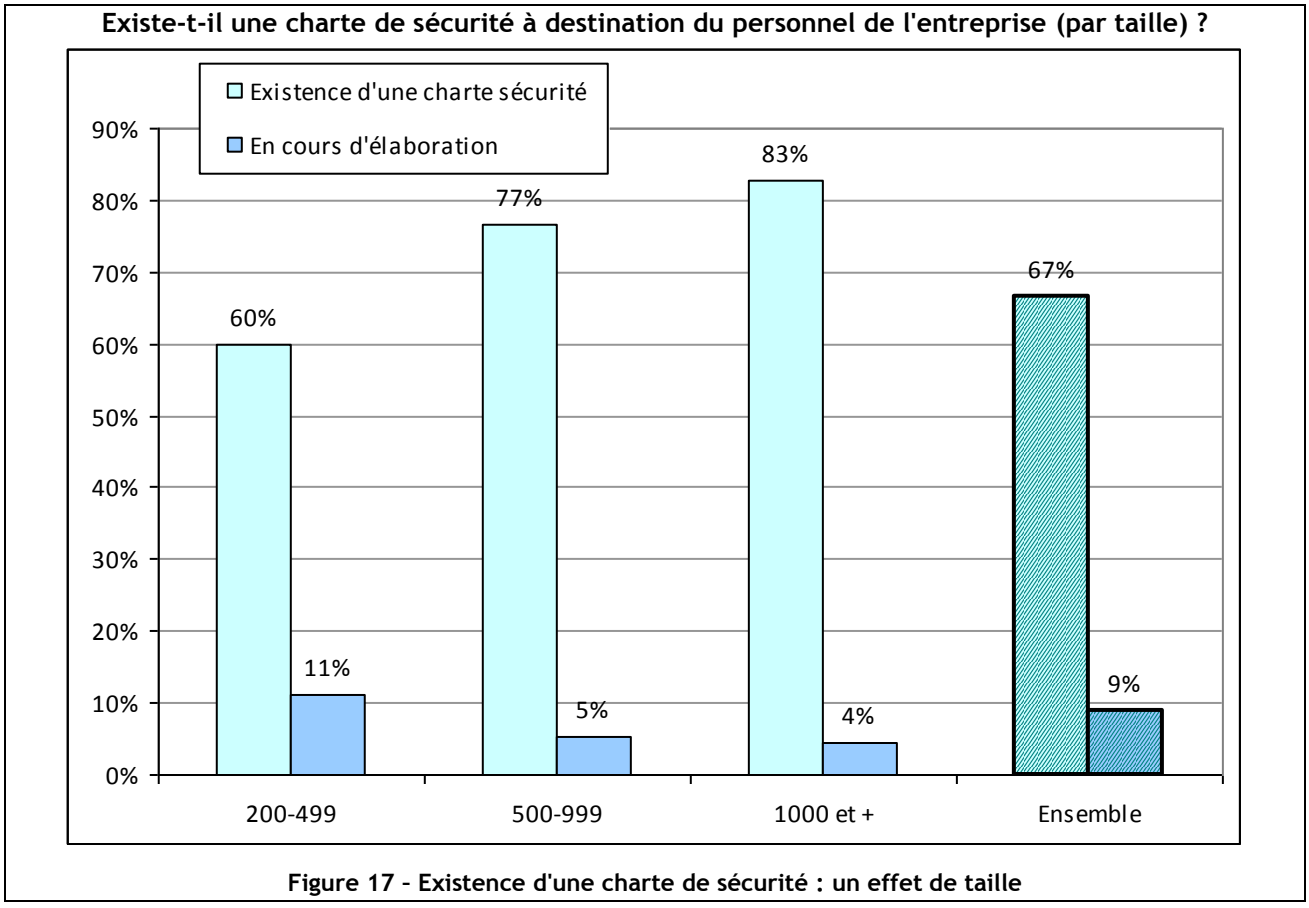

Figure 17 – Existence d'une charte de sécurité : un effet de taille

Dans près de neuf entreprises disposant d'une charte sécurité sur dix (88%), cette charte est communiquée à l'ensemble des collaborateurs (qui la signent dans 40% des cas) et son contenu précise les sanctions disciplinaires applicables dans 53% des cas (-3% vs 2008). Sur ce dernier point, la taille de l'entreprise a une influence : 64% de plus de mille salariés ont intégré les sanctions dans le règlement intérieur, contre 47% pour les PME de 200 à 499 salariés.

La sensibilisation des collaborateurs : une pratique toujours peu répandue

L'existence d'une charte n'est pas toujours complétée par des opérations de sensibilisation des collaborateurs aux bonnes pratiques de sécurité. Seulement un tiers des entreprises (32%, -3% vs 2008) a institué des programmes de sensibilisation à la sécurité de l'information (46% des entreprises de plus de mille salariés).

La panoplie des outils de sensibilisation à la sécurité n'est toujours pas bouleversée par rapport à nos deux dernières enquêtes. Ainsi, les actions les plus simples – publication d'articles sur l'Intranet ou le journal interne (19%) et la sensibilisation des nouveaux arrivants (27%) – sont les plus utilisées. En revanche, leur efficacité n'est pas mesurée dans 63% des cas.

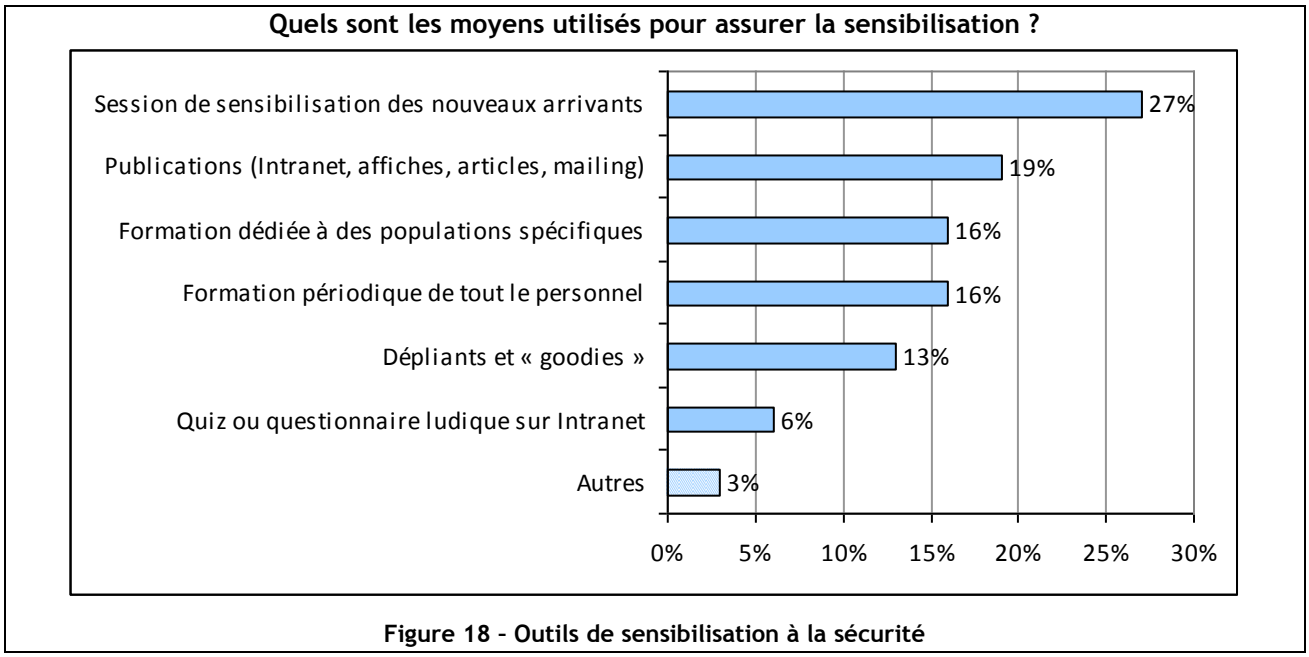

Figure 18 – Outils de sensibilisation à la sécurité

Globalement, nous estimons que les actions de sensibilisation restent encore largement insuffisantes alors que le facteur humain est toujours, à juste titre, présenté comme un des points de faiblesse majeur en termes de sécurité dans l'entreprise : seul 16% du personnel (-2% vs 2008) fait l'objet de formation / information de manière récurrente et seulement 27% des nouveaux arrivants sont sensibilisés (contre 36% en 2008). On préfère se contenter pour l'instant d'une communication standardisée, sous la forme de diffusion d'articles et/ou d'affiches, qui est clairement moins efficace, mais somme toute moins chère…

Thème 9 : Sécurité Physique

La gestion des données sur papier en mal de responsable…

La responsabilité de la sécurité physique des données sur papier est généralement mal identifiée (dans 41% des cas). Or le RSSI (ou le RSI) a un vrai rôle à jouer dans ce domaine. En effet, au-delà des risques d'intrusion informatiques, l'accessibilité des informations sensibles sur papier constitue un enjeu. Le développement des risques liés à l'intelligence économique et à l'espionnage implique une plus grande vigilance et constitue un véritable axe de progrès.

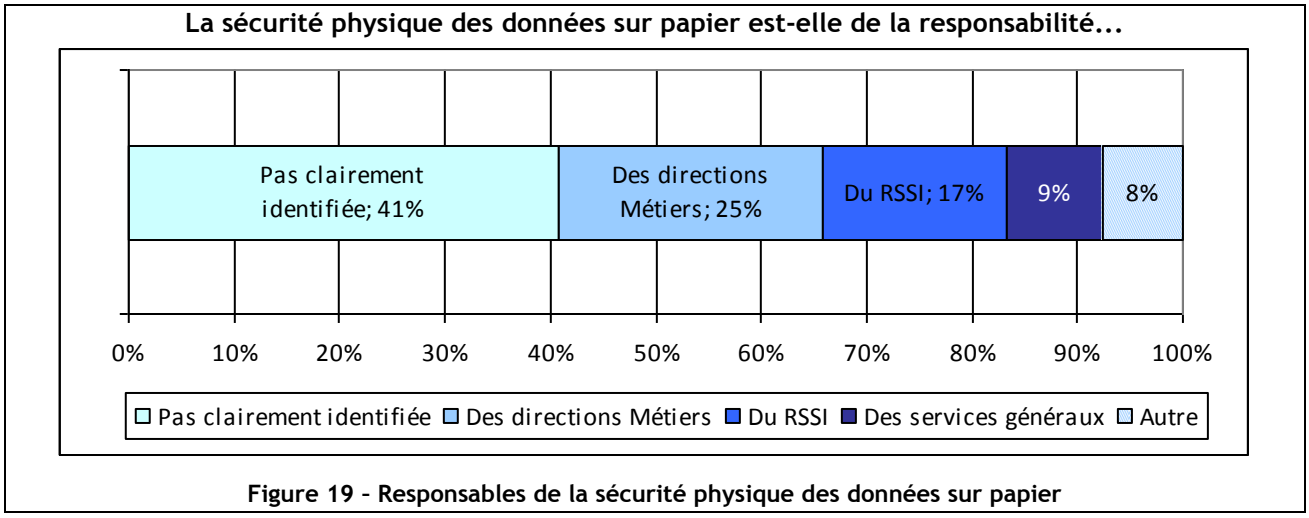

Figure 19 – Responsables de la sécurité physique des données sur papier

Le Responsable des Services Généraux donne les moyens (destructeur de documents, armoire forte, coffre-fort, copieur diskless) en fonction des besoins exprimés par les Directions métiers. Le RSSI ou le RSI, avec le Responsable Sûreté, sont les garants de la bonne cohérence des dispositifs de protection des documents papiers au sein de l'entreprise.

Thème 10 : Gestion des opérations et des communications

Sécurisation des nouvelles technologies

L'évolution des nouvelles technologies connectées avec le SI se stabilise : peu de nouvelles grandes innovations (telles que le wifi, les PDA/Smartphones ou la ToIP) sont apparues sur le marché. D'un autre côté, la politique des entreprises par rapport à l'usage de ces nouvelles technologies mûrit lentement : globalement, l'interdiction pure et simple au sein des politiques de sécurité diminue en tant que méthode retenue pour se prémunir des risques de sécurité induits par leurs usages.

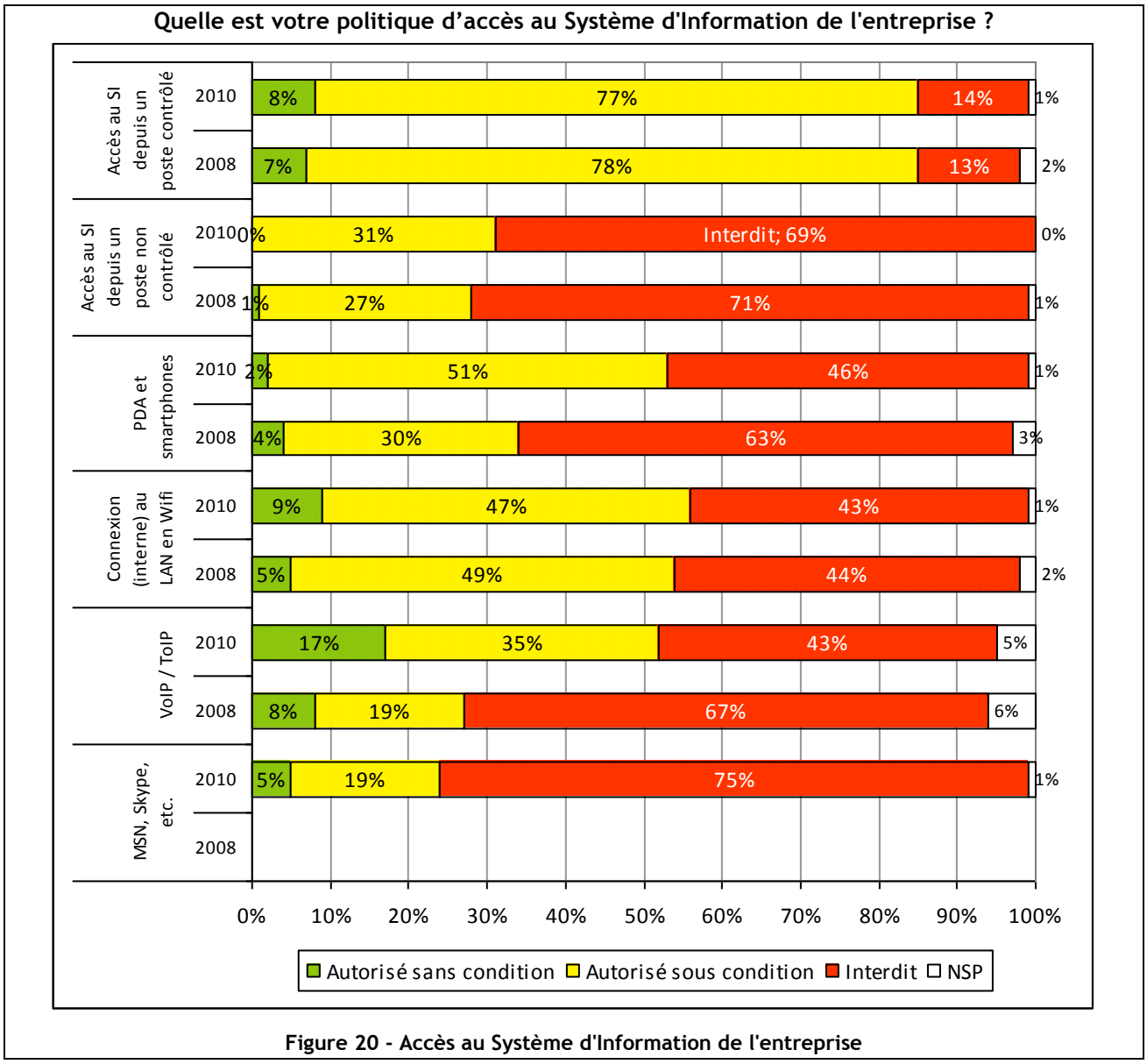

Figure 20 - Accès au Système d'Information de l'entreprise

Un accroissement du nomadisme

Le développement de nouveaux modes de travail « plus efficaces » (avoir accès à sa messagerie de n'importe où), plus « verts » (minimiser les déplacements), voire plus sécuritaires (travailler de chez soi en cas de pandémie) pousse au déploiement des nouvelles technologies liées à la mobilité.

Si l'accès au SI via un ordinateur portable fourni par l'entreprise reste stable, l'usage d'un poste de travail non maîtrisé (cybercafé, PC personnel, etc.) est de plus en plus autorisé (sous condition) pour entrer dans le SI. Compte tenu du besoin de nomadisme grandissant, cette autorisation connaît néanmoins

une hausse limitée (+4%) du fait de la difficulté à maîtriser les vulnérabilités et menaces que ce type d'accès peut engendrer.

Les PDA / smartphones connaissent une augmentation importante de leur usage (plus de la moitié des entreprises l'autorise) alors même que le marché du téléphone portable en général est en baisse. Ces équipements, essentiels pour les entreprises qui ont toujours besoin de plus de réactivité, portent en eux des failles de sécurité (politique de code PIN / mot de passe faible, vol ou perte d'informations confidentielles, installation d'applications comportant du code malveillant, etc.) qui constitueront un défi certain pour les SI de demain.

L'utilisation du wifi en entreprise reste assez stable, en légère augmentation (56% contre 54%) : cette technologie, pour laquelle il existe des systèmes d'authentification et de chiffrement maintenant solides, entre dans le paysage réseau classique du SI des entreprises.

Une hausse attendue du déploiement de la VoIP et de la ToIP

Dans un contexte de réduction des coûts, le déploiement de la VoIP ou de la ToIP constitue toujours dans l'esprit des entreprises une source d'économie importante. Les fortes prévisions d'équipement des années précédentes n'ont pas menti : cette technologie est en solide augmentation et ce alors que les besoins de disponibilité et de qualité du service sont toujours aussi importants.

La messagerie instantanée encore peu autorisée

Nouveauté de l'étude : la messagerie instantanée apparaît comme une nouvelle technologie peu utilisée puisque 75% des entreprises interrogées interdisent son usage. Les problématiques de sécurité liées sont nombreuses (confidentialité et chiffrement des échanges, journalisation des conversations, transmission des virus, fuite d'information, etc.) et le déploiement de cette technologie semble fortement rebuter les DSI car elle représente une source de risques importante. Cette position est cependant à nuancer en considérant que les systèmes de messagerie instantanée d'entreprise, au contraire des systèmes publics, permettent de garder une bonne maîtrise du niveau de sécurité.

Technologies de protection et de gestion des vulnérabilités

Comme lors de l'étude précédente, on distingue clairement 3 technologies faisant l'objet d'un équipement systématique, ou quasi. Ce sont les antivirus/antispywares, les antispams et les firewalls. Concernant les premiers, 40% des entreprises déclarent avoir été malgré tout victimes d'incidents. Sans oublier que « Conficker » est sans doute pour quelque chose dans ces 40%, il n'en reste pas moins que garantir une mise à jour parfaite d'un parc étendu (en quantité, en nombre de sites, en ordinateurs portables) est souvent une tâche ardue…

Les autres technologies ne font pas l'objet d'un usage aussi systématique, avec un niveau d'équipement allant de 10 à 50%.

Quelles technologies de sécurité utilisez-vous pour lutter contre les vulnérabilités, les intrusions ?

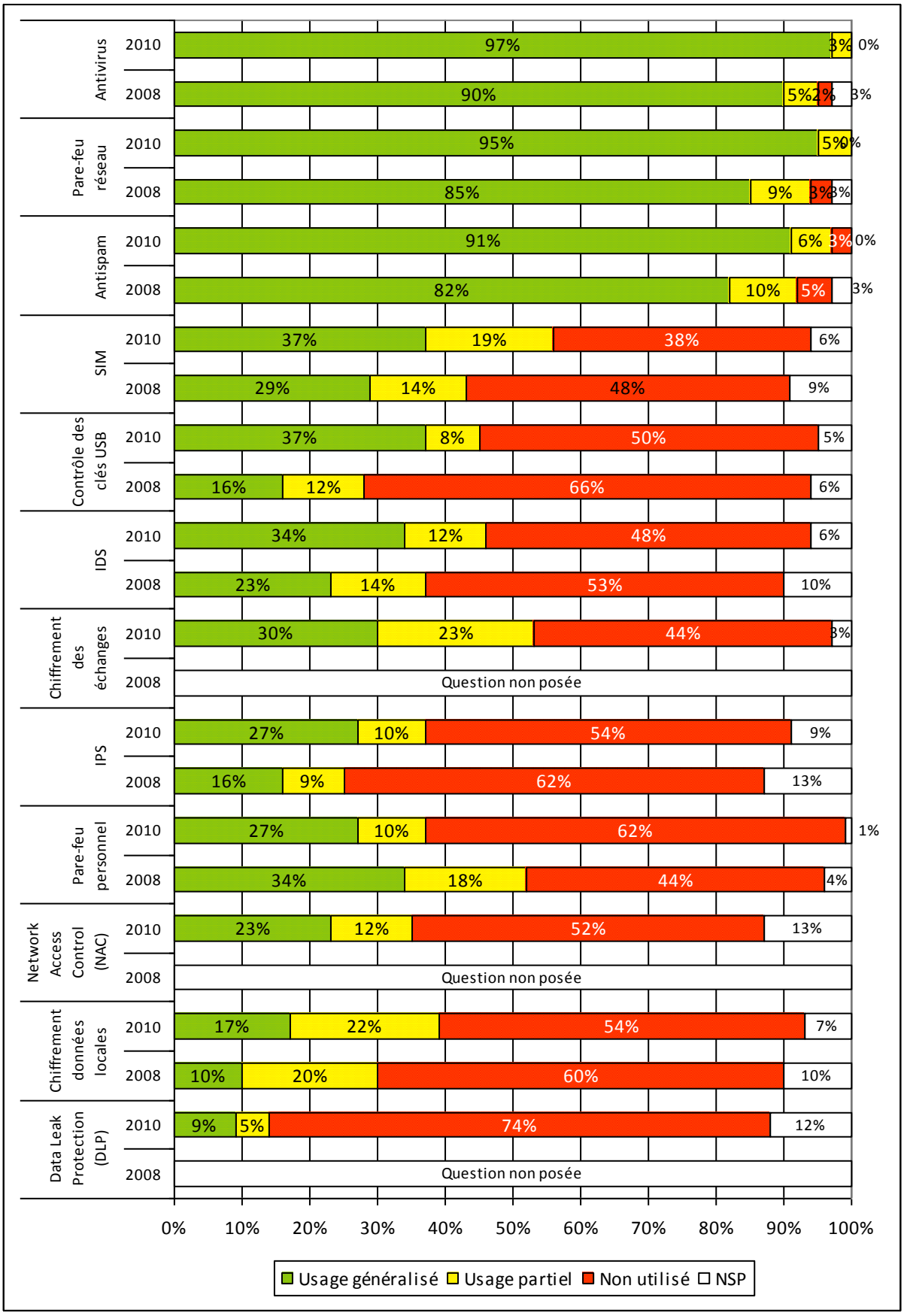

Figure 21 - Technologies de sécurité / lutte antivirale, anti-intrusion, gestion des vulnérabilités

Côté sécurité réseau, les IDS/IPS ont vu leur usage croître de 10% depuis la dernière étude, portant le taux d'équipement des entreprises à environ 50%. 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 (c'est d'ailleurs souvent intégré aux firewalls de type UTM), et peuvent fournir aussi un cloisonnement interne pour limiter l'ampleur d'une infection sans limiter les échanges (et donc les usagers) à l'intérieur du réseau d'entreprise.

Toujours sur le réseau, le NAC qui existe depuis quelques années reste relativement peu implanté (65% des entreprises s'en passent). 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 peut parfois être compliquée.

Venant en complément des infrastructures réseau, les SIMs (qui permettent d'exploiter les journaux en provenance des composants du réseau) équipent de plus en plus d'entreprises : 13% de plus en 2 ans, et la tendance devrait se confirmer pour atteindre le niveau de 60%. En effet, les organisations ont besoin de garder des traces pour des analyses a posteriori d'incidents de sécurité ; et parfois, en allant un peu plus loin, de gérer des alertes et de la corrélation (les deux pouvant être liées). La maturité des produits aujourd'hui sur le marché adresse en général bien la problématique de base (concentration de logs hétérogènes, gestion de leur archivage et des accès qui y sont faits), et propose également des fonctions d'alerte et de corrélation qui, elles, nécessitent un important travail d'analyse préalable (et récurrent) pour être pertinentes dans le cadre de l'entreprise concernée.

Du coté du poste de travail, les pare-feu personnels voient leur présence diminuer de 15% pour arriver à 40% en 2010. Il faut dire que les FW personnels, historiquement surtout déployés sur les parcs d'ordinateurs portables (potentiellement exposés hors du périmètre protégé), disparaissent dorénavant au profit des filtres réseau inclus dans les suites de protection du poste de travail désormais déployées sur les parcs. Ces suites peuvent comprendre un firewall, mais surtout un « Hosts IPS » dont le rôle est également de protéger contre les attaques réseau, mais avec un impact souvent plus léger en termes d'administration. À noter que ces fonctions « host IPS » ont pu révéler leur utilité réelle en permettant dans certains cas de limiter la diffusion de vers tels que « Conficker ».

Le contrôle des périphériques fait également parti des fonctionnalités ajoutées aux suites de protection du poste de travail, facilitant ainsi sa mise en place aujourd'hui de 45% (en progression de 15% par rapport à 2008). Ce contrôle de périphériques qui représente un enjeu important (pour contrôler l'entrée des virus et les fuites de données) n'est pas à proprement parler une nouveauté mais plutôt une remise au goût du jour des politiques de blocage des lecteurs de disquette qui ont existé par le passé (souvent suite à des infections virales…).

Les outils de chiffrement de données utilisateur voient leur niveau de déploiement augmenter avec 40% d'entreprises équipées en 2010, en progression de 10% par rapport à 2008. La spécificité de cette technologie est d'être déployée en majorité sur un périmètre restreint. Les ordinateurs portables restent les plus concernés par cette mesure, étant particulièrement susceptibles de stocker des données importantes (en comparaison des postes fixes qui pourront travailler exclusivement sur le réseau), et étant par nature plus sujets au vol. Le taux d'équipement reste malgré tout relativement faible au regard des parcs de portable en circulation, mais la croissance prévisible du niveau d'équipement reste stable (5% d'intentions d'achat pour l'année 2010).

Le chiffrement des échanges est aujourd'hui bien implanté avec plus de 50% d'entreprises équipées. Il reste utilisé le plus souvent dans un contexte purement réseau (80% des entreprises équipées d'échanges chiffrés le sont pour du VPN) et beaucoup moins pour le chiffrement des échanges serveurs (30% font du https). Il sera d'ailleurs intéressant de surveiller ce dernier indicateur : en effet, de plus en plus d'applications stratégiques ou contenant des données confidentielles sont mises à disposition en mode Web, et sont donc faciles à intercepter pour qui le souhaiterait.

Dernière technologie sur le marché, et surtout la seule à porter sur le contenu des informations en tant que tel, le DLP 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 (15%), mais il faut dire que la technologie est 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

L'information dans les nuages (Cloud Computing), les applications en mode hébergé (SaaS, ASP) ont le vent en poupe. Ce n'est pas un sujet nouveau que d'externaliser tout ou partie de son SI chez un tiers, surtout pour une recherche de coût moindre ou tout simplement par manque de compétences… L'entreprise qui externalise son SI doit alors porter une attention particulière sur le respect par son prestataire d'indicateurs de services, dont la sécurité doit faire partie.

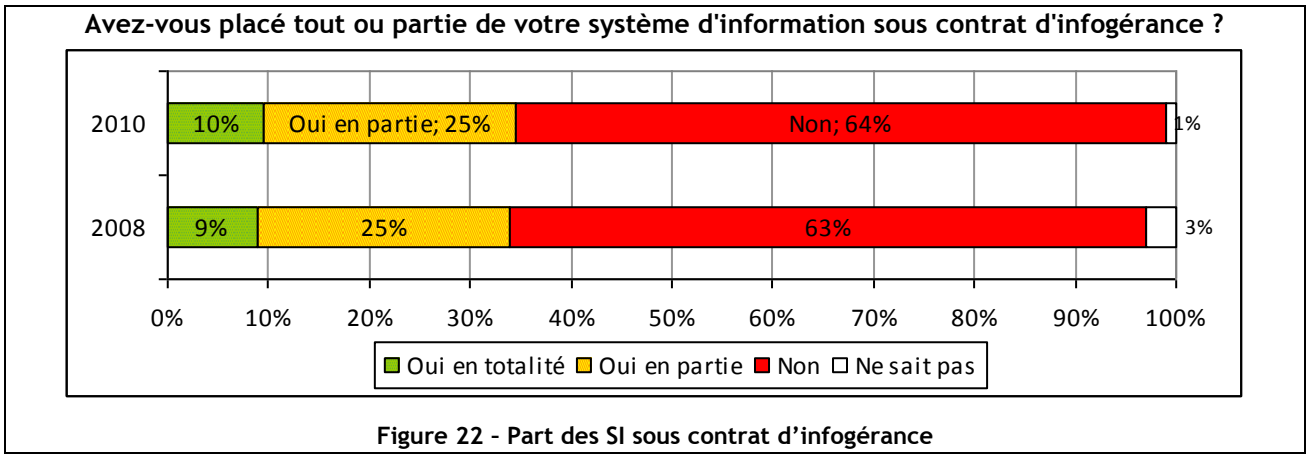

Figure 22 – Part des SI sous contrat d'infogérance

Il semble que cette externalisation progresse très faiblement, le Cloud Computing n'étant donc pas encore mature…

Toutefois, le suivi d'indicateurs de sécurité est plus poussé, signe évident d'une maturité plus forte des SI (ITIL, ISO27000).

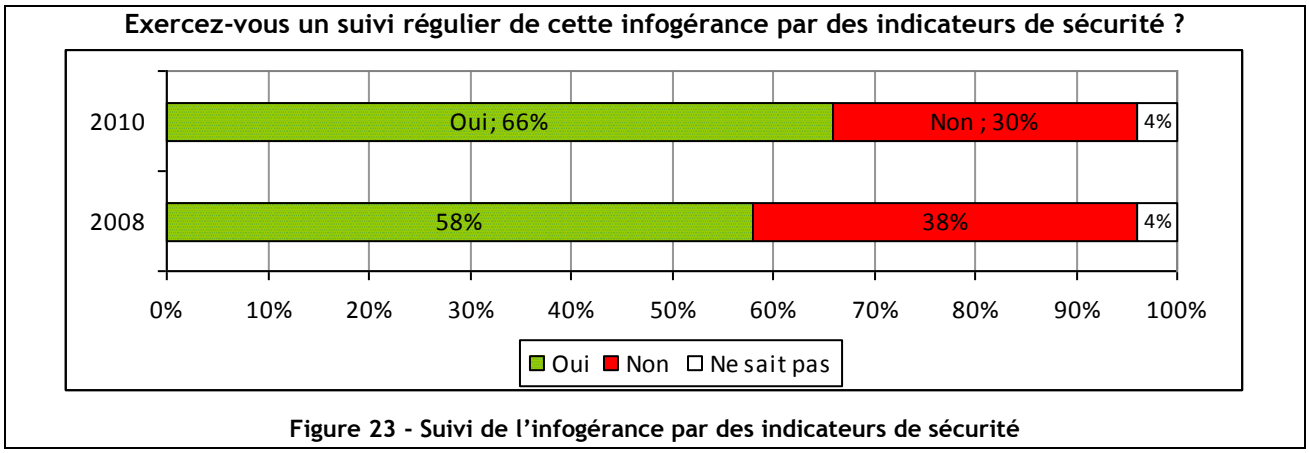

Figure 23 - Suivi de l'infogérance par des indicateurs de sécurité

En revanche, les audits des SI infogérés sont fortement en baisse (28% en 2010, -30% vs 2008), tout en notant qu'apparaissent les audits ponctuels, signe probable de la mise en place d'éléments de contrôles ou d'indicateurs au sein des infogéreurs, souvent liés à la mise en œuvre de bonnes pratiques ou de normes (ITIL, ISO 20000, ISO 27000, etc.) ; ces indicateurs étant alors souvent fournis aux clients.

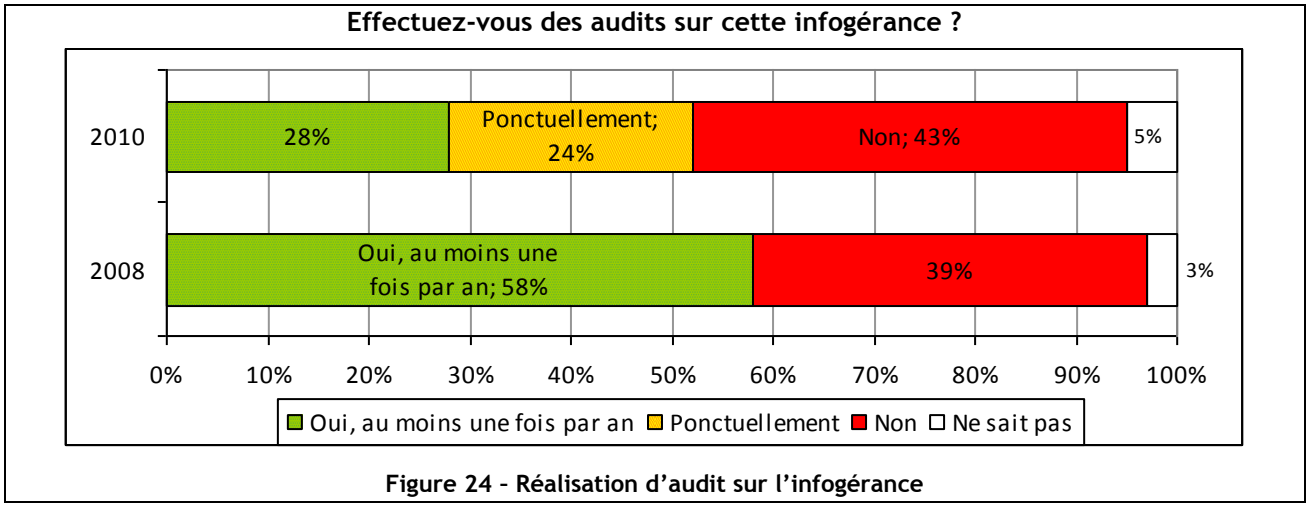

Figure 24 – Réalisation d'audit sur l'infogérance

Thème 11 : Contrôle des accès logiques

On constate que ces technologies restent peu déployées, et surtout que la situation ne semble pas avoir évoluée en deux ans, puisque les résultats 2010 sont presque identiques à ceux de 2010, à l'exception du SSO et du Web SSO. Alors que l'ouverture des systèmes et surtout le nomadisme se sont considérablement accélérés depuis 2006, cette absence d'évolution côté contrôle d'accès est préoccupante.

Stagnation de la biométrie et des certificats

Les moyens d'authentification sont la clé de voûte de l'identité numérique et sont donc un des éléments fondamentaux de sécurisation des SI, notamment pour les aspects liés à la traçabilité. Si la très grande majorité des entreprises n'utilise toujours pas d'authentification forte, ni n'envisage d'expérimenter les diverses solutions disponibles courant 2010, on constate également une stagnation de la biométrie : 3% des entreprises l'utilise largement (-1% vs 2008) et 14% sont en cours d'expérimentation (+1% vs 2008).

Concernant l'utilisation des certificats sur support logiciel ou matériel, on note ici aussi, globalement, une stagnation : 19% pour l'authentification par certificat électronique logiciel (+4% vs 2008) et 7% pour l'authentification forte par certificat électronique sur support matériel (-1% vs 2008).

Tout comme en 2008, il faut noter que les entreprises pionnières en la matière ne sont pas les plus grandes, mais celles dans la tranche de 500 à 999 salariés. Elles sont par exemple 25% (+6% vs 2008) à utiliser largement des certificats logiciels, et 27% (+12% vs 2008) des certificats sur support matériel (carte à puce, clé USB cryptographique, etc.), contre respectivement 21% et 18% sur l'ensemble des entreprises.

Gestion des habilitations : léthargie étonnante

Les modèles de gestion des habilitations n'ont pas évolué en quatre ans, 6 entreprises sur 10 n'ayant pas de gestion par rôle ou par profil métier (tel que le modèle RBAC : Role Based Access Control), et n'envisageant pas à court terme de s'en doter. Ce modèle étant une condition souvent nécessaire à la maîtrise des droits, il est à craindre que ces entreprises ne puissent rationaliser leurs processus de gestion de droits.

Même constat pour la mise en place d'un workflow de validation des habilitations (18%, +3% vs 2008).

Seule la mise en œuvre d'un système de distribution automatique des droits (provisioning) fait une progression sensible, avec 18% d'entreprises disposant de dispositifs pleinement opérationnels stables (+9% vs 2008).

Le faible nombre d'entreprises envisageant de renforcer leur gestion des habilitations en 2010 est surprenant (entre +3 et +5%), puisque les évolutions légales et réglementaires (Loi sur la Sécurité Financière, Sarbanes-Oxley, Solvency II, etc.) tendent à augmenter le niveau d'exigence en matière de traçabilité et de maîtrise des droits d'accès.

Contrôle d'accès et SSO : ils « décollent »… tranquillement !

Les dispositifs de Single Sign-On (SSO et Web SSO) prennent enfin leur envol… Toutefois, les chiffres restent faibles au regard des enjeux :

- SSO, 21% déployé (vs 7% en 2008),
- Web SSO, 8% déployé (vs 3% en 2008).

Reste que près des deux-tiers des entreprises n'envisagent toujours pas de telles solutions, qui apportent pourtant un réel confort aux utilisateurs, facilitant ainsi le respect des politiques de mots de passe plus strictes et une traçabilité accrue.

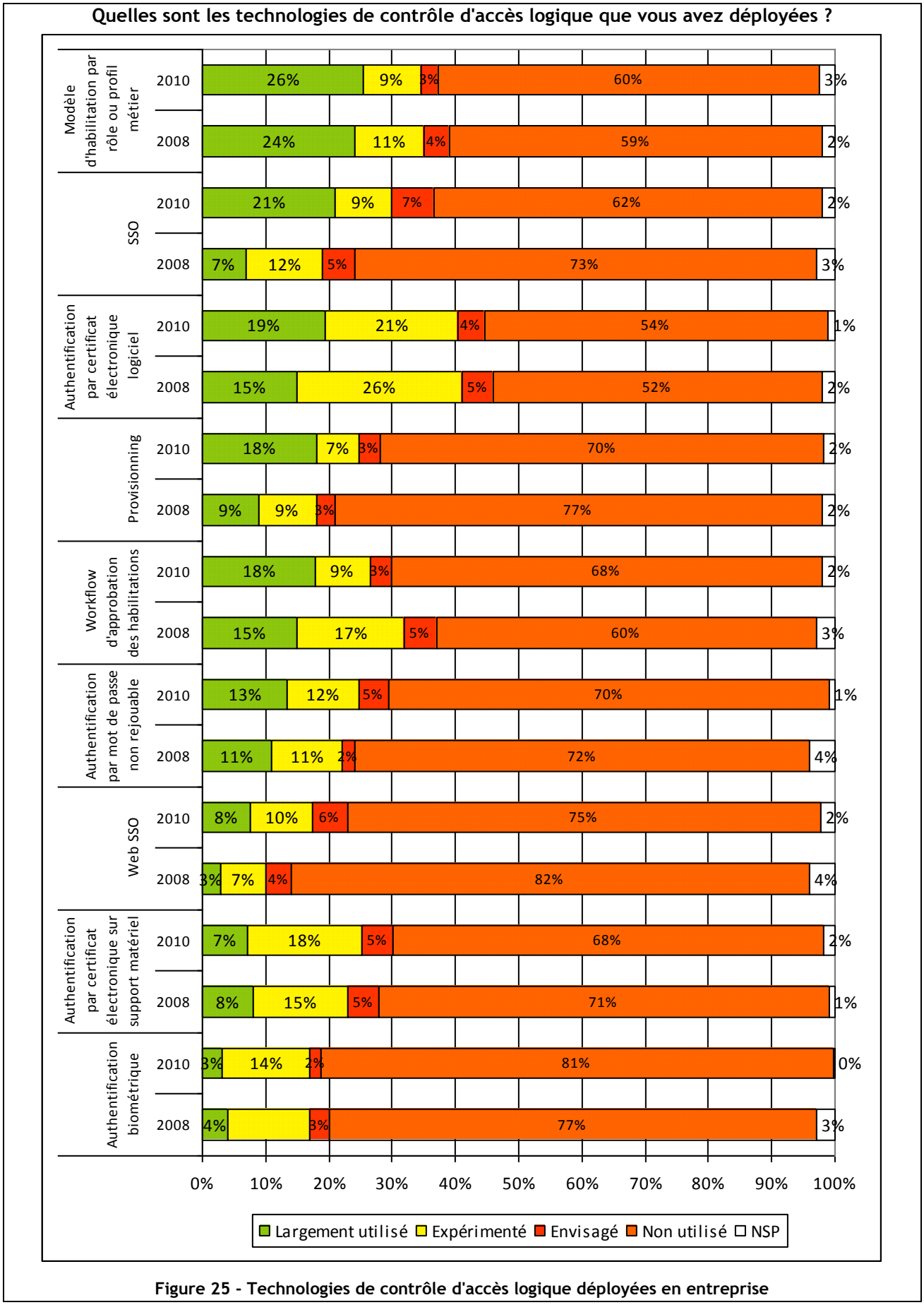

Figure 25 - Technologies de contrôle d'accès logique déployées en entreprise

Thème 12 : Acquisition, développement et maintenance

Veille et patch management en nette progression

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

Cette veille en vulnérabilités et en solutions de sécurité est en nette progression. L'impact des failles publiées et faisant régulièrement la une des journaux aidant sûrement à cette prise de conscience.

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

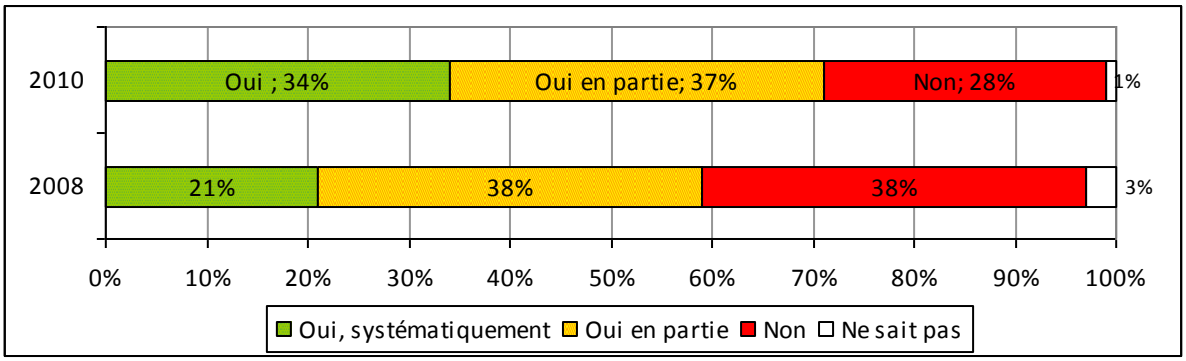

Figure 26 – Veille en vulnérabilités et en solutions de sécurité

De même, la formalisation des procédures opérationnelles de mise à jour est en très forte amélioration indiquant une maturité évidemment plus forte des Systèmes d'Information et de leur rôle central.

Avez-vous formalisé des procédures de déploiement de correctifs de sécurité (patch management) ?

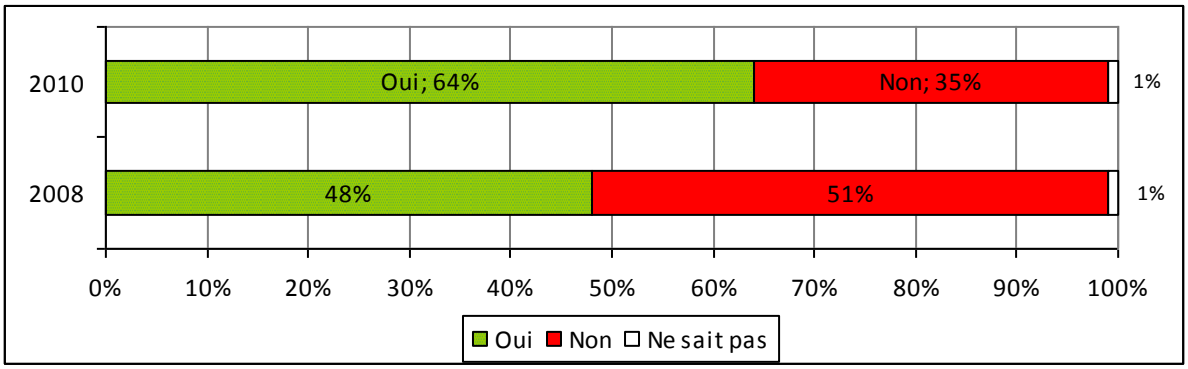

Figure 27 - Formalisation des procédures de déploiement de correctifs de sécurité

Toutefois, cette maturité semble impacter directement les délais de mise en œuvre de ces mises à jour en les augmentant à plus d'une journée.

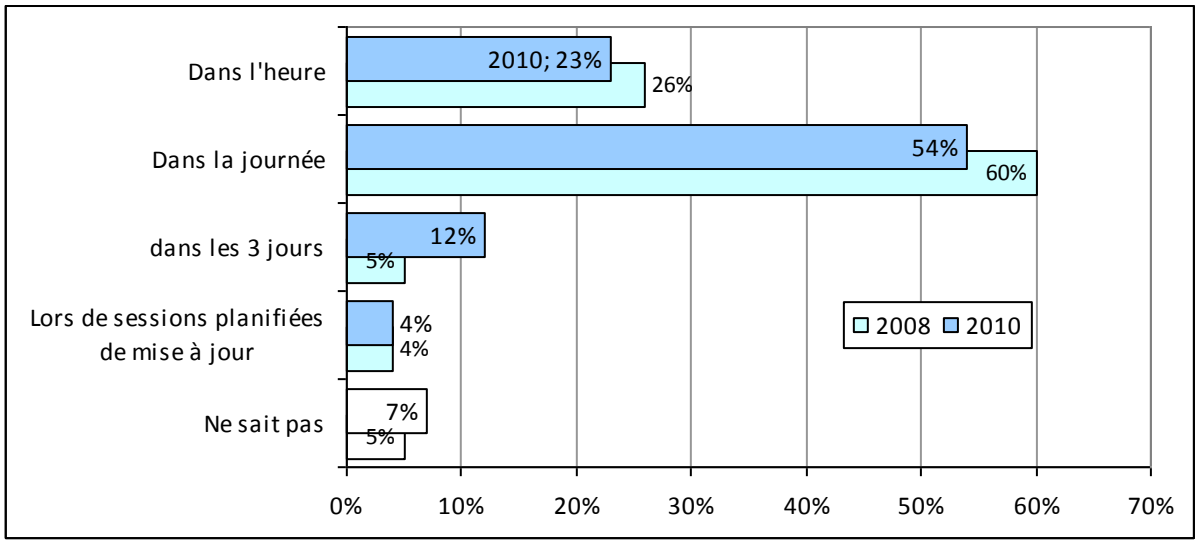

Figure 28 - Délai nécessaire pour déployer les correctifs en cas de menace grave

Concernant les développements, peu de sociétés (20%) déclarent mettre en œuvre des cycles de développements sécurisés. Parmi les entreprises ayant mis en place un cycle sécurisé, la majorité ne colle pas à une méthode « formelle » (INCAS, OWASP CLASP, Cigital DSL, SDLC, etc.), mais applique plutôt des bonnes pratiques pragmatiques.

Thème 13 : Gestion des incidents – Sinistralité

De plus en plus d'entreprises gèrent les incidents de sécurité…

Les entreprises prennent conscience de la nécessité de suivre les incidents de sécurité du SI : un peu plus de la moitié (51%, +12% vs 2008) comprend dorénavant une équipe chargée de collecter et traiter ces incidents. Selon des facteurs comme la taille de l'entreprise ou l'importance accordée à la sécurité du SI, cette équipe correspond à une cellule dédiée à la sécurité (20%) ou mutualisée avec d'autres équipes informatiques (31%).

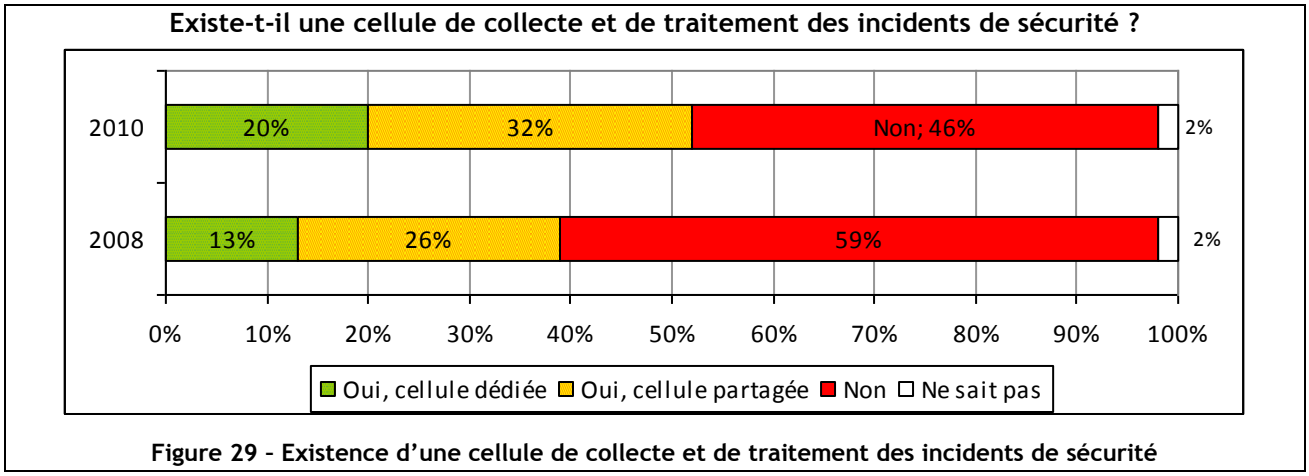

Figure 29 – Existence d'une cellule de collecte et de traitement des incidents de sécurité

Sans surprise, les incidents liés à l'informatique sont en quasi-totalité collectés (94%) tandis que ceux liés aux autres types d'informations ou aux processus sont majoritairement moins associés aux incidents de sécurité du SI (respectivement 39% et 45%).

… mais déposent toujours aussi peu de plaintes

Alors que le nombre d'incidents de sécurité du SI augmente dans les entreprises, les RSSI sont toujours aussi peu enclins à porter plainte (seulement 5%, -1% vs 2008). Le dépôt de plainte comporte un risque d'atteinte à l'image des entreprises qui souhaitent éviter de défrayer la chronique avec des incidents de sécurité impliquant parfois les données de leurs clients, employés, fournisseurs ou partenaires (par exemple : fuite d'information massive).

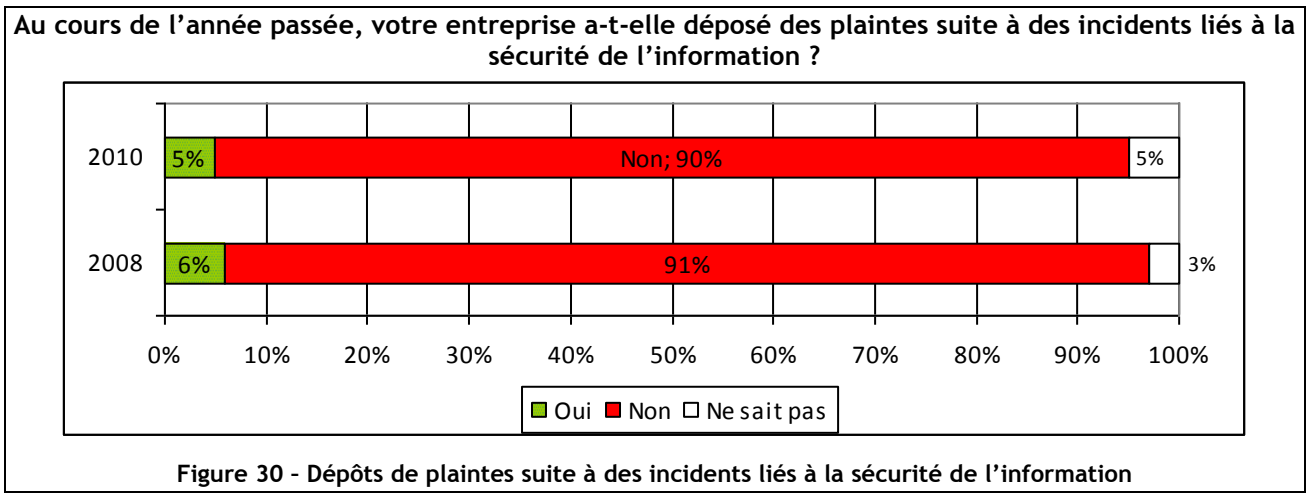

Figure 30 – Dépôts de plaintes suite à des incidents liés à la sécurité de l'information

Par rapport à 2006 et 2008, il n'y a pas de grosse évolution dans les types d'incidents rapportés. Les infections par des virus augmentent (+9% vs 2008), alors que les erreurs de conception diminuent fortement (24% vs 34% en 2008 et 58% en 2006).

Au cours de l'année passée, à quel type d'incidents de sécurité votre entreprise a-t-elle été soumise ?

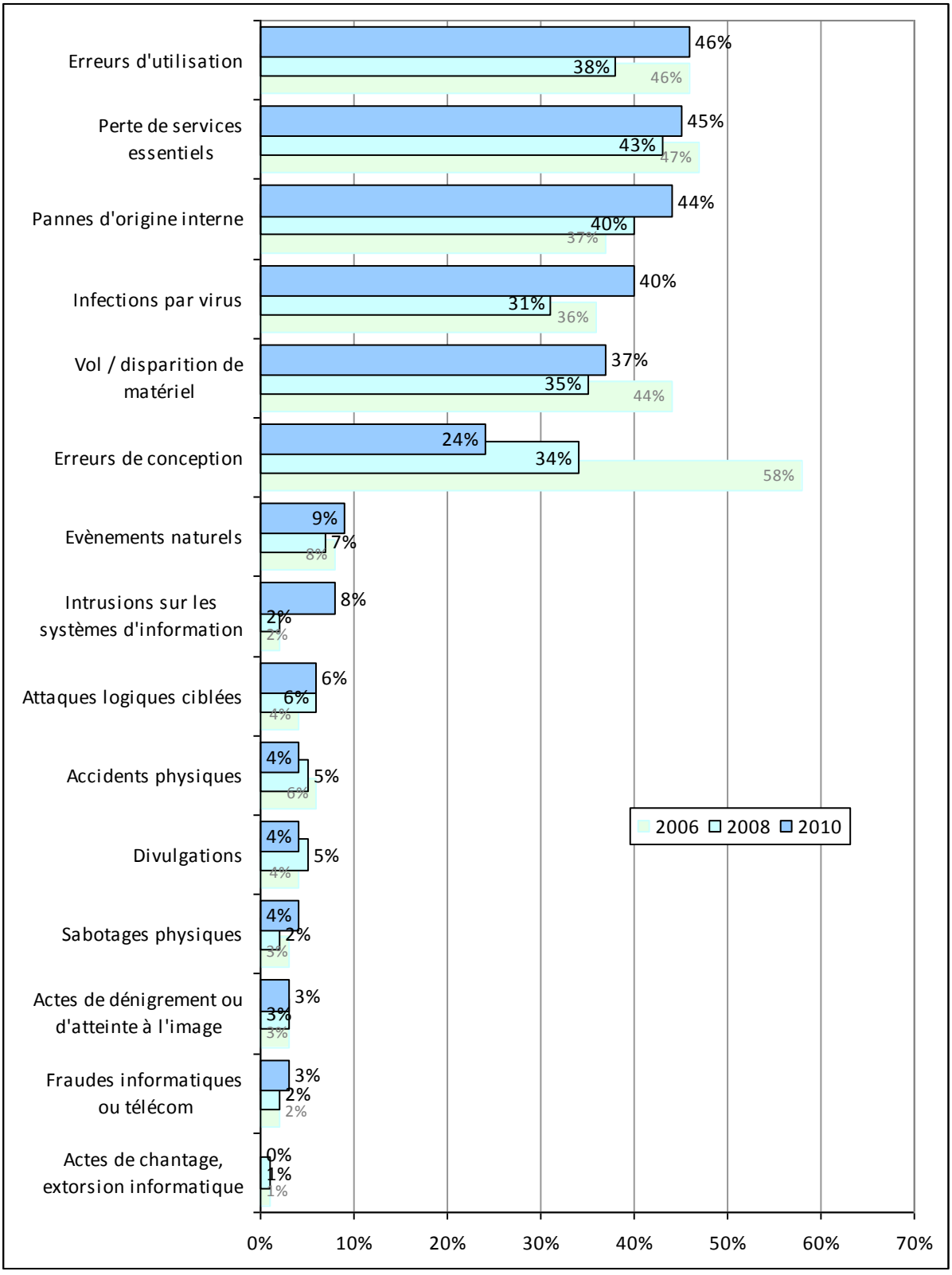

Figure 31 – Typologie des incidents de sécurité

Thème 14 : Gestion de la continuité d'activité

Une gestion de la continuité d'activité globalement bien prise en compte…

Globalement, la gestion de la continuité d'activité semble bien prise en compte par les entreprises. Elle est en forte progression par rapport à l'étude menée en 2008 (+12%). L'augmentation doit résulter en partie des fortes recommandations, voire obligations, de continuité d'activité auxquelles sont désormais confrontées de plus en plus d'entreprises.

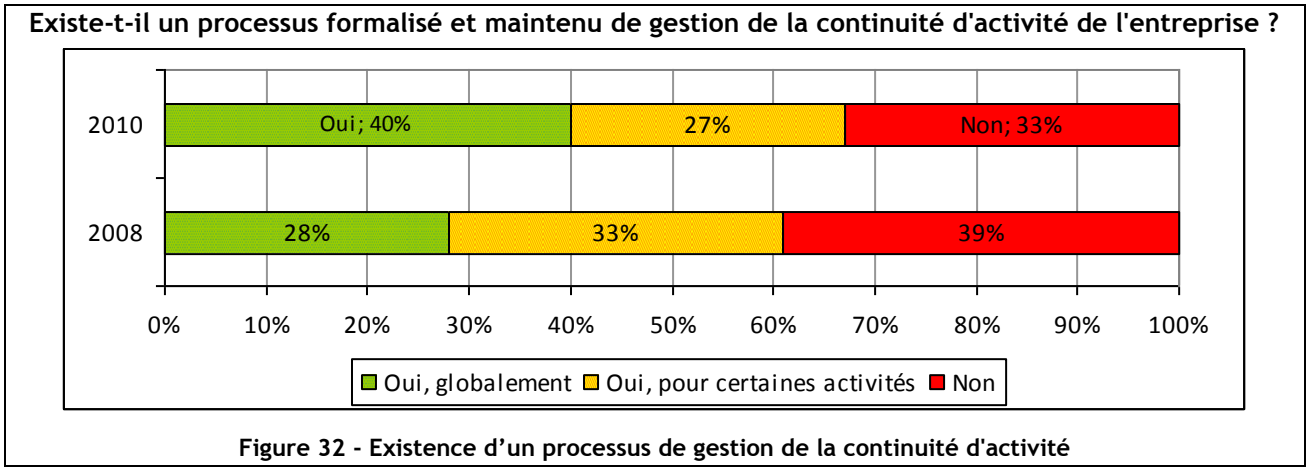

Figure 32 - Existence d'un processus de gestion de la continuité d'activité

Malgré cela, on constate toujours des inégalités. En effet, un tiers des entreprises interrogées n'a toujours pas pris en compte cette problématique au sein de leurs organisations. Ceci étant dit, nous attirons l'attention sur le fait que dans cette étude la gestion de la continuité d'activité couvre essentiellement les enjeux liés aux systèmes informatiques. Or, faut-il rappeler que la continuité d'activité doit d'abord définir les exigences de continuité métier pour ensuite, et seulement ensuite, identifier les moyens techniques permettant d'y répondre. Si près d'une entreprise sur 2 n'identifie pas en amont les besoins métiers en termes de continuité d'activité, alors les moyens informatiques mis en places peuvent-ils convenablement répondre aux besoins métiers des entreprises ?…

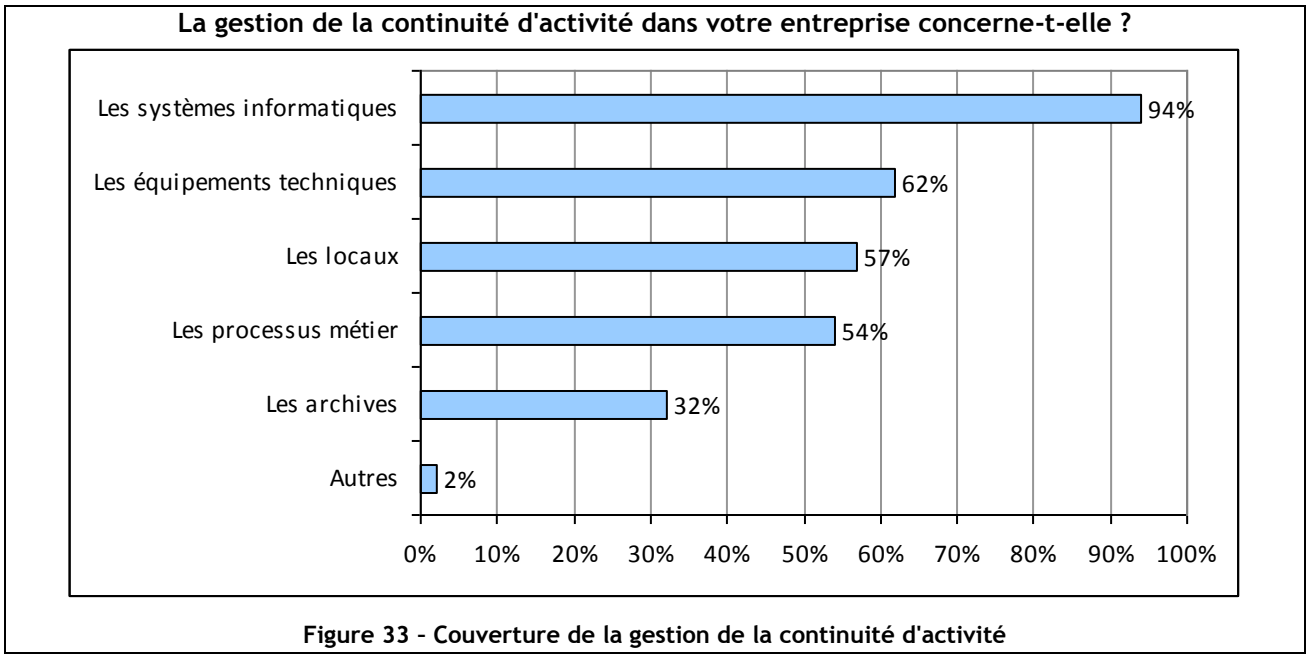

Figure 33 - Couverture de la gestion de la continuité d'activité

Des tests en légère régression…

On constate une faible diminution du nombre de tests réalisés plusieurs fois par an (-4%) mais, à l'inverse, une augmentation significative du nombre de tests réalisés une seule fois par an (+9%). Ceci semble étonnant voire peu rassurant. En effet, le lecteur est en droit de s'interroger sur le fait qu'un seul test réalisé au cours d'une année d'activité puisse correctement couvrir tous les besoins de l'organisation concernée.

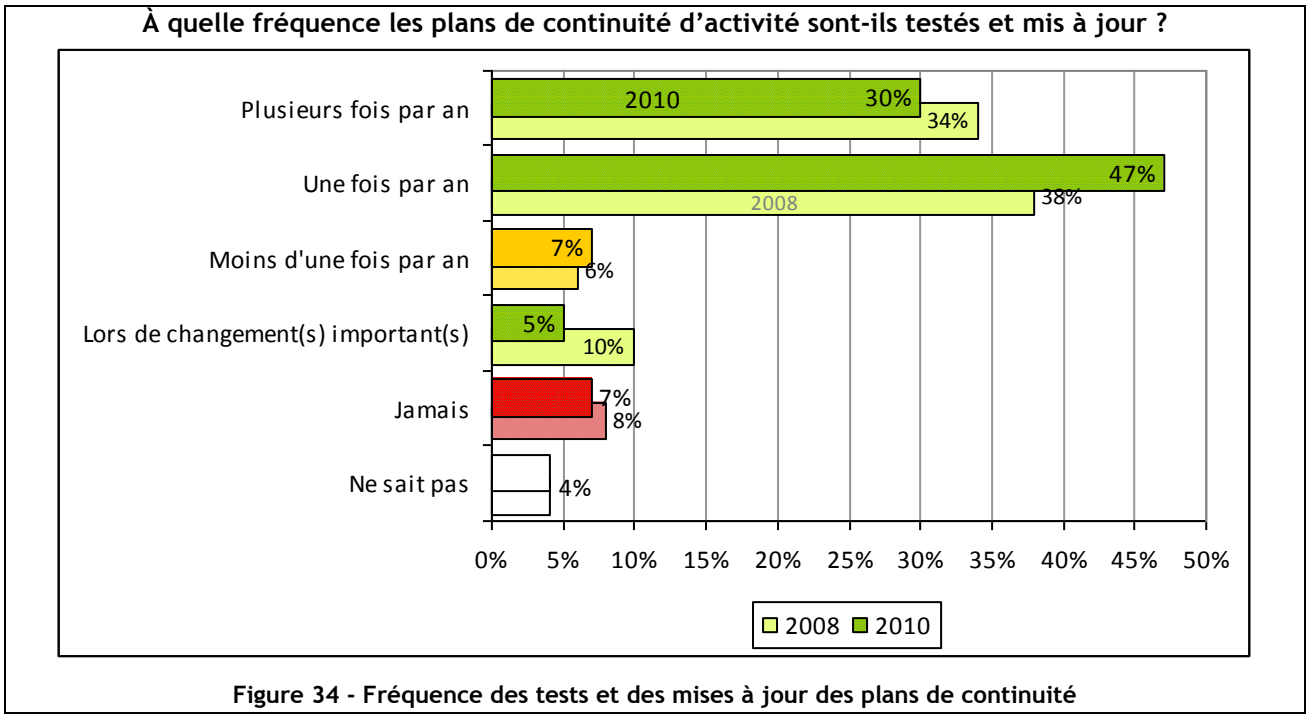

Figure 34 - Fréquence des tests et des mises à jour des plans de continuité

Cela reste peu probable et apporte un doute supplémentaire sur la compréhension de la notion de test dans le cadre d'un plan de continuité d'activité. Enfin, il reste près de 20% des entreprises qui affirment faire des tests seulement lors de changements importants, ne pas en faire du tout ou ne pas savoir. Gageons que cet inquiétant et peu rassurant ratio continue de baisser dans les prochaines années pour le bien des entreprises concernées.

Une vision « informatique » de la continuité : une absence des aspects « métier » ?…

Précédemment, nous avons vu que 67% des entreprises interviewées ont déclaré avoir mis en place globalement ou pour certaines de leurs activités un processus formalisé et maintenu de gestion de la continuité d'activité. Or, on constate que près d'une entreprise sur deux ne dispose pas d'un processus formalisé de gestion de crise. Ceci est singulier voire alarmant car tout PCA englobe forcément des procédures et organisations de gestion de crise en cas d'incident. Pour cette raison, les résultats doivent être pris avec beaucoup de précaution au niveau de la compréhension. En effet, tout processus de continuité d'activité qui ne comprend pas une organisation et une gestion de crise ne peut pas être considéré comme un vrai PCA !

De plus, ces mêmes personnes qui déclarent avoir mis en place des processus de continuité, répondent à 72% qu'elles n'ont pas identifié leurs besoins en RTO et RPO. Cela signifierait que seules les préoccupations des responsables informatiques en matière de RTO et RPO seraient prises en compte et, qu'à l'inverse, celles affichées par les besoins métiers ne le seraient pas. Une fois encore, le lecteur peut s'interroger sur la bonne compréhension de la question par la personne interviewée.

Une répartition des moyens de reprise légèrement différente

Les moyens de sauvegardes classiques continuent à baisser (-9%). À l'inverse, le secours à froid après avoir diminué de 2% entre 2006 et 2008 augmente significativement (+7%). À l'exception de ces deux ratios, on constate des chiffres très comparables d'une étude sur l'autre. Les nouvelles technologies comme les nouveaux moyens de sauvegardes télé-distants qui, pour certains d'entre eux proposent des créneaux horaires précis, sont sans doute à l'origine de ces résultats.

Quels types de solution de secours informatique utilisez-vous pour répondre à des sinistres majeurs ?

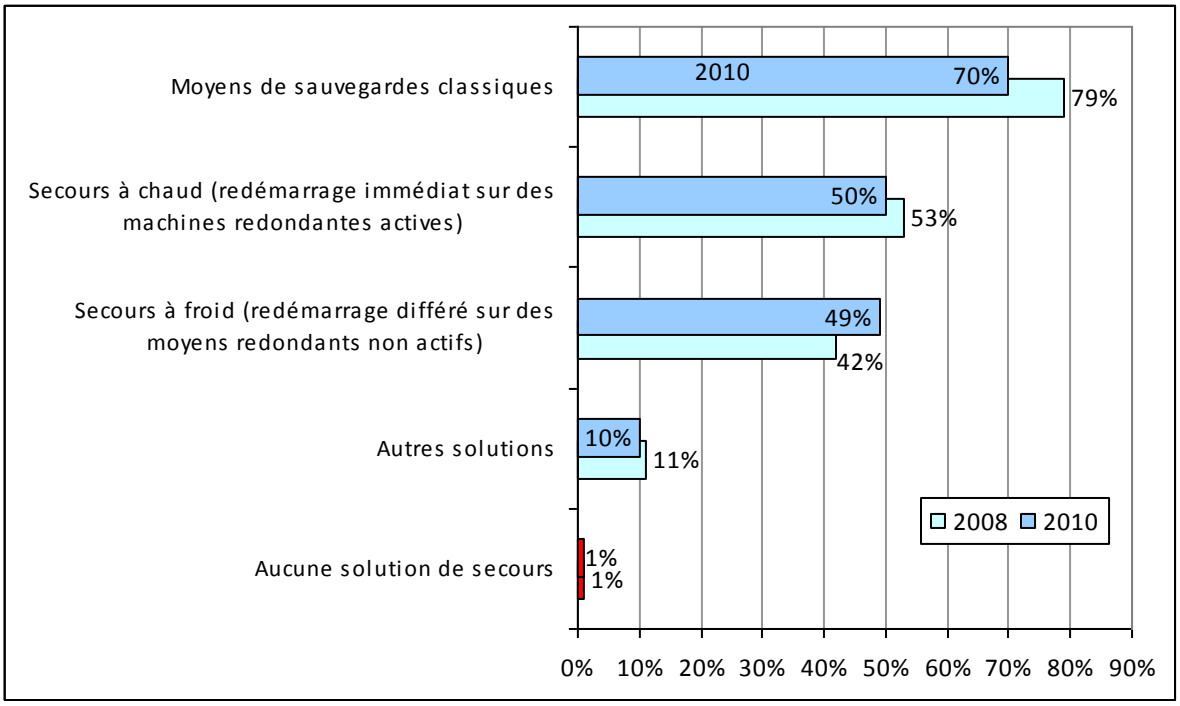

Figure 35 - Types de solution de secours informatique mises en œuvre

Enfin, les coûts en matière de solutions de sauvegardes ont eu tendance à beaucoup baisser ces dernières années. De fait, les acteurs en matières de stockage comme de sauvegardes distantes deviennent accessibles et de plus en plus nombreux.

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.

1/ Conformité avec la loi « Informatique et Libertés »

Une amélioration relative de la conformité avec les obligations de la CNIL

Après avoir stagné entre 2006 et 2008, on observe une amélioration sensible dans la prise en compte des obligations de la CNIL. Elle se traduit par une augmentation de 5% du nombre d'entreprises qui disent être au moins partiellement en conformité amenant à près de 9 entreprises sur 10 répondant être conformes au moins pour les traitements les plus sensibles.

Ces bons chiffres sont à relativiser avec le nombre de Correspondants Informatique et Libertés (CIL) qui, bien qu'augmentant sensiblement (+7% vs 2008), concerne encore moins du tiers des entreprises interrogées. On peut espérer voir ces chiffres s'améliorer suite aux annonces récentes de la CNIL sur l'augmentation du nombre de contrôles en 2010, notamment pour apprécier l'efficacité du CIL.

Votre entreprise met-elle en place un Correspondant Informatique et Liberté tel que défini par la CNIL ?

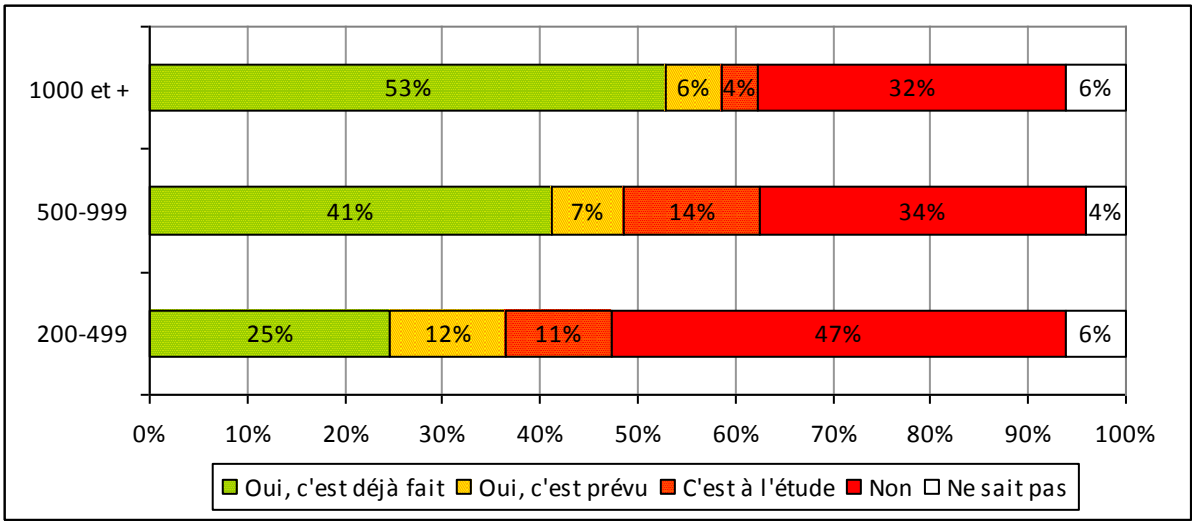

Figure 36 – Existence d'un Correspondant Informatique et Liberté

Une méconnaissance des données traitées

Le questionnaire s'enrichissait cette année d'une question relative aux types de catégories de données personnelles traitées. On pourra trouver surprenant que seulement 75% des entreprises de plus de 200 salariés traitent des données de clients ou prospects et seulement 39% traitent des données bancaires de clients. Faut-il comprendre qu'un quart des entreprises n'ont pas la liste de leurs clients sous forme numérique et que plus de 60% n'utilisent que des factures papier ?…

Les réponses à cette question de l'étude sont cohérentes avec le faible niveau de classification des données effectuées dans les entreprises et on ne pourra que supposer que ces résultats proviennent d'une méconnaissance des données traitées par l'entreprise.

On remarquera que seulement un peu plus de la moitié traitent les traces de connexions Internet des employés. Ce résultat est faible pour une pratique faisant généralement partie des premières mesures de sécurité envisagées ; les réglementations en vigueur poussent en effet à la collecte de ce type d'information.

On pourra par ailleurs se réjouir que la grande majorité des réponses affirmatives indiquant traiter un type de données ont mis en œuvre des mesures de sécurité qu'ils « estiment adaptées », même s'il est impossible d'évaluer objectivement la qualité des mesures en place.

Traitez-vous les types de données suivantes, et si oui estimez-vous avoir mis en place des mesures de sécurité adaptées ?

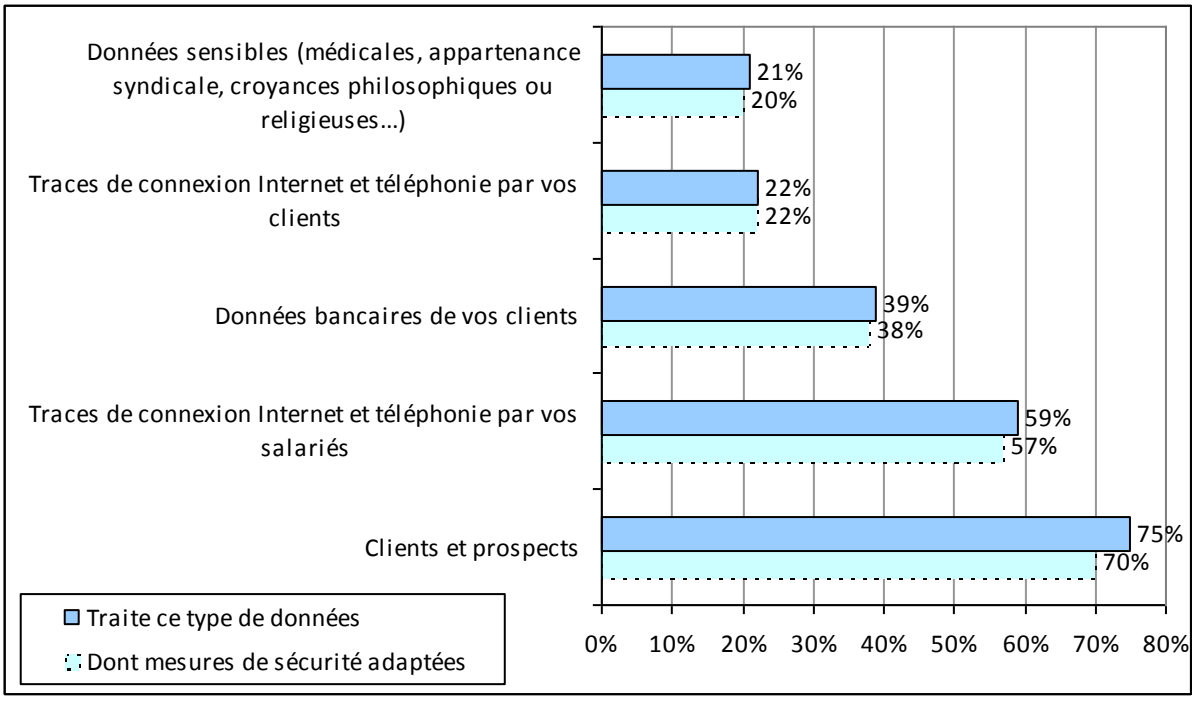

Figure 37 - Types de données traitées par les entreprises et mesures de sécurités mises en œuvre

2/ Les audits

Le nombre des audits menés et leur nature stables sur 4 ans

Plus des deux-tiers (71%) des entreprises mènent au moins un audit une fois par an, alors que 25% n'en mènent pas du tout (-10% vs 2008) !

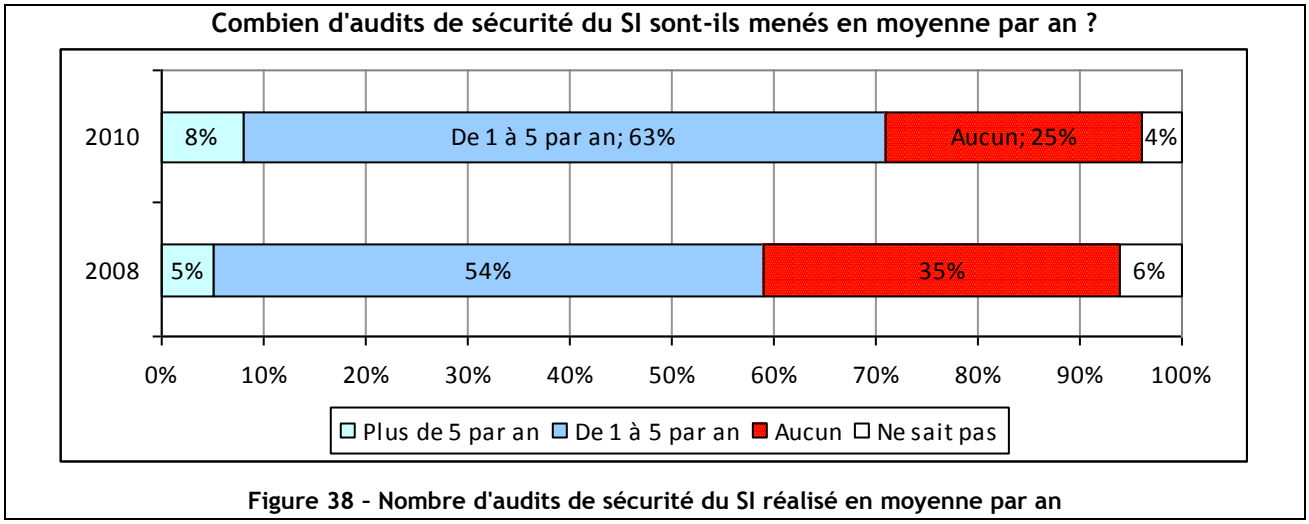

Figure 38 – Nombre d'audits de sécurité du SI réalisé en moyenne par an

Le chiffre de 71% est en progression par rapport à 2008 (+12%) et retrouve le niveau de 2006 où l'on avait noté un bond spectaculaire.

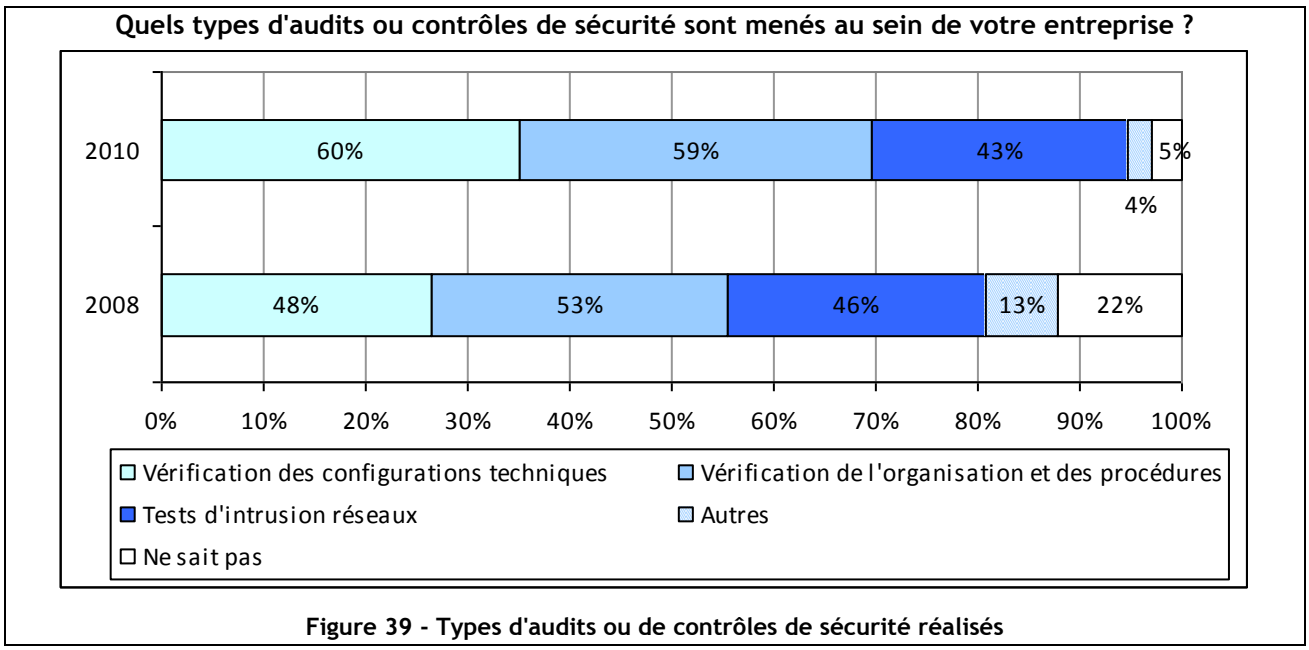

Figure 39 - Types d'audits ou de contrôles de sécurité réalisés

La PSI comme principal moteur

Ces audits sont très largement motivés par la politique interne ou des exigences contractuelles ou réglementaires

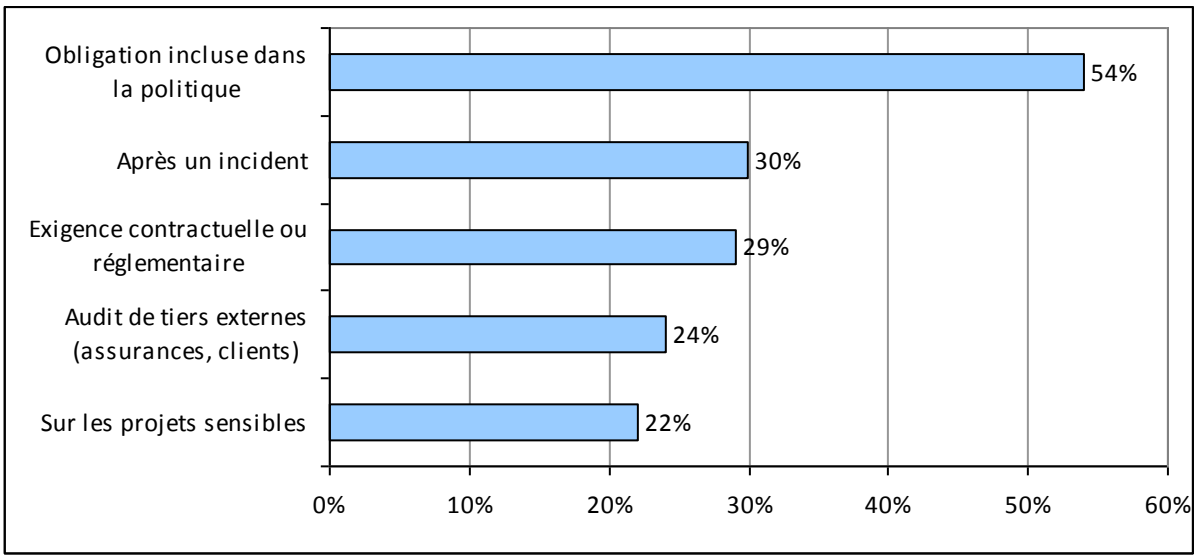

Figure 40 – Motivations pour la réalisation des audits

A noter que la part d'audits menés par un prestataire externe s'est également stabilisée par rapport à l'enquête précédente (24%, -1% vs 2008)

3/ Les tableaux de bord de sécurité

Plus de 65% des entreprises ne mesurent toujours pas leur niveau de sécurité régulièrement

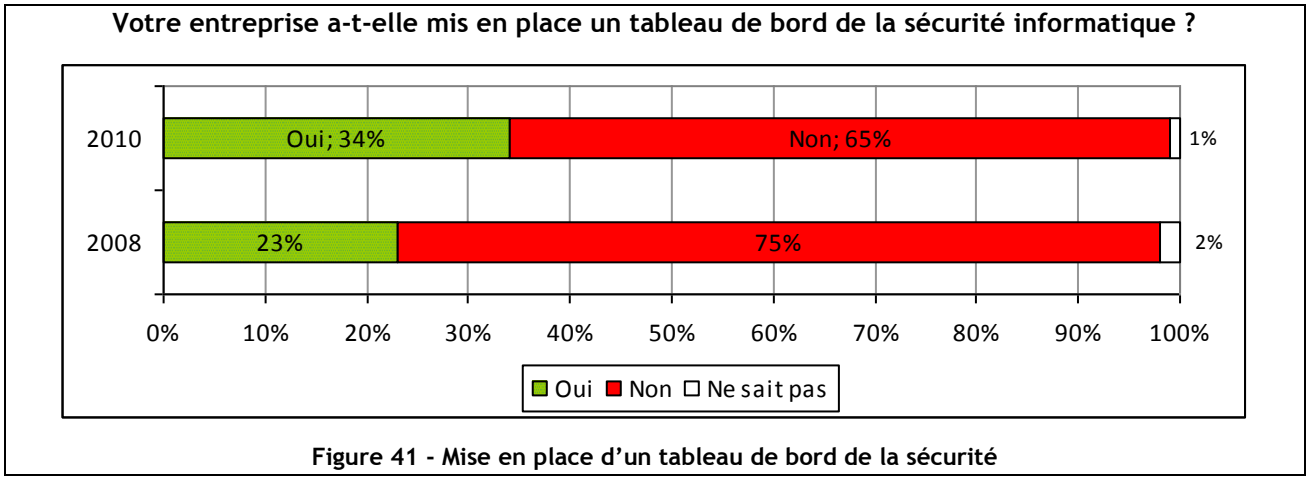

Figure 41 - Mise en place d'un tableau de bord de la sécurité

À noter, la continuité de la forte augmentation des entreprises qui le diffusent à leur Direction Générale (72% contre 52% en 2008 et 28% en 2006).

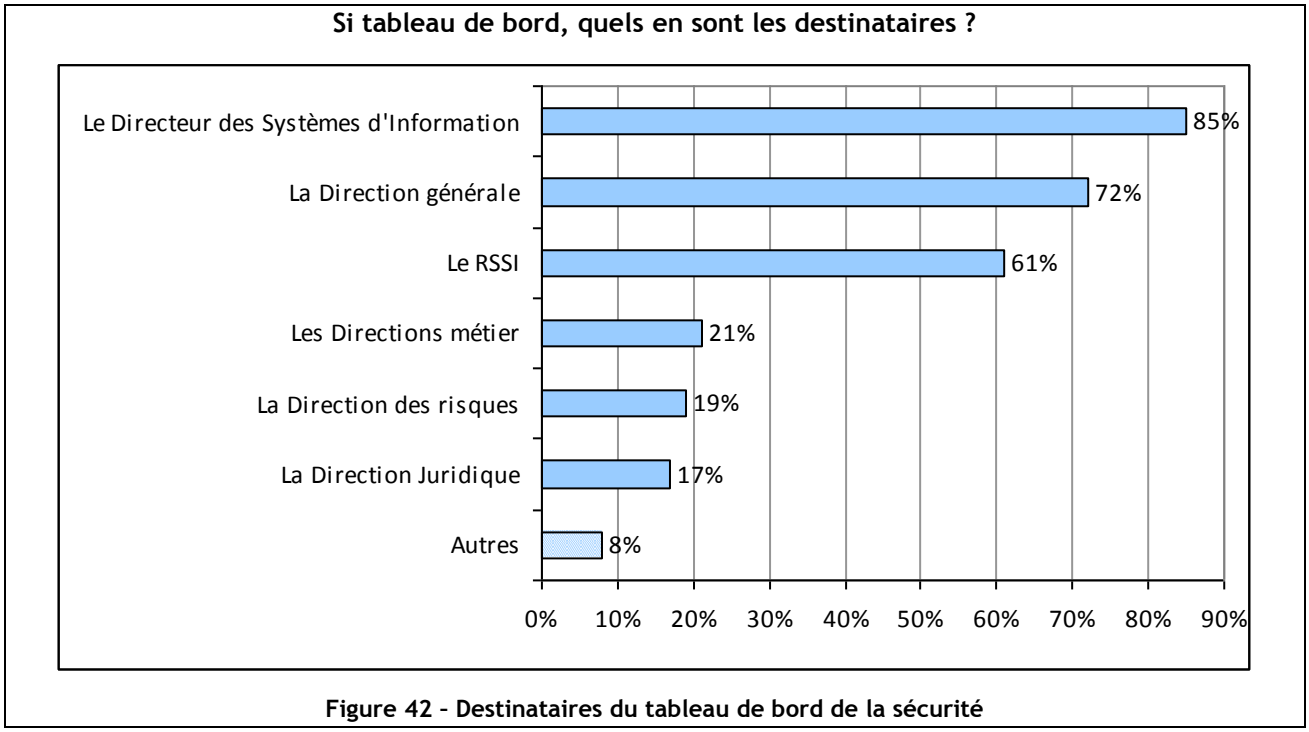

Figure 42 – Destinataires du tableau de bord de la sécurité

Des indicateurs qui évoluent de la technique vers le fonctionnel et la conformité…

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 certains des thèmes les plus importants en matière de pilotage prennent de plus en plus de poids :

- conformité avec les normes : 66%, + 46% vs 2008 !,
- impacts directs et indirects des incidents de sécurité : 45%, +5% vs 2008,
- évaluation des risques métier : 39%, +7% vs 2008,
- suivi du budget consacré à la sécurité de l'information : 37%, +17% vs 2008,
- etc.

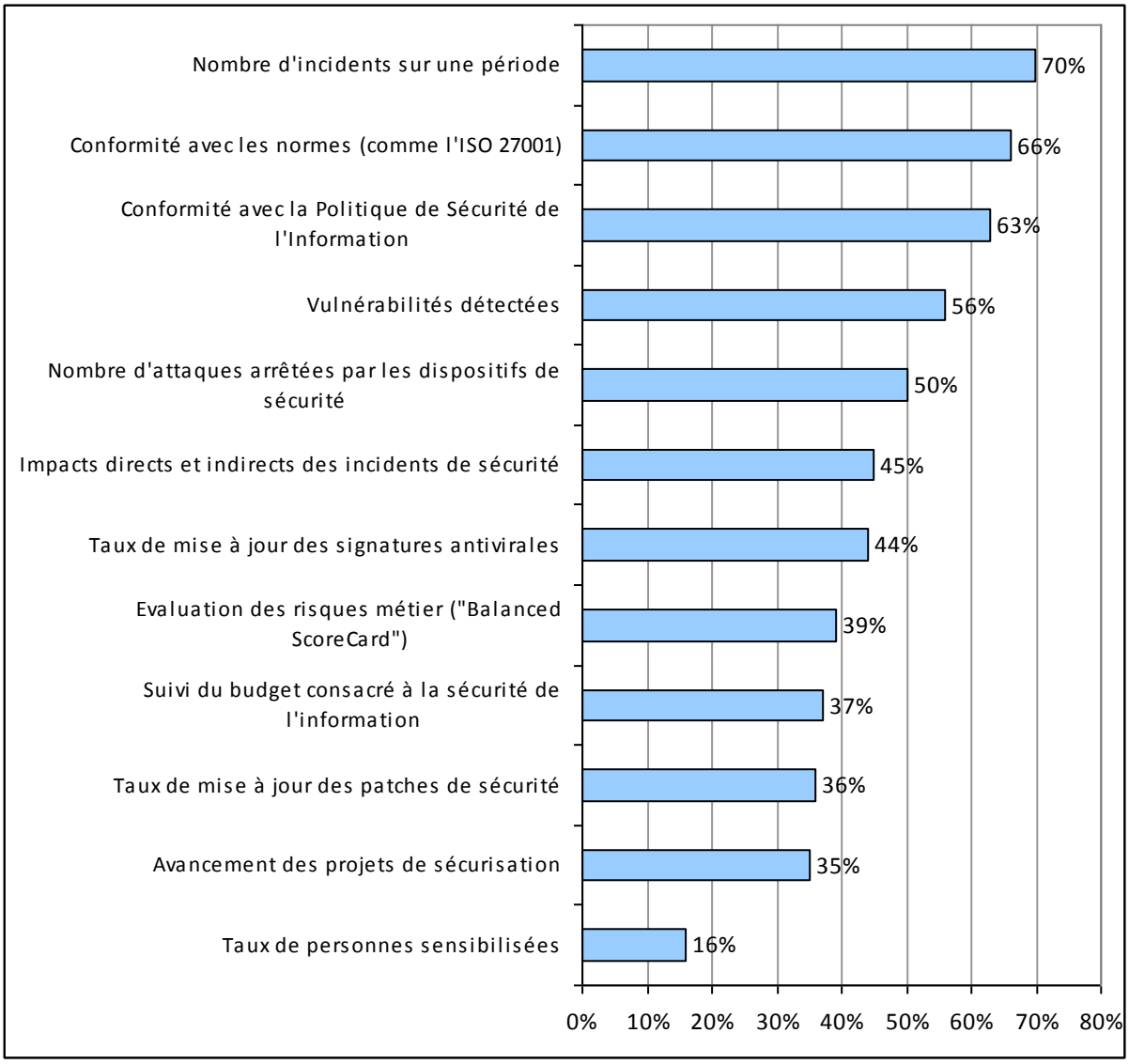

Figure 43 - Indicateurs suivis dans le tableau de bord de la sécurité

Hôpitaux

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

Les Hôpitaux

Présentation de l'échantillon

L'enquête a été réalisée par téléphone en janvier et février 2010 auprès des hôpitaux publics français de plus de 200 lits :

- 151 hôpitaux y ont répondu,
- la personne ciblée était le Responsable de la Sécurité des Systèmes d'Information, ou à défaut, le responsable informatique ou toute autre personne ayant cette question en charge.

Les résultats de l'enquête réalisée en 2006 se référaient à une cible légèrement différente car les hôpitaux de moins de 200 lits étaient aussi inclus : 66% des hôpitaux ayant répondu à l'enquête en 2006 avaient moins de 200 lits, contre 34% de plus de 200 lits (soit environ 63 hôpitaux).

Parmi ces 151 hôpitaux de plus de 200 lits, les établissements de 200 à 500 lits sont en majorité (presque les deux-tiers). Un quart d'entre eux comporte de 500 à 1 000 lits. Dix d'entre eux (soit 7%) comportent plus de 1 000 lits.

Quel est le nombre de lits de votre hôpital ?

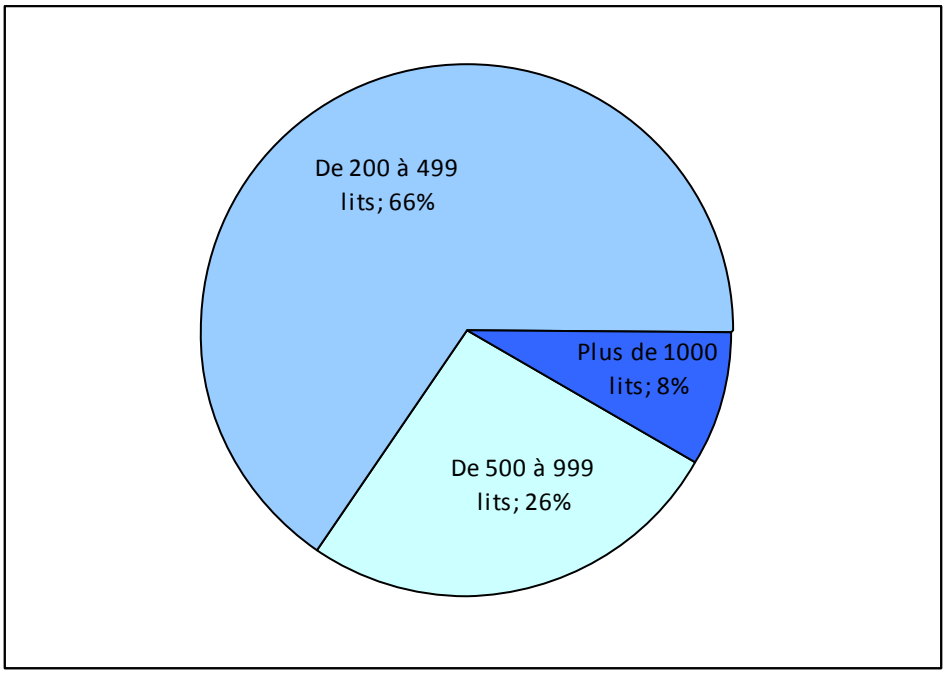

Figure 44 – Taille des hôpitaux interrogés

Le Directeur (ou responsable) Informatique a le plus souvent répondu à l'enquête, dans un tiers des cas, le DSI représentant 17% des cas. Cependant, la cible prioritaire était le Responsable de la Sécurité des Systèmes d'Information (RSSI), qui a pu être joint dans 28% des cas seulement (42 hôpitaux). En effet, dans la majorité des cas, il n'y a pas de RSSI identifié, ni en tant qu'individu ni en tant que fonction.

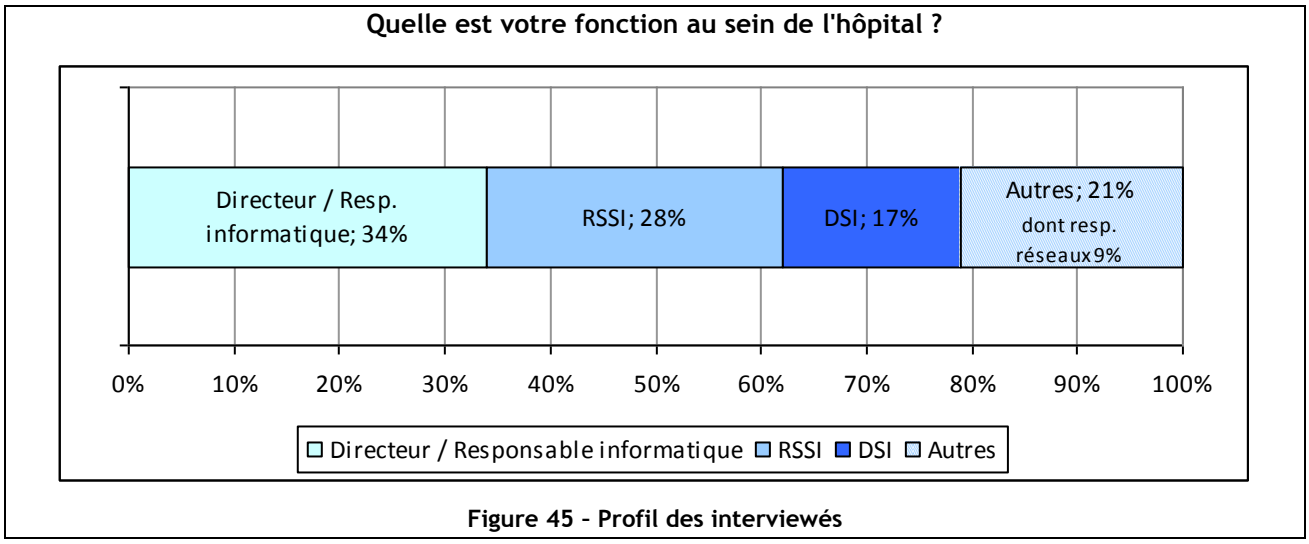

Figure 45 - Profil des interviewés

Budget Informatique

Le budget informatique serait-il une information confidentielle ?

Le taux de réponse à cette question est faible. Il est probable que ce budget SSI ne soit pas toujours connu ou diffusable, surtout s'il est faible. Le taux de réponse est cohérent avec celui de l'enquête sur les entreprises. Il doit être noté que, dans le domaine hospitalier, une partie non négligeable des investissements informatiques est réalisée directement dans les services.

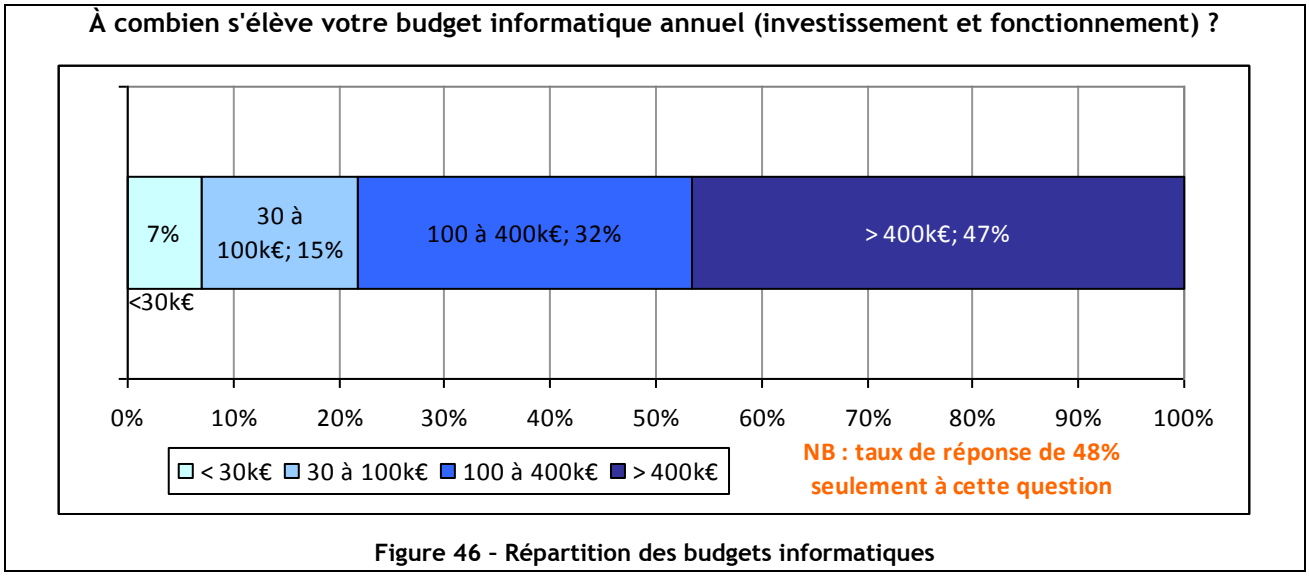

Figure 46 - Répartition des budgets informatiques

Les budgets informatiques sont très disparates. Ils sont globalement inférieurs à ceux constatés pour les entreprises.

Moyenne	1 015 000 €
Minimum	7 000 €
Maximum	12 000 000 €

On peut cependant signaler la difficulté à identifier et isoler ce qui, dans un budget SI, relève de la sécurité. Pour un antivirus c'est évident, mais pour une infrastructure de sauvegarde, est-ce du domaine de la sécurité ou de l'infrastructure ? De plus, lorsque l'on fait l'acquisition de systèmes « tout en un » (comme par exemple les PACS) qui sont livrés nativement en cluster redondés, etc., comment identifier la part sécurité ?

Moyens consacrés à la sécurité de l'information

Deux enseignements se dégagent :

- la capacité des interviewés à identifier leur budget sécurité dans le budget informatique global a fortement diminué : la sécurité des Systèmes d'Information est-elle de moins en moins un sujet en soit ou est-elle devenue un sujet moins urgent ? Le problème est peut-être de définir ce qui est du domaine de la sécurité et ce qui ne l'est pas,
- la part du budget informatique consacrée à la sécurité a diminué : en 2006, 50% des personnes interrogées positionnaient le budget sécurité au delà de 3% du budget informatique. Elles ne sont plus que 38% en 2010.

Quel pourcentage représente le budget sécurité par rapport au budget informatique total ?

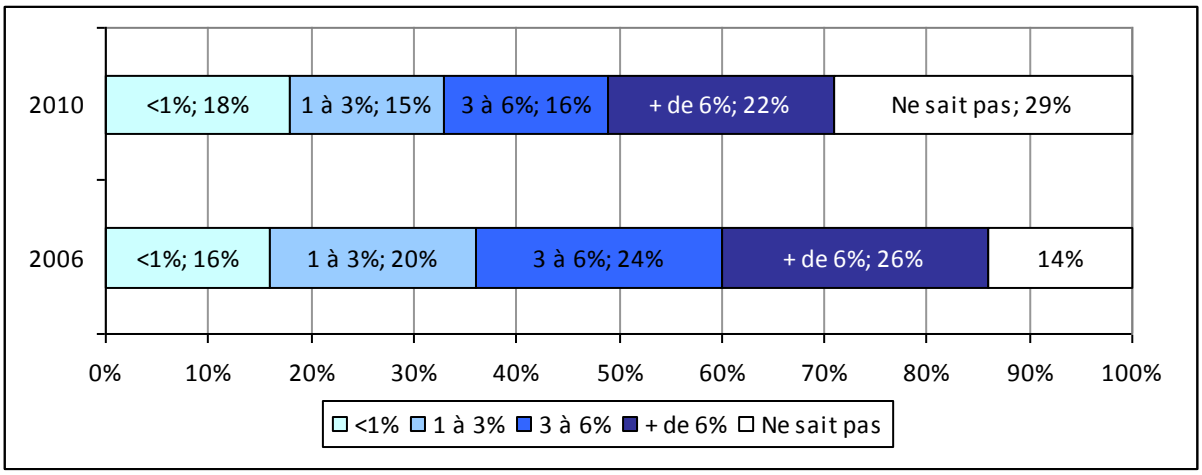

Figure 47 – Part du budget informatique consacrée à la sécurité des Systèmes d'Information

Ce constat est inquiétant, car il doit être corrélé à l'interconnexion de l'informatique médicale avec l'informatique de gestion dans beaucoup d'établissements de santé et donc à une augmentation des risques. À contrario, l'échantillon n'est pas constant et l'importance des petits établissements dans le panel peut expliquer une évolution négative.

Thème 5 : Politique de sécurité

La Politique de Sécurité de l'Information définit notamment les grandes orientations en la matière pour une Organisation, montrant l'implication de la Direction Générale.

Une tendance s'amorce, consistant à lier l'élaboration de la Politique de Sécurité à l'analyse de risques. Selon cette enquête 2010, 63% des hôpitaux ont formalisé leur Politique de Sécurité, au lieu de 55% en 2008. La mise à jour de cette Politique date de moins de deux ans pour 75% de ces hôpitaux.

La politique de sécurité de l'information de votre hôpital s'appuie-t-elle sur des « normes » de sécurité, et si oui lesquelles ?

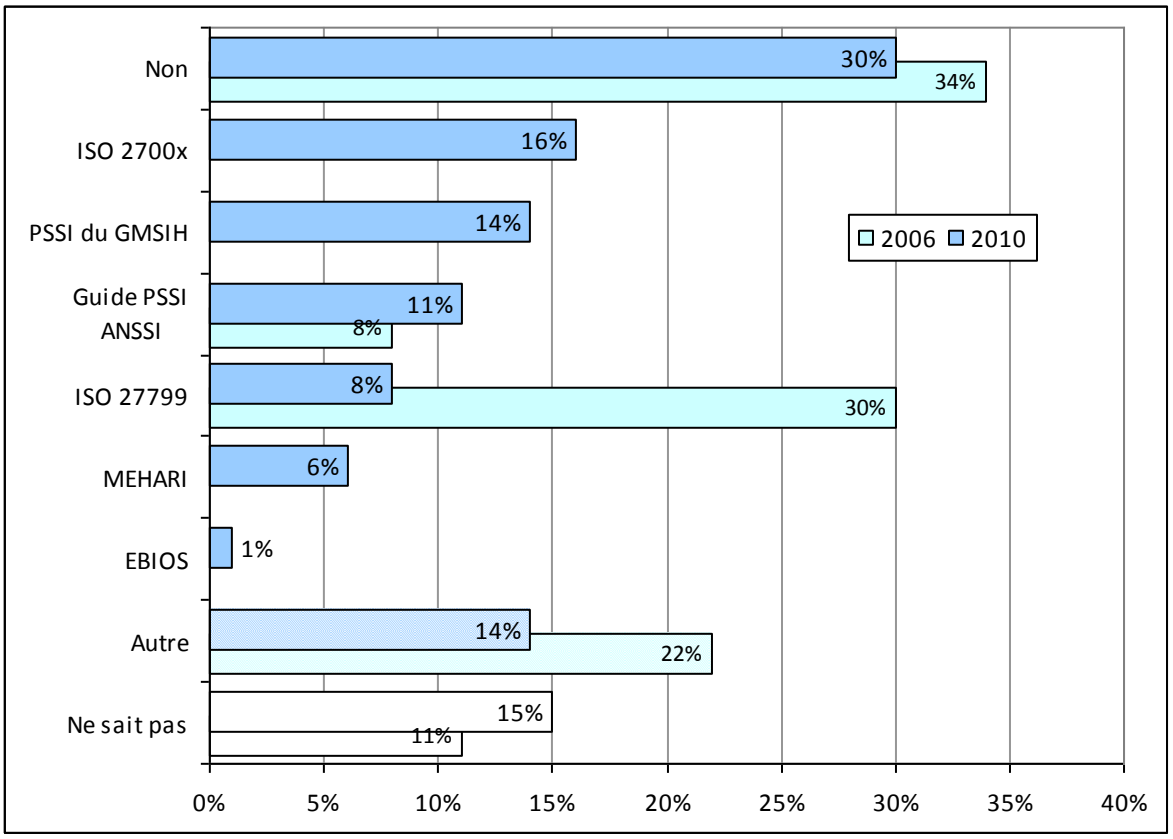

Figure 48 – « Normes » de sécurité utilisée pour « supporter » la Politique de Sécurité de l'Information

Les établissements hospitaliers s'appuient sur des normes (2700x, 27799, etc.) pour élaborer leur Politique de Sécurité.

En revanche, l'utilisation de modèles se développe. Le GMSIH (Groupement pour la Modernisation du Système d'Information Hospitalier) a produit un modèle de Politique, et les hôpitaux sont aujourd'hui 14% à s'en inspirer pour l'élaboration de leur propre Politique de sécurité.

Par ailleurs, 8% au moins s'appuient sur une méthode de gestion des risques pour l'élaboration de leur Politique.

Une implication forte de la Direction Générale

Lorsqu'une Politique de Sécurité existe, les résultats de l'enquête 2010 révèlent que la Direction Générale soutient cette Politique à 94% contre 99% en 2006.

La Sécurité apparaît souvent comme une préoccupation de la Gouvernance des hôpitaux. La montée en puissance des contraintes législatives et réglementaires n'est probablement pas étrangère à cette tendance.

En revanche, l'implication des RSSI indique manifestement que, dans la majorité des cas, le rôle du RSSI au niveau Gouvernance du Système d'Information n'est pas avéré.

L'implication de la Direction Générale recouvre-t-elle une implication plus large des différentes composantes métiers des hôpitaux (les médecins, les laboratoires, les soignants, etc.) ? Cela semble souhaitable…

En effet des organismes tels que l'AFAI ou l'ISACA recommandent que les projets IT soient corrélés aux projets métier auxquels ils contribuent, et gérés en tant que composantes de ces projets métier.

Quelles sont les entités ayant contribué à l'élaboration de la Politique de sécurité ?

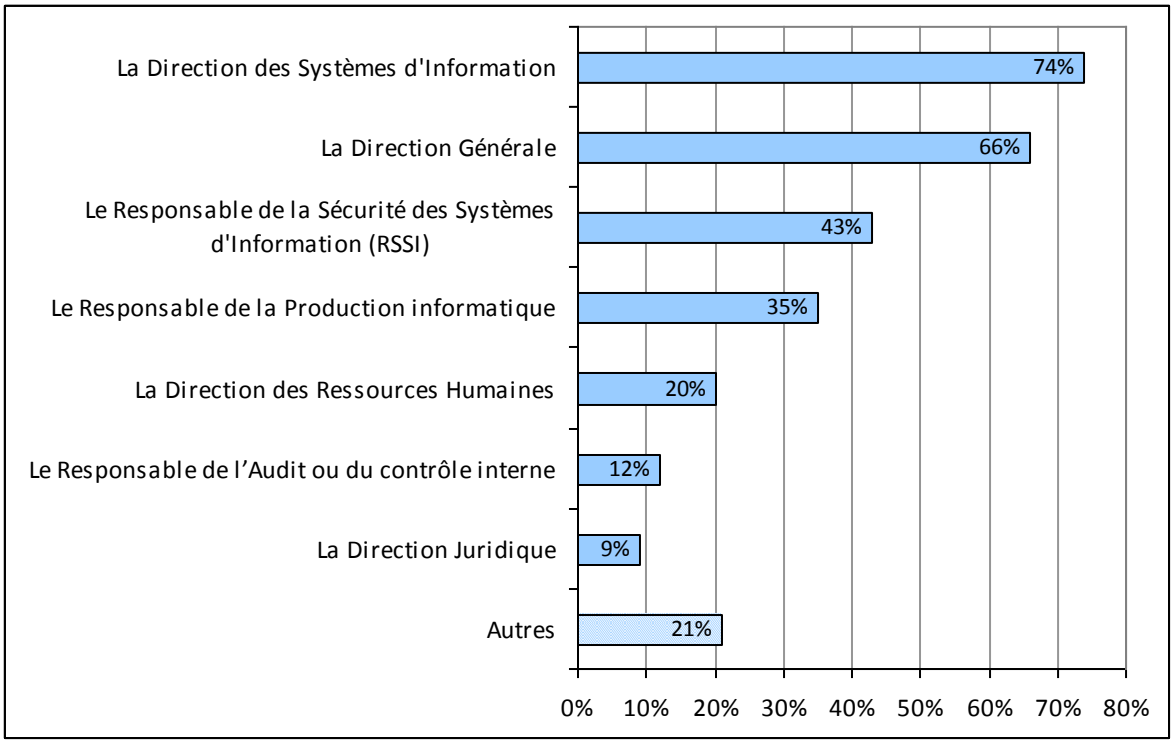

Figure 49 – Entités ayant contribué à l'élaboration de la Politique de sécurité

Il est essentiel que les arbitrages concernant les projets IT majeurs soient rendus au niveau de la Gouvernance d'une Organisation. Ainsi l'on peut espérer que les projets IT et les objectifs du SI soient alignés sur les objectifs stratégiques de l'Organisation. C'est ce que recommande l'AFAI, à travers les onze vecteurs de valeur du SI (cf. sites de l'AFAI, du CIGREF, etc.).

Dans ce contexte, la Sécurité, facteur clé de la performance, de la fiabilité, de la pérennité d'un SI, est nécessairement prise en compte au niveau de la Gouvernance du Système d'Information. Les projets SI, dont les projets Sécurité, par leur contribution aux projets métier, sont vecteurs de création de valeur dans les hôpitaux, comme dans toute organisation.

Thème 6 : Organisation et moyens

Le RSSI : une présence en progression constante…

La fonction de RSSI ou de RSI s'impose peu à peu dans le monde hospitalier : elle est clairement identifiée et attribuée dans 37% des cas en 2010 contre 27% en 2006. Cependant, cette fonction semble de moins en moins assurée par une personne dédiée : 41% des cas en 2006 vs 23% en 2010.

La fonction de RSSI/RSI subit une évolution nette vers un rattachement au périmètre du DSI, tendance déjà observée lors de notre précédente enquête, ou vers les DAF (Directions Administratives et Financières).

Le DSI s'affirme de plus en plus comme le « garant » de la sécurité des Systèmes d'Information. Les Responsables sécurité lui sont de plus en plus rattachés (32% en 2006 vs 36% en 2010) et de moins en moins à la Direction Générale (45% en 2008 vs 34% en 2010). La DAF hérite de la fonction sécurité dans 12% des cas contre 5% en 2008.

La principale observation semble être un recul du rattachement du Responsable Sécurité à la Direction Générale.

Il serait intéressant d'évaluer si cette évolution signifie un éloignement des fonctions Sécurité et Systèmes d'Information de la Gouvernance de l'Organisation. Il se peut, en effet, que ce recul s'explique par le rattachement croissant de la Sécurité au DSI et au DAF. Or, si ceux-ci sont effectivement présents dans les instances de Gouvernance, la représentativité de la Sécurité dans les instances de Gouvernance resterait alors stable.

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

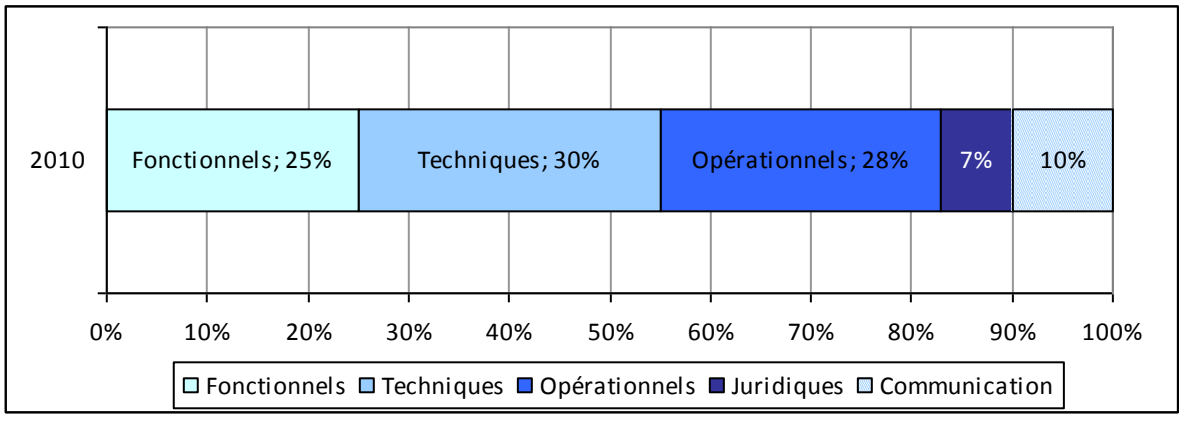

Figure 50 – Temps consacré par le RSSI aux différentes tâches

Les fonctions opérationnelles et techniques représentent l'activité principale du Responsable Sécurité (58%). Les aspects fonctionnels, davantage orientés vers le management de la sécurité (Politique sécurité, analyse de risques, etc.), représentent seulement 25% de la charge du RSSI.

Combien de personnes travaillent exclusivement à la sécurité de l'information au sein de votre hôpital ? Nous nous sommes interrogés quant à la pertinence de comparer brutalement certains chiffres : par exemple, la réponse « Pas d'équipe sécurité permanente » passe de 24% en 2006 à 38% en 2010. Cela peut paraître très négatif au premier abord. Certes, cela corrobore la baisse de fonction sécurité portée par une personne dédiée (41% en 2006 vs 23% en 2010), mais cela est-il représentatif dans l'ensemble du monde hospitalier ?

Thème 7 - Gestion des biens / Inventaire

Inventaire des informations et de leur support

On constate que 57% seulement des hôpitaux interrogés ont procédé à l'inventaire des informations en totalité (15%) ou en partie (informatique ou hors informatique). Ce qui est peu si l'on considère que cet inventaire est la base des analyses de risques.

Avez-vous inventorié toutes les informations (et leur support) de votre hôpital et leur avez-vous attribué un propriétaire ?

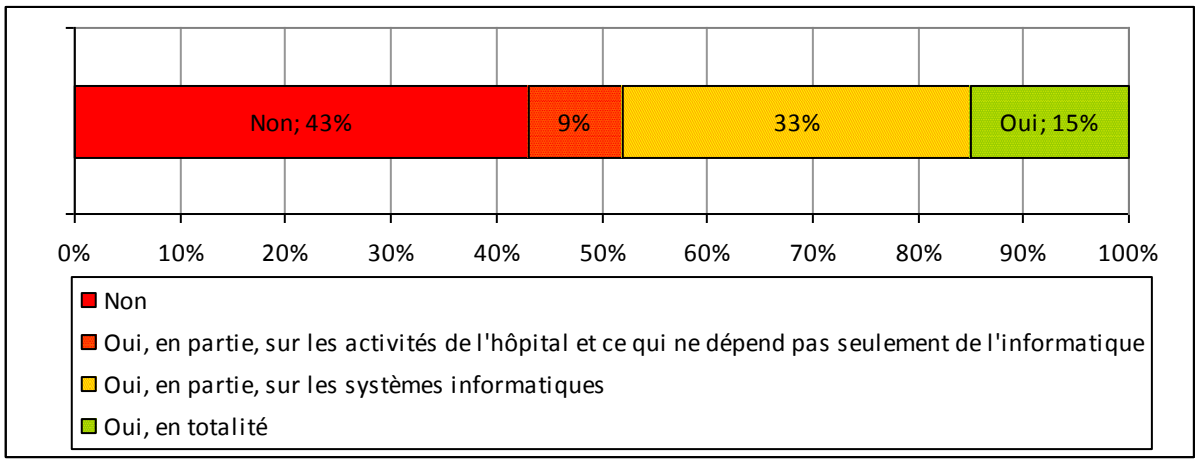

Figure 51 – Réalisation de l'inventaire des informations

Le classement des informations, lui, est réalisé par la moitié des hôpitaux (48%), selon les critères de confidentialité (dans 82% des cas), de Disponibilité (62%, ce qui est à rapprocher de l'existence de plans de continuité) et d'Intégrité (48%) ou Autres (traçabilité, Preuve, etc.….), ceci avec, en moyenne, deux ou trois niveaux de sensibilité par critère.

Gestion des biens / Analyse de risques

L'analyse de risques devrait s'imposer peu à peu aux structures hospitalières, notamment en raison :

- du décret « Confidentialité » du 15/07/2006 qui y fait référence,
- du lobbying réalisé par le GMSIH (ANAP aujourd'hui) avec une proposition de méthodologie.

Avez-vous réalisé une analyse formelle, basée sur une méthode, des risques liés à la SSI ?

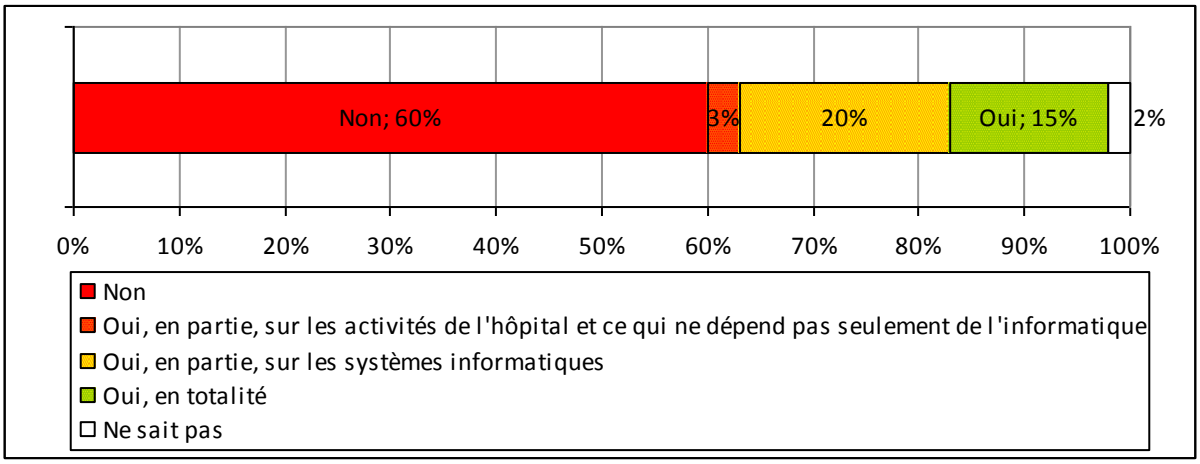

Figure 52 – Réalisation d'une analyse des risques

Globalement, les analyses de risque menées en 2010 se sont traduites par des plans d'actions de manière plus systématique.

Le Responsable Sécurité est clairement reconnu comme le porteur de cette activité : 43% en 2010 contre 35% en 2006. La tendance déjà amorcée en 2006 se confirme.

Cependant, il est difficile de comparer 60% de « Non » en 2010 à 40% seulement en 2006, car le libellé en 2010 comporte le mot analyse « formelle ».

Pour ce qui est de la méthode d'analyse des risques utilisée, la référence méthodologique privilégiée est celle proposée par le GMSIH.

Thème 8 – Ressources humaines

En quatre ans, les hôpitaux ont adopté les chartes de sécurité

Certes, le mouvement ne s'est pas amplifié au point d'assister à une généralisation, mais les progrès sont sensibles : la proportion d'établissements ne disposant d'aucune charte de sécurité a ainsi diminué de moitié (de 42% en 2006 à 21% en 2010), surtout dans les hôpitaux de plus de 500 lits.

Ces chartes font l'objet d'une diffusion plus large : elles sont signées par tous les salariés dans plus de la moitié des établissements.

Par ailleurs, ces chartes constituent des outils de management : des sanctions disciplinaires sont en effet prévues dans le règlement intérieur, en cas de manquement à la charte, dans la quasi-totalité des établissements (46% ont institué le principe de sanctions, 47% sont en cours de formalisation).

Il reste toutefois un chantier pour lequel des progrès restent à faire : celui de la sensibilisation plus générale des salariés à la sécurité de l'information. Dans plus de la moitié des établissements (et les deux tiers des établissements de moins de 500 lits), ni les contrats de travail ni les descriptifs de postes ne font état des responsabilités et des exigences en matière de sécurité des Systèmes d'Information.

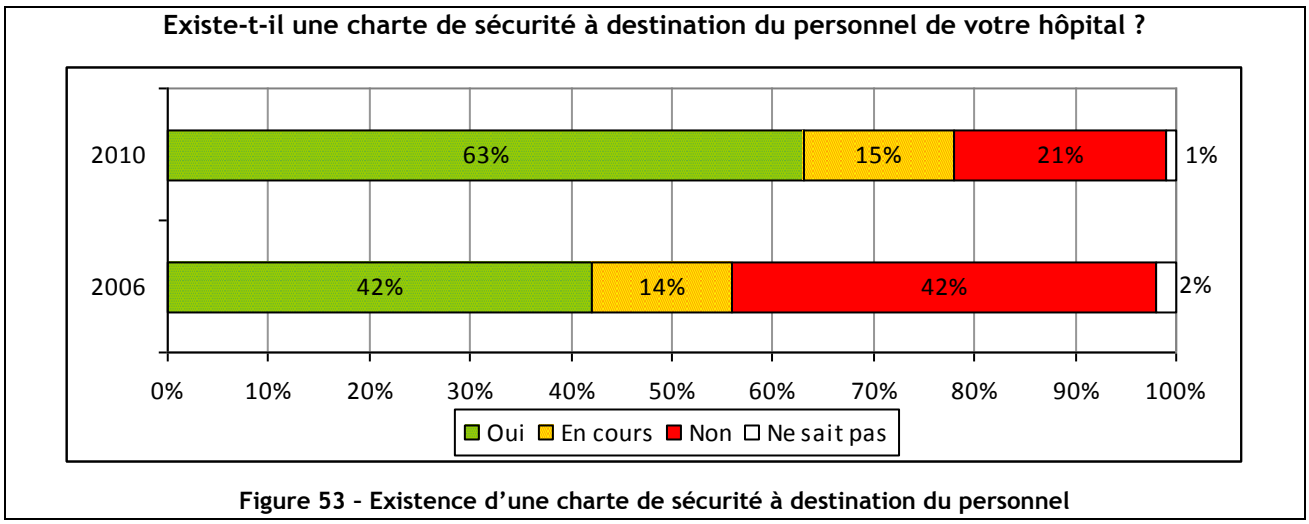

Figure 53 – Existence d'une charte de sécurité à destination du personnel

Cette situation se mesure également avec un autre indicateur : l'existence d'un programme de sensibilisation à la sécurité. Dans les deux-tiers des établissements, il n'existe aucun programme de ce type, proportion qui n'a pas évalué entre nos deux enquêtes. Et lorsque de tels programmes existent, les impacts ne sont pas mesurés dans huit cas sur dix. En quatre ans, la hiérarchie des outils utilisés a évolué : les sessions de sensibilisation systématiques pour les nouveaux arrivants sont désormais privilégiées (dans 50 % des établissements, contre 30 % en 2006) alors que dans l'enquête précédente, les établissements mentionnaient davantage les publications (Intranet, mailing, affiches, articles, etc.) et la formation périodique comme outils principaux de sensibilisation.

Si charte de sécurité, quels sont les moyens utilisés pour assurer la sensibilisation ?

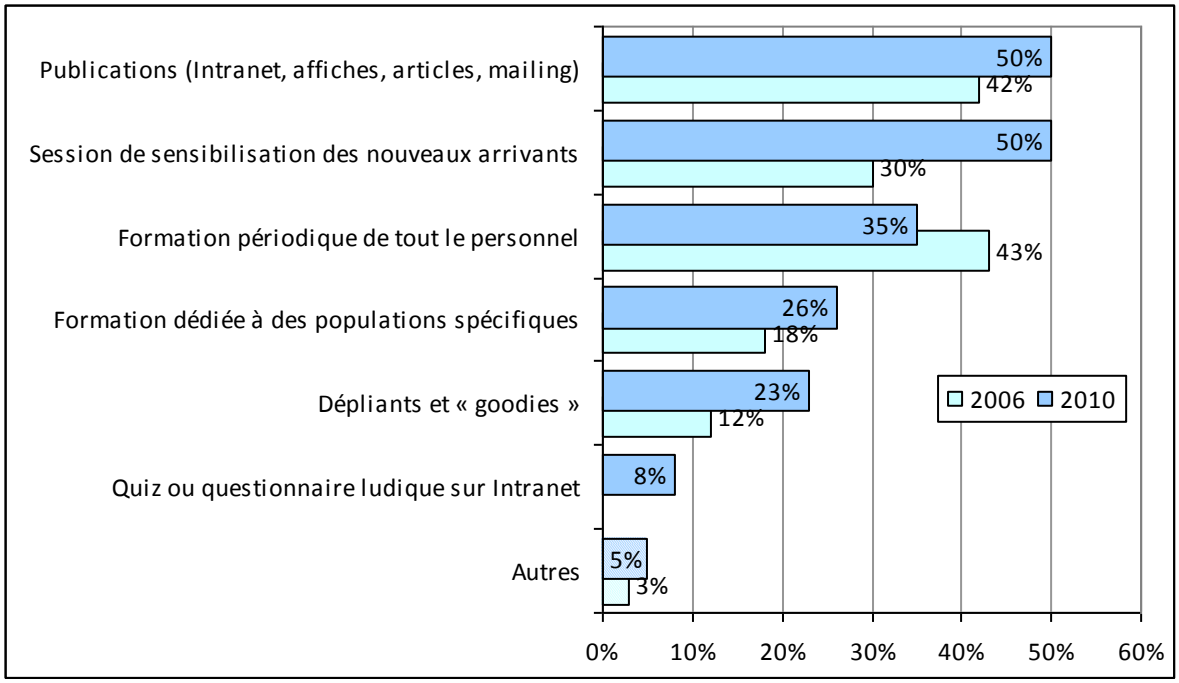

Figure 54 – Moyens utilisés pour assurer la sensibilisation du personnel

Thème 9 – Sécurité physique du dossier patient papier

Responsabilité sur le dossier patient

La question porte sur le dossier patient papier. Il est alors relativement logique que celui-ci ne soit pas du ressort du RSSI mais du professionnel de santé. Il est en revanche assez étonnant que, pour 26% des sondés, les responsabilités ne soient pas clairement identifiées. La séparation des fonctions entre la DIM (Direction de l'informatique médicale) et la DSI dans les établissements peut expliquer que le dossier patient ne soit pas considéré comme du ressort du RSSI.

Cependant, parle-t-on de la responsabilité de la définition des métarègles d'accès au dossier papier, des dossiers papier en général, des archives des dossiers papier ? En général, les métarègles sont du ressort du DIM, les dossiers papiers des patients présents sont de la responsabilité de l'unité fonctionnelle hébergeante (donc médecin traitant et chef de service), alors que les archives médicales peuvent être gérées soit par le DIM, soit par la DSI, soit par les services généraux.

Thème 10. Gestion des communications et des opérations

Sécurité liée aux nouvelles technologies

Comme lors de la précédente étude, les hôpitaux se montrent globalement moins permissifs que les entreprises dans l'utilisation des nouvelles technologies. D'un autre côté, on observe une diminution de leur interdiction pure et simple.

Pourriez-vous positionner votre politique de sécurité sur les aspects suivants ?

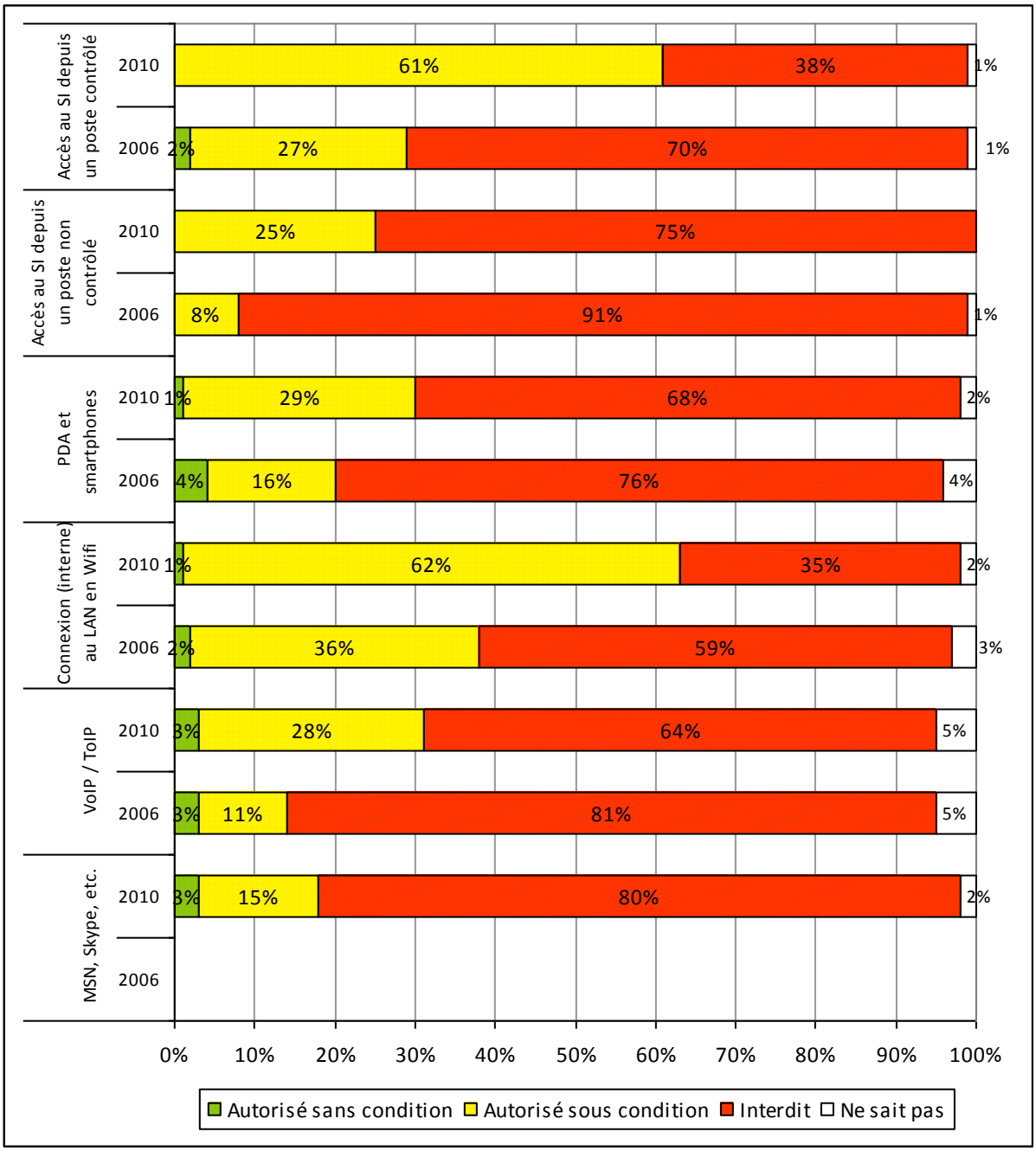

Figure 55 – Sécurité des nouvelles technologies

L'utilisation des postes nomades fournis par l'établissement est de plus en plus répandue et acceptée. En revanche, plus d'accès sans condition. Le domaine hospitalier est en retrait par rapport aux entreprises (+ de 75% des entreprises autorisent les accès sous condition par des postes nomades et prés de 10% les

autorisent sans condition). Mais on peut s'interroger sur le bien-fondé de cette tendance : autoriser l'accès à son SI sans conditions depuis l'extérieur relève du suicide informatique…

L'accès à partir de postes de travail non maîtrisés est en augmentation mais reste largement interdit. Au vu des budgets informatiques et de la proportion de ces budgets dédiée à la sécurité des Systèmes d'Information, il est peu probable que ces consignes s'appuient sur des dispositifs techniques limitant, voire interdisant la connexion d'un équipement n'appartenant pas à l'établissement.

Les réseaux sans fil prennent de plus en plus d'ampleur. Les hôpitaux sont ici en avance par rapport aux autres entreprises. Ceci est logique car les technologies sans fil permettent de gérer les déplacements du personnel médical. Il est en revanche étonnant que l'extension des réseaux sans fil ne soit pas corrélée avec la mise en œuvre de périphérique de type PDA, domaine où même si la proportion à quasiment doublée, le monde hospitalier reste en retrait par rapport au monde de l'entreprise. Les résultats seraient éventuellement différents si la question avait porté uniquement sur les PDA et pas sur le couple PDA/Smartphone. On peut donc s'interroger sur l'usage de ces réseaux sans fil dans les plus de 30% d'établissement qui n'utilisent pas de terminaux mobiles. On peut éventuellement y voir une facilité pour éviter un câblage ou une extension de câblage.

En fait, la raison est simple : la question n'est pas l'accès depuis les PDA, mais l'accès depuis les applications tournant sur les PDA. A ce jour elles sont très peu nombreuses.

Il doit être rappelé que les technologies wifi, outre les risques liés à la confidentialité qui peuvent être réglés, présentent des risques intrinsèques de perturbation et de dysfonctionnement, antinomiques de réseaux critiques tels que ceux présents dans les hôpitaux.

L'usage de la téléphonie sur IP s'étend au sein des établissements où elle a presque triplée en trois ans. L'usage de la messagerie instantanée reste faible. Globalement, la proportion d'établissement qui autorise l'une ou l'autre des technologies sans condition reste faible, voire diminue.

Les hôpitaux ne résistent pas au nomadisme

Les hôpitaux, plutôt frileux vis-à-vis du nomadisme en 2006 (accès extérieurs interdits à 70% pour les postes nomades et 91% pour les postes non maîtrisés, rejet des PDA / smartphones à 76% et du wifi à 59%), semblent dorénavant mieux maîtriser les technologies associées et autoriser leur utilisation sous condition. Malgré le risque sur la confidentialité des données manipulées, les chiffres autour du nomadisme augmentent et se rapprochent de ceux des entreprises : de 15 à 30% d'augmentation pour l'accès des postes nomades, des postes non maîtrisés et du wifi. Seule exception : les PDA / smartphones, pourtant en hausse (+10%), restent bien moins autorisés qu'en entreprise (30% contre 53%). L'explication de ce phénomène réside principalement dans les risques de perturbations, avérés ou non, sur les équipements sensibles des hôpitaux.

Quant à la VoIP et la ToIP, 31% des hôpitaux (contre 14% précédemment) se déclarent « favorables » à leur utilisation : à l'instar des entreprises, les hôpitaux déploient de plus en plus cette technologie avec des besoins en disponibilité et en qualité de service à un niveau similaire voire supérieur.

Enfin, au vu des risques de sécurité liés à l'utilisation de la messagerie instantanée, cette technologie est là aussi peu autorisée (interdiction à 80% pour les hôpitaux contre 75% pour les entreprises).

Lutte antivirale

Les niveaux d'équipement des hôpitaux sont du même ordre que ceux constatés pour les entreprises, hormis en ce qui concerne la technologie du chiffrement des données. Ceci amène à penser que la démarche de sécurisation est la même pour les entreprises et les hôpitaux, les technologies étant aujourd'hui globalement communes.

L'utilisation du chiffrement des données utilisateur est globalement inférieure de 10% à ce qu'on trouve en entreprise, mais le plus intéressant est de voir que, dans le cas des hôpitaux, la majorité des machines chiffrées sont des ordinateurs fixes, ce qui explique une démarche plus axée sur la confidentialité des données que sur le vol d'équipements portables. Ceci est en effet compréhensible étant donné le niveau de confidentialité des données médicales. On voit ici que si les technologies sont communes avec les entreprises, les risques à adresser peuvent être parfois différents.

Infogérance

Moins d'infogérance dans les hôpitaux

Il apparaît que de moins en moins d'hôpitaux ont recours à l'infogérance (26%, soit une diminution de 11% depuis la précédente étude), ce qui constitue une différence notoire avec les entreprises pour lesquelles la proportion reste stable (autour de 35% externalisent la fonction SI en partie ou en totalité). Cette baisse peut être imputée à plusieurs raisons non exclusives : fort besoin de confidentialité, manque de confiance dans l'infogérance, ré-internalisation suite à des expériences d'infogérance n'ayant pas atteint les objectifs de qualité ou de sécurité escomptés…

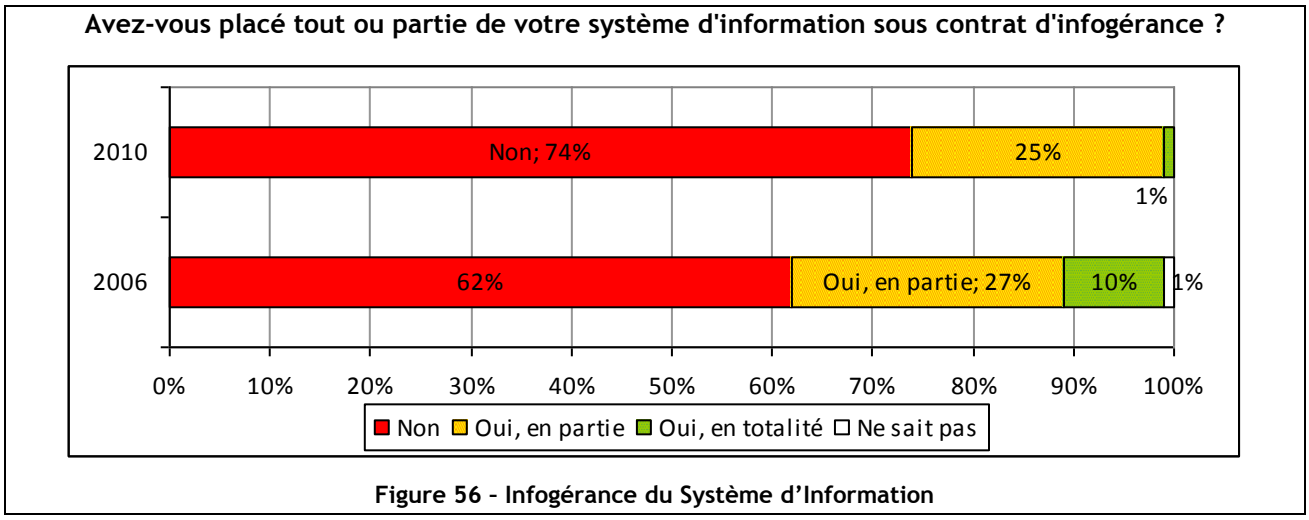

Figure 56 – Infogérance du Système d'Information

Un contrôle de la sécurité des contrats d'infogérance limité…

S'il y a moins de suivi régulier de l'infogérance par des indicateurs de sécurité, les hôpitaux sont plus nombreux en 2010 à exercer leur droit de regard sur les prestations associées via des audits de sécurité au moins ponctuels.

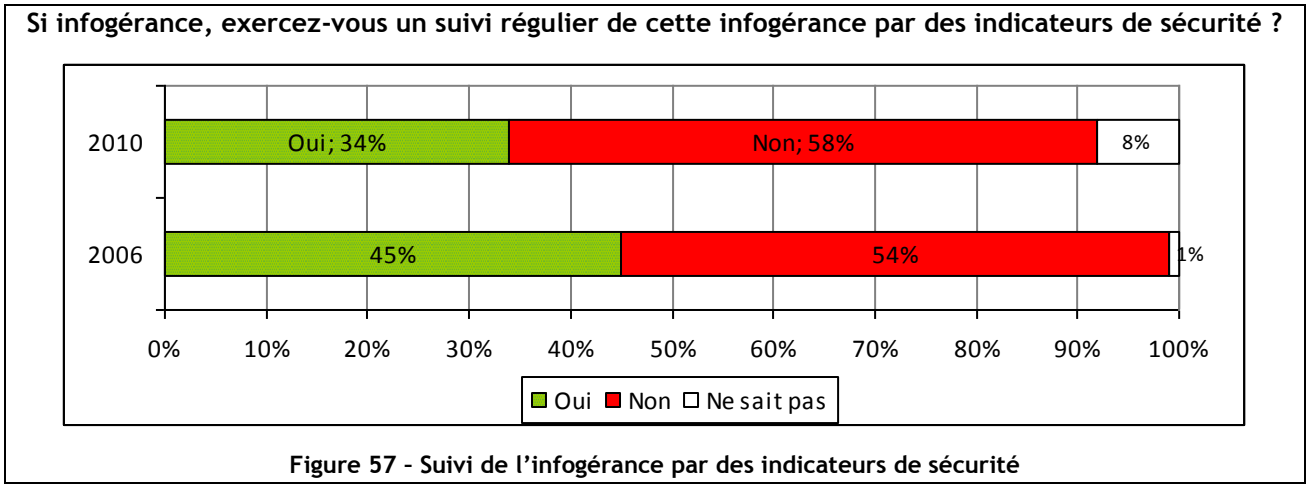

Figure 57 – Suivi de l'infogérance par des indicateurs de sécurité

Néanmoins, ce chiffre (31%) reste relativement faible et dénote globalement un contrôle de la sécurité limité dans les contrats d'infogérance.

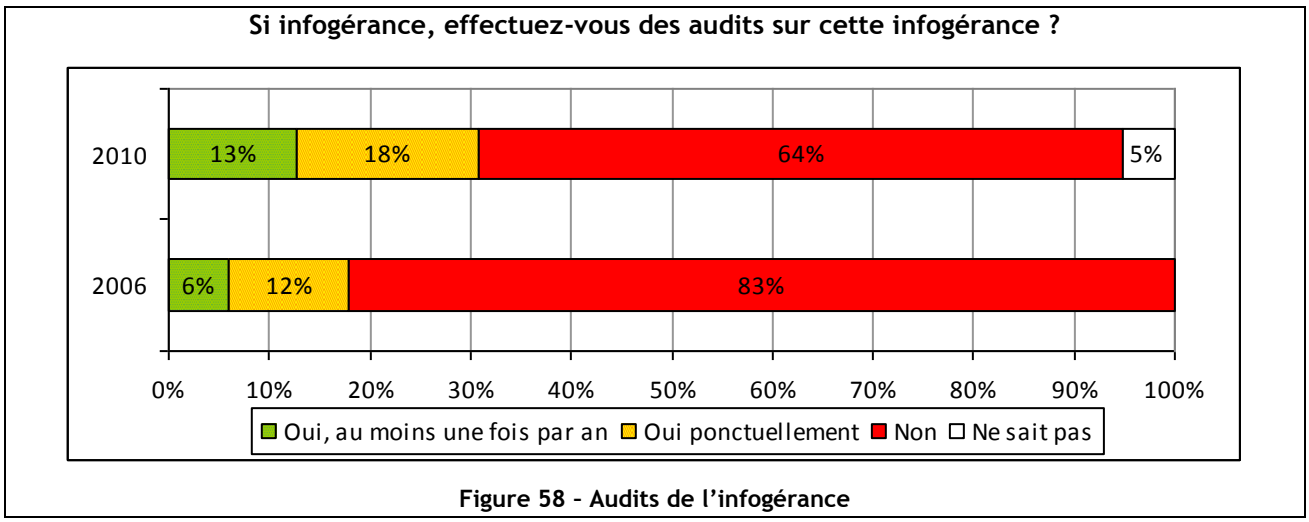

Figure 58 – Audits de l'infogérance

Thème 11 – Contrôle d'accès

Globalement, les établissements hospitaliers ont, depuis la dernière enquête, progressés dans l'adoption et la mise en œuvre des moyens de contrôles d'accès.

Les SSO (Single Sign On) ainsi que l'authentification forte par certificat électronique sur support matériel (carte à puce ou clé à puce) vont poursuivre leur diffusion dans plus d'un quart des établissements hospitaliers (respectivement 29% et 25% vont s'équiper en 2010). Le SSO est déjà le mécanisme le plus utilisé, de façon totale ou partielle, avec un établissement sur cinq équipé.

En matière de gestion des droits, il reste des insuffisances liées à l'absence de procédure formelle d'enregistrement, de révision et de désinscription des droits des utilisateurs, dans plus d'un établissement sur deux (55%).

Une procédure formelle d'enregistrement, de révision et de désinscription existe-t-elle ?

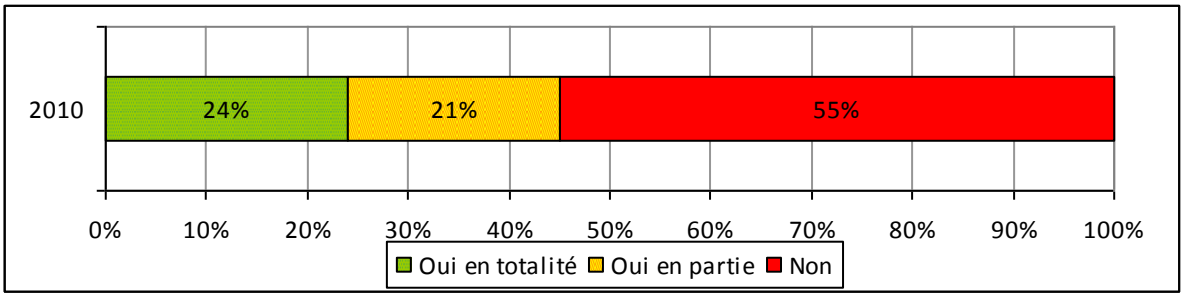

Figure 59 – Existence d'une procédure formelle d'enregistrement, de révision et de désinscription

Des règles de constitution et de péremption des mots de passe existent-elles pour tous les accès ?

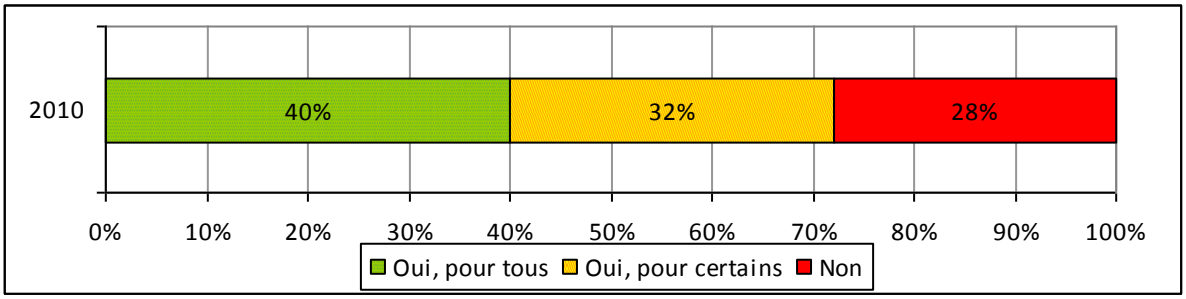

Figure 60 – Existence de règles de constitution et de péremption des mots de passe

De même, il n'y a aucun contrôle des mots de passe (pour leur constitution et leur péremption) dans un tiers des établissements.

Thème 12 - Acquisition développement et maintenance du SI

Veille sur les vulnérabilités

Les réponses aux questions relatives à la veille sur les vulnérabilités et les délais de déploiement des correctifs semblent marquer le pas par rapport à l'enquête 2006.

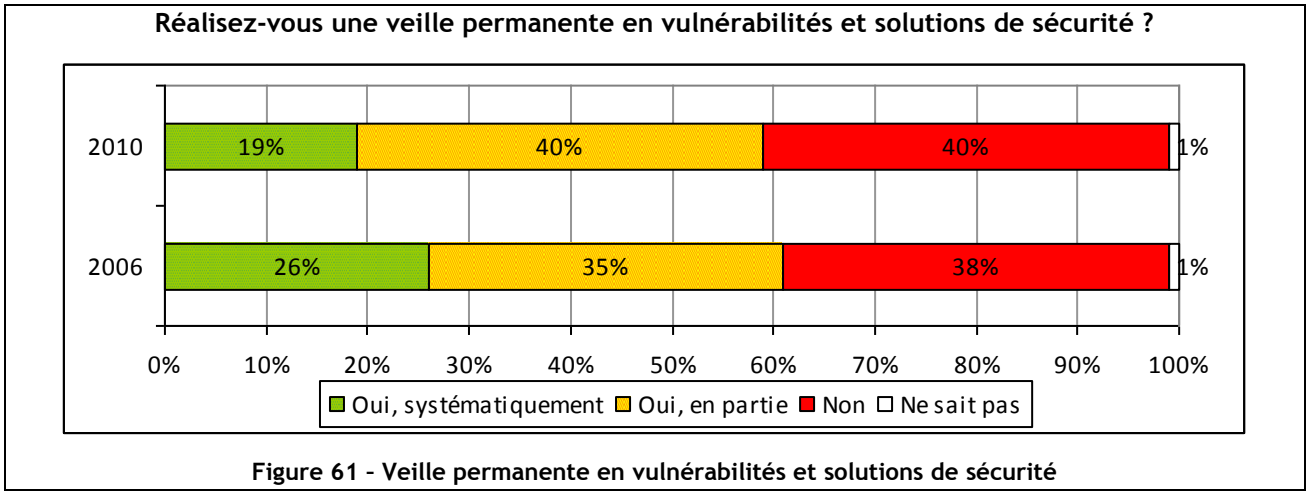

Figure 61 – Veille permanente en vulnérabilités et solutions de sécurité

La diminution constatée d'efficacité visible sur les tableaux correspond plus à l'élargissement du périmètre qu'à une diminution de l'efficacité des établissements interrogés en 2006. En effet, il est assez peu probable que les établissements de moins de 200 lits mettent en place des traitements ayant besoin d'une masse critique importante comme la veille ou le traitement des correctifs. Une forme de mutualisation sur ces sujets est peut être à inventer…

En revanche, nous constatons avec satisfaction un progrès, même modéré en matière de mise en place des procédures formalisant la gestion des correctifs. Ceci est d'autant plus important que la sinistralité due aux erreurs de conception des logiciels est en nette progression autant du point de vue du nombre que, surtout, de leur gravité. Il doit être noté que ce progrès n'a pas permis une amélioration des performances mais au contraire une dégradation. Doit-on y voir une meilleure maitrise et donc des réponses plus exactes ? Ceci est probable. Il est également intéressant de constater la même tendance dans les réponses des entreprises.

L'existence d'un processus de déploiement des correctifs en progression

Il semble que si l'on détecte moins bien et moins globalement les failles, les processus pour déployer les correctifs soient, eux, de plus en plus formalisés : 47% des hôpitaux du panel, contre 34% en 2006.

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

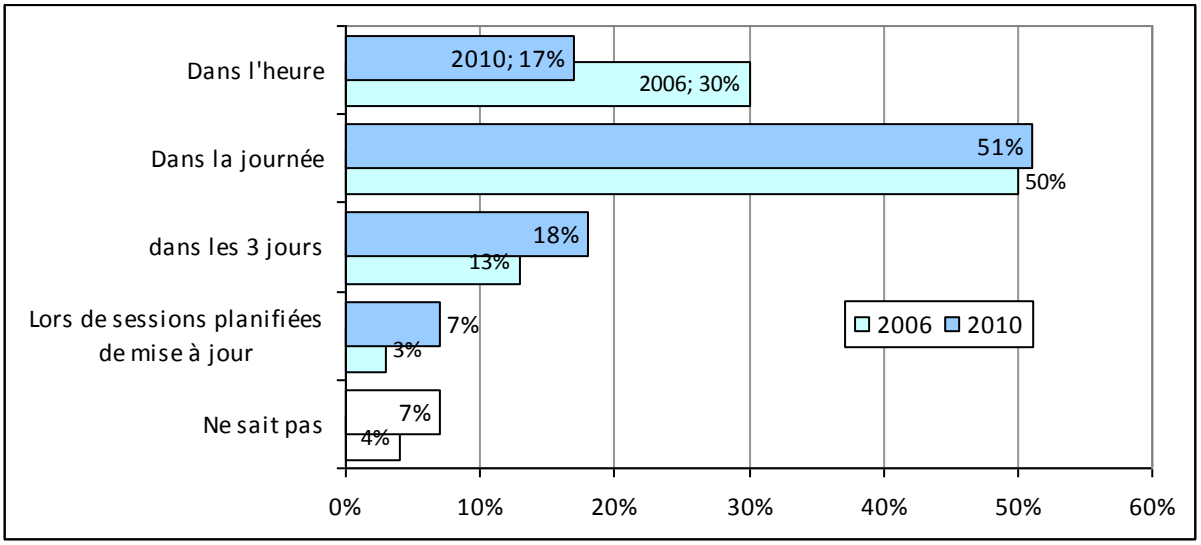

Figure 62 – Délai moyen nécessaire pour déployer les correctifs

Les résultats sur le déploiement des correctifs sont étonnants. En effet, la meilleure définition des processus de déploiement n'a pas permis une amélioration des performances mais au contraire une dégradation. Doit-on y voir une meilleure maitrise et donc des réponses plus exactes ? Ceci est probable. Il est également intéressant de constater la même dérive dans les réponses des entreprises.

In fine, il en reste néanmoins que plus de 80% des établissements sondés semblent capable de déployer des correctifs en moins de 3 jours en cas d'urgence alors que seuls 19% sont sûrs d'être alertés par leur dispositif de veille…

Thème 13 – Gestion des incidents

Les incidents de sécurité sont de mieux en mieux détectés

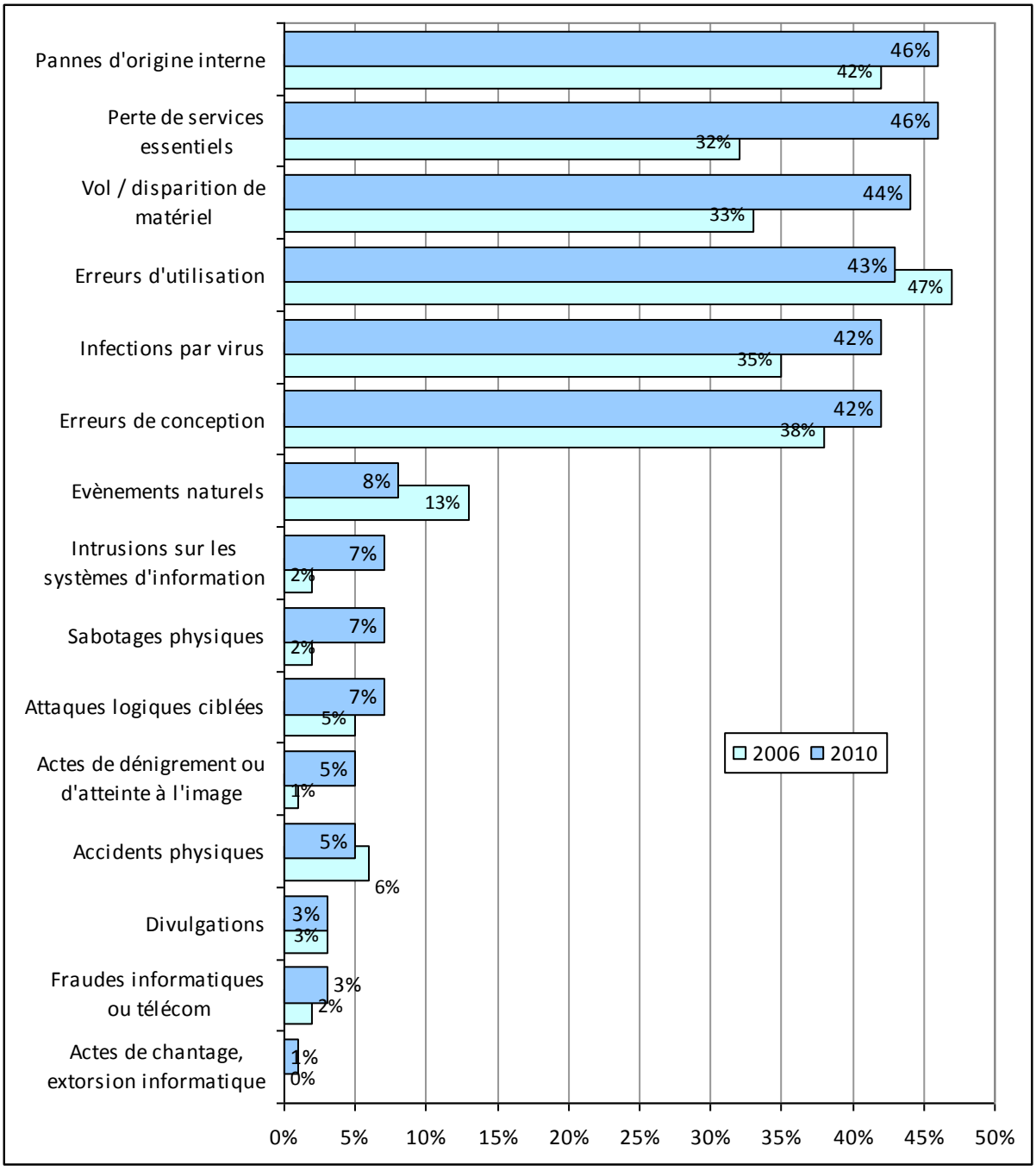

Figure 63 – Types d'incidents survenus

L'augmentation de la perte de services essentiels est forte

Une cause probable pouvant être l'augmentation de la pénétration des Systèmes d'Information dans les actes médicaux conjuguée à l'interconnexion accrue de ces systèmes avec des moyens informatiques traditionnels.

Nature de l'incident	Origine			nombre moyen d'incidents	Impact		
	interne	externe	inconnue		faible	moyen	élevé
Perte de services essentiels	65%	34%	1%	4,5	43%	35%	22%
Pannes d'origine interne				5,4	47%	25%	28%
Vol / disparition de matériel	26%	7%	67%	5	85%	12%	3%
Erreurs d'utilisation	93%	0%	7%	42,2	71%	21%	8%
Erreurs de conception	43%	49%	8%	20,1	49%	35%	16%
Infections par virus	11%	64%	24%	9,8	59%	22%	19%

Figure 64 – Natures des principaux incidents survenus

L'année 2010 marquée, notamment, par l'infection massive du vers « Confiker » laisse à penser qu'une relation pourrait être faite entre l'augmentation des infections virales et la perte de services essentiels. En effet, ce malware a infecté près de la moitié des CHU de France avec parfois des interruptions de service quasi-totales pendant des durées pouvant aller jusqu'à 3 semaines. Les dernières infections massives du même ordre étaient dues à "I Love You" et autres malwares similaires.

L'ouverture de ces systèmes à du personnel externe pouvant utiliser des moyens véhiculant des codes malveillants, tels que les clés USB ou autres supports amovibles, est un facteur de risque nécessitant une prise en considération.

On peut aussi se demander si, tout simplement, ce nombre de pertes de services en forte augmentation n'est pas dû au fait que le panel 2010 comporte de plus gros hôpitaux qu'en 2006, et qu'ils ont une meilleure connaissance (grâce à de meilleurs circuits de remontée) de leurs incidents. Et ce d'autant plus que la taille des hôpitaux augmentant, il est normal que le nombre de pertes de services augmente aussi.

Une autre piste à explorer se situe du côté de la qualité de service des fournisseurs de service essentiels (FAI, électricité, etc.), soumis à une concurrence violente, et à des mises en place de nouvelles infrastructures encore en cours de stabilisation.

Une évolution paraît de prime abord notable depuis l'étude précédente : elle concerne le ressenti en matière d'intrusions sur les systèmes d'information qui atteint un taux remarquable de 7% d'hôpitaux déclarant avoir rencontré de tels incidents (l'étude ne distinguant pas les tentatives des intrusions effectivement réussies). Ce chiffre est cohérent avec le déploiement de plus en plus courant d'outils de détection ou de prévention des intrusions et ne peut être interprété comme une évolution de ce type de risques.

Les vols de matériels ont progressé de plus d'un tiers

Avec 44% des hôpitaux déclarant avoir rencontré des incidents de cette nature, avec le plus souvent un impact faible. De tels chiffres sont liés à la nature même des hôpitaux qui accueillent quotidiennement du public et au développement des outils nomades. Ces disparitions de matériels devraient plus fréquemment déboucher sur des dépôts de plainte. Toutefois ces malveillances sont celles qui entrainent l'impact le plus faible. La confirmation de cette tendance, inévitable dans un tel environnement, doit inciter les hôpitaux à développer l'utilisation du chiffrement ou de toutes techniques permettant de diminuer l'impact de tels vols ou disparitions de matériels, notamment sur les postes informatiques portables.

L'évolution des erreurs de conception, les pannes d'origine internes ainsi que la baisse des erreurs d'utilisation, sont difficilement interprétables compte tenu de l'évolution du périmètre de l'étude et devront être confirmés dans les prochaines études et devront naturellement faire l'objet d'une attention particulière.

En effet les pannes d'origine internes sont celles ayant l'impact le plus élevé. Les erreurs de conception, significativement plus nombreuses, une menace réelle à l'impact fort.

Les erreurs d'utilisation étant les plus fréquentes, sont aussi celles, qui après le vol de matériel, ont l'impact le plus faible.

Les résultats des types d'incidents identifiés démontrent clairement une baisse des causes accidentelles (évènements naturels) alors que les causes malveillantes progressent.

Une gestion des incidents de sécurité qui marque le pas

Comme la gestion des correctifs, la gestion des incidents de sécurité semble marquer le pas. Encore une fois, les différences constatées entre 2006 et 2010 ne sont pas suffisamment significatives au vu de la modification du panel de l'enquête.

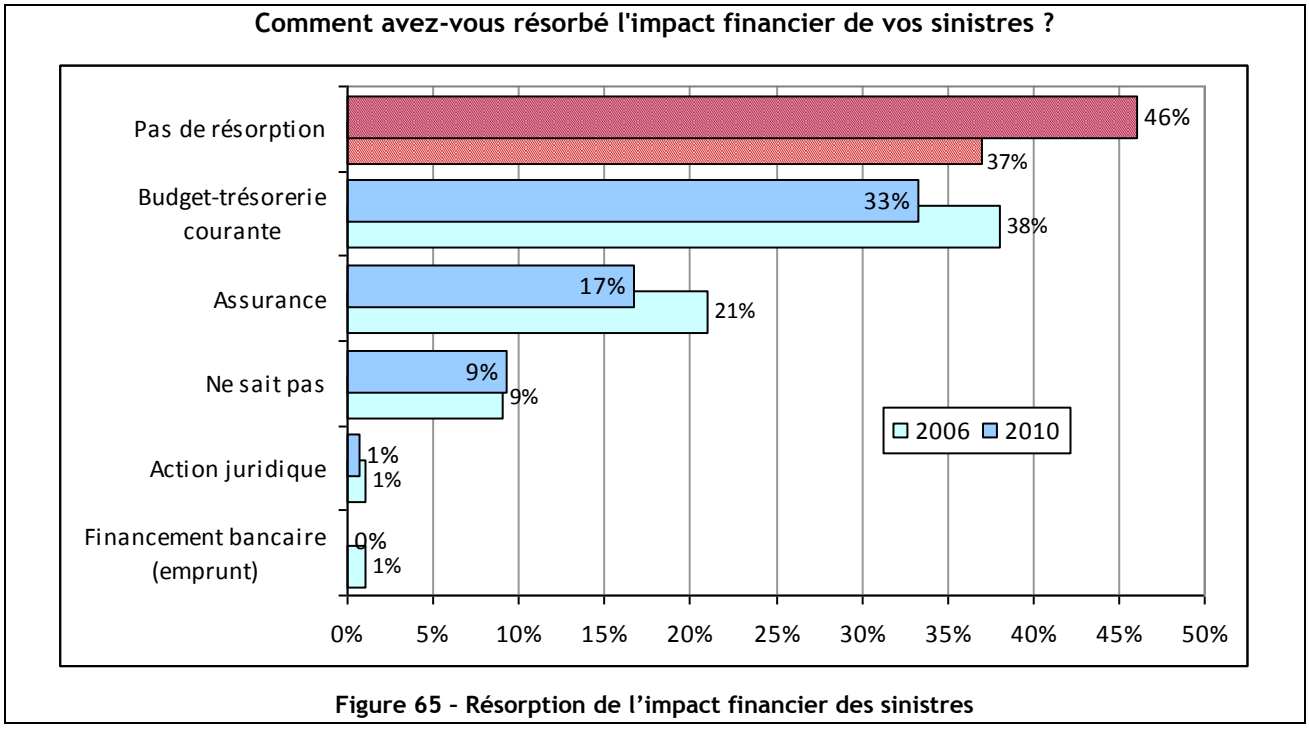

Figure 65 – Résorption de l'impact financier des sinistres

Ainsi, la diminution du dépôt des plaintes n'est pas significative par rapport à la modification du panel, les grands établissements ont des structures spécifiques pouvant prendre plus aisément cette problématique en charge. De même en ce qui concerne l' « augmentation » apparente du nombre d'incidents. Tout ceci est à mettre en rapport avec la dépendance croissante des établissements par rapport à leur Système d'Information.

Concernant la question relative aux impacts financiers, les chiffres doivent être lus avec prudence. Si le risque financier est important, il ne faut pas oublier que la notion de « risque vital » a une signification très concrète dans le milieu hospitalier, qui ne correspond pas à la notion de « faillite » des entreprises privées. Il est probable que certaines réponses ont pris en compte l'idée de l'analyse du risque au delà du risque financier.

Thème 14. Gestion de la continuité

Globalement, maintenant plus de la moitié des établissements interrogés déclarent avoir formalisé le processus de gestion de la continuité de service : 22% d'entre eux l'ont fait globalement.

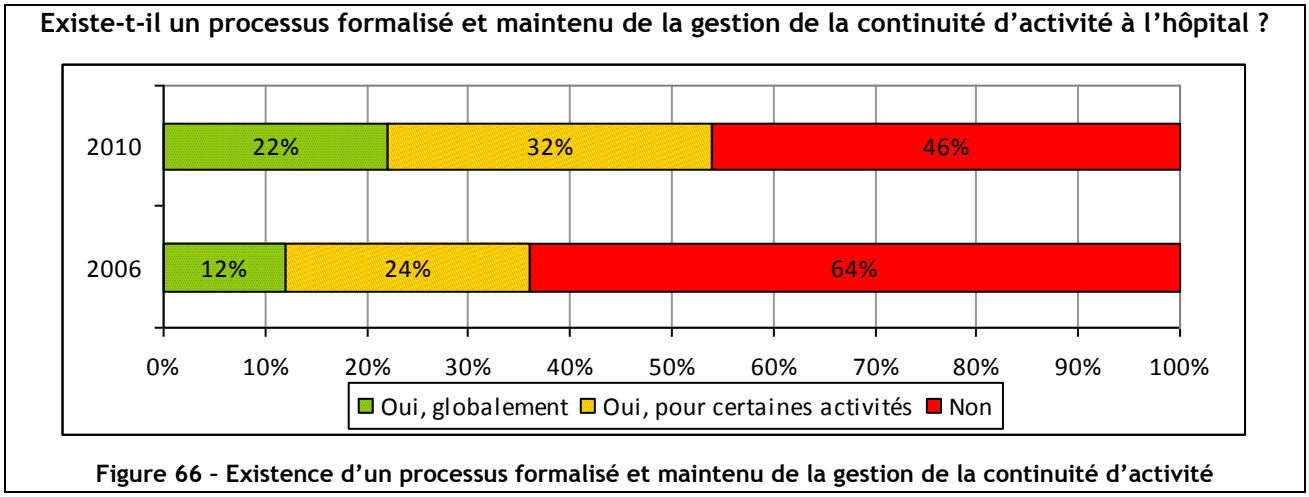

Figure 66 – Existence d'un processus formalisé et maintenu de la gestion de la continuité d'activité

Malgré une forte progression (+18%) par rapport à 2006, il reste toujours près d'un hôpital sur deux qui n'a toujours pas traité la gestion de la continuité d'activité. Il est à parier que cela est à corréler avec la forte augmentation de la dépendance des hôpitaux à leur SIH dans des secteurs particulièrement critiques (imagerie, laboratoire, mais aussi prescription connectée, etc.).

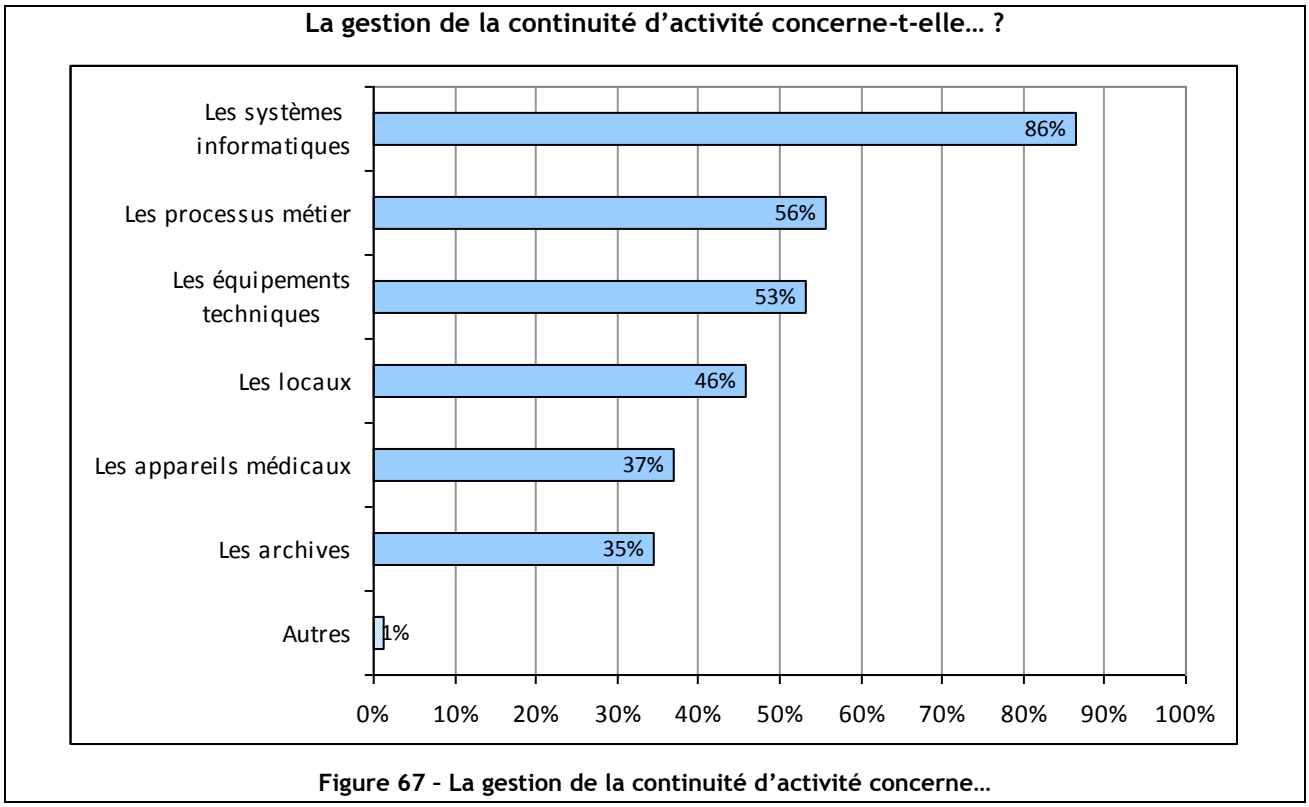

Figure 67 – La gestion de la continuité d'activité concerne…

La gestion de la continuité d'activité reste essentiellement technique

On ne doit donc pas parler d'un PCA (Plan de Continuité d'Activité au sens métier du terme) mais plutôt de PSI (Plan de Secours Informatique, qui ne concerne que les infrastructures techniques). Le PRA-PCA aborde encore trop peu souvent les aspects métiers, qui sont le maillon faible de cette continuité. A quoi sert, en effet, de disposer d'équipements de secours si les personnels ne connaissent pas la procédure pour les utiliser en cas de panne globale du système ?

Le chiffre le plus surprenant concerne celui des équipements médicaux : pourtant, la plupart des services biomédicaux sont rompus depuis longtemps à la continuité d'appareils médicaux dit vitaux (console de surveillance, respirateurs artificiels).

À quelle fréquence les plans de continuité d'activité sont-ils testés et mis à jour ?

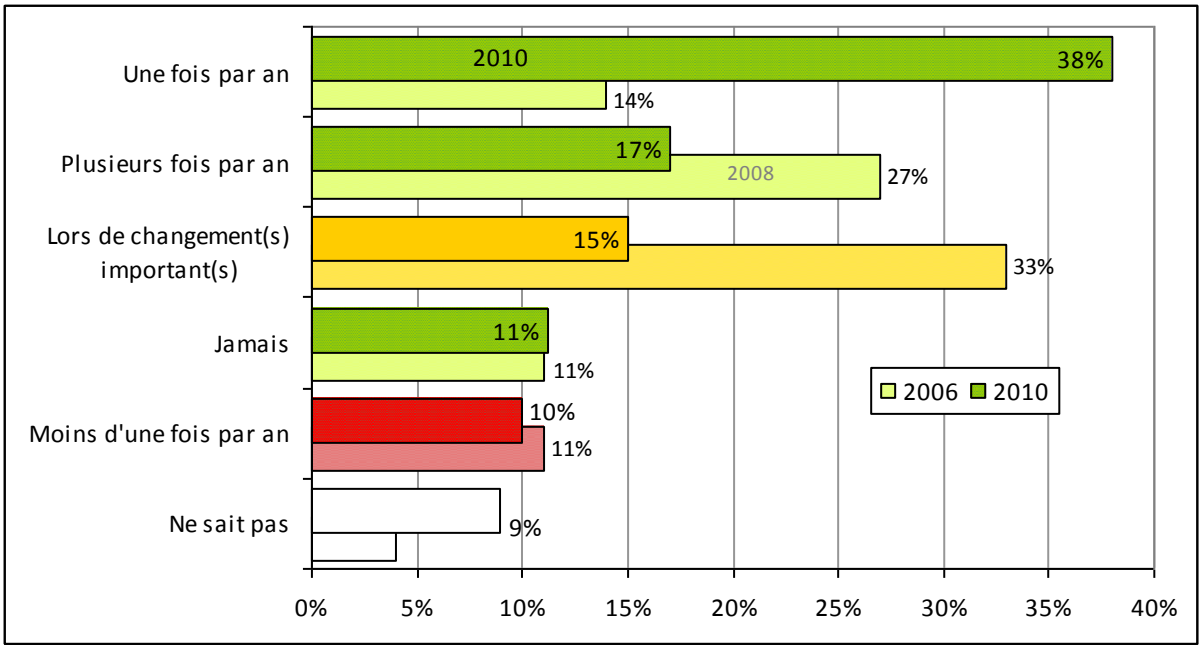

Figure 68 – Fréquence des tests et mises à jour des plans de continuité d'activité

Globalement, les PCA sont testés et mis à jours au moins une fois par an ou à l'occasion de changements importants. Ce qui est surprenant c'est que l'on constate (comme pour les entreprises), une diminution par rapport à 2006 du nombre de tests réalisés plusieurs fois par an (-10%). A l'inverse, on remarque une forte augmentation du nombre de tests réalisés une fois par an (+14%). Là encore, on peut s'interroger sur le bien fondé d'un seul test mené dans l'année. En effet, ce seul test peut-il s'avérer concluant pour s'assurer du bon dispositif de continuité d'activité de l'hôpital concerné ?

Les résultats dans leurs globalités sont certainement du aux mêmes raisons de dépendance croissante des hôpitaux vis-à-vis de leurs SIH. Encore faudrait-il comprendre et décrypter ce qui est couvert par ces tests.

En effet, s'il ne s'agit que de tests de bascule technique, c'est bien mais cela reste insuffisant. Là aussi, il faudrait que les responsables des PCA au sein des hôpitaux parviennent d'avantage à inclure les contributions métier.

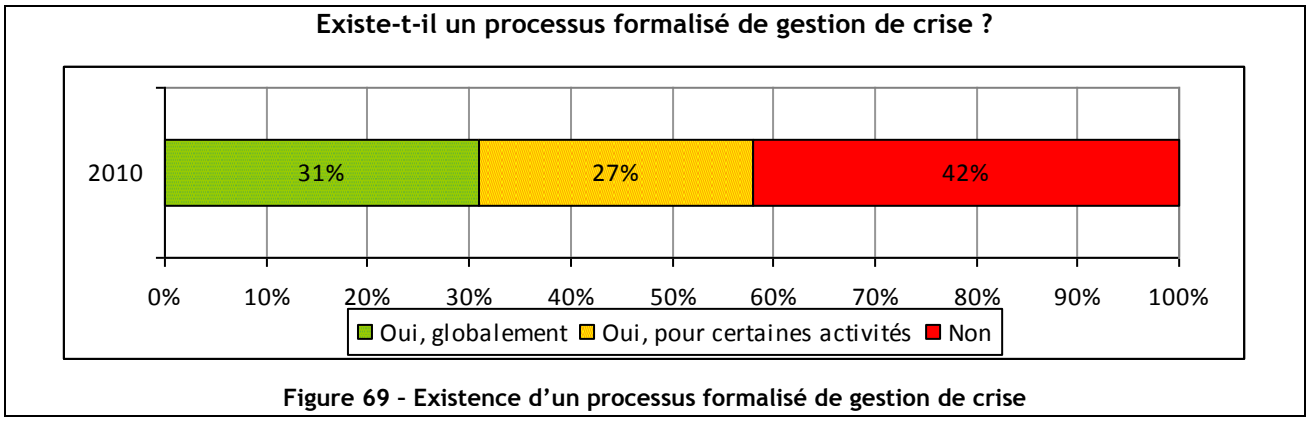

Figure 69 – Existence d'un processus formalisé de gestion de crise

Près d'un tiers des hôpitaux disposent d'un processus formalisé de gestion de crise

C'est est un bon score mais à modérer face aux 42% des hôpitaux qui n'en disposent pas ! Ce qui est surprenant, c'est que le résultat des hôpitaux en matière de gestion de crise est supérieur à celui des entreprises, alors que ces dernières sont pourtant plus nombreuses à avoir mis en place des PCA.
La gestion de crise semble donc mieux maitrisée par les hôpitaux, sans doute au regard de la criticité de leur obligations en cas d'incident grave. Toutefois, tous ces résultats doivent être pris avec grande précaution en termes de compréhension. Est-il utile de rappeler que tout processus de continuité d'activité englobe obligatoirement une gestion de crise ?

Plus de 80% des mêmes personnes interrogées qui déclarent avoir mis en place des processus de continuité, répondent pourtant qu'elles n'ont pas identifié leurs RTO et RPO ! Il s'agit certainement d'une question délicate à poser à une direction métier – et celle pour laquelle il est le plus facile d'obtenir une réponse. « Combien de temps pouvez-vous supporter que votre système informatique s'arrête » déclenche souvent un regard étonné de la part de l'interlocuteur. Ce dernier répond le plus souvent que « tout doit être mis en œuvre pour qu'il n'y ait jamais d'arrêt ». Ajoutons enfin à cela qu'il n'y a pas ou très peu de culture de risque à l'hôpital, et pas seulement dans le domaine des Systèmes d'Information.

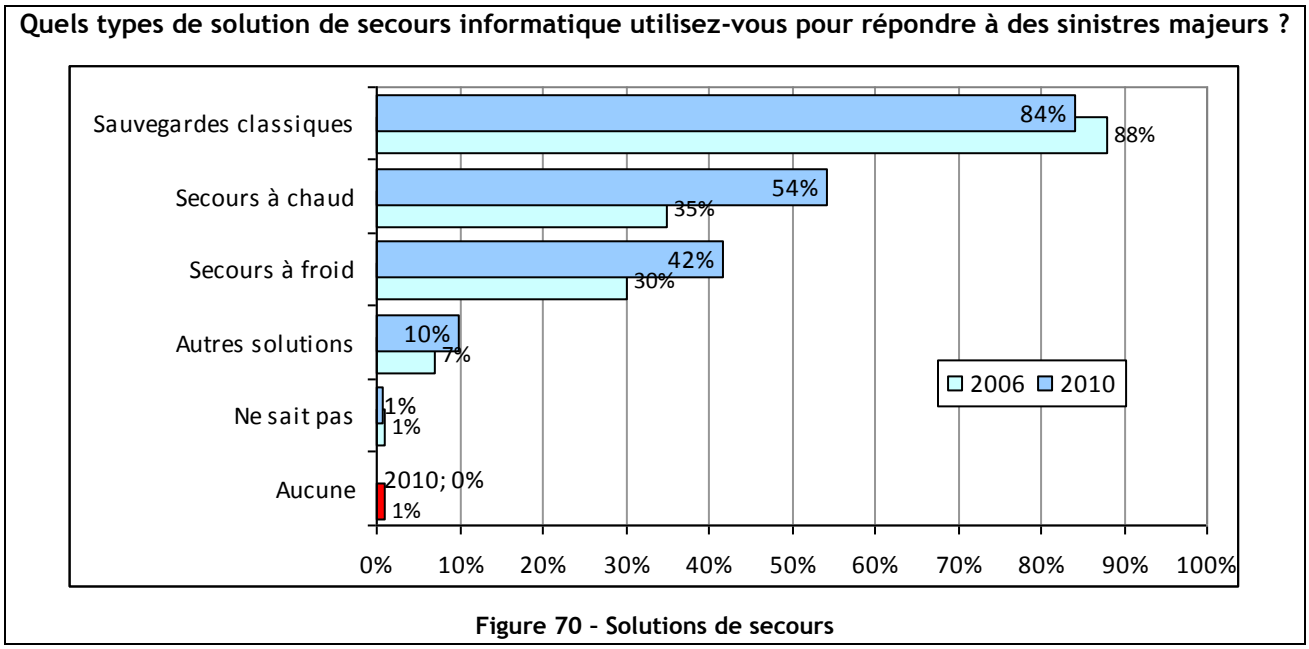

Figure 70 – Solutions de secours

Une progression globale de solution de secours informatiques s'affiche au regard de l'ensemble de ces résultats. Ces derniers montrent de fortes corrélations avec ceux constatés auprès des entreprises.

À l'inverse, le secours à froid comme le secours à chaud augmentent considérablement. Là aussi, les nouvelles technologies comme les nouveaux moyens de sauvegardes télé distants sont sans doute à l'origine de toutes ces augmentations à l'exception des moyens de sauvegardes classiques qui baissent d'environ 6%.

Ces dernières années, la baisse des coûts des solutions de sauvegardes et/ou de redémarrage à chaud comme à froid permettent sans aucun doute aux RSSI des hôpitaux de mieux appréhender leurs solutions de secours informatiques.

Thème 15 - Conformité

Une conformité aux lois et règlements en légère augmentation

Une progression de quatre points s'est opérée en 2010, par rapport à 2006, sur la conformité aux obligations de la CNIL : 94% des hôpitaux interrogés estiment être en conformité totale ou sur les traitements les plus sensibles.

De même, la mise en place d'un Correspondant Informatique et Liberté (tel que défini par la CNIL) progresse nettement : cette mise en place est faite ou décidée dans 43% des hôpitaux (contre 37% en 2006). En revanche, 38% des hôpitaux ne l'a encore ni fait ni prévu, cette fonction entrant probablement dans le périmètre d'un autre poste.

A la question « Votre hôpital est-il soumis à des lois et/ou règlementations spécifiques en matière de sécurité des informations », 31% des répondants répondent « non » ou ne savent pas.

Or, la confidentialité des données personnelles médicales sur informatique obéit aux textes relatifs au secret de la vie privée (art. 9 du Code civil), au secret médical (art. R 4127-4 du Code de la santé publique et, pour le secret professionnel, art. 226-13 du Code pénal), à la loi garantissant la confidentialité des correspondances privées par voie de télécommunications, notamment celles qui concernent la santé, et à la loi Informatique et Libertés qui exige, elle aussi, la confidentialité et la sécurité des données (art. 29). En effet, selon la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, les droits du patient et les devoirs du médecin concernant les dossiers médicaux informatisés sont les suivants : le droit à l'information (article 28) et le droit à l'opposition et à l'oubli (article 26), le droit de contestation et de rectification (article 36), et le droit à la sécurité (article 29).

Par ailleurs, la loi relative à l'assurance maladie créant le dossier médical personnel (DMP) pour chaque assuré social a été adoptée le 13 août 2004. Actuellement, le DMP a pu être expérimenté par 17 sites pilotes désignés dans la circulaire DHOS/E3 n°2006-281 du 28 juin 2006 relative à la mise en œuvre du dossier médical personnel par les établissements de santé. Nous pouvons citer notamment les CHU de Lille, Strasbourg, Toulouse ou encore Amiens mais également des établissements de soins privés. Le décret confidentialité du 15 mai 2008 a concrétisé les recommandations de la CNIL, dans la mesure où il impose l'utilisation de la Carte Professionnel de Santé (CPS) comme procédé d'identification et d'authentification pour toute transmission ou accès aux données de santé, et plus particulièrement au DMP, y compris au sein d'une même structure.

Cette méconnaissance des lois peut donc surprendre : le profil du répondant est-il en cause, ou sa sensibilisation aux aspects juridiques de la sécurité ?

Audits de sécurité : une pratique restant à améliorer…

Concernant les audits de sécurité du SI, la fréquence annuelle est très variable :

- la moitié du panel n'en réalise aucun (quelle que soit la taille de l'établissement),
- 34% des établissements de moins de 500 lits en réalisent 1 à 2 par an (45% pour les hôpitaux de plus de 500 lits),
- et 12% en réalisent plus de 3 par an.

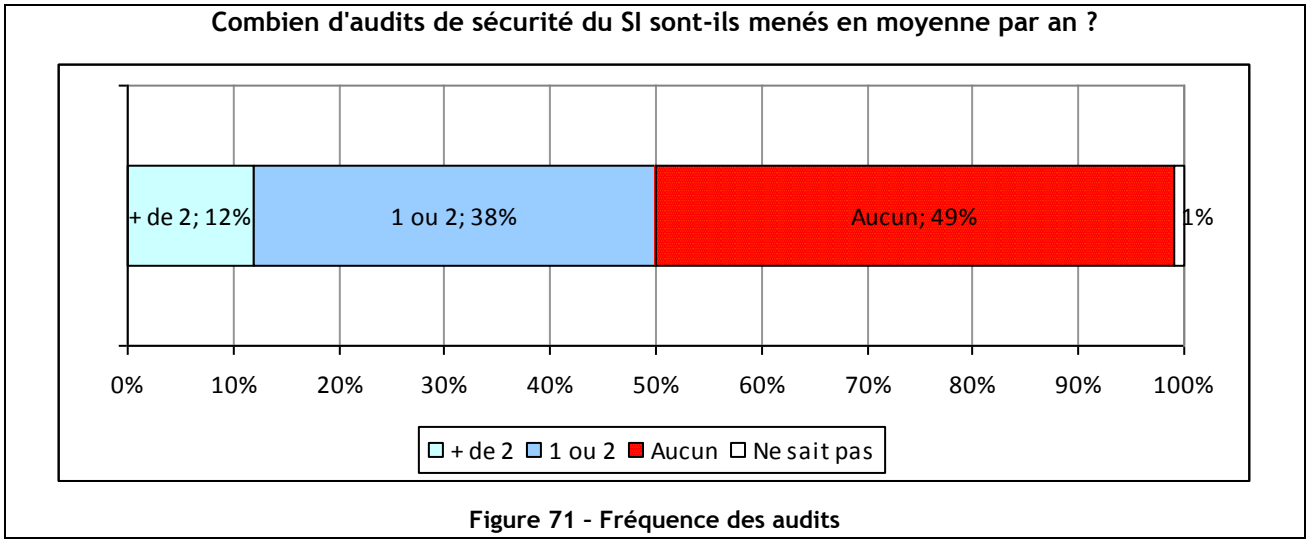

Figure 71 – Fréquence des audits

On peut penser que l'interprétation du terme « audit » est en jeu : dans le monde médical, l'audit est une procédure différente des contrôles de routine. Il est habituellement effectué par un auditeur interne dédié, ou un cabinet extérieur.

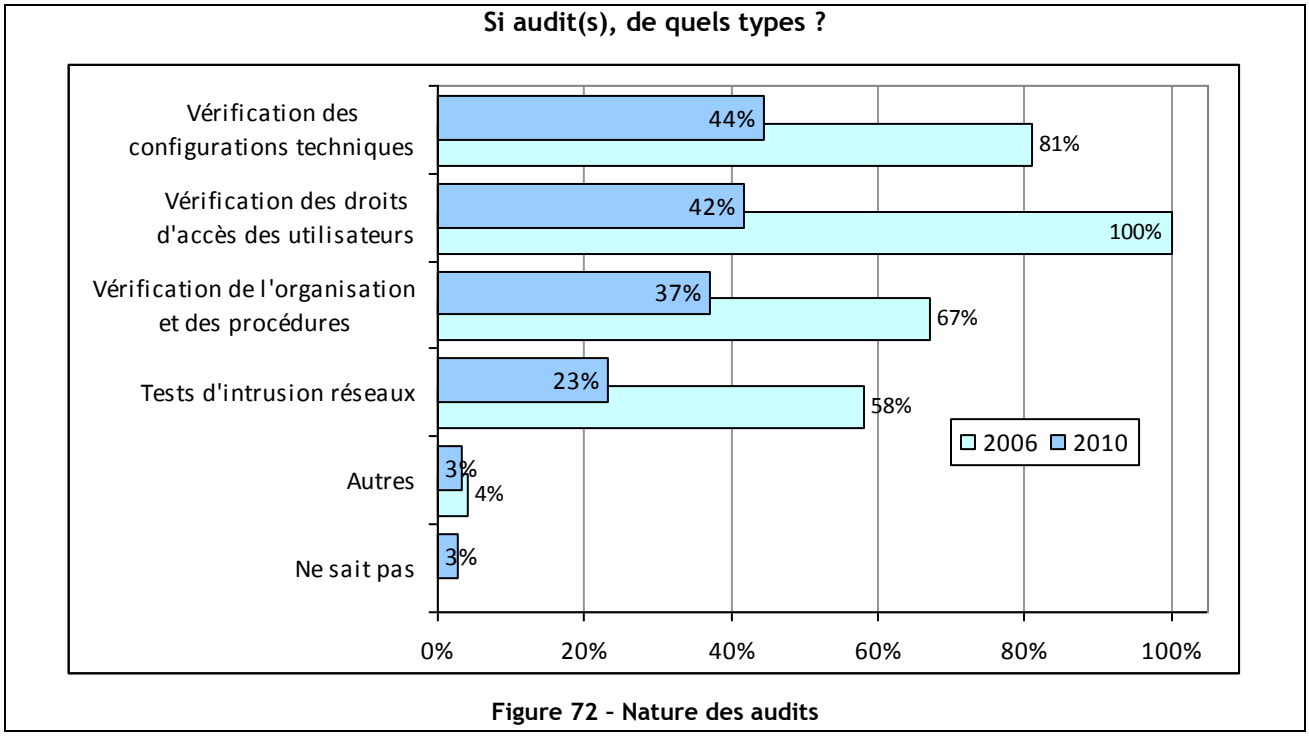

Figure 72 – Nature des audits

Dans la question suivante, on voit que les différentes natures des « audits » et leur périmètre expliquent la variabilité de cette fréquence.

Ainsi, pour les hôpitaux « pratiquant des audits », seuls 37% procèdent à une vérification totale du périmètre Sécurité (organisation et procédures), ce qui est en nette régression par rapport à 2006 et compte tenu de la taille des établissements interrogés.

Le reste des audits est technique : tests d'intrusion (23%), configurations techniques (44%), droits d'accès (42%). Il est très étonnant de voir qu'en 2006 tous les hôpitaux interrogés contrôlaient leurs droits d'accès, y compris les hôpitaux de « petite » taille, contre 42% en 2010 : quelque soit la taille de l'hôpital, et a fortiori pour les grands établissements, ceci devrait faire partie des incontournables.

Les motivations qui déclenchent ces audits sont de diverses natures : politique de sécurité (à 46%), en raison de projets « sensibles » (46%), contractuelle ou règlementaire (38%), demandés par les tutelles ou les assureurs (10%).

Par ailleurs, 38% des audits sont déclenchés suite à un incident. Malheureusement comme souvent, c'est à la suite d'un sinistre que l'on prend conscience de la nécessité de prendre des mesures de protection. C'est aussi vrai dans le domaine de la sécurité civile (par exemple un carrefour dangereux) que dans celui des Système d'Information. L'hôpital n'échappe pas à la règle.

À noter que 30% des répondants ne savent pas pourquoi ces contrôles sont pratiqués : on peut supposer qu'ils ne sont pas responsables de les pratiquer eux-mêmes.

Tableaux de bord de la sécurité informatique : une quasi-absence surprenante

Sans progression depuis 2006, de façon surprenante si l'on considère que les hôpitaux interrogés en 2010 étaient de plus gros établissements (plus de 500 lits), très peu d'hôpitaux ont mis en place des tableaux de bord de suivi de la Sécurité informatique : seulement 7% (soit 10 hôpitaux).

Pour ces dix hôpitaux, les indicateurs suivis sont les suivants :

- nombre d'incidents sur une période,
- conformité avec les normes (comme ISO 27001),
- vulnérabilités détectées,
- nombre d'attaques arrêtées,
- impacts directs et indirects des incidents,
- taux de mise à jour des signatures antivirales,
- évaluation des risques métiers,
- suivi du budget consacré à la sécurité,
- taux de mise à jour des patches de sécurité,
- avancement des projets de sécurisation,
- taux de personnes sensibilisées.

Internautes

- Présentation de l'échantillon
- Partie I – Identification et Inventaire
- Partie II – Perception de la menace résultant de la connexion à Internet et sensibilité de l'utilisateur
- Partie III – Les usages de l'internaute
- Partie IV – Moyens et comportements de sécurité

Les Internautes

Présentation de l'échantillon

Deux ans après la première enquête lancée par le CLUSIF sur les pratiques et les comportements des particuliers autour d'Internet à partir de leurs équipements personnels, cette nouvelle étude a été réalisée fin 2010 à partir d'un échantillon de 1000 personnes.

Comme pour la première étude, 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.

Il peut être utile de rapprocher les résultats obtenus par l'enquête et ceux d'une étude réalisée par l'ARCEP (Autorité de Régulation des Communications Électroniques et des Postes), à la même époque (fin 2009), étude qui indiquait 19,7 millions d'abonnements Internet[1], dont 3,6% par modem, 95% par ADSL et 1,5% à très haut débit (par fibre optique). Par ailleurs, l'ARCEP a noté une croissance des abonnements proche de 10% pendant l'année 2009.

[1] Par ailleurs, l'INSEE comptabilise 31 millions de logements en France et environ 24 millions de ménages fin 2009.

Partie I – Identification et inventaire

L'enquête 2010 montre une progression certaine dans l'inventaire des ordinateurs et l'utilisation d'Internet par rapport à l'étude de 2008.

Ainsi, la part des foyers possédant 3 ordinateurs familiaux ou plus a cru de 16% à 21% en 2 ans.

La connexion à Internet est permanente (dès que l'ordinateur est allumé) pour 80% des internautes, ce qui est stable.

En ce qui concerne les abonnements, les résultats de l'enquête indiquent des valeurs proches de ceux de l'ARCEP : les liaisons par modem sont marginales (2%) tandis que les liaisons ADSL à plus de 1 Mbps (en très haute majorité) ou par câble, représentent 87% des raccordements au domicile et que 65% utiliseraient une liaison à plus de 10 Mbps.

Vers la boîte de raccordement ADSL ou câble (« box »), l'utilisation d'une liaison wifi depuis leur installation familiale croît de 51% à 59%. Très probablement, il s'agit de remplacements de postes plus anciens au profit de systèmes intégrant une antenne wifi.

De nouveaux équipements (blackberry, iphone, etc.) et de nouveaux moyens d'accès sans fil à Internet se développent (Edge/3G) qui permettent d'établir des connexions en dehors du domicile.
Parmi les internautes disposant de connexions mobiles (wifi ou 3G), 58% déclarent établir des connexions en déplacement hors de leur domicile (23% souvent et 35% plus rarement).

Plus l'internaute est jeune ou réside dans une grande agglomération (surtout Paris) plus il dispose d'un PC portable et utilise le wifi ou une connexion mobile, de même s'il y a au moins 2 ordinateurs dans le foyer.

De manière plus significative, 80% des utilisateurs de PC portables utilisent une connexion wifi contre moins de 30% pour les ordinateurs de bureau.

Le nombre d'ordinateurs par foyer et la facilité de se connecter en mode sans fil, grâce au wifi augmentent avec des taux équivalents à celui du raccordement des ménages à Internet (environ 10% par an).

L'enquête permet de relever aussi l'utilisation notable des équipements de mobilité (PC portables et téléphones 3G) hors du domicile (la croissance de ces possibilités sera au programme de la prochaine enquête).

Partie II – Perception de la menace résultant de la connexion à Internet et sensibilité de l'utilisateur

Protection des fichiers, du matériel et de la vie privée

Le sentiment d'insécurité diminue légèrement par rapport à l'étude précédente : les internautes sont moins inquiets face aux risques liés à leurs fichiers ou leurs matériels (25% en 2008 « risque important ou très important » vs 23% en 2010).

Pensez-vous que la connexion à Internet de votre ordinateur fait courir des risques à vos fichiers et à votre matériel ?

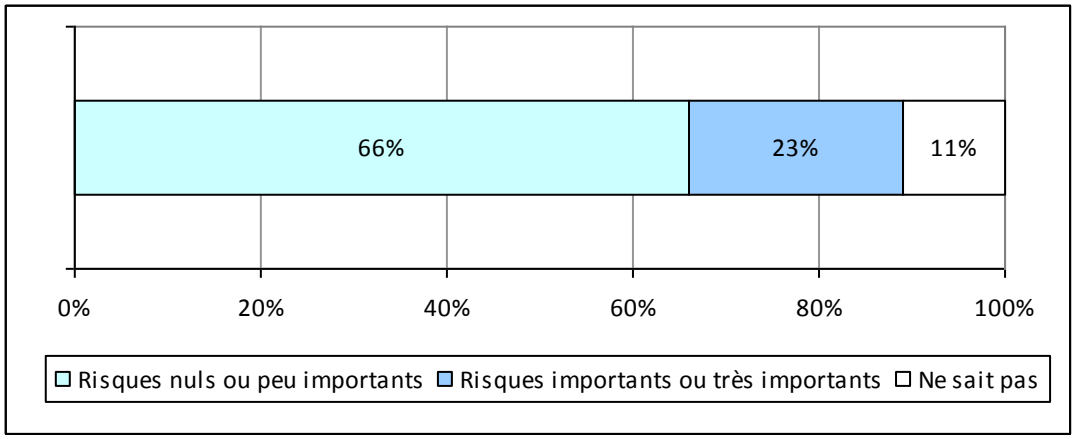

Figure 73 – Menaces sur les fichiers et le matériel

En revanche, le sentiment de danger concernant la protection de la vie privée augmente (mise en danger de la vie privée fortement ou un peu 60% en 2008 vs 73% en 2010).

Pensez-vous que l'utilisation d'Internet peut mettre en danger la protection de votre vie privée ?

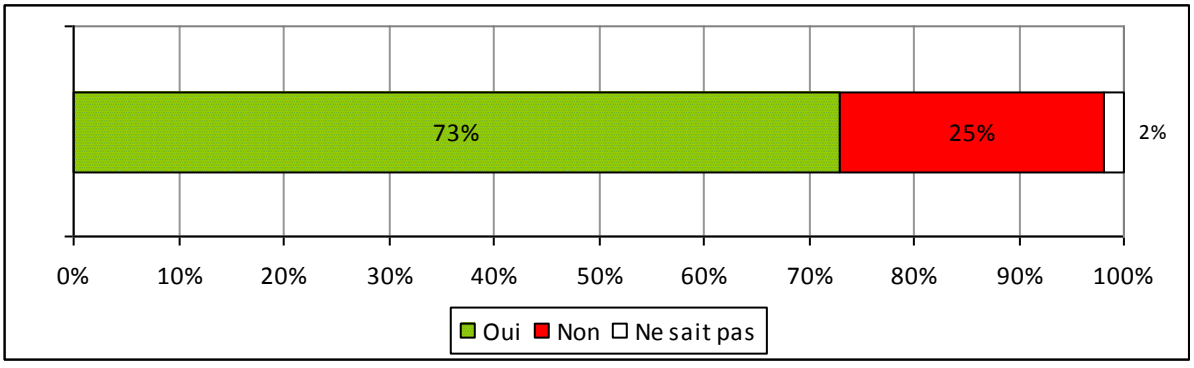

Figure 74 – Menaces sur la vie privée

Il n'y a pas forcément un rapport entre le sentiment d'insécurité vis-à-vis d'Internet et le risque concernant leurs données personnelles. Une explication possible est que ces données ne sont plus uniquement sur l'ordinateur personnel.

L'évolution ressentie de l'exposition aux risques de l'informatique personnelle est relativement stable par rapport à 2008.

Selon vous, quelle est l'évolution ressentie de l'exposition aux risques ?

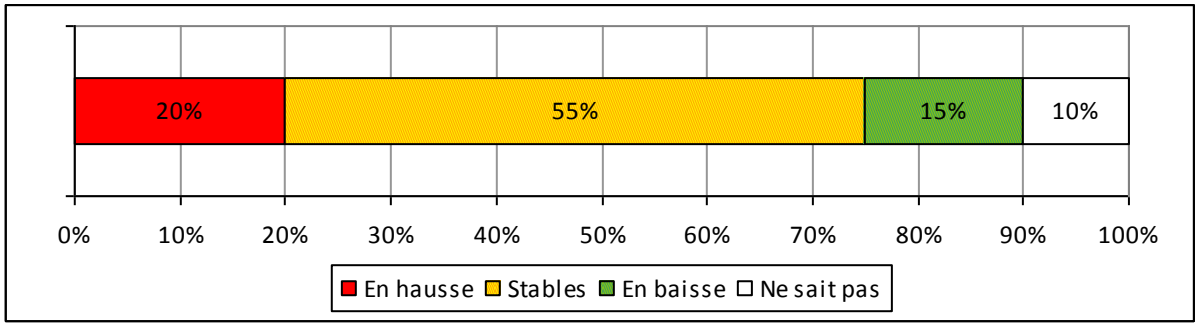

Figure 75 – Évolution des dangers

La perception des menaces liées aux escroqueries à la carte bancaire (phishing) est relativement stable. La perception de la menace liée au spam augmente très légèrement.

Selon vous, en l'absence de protection adaptée de votre informatique personnelle, le spam et le phishing représentent-t-ils un risque… ?

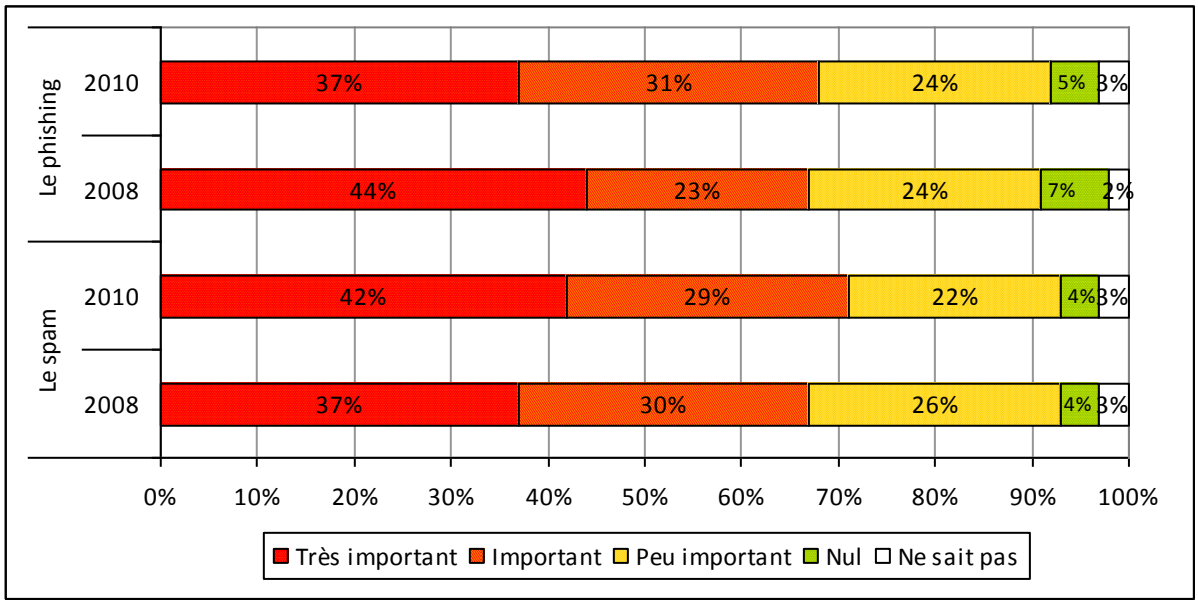

Figure 76 – Évolution de la perception des menaces liées aux spams et au phishing

La perception du risque d'Intrusion est légèrement en baisse. Malheureusement, les intrusions ne sont généralement pas détectées ce qui peut expliquer cette confiance. On observe les mêmes évolutions vis-à-vis des virus, et des logiciels espions.

Selon vous, en l'absence de protection adaptée de votre informatique personnelle, les intrusions, les virus et les logiciels espions représentent-t-ils un risque… ?

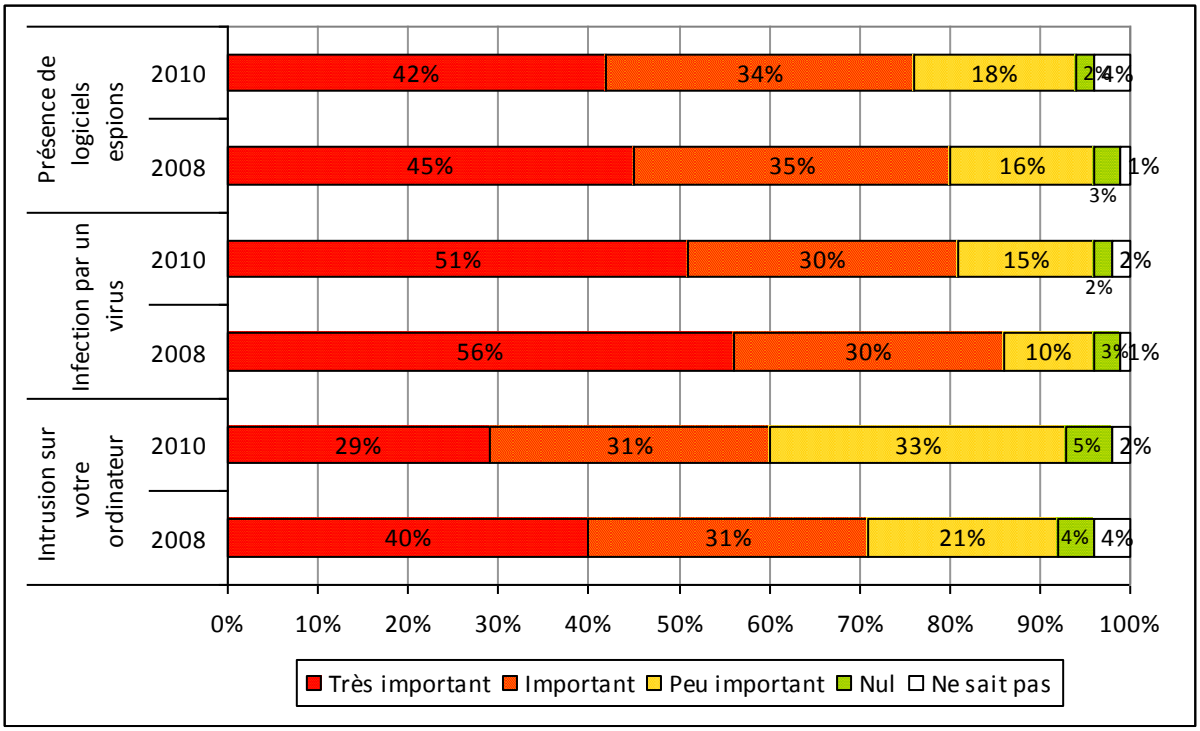

Figure 77 – Évolution de la perception des menaces liées aux intrusions, aux virus et aux logiciels espions

Il n'y a pas d'évolution importante du ressenti du risque de vol d'identité, malgré l'explosion de l'usage des réseaux sociaux.

Selon vous, en l'absence de protection adaptée de votre informatique personnelle, le vol d'identité représente-t-il un risque… ?

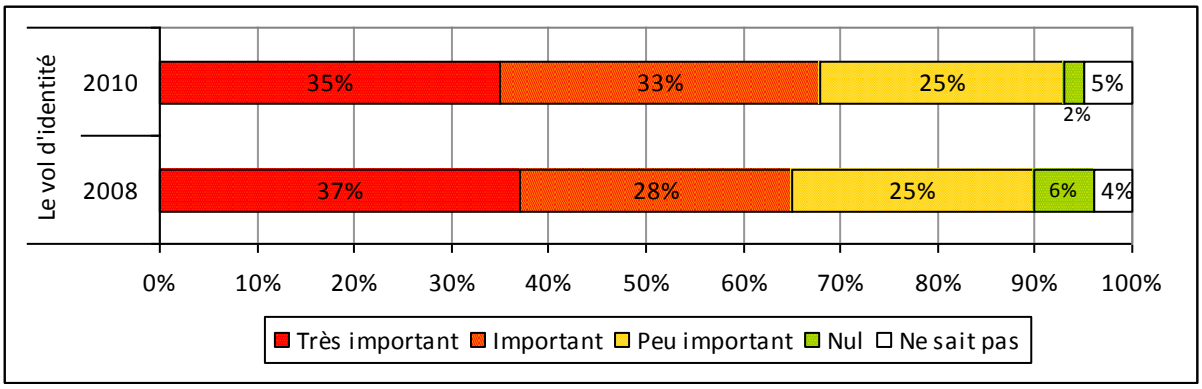

Figure 78 – Évolution de la perception des menaces liées au vol d'identité

La perception du risque de panne électrique n'évolue pas, malgré l'augmentation de l'usage des portables. On note peu de différence entre grandes villes et zones rurales.

La perception de la menace de piratage de l'accès wifi n'évolue pas depuis le dernier rapport. En revanche, une nouvelle question portant sur le risque de connexion à un faux accès wifi montre le manque de sensibilisation des Internautes à cette menace. Il s'agit du risque que son PC se connecte à un faux hot-spot ou à un accès pirate se faisant passer pour un accès déjà paramétré dans le PC. Une fois connecté, le propriétaire du faux accès wifi est en mesure d'écouter le trafic échangé entre le PC et les sites web visités, y compris ceux qui sont sécurisés par certificats.

Selon vous, en l'absence de protection adaptée de votre informatique personnelle, le wifi représente-t-il un risque… ?

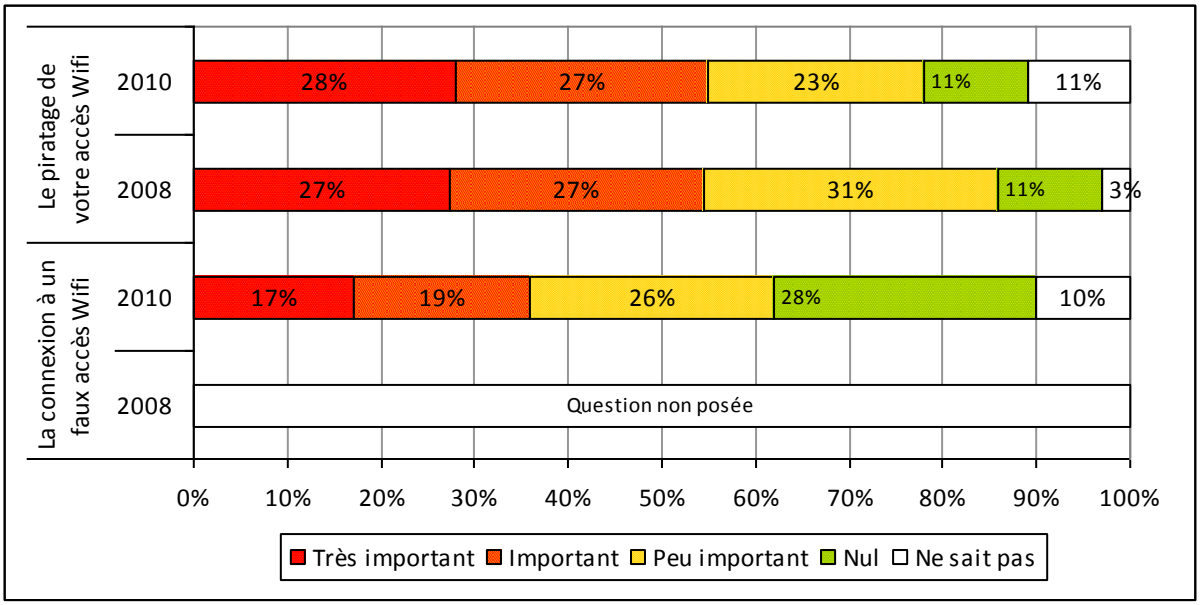

Figure 79 – Perception des menaces liées au wifi

Les Internautes diminuent très légèrement l'usage des protections telles les firewalls, anti-virus et d'une façon encore plus marquée en ce qui concerne les anti-spam.

Selon vous, ces situations peuvent-elles être vues comme facteurs aggravants quant aux menaces d'Internet ?

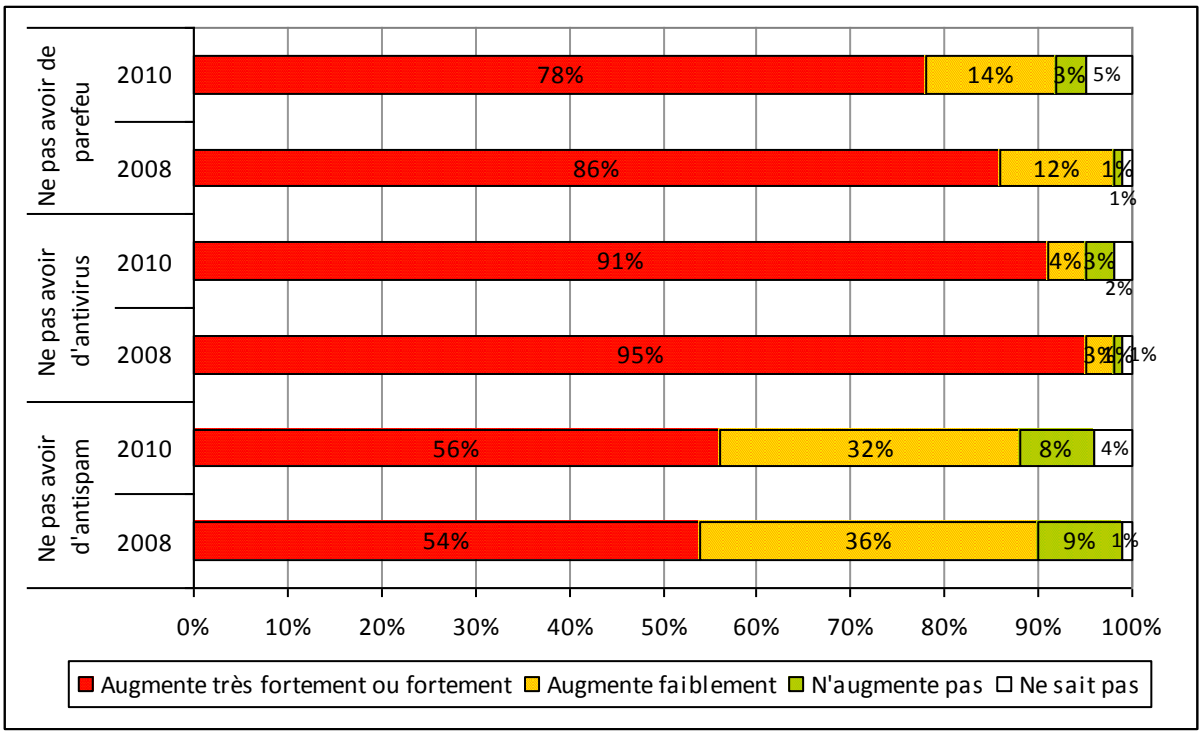

Figure 80 – Perception des facteurs aggravant les risques

Nous constatons une augmentation assez faible de la prise de conscience du danger de divulguer ses coordonnées sur Internet (75% en moyenne en 2008 à 81% en 2010). Ceci malgré l'arrivée des sites de réseaux sociaux et les incitations aux échanges de ce type de données qu'ils génèrent.

Partie III – Les usages de l'internaute

Bien qu'établi de manière quasi permanente, l'accès à Internet n'est pas la seule activité recherchée par les internautes, avec une bonne stabilité par rapport à l'enquête de 2008 :

- 96% stockent et manipulent des photos ou des vidéos,
- 90% traitent des documents personnels (courriers, comptabilité, etc.),
- seuls 42% traitent des documents professionnels (ce chiffre est en baisse par rapport aux 49% de l'enquête 2008).

En ce qui concerne le paiement d'achats en ligne, les blocages semblent fortement diminuer, ainsi 90% des internautes déclarent accepter de le faire (sous conditions pour 68% et même sans condition pour 22% d'entre eux).

Parmi les conditions qui facilitent cette acceptation conditionnelle, il apparaît que le chiffrement de la liaison vers le vendeur (https) est de loin un élément facilitateur (99% y font confiance), ensuite l'on trouve la notoriété de l'enseigne accédée (72% de confiance) ou l'utilisation d'une e-card (68%).

Travail à la maison ?

L'enquête confirme bien que l'ordinateur familial est utilisé uniquement pour un usage privé par 70% des personnes, 23% faisant un usage mixte et 2% un usage strictement professionnel. Les jeunes (15-24 ans) étant deux fois plus nombreux (46%) à déclarer panacher un usage privé et « professionnel ».

Utilisez-vous votre ordinateur familial pour un usage personnel et/ou professionnel ?

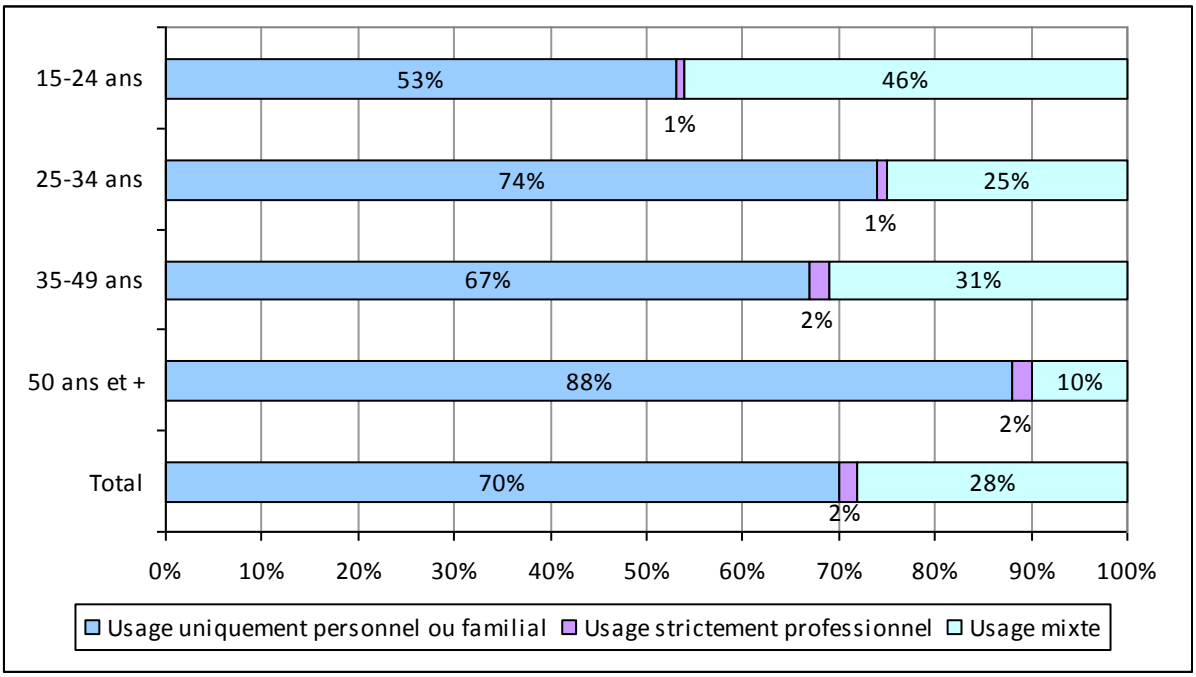

Figure 81 – Types d'usage de l'ordinateur familial

Les Internautes évoluent peu dans leur comportement vis-à-vis de la connexion à distance au réseau de leur entreprise. Utiliser l'ordinateur familial pour réaliser des travaux professionnels apparaît comme une solution de secours.

A quelle fréquence utilisez-vous Internet pour vos connecter à distance au réseau de votre entreprise

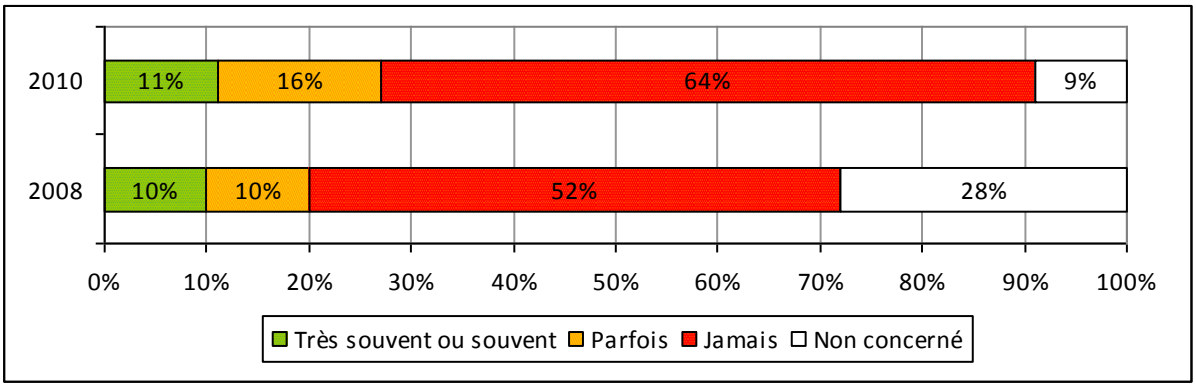

Figure 82 – Connexion à distance aux réseaux d'entreprises

Internet pour quoi faire ?

Le recours à Internet permet principalement aux internautes de surfer et d'envoyer des mails. Les jeunes générations font un usage très fréquent des messageries instantanées. L'utilisation de la VoIP et de la visioconférence restent rare (16% des internautes l'utilisent régulièrement).

Le jeu multi-joueurs en ligne n'a pas vraiment trouvé son public (14% des internautes jouent régulièrement). Les démarches administratives (46%) et bancaires (52%) commencent à entrer dans les mœurs du fait de leur côté pratique et du gain de temps que cela permet. Les internautes sont principalement des consommateurs d'information et n'en injectent que peu dans les réseaux. Les réseaux sociaux, par leur côté virtuel, ont vraiment trouvé un public (39%), mais les sites de rencontre sont peu fréquentés (4% des internautes l'avouent).

Une augmentation certaine du téléchargement (musique, film, logiciel) semble apparaître, d'autant que les chiffres ne reflètent pas forcement la réalité du fait de la sensibilité des questions (téléchargement légaux/illégaux).

A quelle fréquence utilisez-vous Internet pour télécharger des films ou des vidéos ?

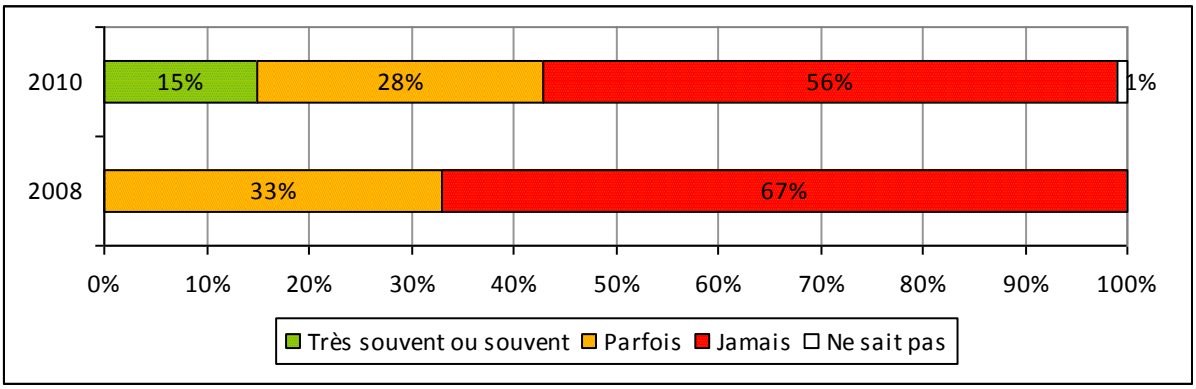

Figure 83 – Téléchargements de films et vidéos

Quelles données ?

Les internautes stockent sur leurs machines tout type de données personnelles (courriers, comptabilité, images, vidéo, musique, etc.).

La moitié des personnes interrogées déclarent ne pas conserver de données professionnelles sur leur ordinateur personnel, après traitement. Cela tendrait à prouver qu'ils ont conscience des risques de responsabilité liés à la détention de données à caractère professionnel dans la sphère privée.

Utilisez-vous votre ordinateur familial pour stocker et manipuler des documents professionnels ou de travail ?

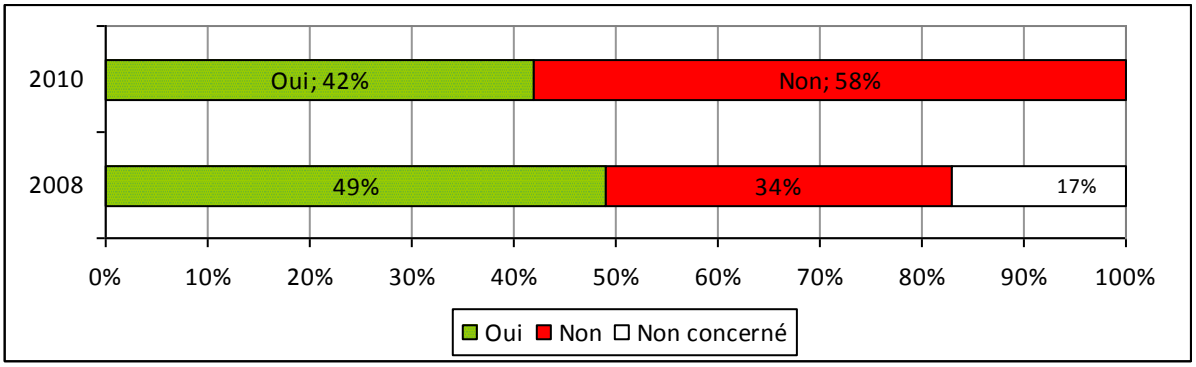

Figure 84 – Usage de l'ordinateur familial pour stocker ou manipuler des documents de travail

On pourrait aussi en conclure que l'usage de l'ordinateur personnel pour des actions professionnelles n'est qu'occasionnel.

Qui fait quoi… ?

Même si les catégories socioprofessionnelles supérieures et les inactifs ont recours à l'ordinateur d'une façon plus systématique, on notera cependant que les écarts entre les différentes populations ne sont plus significatifs.

Communiquez-vous via des réseaux sociaux comme Facebook, MySpace, etc. ?

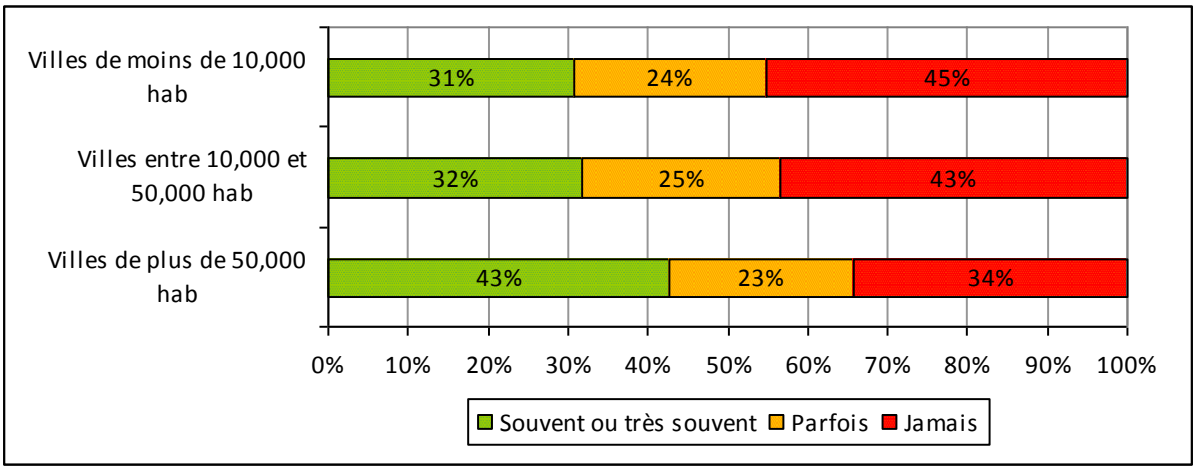

Figure 85 – Usage des réseaux sociaux

L'utilisation des outils technologiques croît en fonction de l'importance de population, ce qui s'explique par le fait que les zones à forte concentration d'habitants bénéficient historiquement d'une meilleure infrastructure de communication. Cependant, les zones rurales semblent rattraper les autres environnements, ce qui laisse supposer que le retard se comble.

De manière logique, ce sont les catégories socioprofessionnelles les plus élevées qui manipulent le plus souvent des données professionnelles dans leur sphère privée, avec les outils informatiques domestiques.

Paiement en ligne : « oui » mais…

Les internautes n'ont pas encore une parfaite confiance dans les solutions de paiement en ligne et demandent des garanties. Ils sont encore réticents à acheter et à vendre sur Internet. Dans le cas du paiement en ligne, ce n'est pas le montant, ni la réputation du site qui motive ou non un achat, mais les internautes réclament de plus en plus un environnement sécurisant adapté (chiffrement, paiement sécurisé, certificats, etc.).

On notera cependant que même s'il y a toujours des réticences aux transactions en ligne, l'acceptation s'est considérablement améliorée depuis l'enquête de 2008 et que les internautes ont de plus en plus d'exigences de sécurité.

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

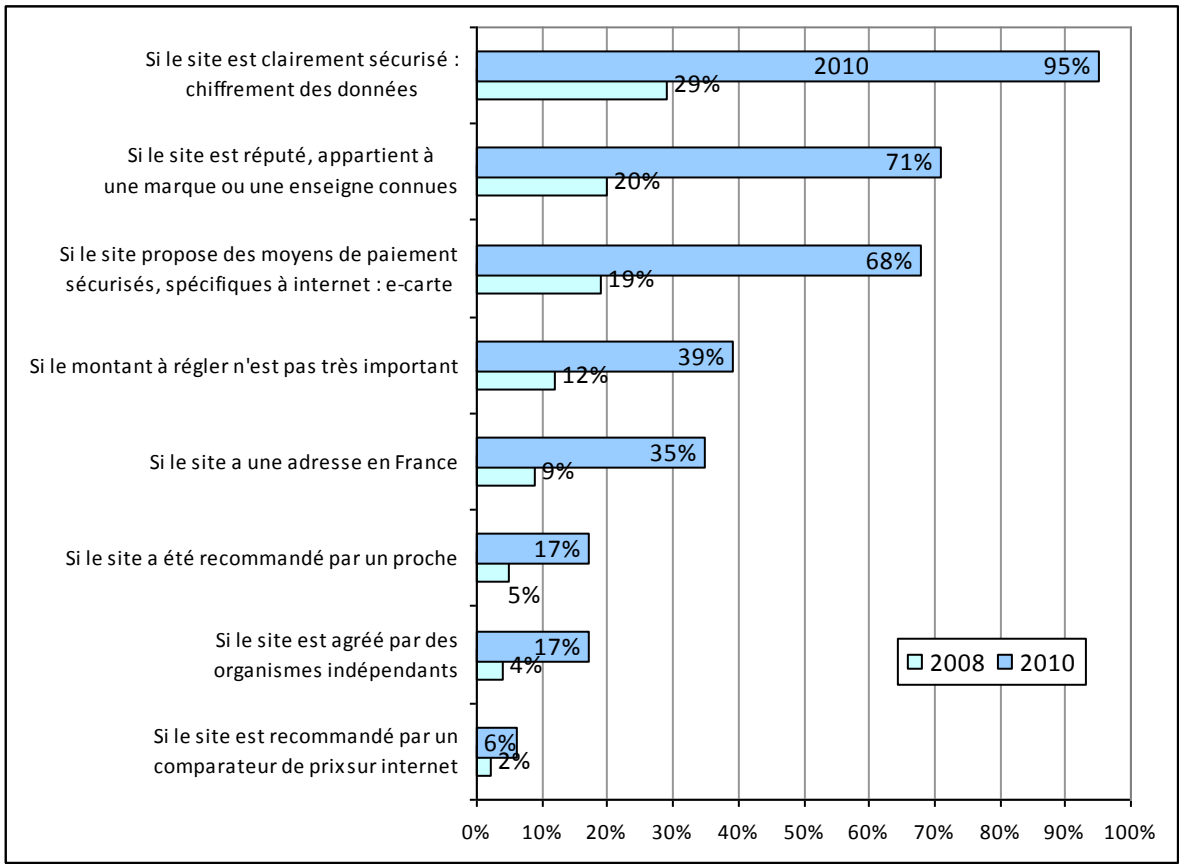

Figure 86 – Critères de confiance dans la sécurité pour les paiements en ligne

Données personnelles

D'après l'enquête, les internautes semblent confier assez facilement les données personnelles les concernant aux formulaires de demande de renseignement des sites visités. Ils ne perçoivent peut-être pas clairement les dangers qui consistent à alimenter des fichiers de données personnelles et font confiance, tant que leurs valeurs financières ne sont pas sollicitées.

Remplissez-vous facilement un formulaire sur Internet contenant des informations personnelles ?

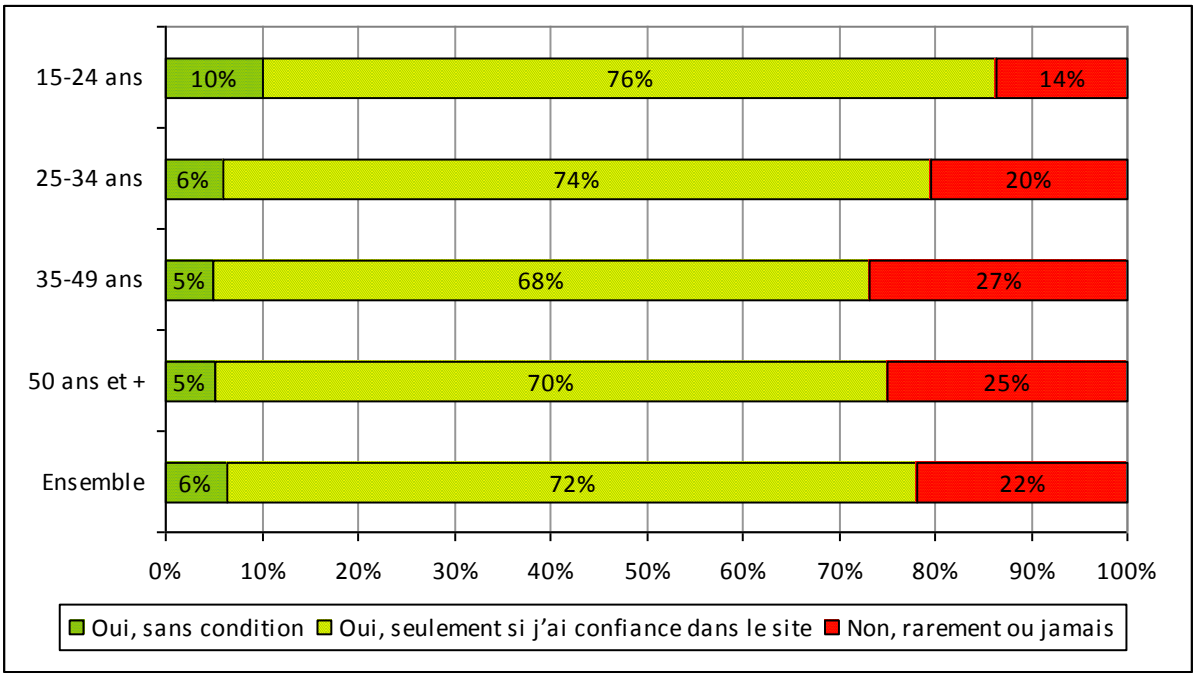

Figure 87 - Critères de sécurité pour les paiements en ligne

Partie IV – Moyens et comportements de sécurité

Protections

Du fait de leur implantation dans les foyers, les ordinateurs sont peu protégés par des mots de passe ou des contrôles biométriques. En revanche, les mises à jour de sécurité semblent être déployées régulièrement par plus de la moitié des internautes, qu'il s'agisse de déploiement automatique ou manuel.

Les mesures de protection professionnelles sont très peu utilisées sur l'ordinateur familial : 80% n'utilisent pas de chiffrement, 88% n'ont pas d'antivol physique et 65% n'ont pas de protection de leur alimentation électrique.

Les utilisateurs ont plutôt un sentiment de sécurité dans leur usage de l'informatique domestique.

Mise à jour

Nous constatons une baisse de la mise à jour automatisée des systèmes ou logiciels. Est-ce dû à une volonté de mieux contrôler ou à un réel problème de comportement ? Dans tous les cas, la perception du risque est très importante (64%). La fréquence de mise à jour manuelle reste insuffisante pour un quart des sondés (25% moins souvent qu'une fois par mois).

Votre ordinateur est-il régulièrement mis à jour automatiquement (OS, antivirus, etc.) ?

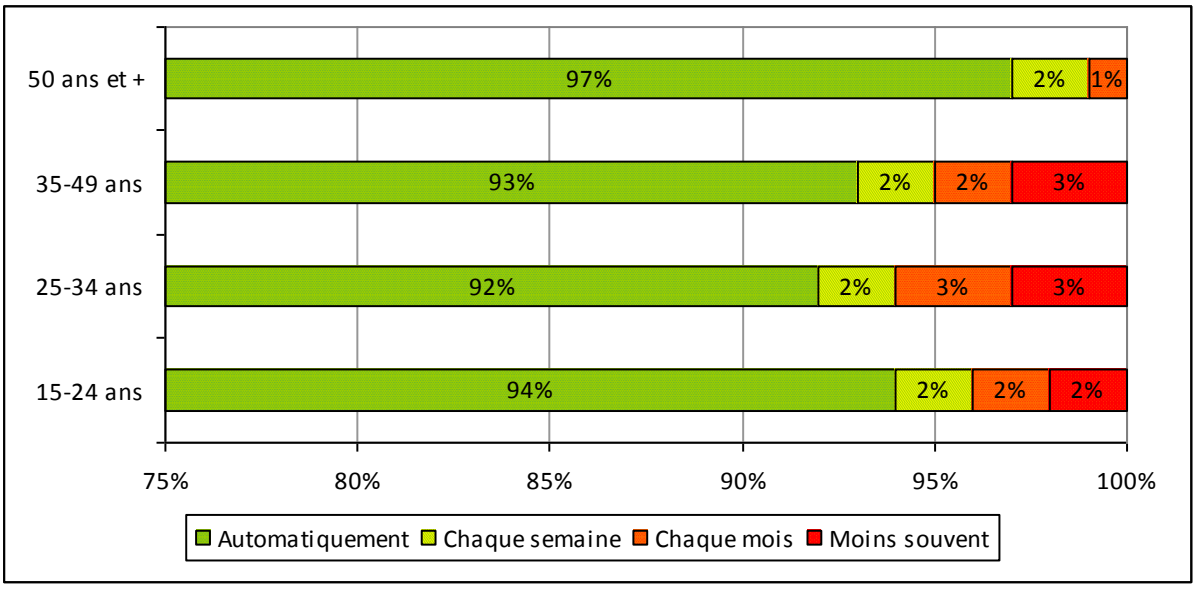

Figure 88 - Politique de mise à jour

Dispositif de contrôle parental

Les dispositifs de contrôle parental concernent sans surprise les internautes de 35 à 49 ans (40%), mais on note une baisse globale (de 40% à 36%) de leur utilisation.

Protection électrique

Les dispositifs de protection électrique sont légèrement plus utilisés (24% en 2008 à 27% en 2010). Ces dispositifs concernent plutôt les internautes âgés (35% des +50 ans) et moins les jeunes internautes (14% de 15-24).

On note une disparité par tranche d'âge (35% des +50 ans, 14% de 15-24) et par région.

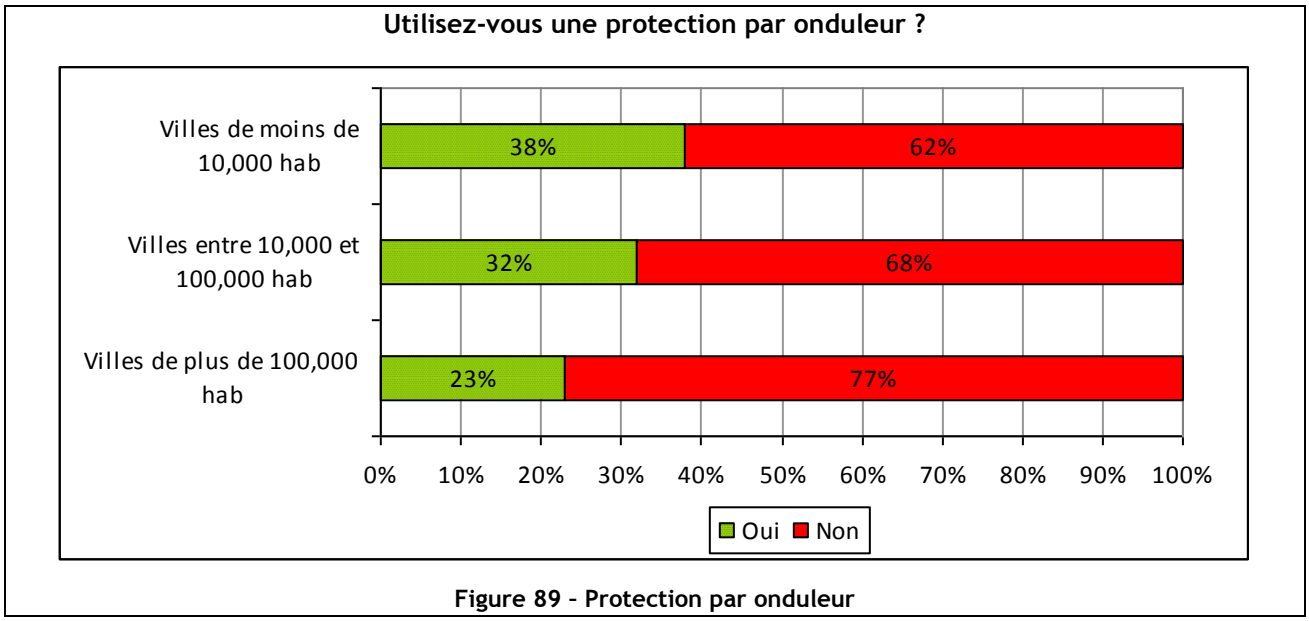

Figure 89 – Protection par onduleur

Biométrie

L'usage de la biométrie est en augmentation (de 4% en 2008 à 11% en 2010). Cette évolution pourrait être due à l'équipement par défaut des PC portables. Les internautes ayant une perception globale des risques encourus sont plutôt plus équipés (18%), alors que les internautes âgés le sont moins (8%).

Chiffrement

Les outils de chiffrement sont toujours aussi peu utilisés (8%).

Mot de passe

On note une diminution importante de l'usage des mots de passe d'ouverture de session. Cette évolution est probablement liée à l'augmentation du nombre d'ordinateur par foyer (ceux ci étant moins partagés entre plusieurs personnes).

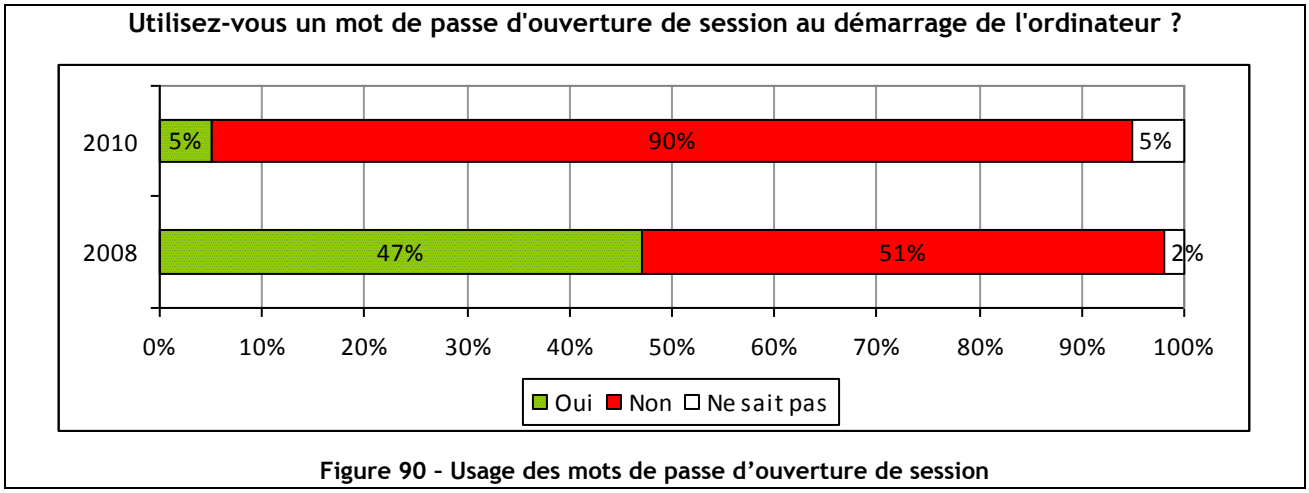

Figure 90 – Usage des mots de passe d'ouverture de session

Toutefois, ce point peut paraître inquiétant dans la mesure où l'ordinateur personnel est de plus en plus portable et utilisé en dehors du domicile.

Anti-virus

Une légère baisse (95% en 2008 à 91% en 2010) de l'usage des anti-virus est constatée. L'installation d'anti-virus par défaut est peut-être une explication de ce fort taux d'usage.

Firewall, anti spam et anti spyware

Ces outils subissent une baisse identique au résultat de la question portant sur l'anti-virus. On observe une nette hiérarchie dans l'usage de ces outils.

Utilisez-vous les moyens de protection suivants pour garantir la sécurité de votre ordinateur familial ?

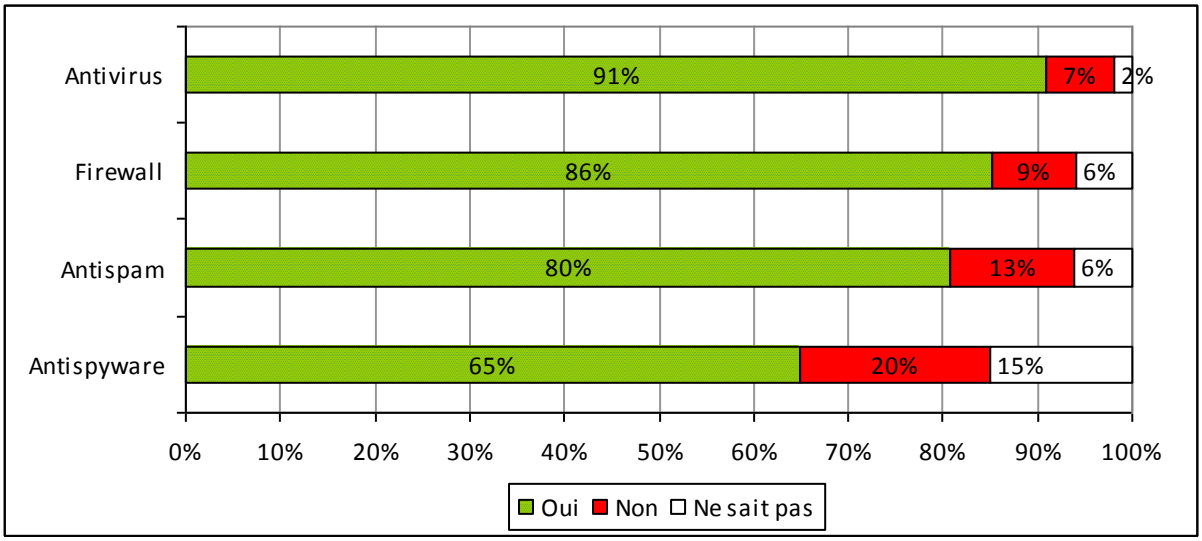

Figure 91 – Usage protections poste de travail

Sauvegarde

La sauvegarde est une pratique en forte augmentation.

Sauvegarder-vous régulièrement le contenu de votre ordinateur ?

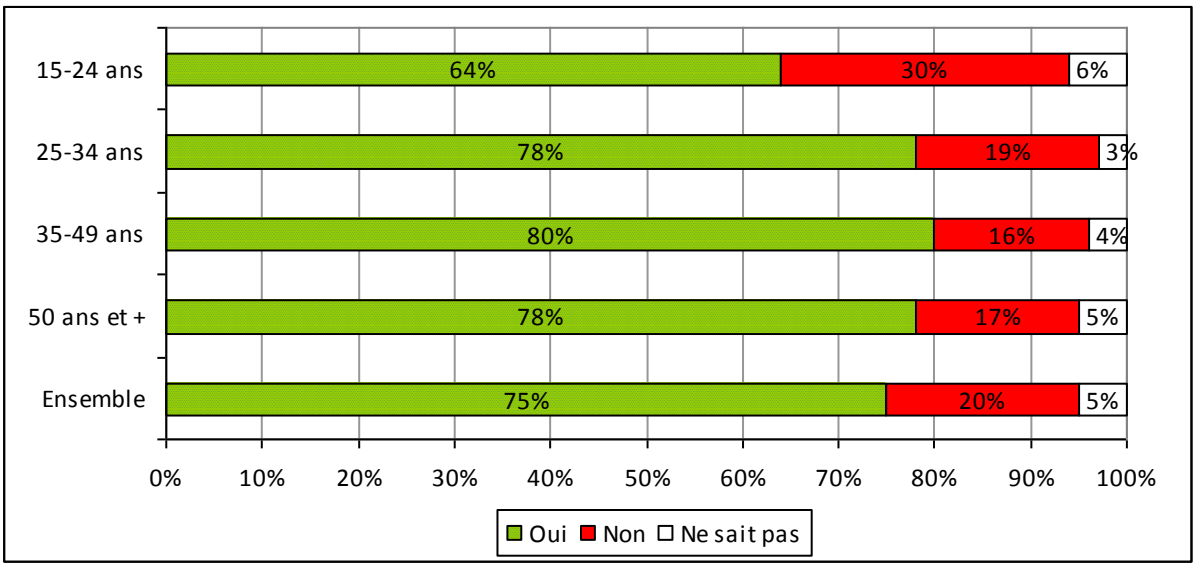

Figure 92 – Politique de sauvegarde

La sensibilisation des utilisateurs, l'offre de logiciel de sauvegarde, la baisse des coûts des supports de sauvegarde sont des explications à cette augmentation.

Wifi

La sécurité du wifi ne montre pas de changement depuis 2008. On note une différence notable entre les +50 ans (66%) et les 25-34 (86%).

Sentiment sécurité

Le sentiment de sécurité est en légère baisse, sans évolution majeure ; cette évolution est cohérente avec l'évolution de la perception des risques et des menaces par les internautes. La grande majorité (91%) se sent plutôt ou totalement en sécurité.

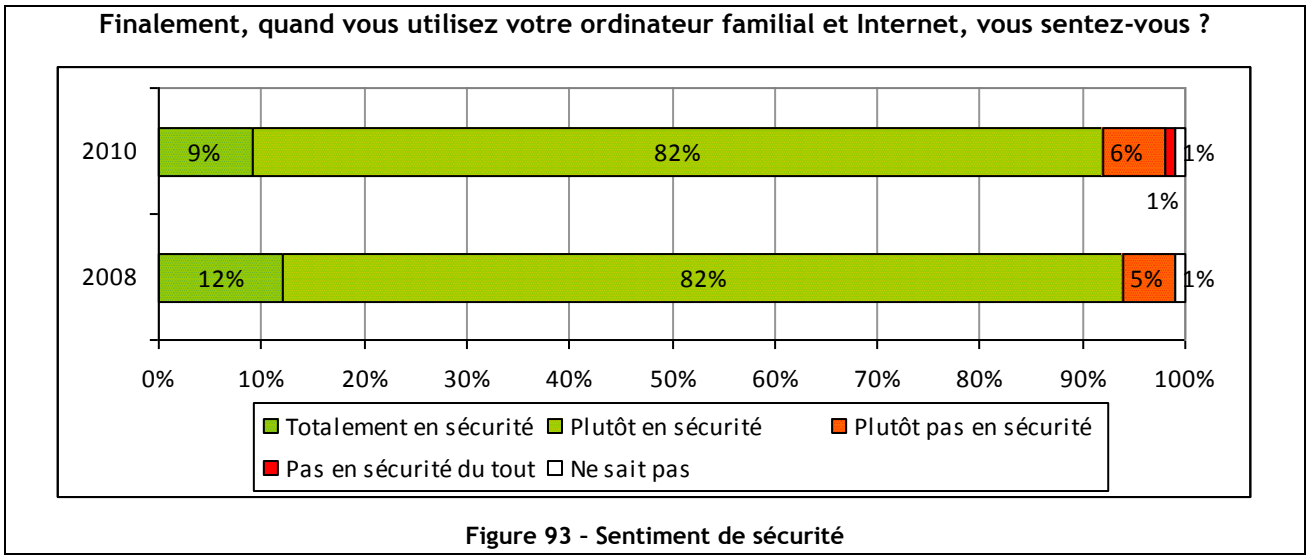

Figure 93 – Sentiment de sécurité

Le sentiment de sécurité est accru chez les jeunes : ils sont 17% à se sentir totalement en sécurité contre une moyenne de 9% sur le reste de la population. On pourra expliquer ce chiffre par un sentiment de meilleure maîtrise de l'outil et une conscience plus faible des risques.

Annexe

- Glossaire

Glossaire[2]

Terme	Définition
AFAI	Association Française de l'Audit et du Conseil Informatiques. http://www.afai.asso.fr/.
ANSSI	Agence nationale de la sécurité des systèmes d'information. http://www.ssi.gouv.fr/index.html.
ARCEP	Autorité de Régulation des Communications Électroniques et des Postes. http://www.arcep.fr/.
ASIP	Agence des Systèmes d'Information Partagés de santé. http://www.asipsante.fr/.
CIGREF	Club Informatique des GRandes Entreprises Françaises. http://www.cigref.fr/.
CLUSIF	CLub de la Sécurité de l'Information Français. http://www.clusif.asso.fr/.
CNIL	Commission nationale de l'informatique et des libertés. http://www.cnil.fr/.
CPS	Carte Professionnel de Santé
CSP	Catégorie socioprofessionnelle. Caractérisation de la population active française en classes et professions, établie par l'INSEE. http://www.insee.fr/fr/nom_def_met/nomenclatures/prof_cat_soc/pages/pcs.htm.
DHOS	Direction de l'hospitalisation et de l'organisation des soins. http://www.travail-solidarite.gouv.fr/le-ministere,149/presentation-et-organigramme,294/le-ministre-du-travail-de-la,747/direction-de-l-hospitalisation-et,5620.html.
DMP	Dossier Médical Personnel
DSI	Directeur des Systèmes d'Information.
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité, développée par l'ANSSI. http://www.ssi.gouv.fr/site_article45.html.
GIP-CPS	Groupement d'Intérêt Public - Carte de Professionnel de Santé. http://www.gip-cps.fr/.
ISO 27002	Norme internationale constituant un « guide de bonnes pratiques » en matière de sécurité de l'information (anciennement ISO 17799).
MEHARI	Méthode d'analyse des risques, développée par le CLUSIF. http://www.clusif.asso.fr/fr/production/mehari/.
PACS	Picture Archiving and Communication Systems ou Système d'archivage électronique d'archives radiologiques.

[2] En complément de ces quelques définitions, le lecteur est invité à se référer au « **Glossaire des menaces** », en ligne sur le site du CLUSIF sur http://www.clusif.asso.fr/fr/production/glossaire/.

Terme	Définition
PCA	Plan de Continuité d'Activité. On parle parfois de PSI, Plan de Secours Informatique. Outre que cette appellation ne prend pas en compte les métiers de l'entreprise, nous n'utilisons pas cet acronyme pour éviter toute confusion avec la Politique de Sécurité de l'Information. Les anglo-saxons utilisent l'acronyme BCP pour *Business Continuity Plan*.
PRA	Plan de Reprise d'Activité.
PSI	Politique de Sécurité de l'Information. Ensemble des critères permettant de fournir des services de sécurité (ISO 7498-2)
PSSI	Guide d'élaboration de politiques de sécurité des systèmes d'information de la DCSSI. http://www.ssi.gouv.fr/site_article46.html.
RSSI	Responsable Sécurité des Systèmes d'Information.
SIM	Security Information Management. Outil de collecte, de reporting et d'analyse des différentes sources d'information liée aux événements de sécurité du Système d'Information.
SMSI	Système de Management de la Sécurité de l'Information. En anglais, ISMS (Information Security Management System).
SSI	Sécurité des Systèmes d'Information.
SSO	Single Sign-On. Système permettant à un utilisateur du Système d'Information de ne s'authentifier qu'une seule et unique fois pour accéder à différentes applications.
ToIP	Téléphonie sur IP.
VoIP	Voix sur IP (acronyme de Voice over Internet Protocol).

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.asso.fr

Téléchargez les productions du CLUSIF sur
www.clusif.asso.fr