Menaces informatiques et pratiques de sécurité en France

Edition 2008

- LES ENTREPRISES DE PLUS DE 200 SALARIÉS
- LES COLLECTIVITÉS LOCALES
- LES INTERNAUTES

Club de la Sécurité de l'Information Français

Remerciements

Le CLUSIF remercie les personnes qui ont participé à cette étude :

NOM	ENTITE
M. BELLEFIN Laurent	SOLUCOM GROUP
M. CHIOFALO Thierry	SDV
M. CONSTANT Paul	CONSULTANT
Mme DILIGENT Perrine	BYWARD LIMITED
M. FAUVEL Marc-Noël	MAIRIE DE RUEIL MALMAISON
M. FREYSSINET Eric	GENDARMERIE NATIONALE
M. GOJAT Pierre	ORANGE BUSINESS SERVICES
M. GRASSART Paul	AGERIS CONSULTING
M. GUERIN Olivier	CLUSIF
M. HAMON Bruno	GROUPE LEXSI
M. JOUAS Jean-Philippe	CLUSIF
M. LOINTIER Pascal	AIG EUROPE
M. MOURER Lionel	BULL
M. PAGET François	MCAFEE
M. RENAUDINEAU Patrice	NANTES METROPOLE
M. ROSE Philippe	BEST PRACTICES SYSTEMES D'INFORMATION
M. ROULE Jean-Louis	CLUSIF

Le CLUSIF remercie aussi vivement les représentants des entreprises et collectivités 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.

Editorial

A travers cette édition 2008 de son enquête sur les menaces informatiques et les pratiques de sécurité, le CLUSIF réalise de nouveau un bilan approfondi de la sécurité de l'information en France. Cette enquête se veut être une référence de par la taille et la représentativité des échantillons d'entreprises et de collectivités locales interrogés. Elle se veut par ailleurs très complète puisqu'elle passe en revue un large panel de thèmes relatifs à la sécurité des systèmes d'information.

Et cette année, elle élargit son périmètre, avec un large volet consacré aux pratiques des particuliers utilisateurs d'Internet à domicile. L'usage de l'informatique et d'Internet à la maison est maintenant largement banalisé. Le comportement des utilisateurs de l'informatique en entreprise est de plus en plus souvent influencé par la pratique privée, et les frontières entre les deux mondes deviennent plus floues. Notre enquête le montre : un tiers des internautes utilisent l'ordinateur familial aussi à des fins professionnelles, ce qui pose quelques questions sur la protection des données de l'entreprise… Et si les internautes sont globalement prudents dès qu'il s'agit d'achat sur Internet, et semblent conscients de l'utilité des outils de protection (antivirus, pare feu personnels, etc.), ils ne se sentent que pour une minorité d'entre eux véritablement en « insécurité » sur Internet.

Coté entreprise, cette édition 2008 fait ressortir un inquiétant sentiment de stagnation. Entre 2004 et 2006 des progrès notables avaient été fait, en particulier dans le domaine de la formalisation des politiques et des chartes de sécurité. Mais depuis, il semble bien que la mise en application concrète de ces politiques soit restée un vœu pieu. 40 % des entreprises ne disposent toujours pas de plan de continuité d'activité pour traiter les crises majeures, contre 42 % en 2006. Et 30 % d'entre elle disent ne pas être en conformité avec la Loi Informatique et Liberté…

Pour autant, la menace ne faiblit pas et notre enquête montre de nouveau que les malveillances et les incidents de sécurité sont bien réels, avec une présence toujours active des attaques virales, des vols de matériel, et un accroissement des problèmes de divulgation d'information et des attaques logiques ciblées. Et l'actualité récente n'a cessé de démontrer les graves impacts des déficiences en matière de sécurité (fraude bancaire, divulgation de données personnelles, etc.)

Sortir des politiques de sécurité « alibi », que l'on rédige pour se donner bonne conscience, pour aller vers des pratiques concrètes, réellement ancrées dans les processus de gestion de l'information, voilà donc l'enjeu pour les années à venir…

Laurent BELLEFIN
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 2008 a été réalisée au cours des mois de janvier, février et mars 2008, 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 : 354 entreprises de cette catégorie ont répondu à cette enquête,
- les collectivités, c'est-à-dire les mairies des communes de plus de 30 000 habitants, les communautés de communes et les communautés d'agglomérations, les conseils généraux et les conseils régionaux : 194 collectivités ont accepté de répondre à cette enquête,
- les particuliers internautes : 1139 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 qui décrit 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 de 5 à 15 sont les suivants :

- 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 des ressources humaines (charte, sensibilisation) ;
- 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).

Seul le thème 9, qui porte sur la sécurité physique, a été laissé de coté.

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

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

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.

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 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

Le CLUSIF souhaitait, pour l'édition 2008 de cette enquête, interroger exactement le même échantillon d'entreprises que celui interrogé en 2006, 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 :

- BTP
- Commerce
- Industrie
- Services, banques, assurances
- Transport
- Télécoms

354 entreprises ont répondu à la sollicitation du CLUSIF, avec un taux d'acceptation d'environ 6 % (en baisse par rapport à 2006) : sur 100 entreprises contactées, seulement 6 ont accepté de répondre à nos questions, ce qui a impliqué d'appeler environ 6 000 entreprises ! 307 entreprises ont répondu par téléphone (entretien de 32 minutes en moyenne), les autres ont préféré répondre aux questions en direct par Internet sur un espace dédié et sécurisé.

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.

	De 200 à 499 salariés	**De 500 à 999 salariés**	**+ de 1000 salariés**	**Total**	**Total en %**		**Données INSEE**
BTP	2		3	5	1 %	→	**6 %**
COMMERCE	27	4	12	43	12 %	→	**17 %**
INDUSTRIE	96	32	35	163	46 %	→	**43 %**
SERVICES	51	16	48	115	32 %	→	**25 %**
TRANSPORTS—TELECOMS	9	9	8	26	7 %	→	**9 %**
Total	185	61	106	352[1]	100 %		
Total en %	52 %	17 %	30 %				

Redressement → ↓ ↓ ↓

Données INSEE	**66 %**	**19 %**	**15 %**

Redressement ↑

Au sein de chaque entreprise, nous avons cherché à interroger en priorité le **Responsable de la Sécurité des Systèmes d'Information** – RSSI – (pour 21 % des entreprises interrogées mais 43 % dans les plus de 1000 salariés), ou à défaut, en particulier dans les plus petites entreprises de notre échantillon, le responsable informatique (pour 50 % des entreprises interrogées). Toutes tailles et secteurs confondus, les personnes sondées sont, à 66 %, des DSI[2], des Directeurs informatiques ou des RSSI.

[1] Le lecteur attentif notera que nous annonçons par ailleurs 354 répondants, ce qui est exact. Ce tableau, issu d'une compilation intermédiaire n'en recense toutefois que 352, ce qui n'impacte pas les ratios.
[2] Voir glossaire

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)

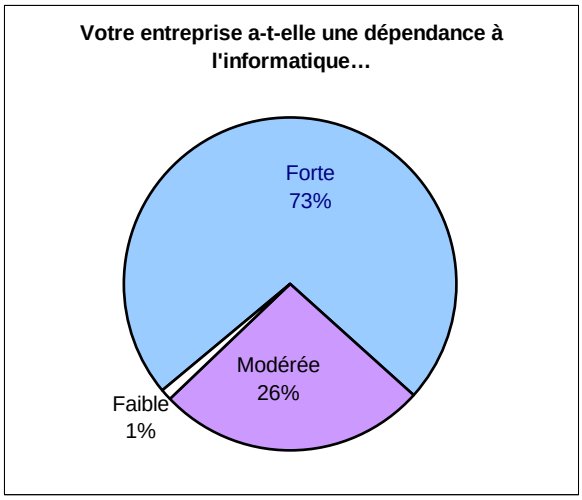

Figure 1 : dépendance des entreprises à l'informatique

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

Un budget informatique moyen à 1,9 million €

Lorsqu'on les interroge sur leur budget informatique, seulement 25 % des entreprises répondent. Pour celles qui « parlent », un tiers des entreprises interrogées ont un budget compris entre 1 et 2 millions d'euros. 10 % des budgets sont supérieurs à 5 millions d'euros pour un maximum de 100 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 dévolu à la sécurité de l'information.
Peu d'évolution entre les résultats des années précédentes et ceux que nous découvrons aujourd'hui. Sauf peut-être que les responsables sécurité ont encore un peu plus de difficultés à se positionner puisque 30 % d'entre eux avouent ne pas savoir quel poids leur budget représente dans le budget informatique. Un référentiel d'identification des coûts relevant de la sécurité du système d'information permettrait d'en dessiner les contours plus nettement. Lorsque ce budget est clairement identifié par rapport au budget informatique, on ne peut que constater une grande hétérogénéité.

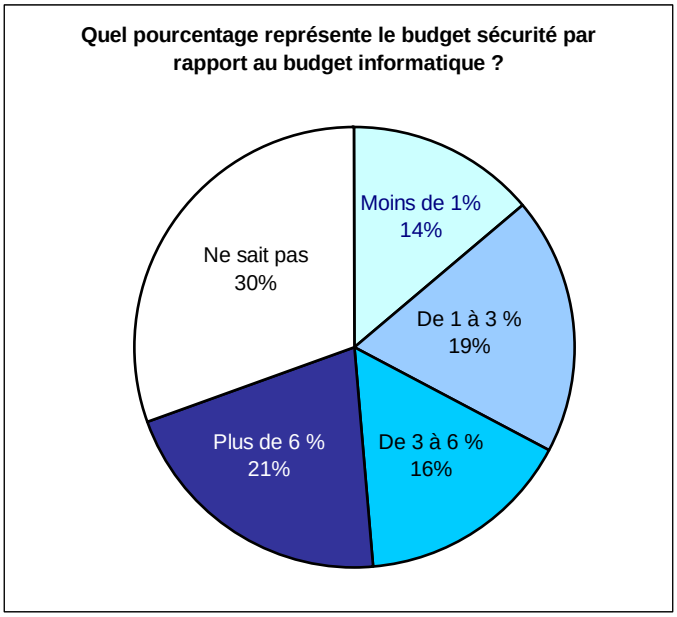

Figure 2 : part du budget informatique alloué à la sécurité dans les entreprises

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. Cet inquiétant sentiment de stagnation est heureusement relativisé par quelques augmentations : une entreprise sur deux du secteur des services, banques et assurances a augmenté son budget cette année, parfois de manière très importante (28 % des entreprises de ce secteur ont noté une augmentation de plus de 10 % de leur budget).

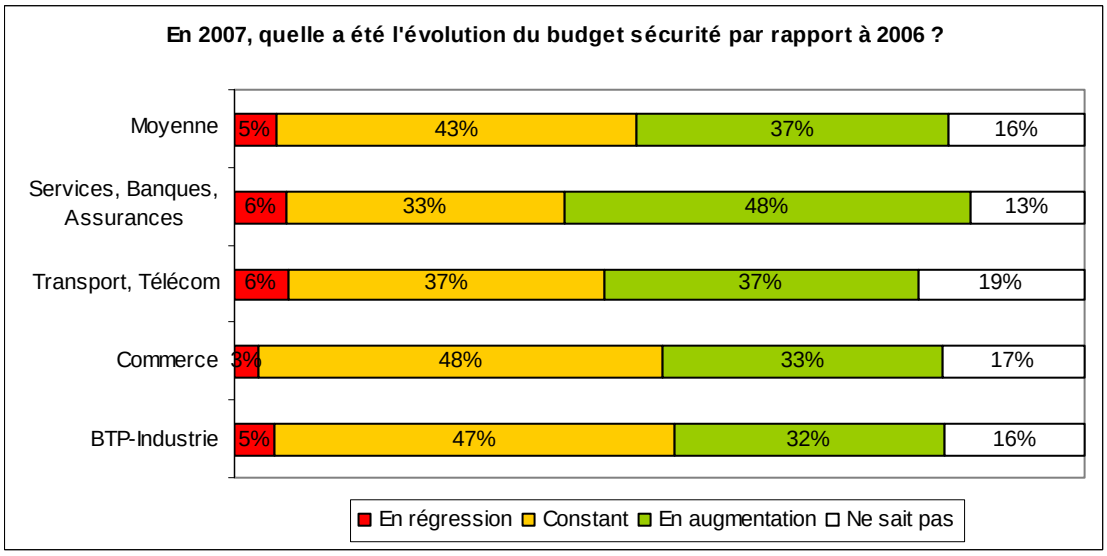

Figure 3 : évolution du budget sécurité selon les secteurs d'activités

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 (36 %) : les contraintes organisationnelles.
- 2ème raison citée (35 %) : le manque de budget.
- 3ème raison citée (27 %) : la réticence de la hiérarchie, des services ou des utilisateurs.
- 4ème raison citée (23 %) : le manque de personnel qualifié.
- 5ème raison citée (8 %) : la réticence de la Direction des Systèmes d'Information.

Les deux freins principaux sont les contraintes organisationnelles (qui ressortent comme un frein plus important qu'il y a deux ans) et le manque de moyens budgétaires dont nous n'avons pas fini de nous alarmer.

Au chapitre des bonnes nouvelles, l'utilisateur du système d'information ne semble pas systématiquement perçu comme une gêne par les RSSI, souhaitons qu'il soit même considéré comme un allié dans la réalisation de leurs objectifs. De même, la DSI semble être résolument un atout dans la manche du RSSI.

Le manque de personnel qualifié était le frein numéro 2 en 2006 et rétrograde aujourd'hui en 4ème position. Le détail des réponses montre un résultat moins satisfaisant qu'il n'y parait puisque 53 % des RSSI, soit plus d'un sur deux, dénoncent ce manque de personnel comme frein majeur (choix un ou choix deux des freins les plus importants). L'agitation frénétique du marché de l'emploi dans le secteur de la SSI et l'augmentation du nombre d'offres sont d'ailleurs d'autres témoins de cette insatisfaction récurrente.

Thème 5 : Politique de sécurité

Une stagnation dans la formalisation des politiques de sécurité de l'information…

La mise en œuvre d'une Politique de Sécurité de l'Information (PSI) est une étape importante dans la mise en place des règles de bonne gouvernance du SI en entreprise. 55 % des entreprises sont dotées d'une telle PSI ; toutes entreprises confondues, les chiffres n'ont que peu évolué par rapport à 2006 (moins 1 %). Toutefois, un recul assez net (moins 6 % sur 2006) est à noter pour les grandes entreprises, même si elles restent les plus avancées.

On peut y voir une meilleure compréhension du terme PSI : ce dernier ne faisant plus référence seulement à un document « simpliste », mais à un « cadre complet » (prise en compte des risques métiers, document « chapeau » et « d'applications », procédures complètes allant vers le SMSI[3]…). De fait, le travail des RSSI ainsi que des associations professionnelles est loin d'être terminé…

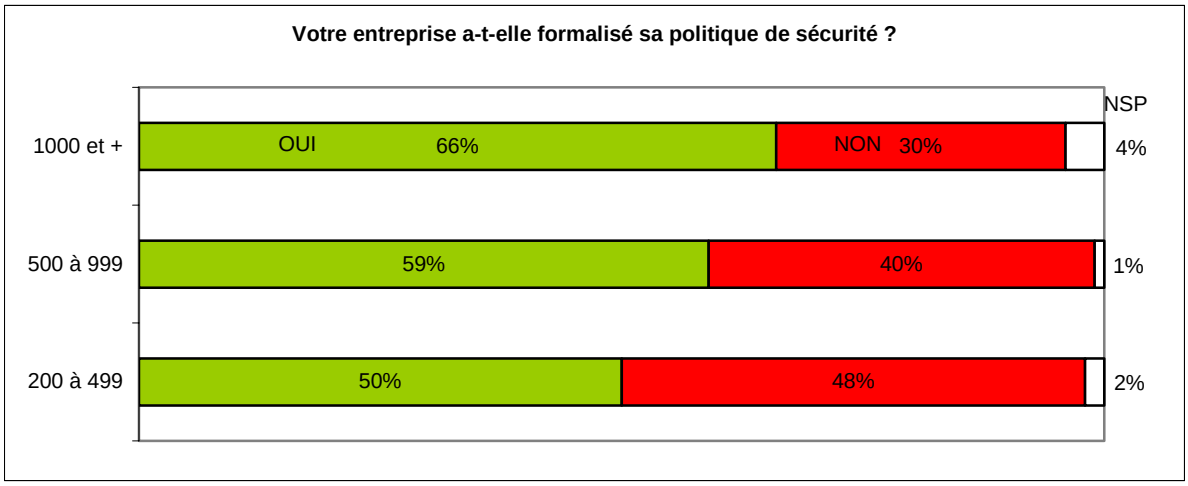

Figure 4 : existence d'une politique sécurité en fonction de la taille de l'entreprise

…mais une utilisation des normes du domaine en légère régression

Aujourd'hui, 47 % des entreprises s'appuient sur une « norme » pour formaliser leur PSI (- 1 % par rapport à 2006). Les normes ISO 2700x (ou ISO 17799) arrivent en tête, en particulier dans les grandes entreprises (32 % d'entre elles utilisent l'ISO) se positionnant clairement comme la référence en la matière ; avec toutefois – 11 % par rapport à 2006 !

[3] Voir glossaire

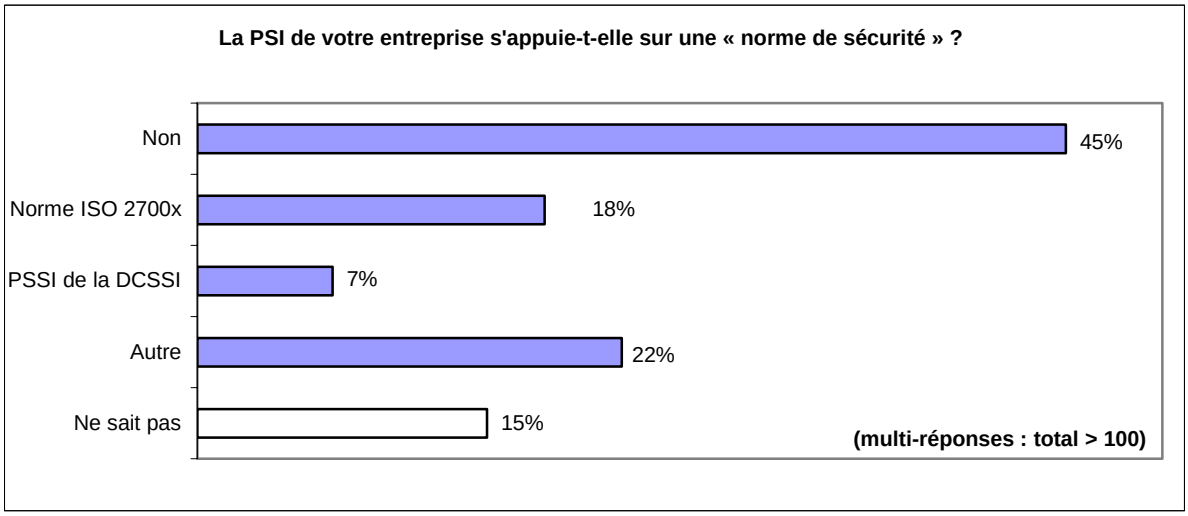

Figure 5 : appui de la PSI entreprise sur une « norme » de sécurité

Toutefois, les « normes » ne sont pas les seules bases utilisables pour mettre en œuvre une démarche de sécurisation du SI formelle et cohérente. Il existe également des « cadres métiers » spécifiques à certains secteurs (santé, certaines industries, etc.) permettant de formaliser des bonnes pratiques sans faire référence à une norme (ce que font 22 % des entreprises).

Néanmoins, ces normes constituent un guide intéressant pour assurer une bonne couverture des thématiques de sécurité à aborder par un RSSI. L'intérêt de telles normes est notamment de garantir la complétude des thèmes traités par la PSI, et pourquoi pas, comme le pensent certains acteurs du marché, de viser une certification des entreprises, telle que cela est pratiqué dans le domaine de la qualité.

Une démarche portée par la Direction Générale ?

Dans 95 % des cas, la PSI est soutenue explicitement par la direction générale de l'entreprise (59 % en totalité, 36 % en partie) ; ceci démontre bien la volonté du management de doter leur entreprise d'un cadre formel, d'une vraie culture de la sécurité des systèmes d'information, et aussi leur souhait de mobiliser les salariés autour de la mise en œuvre de cette politique. La pression réglementaire renforcée suite aux scandales liés à la mauvaise gestion de certaines entreprises, et les incidents fréquents et largement médiatisés concernant par exemple la divulgation d'informations confidentielles (très focalisée aujourd'hui sur les données personnelles), vont continuer à pousser les entreprises à mettre en place des règles de gouvernance plus strictes en matière de sécurité de l'information.

Mais trop souvent, comme le montrent les autres chiffres de notre enquête, les directions générales perçoivent mal l'ampleur des chantiers à lancer pour que ces politiques soient réellement mises en application, et ne dégagent pas les moyens et l'énergie nécessaires à cette mise en application. Pourtant, lorsque la politique est rédigée et validée, le travail commence seulement…

Thème 6 : Organisation de la sécurité et moyens

Le RSSI, une responsabilité trop peu identifiée et attribuée

37 % des entreprises disposent d'une fonction RSSI clairement identifiée, dont 16 % à temps plein (fonction unique) et 21 % à temps partagé (plusieurs fonctions).

La présence de RSSI identifiés croît régulièrement avec la taille de l'entreprise :

- 31 % des entreprises pour un effectif de 200 à 499 personnes,
- 39 % entre 500 et 999 personnes,
- 61 % au-delà de 1000 personnes.

Cette attribution formelle de la sécurité de l'information à un RSSI est en régression visible depuis l'étude 2006 (il y avait 42 % de RSSI en 2006). Les responsables informatiques semblent souvent « reprendre la main » sur cette fonction en se l'attribuant directement. Lorsqu'il n'y a pas de RSSI à temps plein, cette fonction est en effet assurée à plus de 50 % directement par le DSI ou responsable informatique Ce rôle peut aussi être assuré par des responsables de haut niveau (jusqu'au DG) ou transversaux (finance, contrôle interne, etc.), voire par un consultant externe (6,5 %).

Le RSSI, un rattachement (enfin !) plus fréquent à la direction générale

Ici, l'évolution est évidente : aujourd'hui, le poste de RSSI, lorsqu'il existe, est rattaché à la direction générale dans 45 % des cas (+ 6 % / 2006) et 32 % à la DSI (- 9 % / 2006). L'évolution vers une relative indépendance du RSSI par rapport aux fonctions informatiques se poursuit, 68 % des RSSI n'y étant plus rattachés.

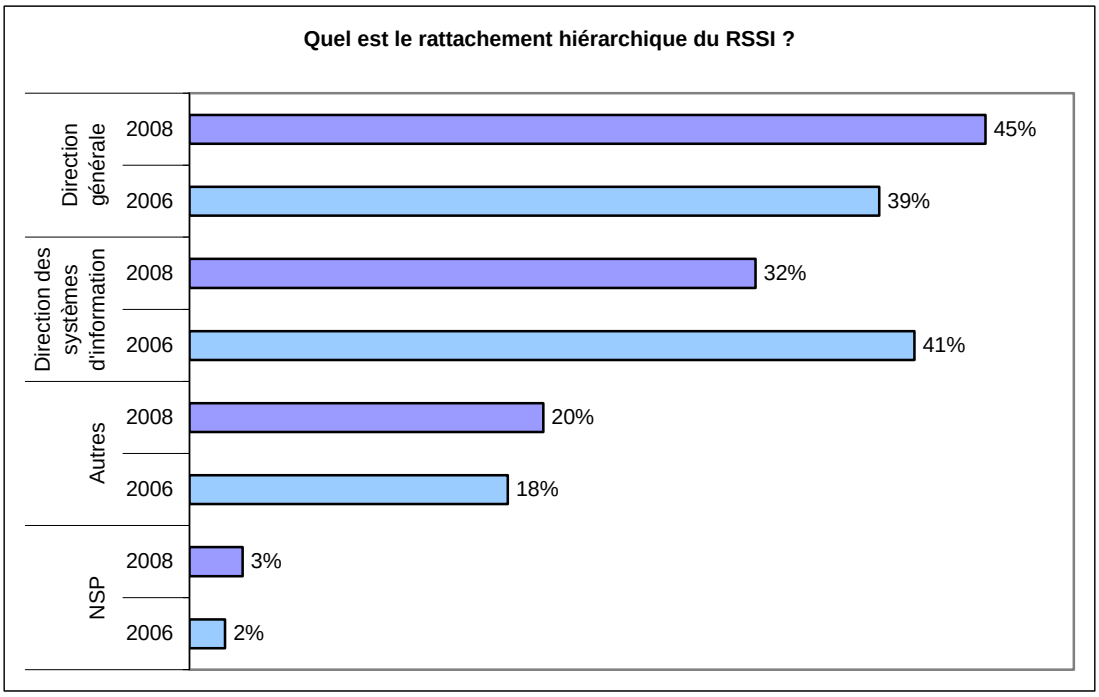

Figure 6 : rattachement hiérarchique du RSSI dans l'entreprise

Le RSSI : une fonction équilibrée entre l'opérationnel, le technique et le fonctionnel

Le RSSI voit son rôle réparti en 3 tiers quasiment identiques. On peut y voir une répartition « idéale » mise à l'épreuve du terrain des fonctions dévolues au RSSI.

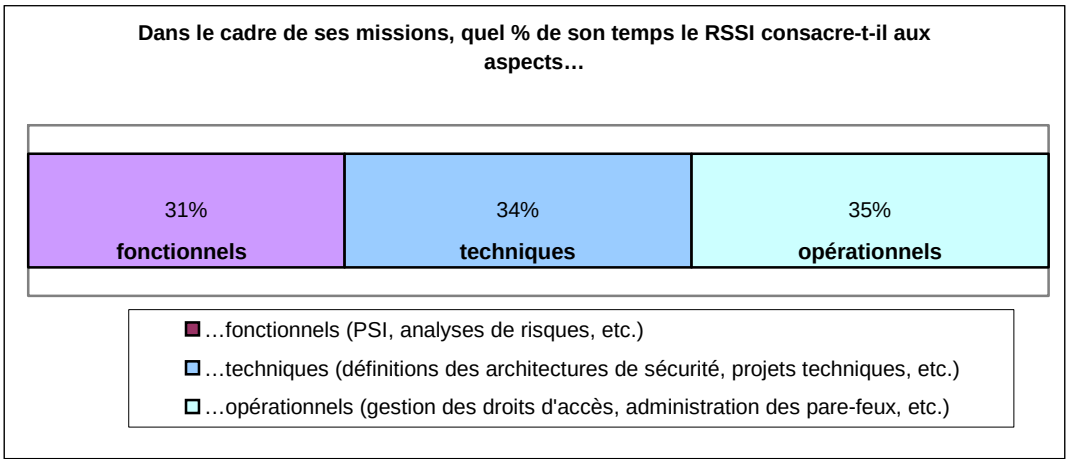

Figure 7 : répartition des missions du RSSI

Le RSSI est souvent un homme seul

Il n'y a pas d'équipe assignée en permanence à la sécurité de l'information dans 43 % des entreprises en moyenne. S'il y a une équipe permanente dédiée à la sécurité, elle comprend 1 à 2 personnes pour 41 % des entreprises, 3 à 5 personnes pour 12 % des cas et ne dépasse 5 personnes que dans 2 % des cas.

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, notamment dans les cas de contraintes fortes (24/7 par exemple).

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

Une pratique de l'analyse de risque qui se développe

Seulement 30 % des entreprises interrogées affirment réaliser une analyse globale des risques liés à la sécurité de leur SI. Toutefois, en prenant en compte les entreprises qui effectuent des analyses de risque partielles, on obtient le chiffre de 60 %. Et elles utilisent les résultats de ces travaux pour définir leurs priorités d'action dans le domaine de la sécurité des SI pour 41 % d'entre elles.

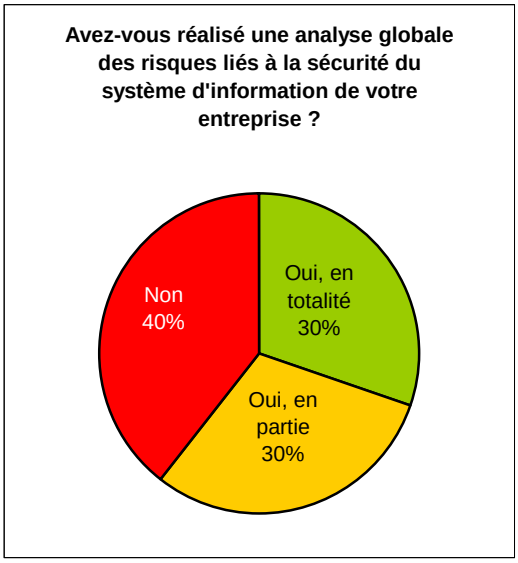

Figure 8 : analyse des risques réalisée en entreprise

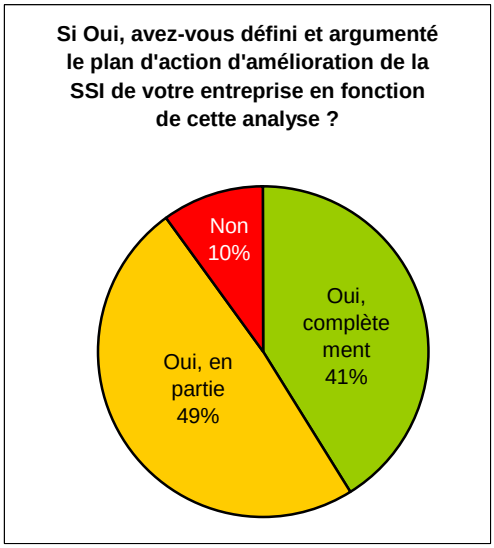

Figure 9 : processus d'amélioration de la sécurité du SI

La notion de risques liés à la sécurité des SI est donc maintenant reconnue et prise en compte pour l'élaboration des plans d'amélioration de la sécurité par une grande majorité des entreprises. C'est une excellente nouvelle, même si ces chiffres paraissent optimistes pour les experts du CLUSIF. Cette notion d'analyse de risque reste encore trop souvent informelle, l'utilisation des méthodes rigoureuses d'analyse, telle que la méthode MEHARI[4] par exemple, étant encore trop peu répandue.

La prise en compte des risques pour les nouveaux projets informatiques ne semble pas formalisée puisqu'elle n'est systématique que pour 36 % des entreprises. Pour les autres, 37 % ne réalisent pas systématiquement d'analyse de risques pour ces nouveaux projets informatiques et 24 % n'en font jamais. Le chiffre des entreprises réalisant systématiquement ou parfois ces analyses (73 %) reste toutefois stable par rapport à 2006.

[4] Voir glossaire

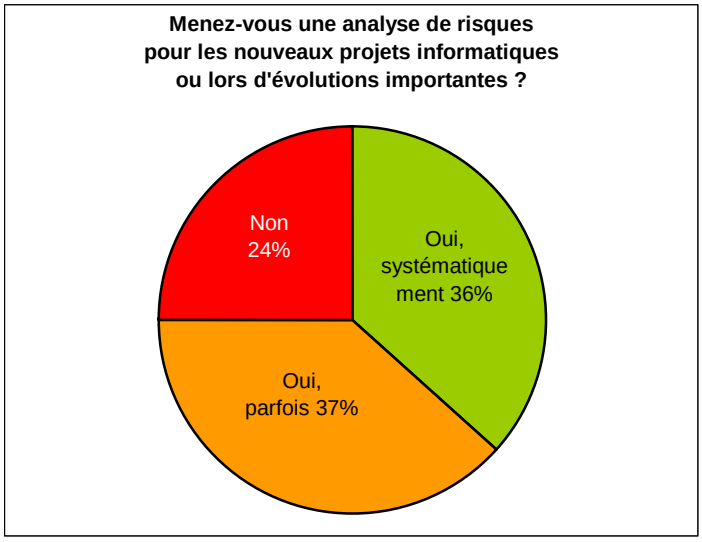

Figure 10 : prise en compte des risques dans les projets

Le RSSI toujours leader sur l'analyse des risques

Le RSSI est en charge de l'analyse des risques dans 35 % des cas. Seules 12 % des entreprises confient cette analyse aux « responsables métiers » qui sont à l'origine des projets informatiques. Cette proportion augmente un peu dans les grandes entreprises de plus de 1000 salariés (14 % des cas) mais semble en net recul par rapport à 2006.

Cette proportion devrait pourtant augmenter progressivement dans le futur : il est cohérent que les métiers soient chargés de se prononcer sur les risques acceptables pour l'entreprise, même s'il s'agit de risques impactant le SI. Le rôle du RSSI est de faire le lien entre les exigences de ces responsables métiers et les responsables de l'informatique.

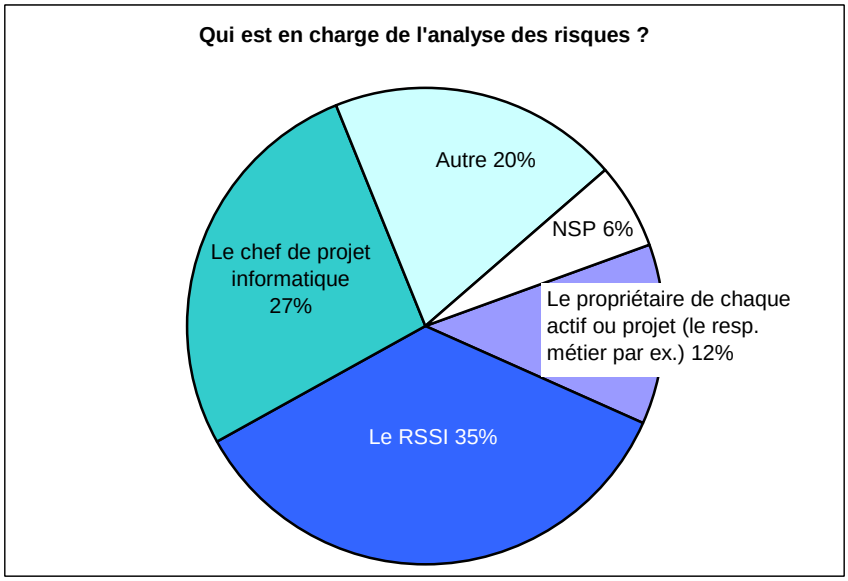

Figure 11 : les acteurs de l'analyse des risques

Thème 8 : Sécurité liée aux Ressources Humaines

Chartes de sécurité : un palier semble atteint

La proportion d'entreprises qui déclarent disposer d'une charte sécurité n'a pas progressé entre 2006 et 2008. On note même une légère régression (50 % des entreprises en 2008, contre 55 % lors de l'enquête 2006). Même si le ratio peut sembler déjà élevé (une entreprise sur deux a établi une charte sécurité), ce document, qui contribue de manière importante à la sensibilisation des utilisateurs et à la réglementation de leurs pratiques, est loin d'être généralisé. Les entreprises de plus de 1000 personnes (avec près de 60 %) ainsi que celles du secteur des services (62 %) ont une longueur d'avance, signe d'une certaine maturité de la politique de sécurité et de moyens plus conséquents.

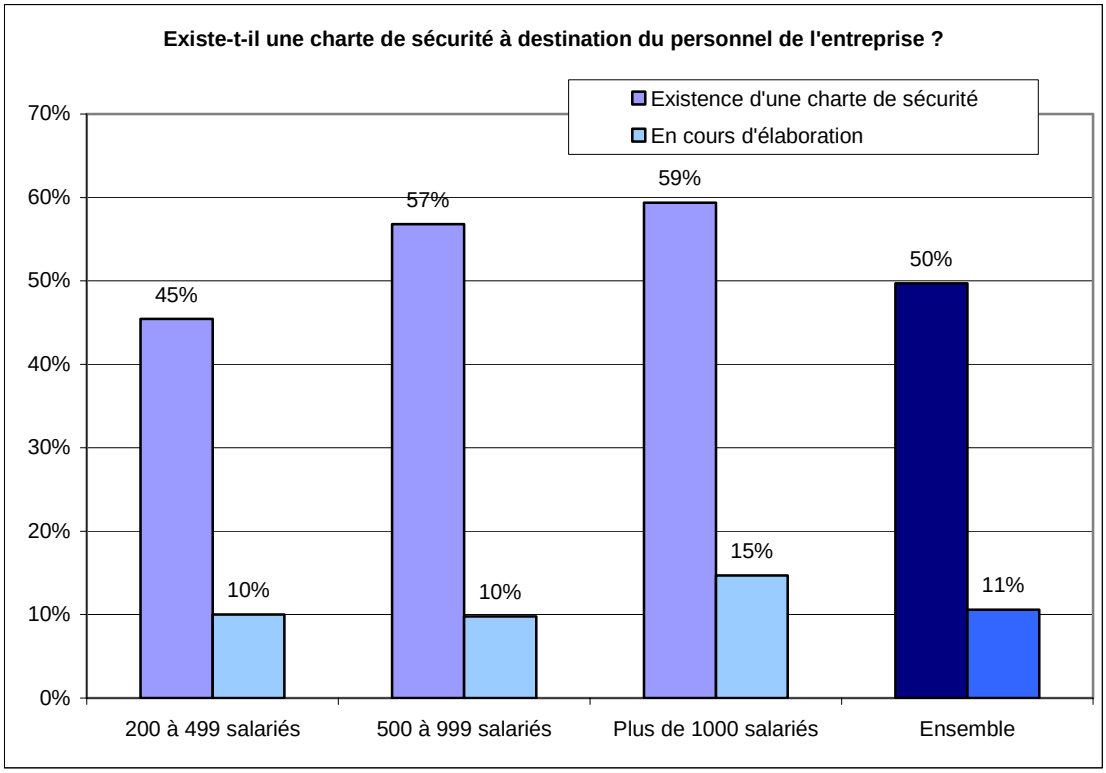

Figure 12 : existence d'une charte de sécurité, un effet de taille

Dans huit entreprises disposant d'une charte sécurité sur dix, cette charte est communiquée à l'ensemble des collaborateurs (qui la signent dans un cas sur deux) et son contenu précise les sanctions disciplinaires applicables dans 56 % des cas. Sur ce dernier point, la taille de l'entreprise a une influence : sept entreprises de plus de mille salariés sur dix ont intégré les sanctions dans le règlement intérieur, contre 51 % pour les PME de 200 à 499 salariés.

La sensibilisation des collaborateurs : une pratique encore 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 (35 %) ont institué des programmes de sensibilisation à la sécurité de l'information (53 % des entreprises de plus de mille salariés). La panoplie des outils de sensibilisation à la sécurité et leur hiérarchie n'a pas été bouleversée par rapport à notre dernière enquête. Ainsi, les actions les plus simples (publication d'articles sur l'Intranet ou le journal interne) sont les plus plébiscitées, ce qui était déjà le cas en 2006. En revanche, leur efficacité n'est pas mesurée dans huit entreprises sur dix.

Lors de la précédente enquête, la publication sur différents supports avait été citée par les deux tiers des entreprises comme l'un des outils de sensibilisation privilégié. En 2008, les entreprises ne sont que 42 % à citer ces outils. On aurait pu s'attendre à ce que ce tassement soit le reflet d'une montée en puissance d'autres méthodes, ce qui n'est pas le cas. En particulier, les sessions de formation ne se développent pas. Si l'on est optimiste, on peut y voir le résultat, sur le plan humain, d'une intériorisation de certaines bonnes pratiques par les utilisateurs ; sur le plan technologique d'une meilleure efficacité des mécanismes de sécurité mis en place et, sur le plan organisationnel, d'une meilleure diffusion de la culture sécurité.

Mais nous estimons que les actions de sensibilisation restent encore largement insuffisantes au regard des enjeux : seuls 18 % du personnel fait l'objet de formation/information de manière récurrente. 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…

Dans un même esprit, soulignons également le faible taux de sensibilisation des nouveaux arrivants dans l'entreprise (36 %) alors que le facteur humain est toujours, à juste titre, présenté comme un des points de faiblesse majeurs en termes de sécurité dans l'entreprise.

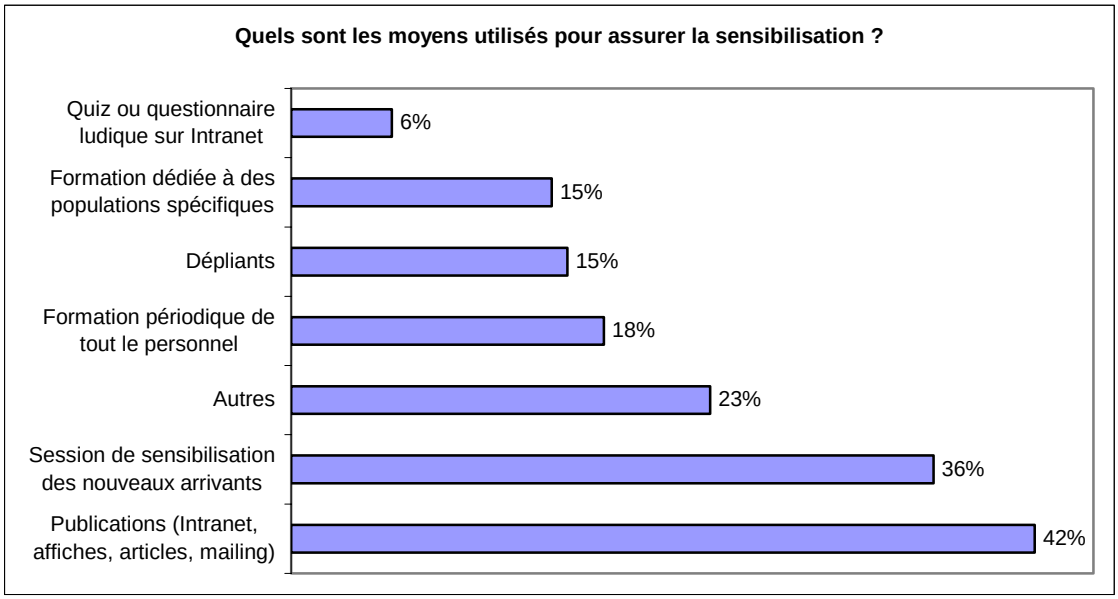

Figure 13 : outils de sensibilisation à la sécurité

Thème 10 : Gestion des opérations et des communications

Sécurisation des nouvelles technologies

Bien qu'elle ait diminué par rapport à l'étude 2006 (sauf pour les PDA/*smartphones*, dont l'usage a fait l'objet d'un recadrage important), l'interdiction des nouvelles technologies qui induisent des risques de sécurité est encore souvent la méthode retenue pour se prémunir de ces risques dans les entreprises.

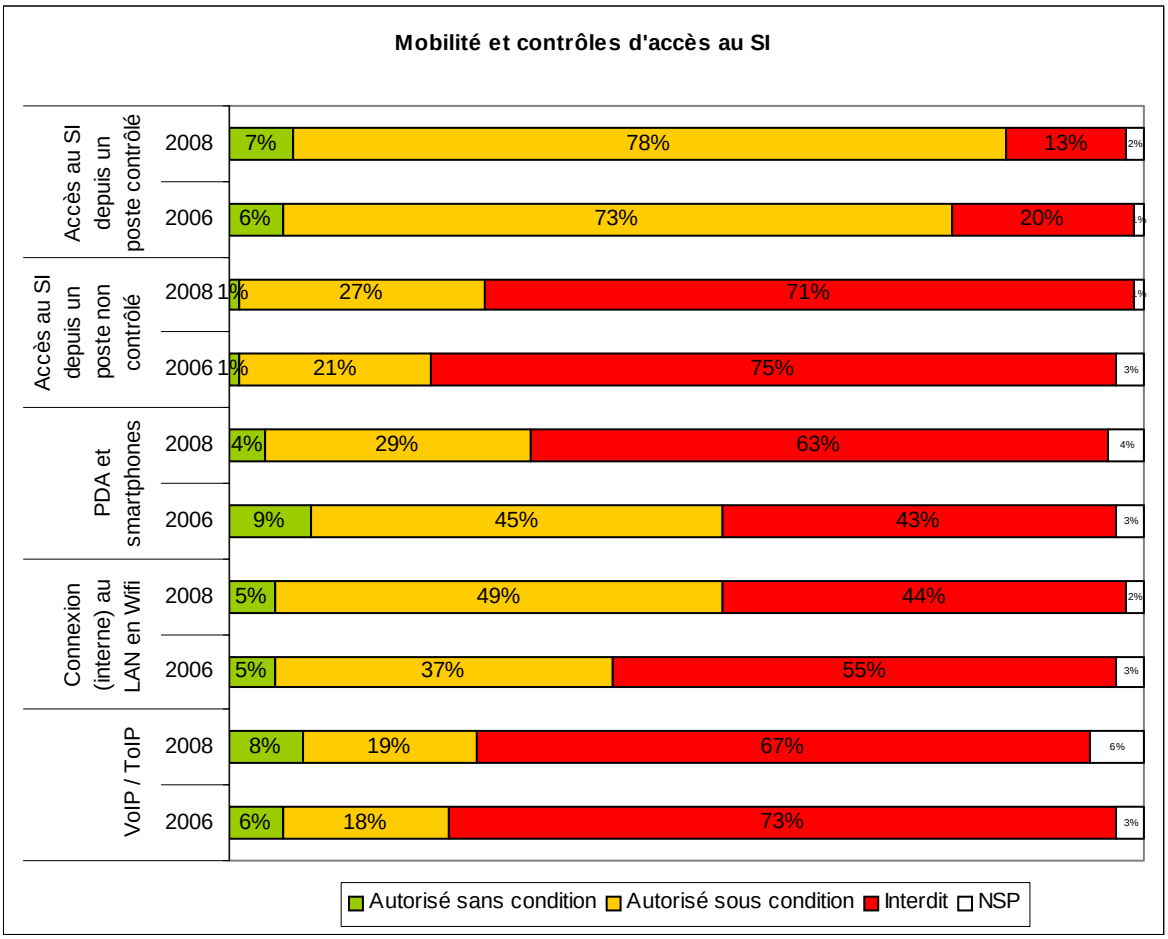

Figure 14 : mobilité et contrôles d'accès au système d'information

L'informatique mobile sous contrôle

La mobilité est un sujet qui va rester au cœur de l'actualité eu égard aux nouveaux modes de travail en vigueur dans les entreprises (rester connecté, tout le temps, avec au minimum un accès à la messagerie et dans certains cas à un logiciel tel que CRM pour des flottes commerciales). Il est donc logique que nous constations un effort d'ouverture à ces nouvelles technologies, même si celles-ci créent de nouvelles vulnérabilités. Aujourd'hui on accède au système d'information de l'entreprise :

- avec l'ordinateur portable fourni par l'entreprise, en légère hausse par rapport à 2006. Dans 78 % des entreprises, la fourniture d'ordinateurs portables ne va pas sans les moyens de connexion à l'entreprise,
- avec un poste de travail quelconque, un PC dans un cybercafé ou encore celui de la maison (27 % des entreprises, en légère hausse),
- avec un PDA/*smartphone* (33 %, en baisse cette fois). Le cas des *smartphones* est particulier : malgré la croissance du parc de ces équipements que nous constatons tous, les

usages sont plus souvent interdits par les entreprises qu'en 2006. Cela traduit sans aucun doute la volonté de reprise sous contrôle d'une flotte d'équipements qui étaient auparavant à cheval entre deux mondes : la « téléphonie » d'entreprise et personnelle.

Lorsqu'elles sont mises en œuvre, les mesures de sécurité utilisées couvrent assez bien la problématique liée au contrôle de la sécurité périmétrique, en faisant appel à des technologies désormais habituelles comme l'authentification forte ou encore le chiffrement (SSL, IPSec, etc.). Mais malheureusement, le pourcentage des entreprises utilisant ces technologies reste assez faible.

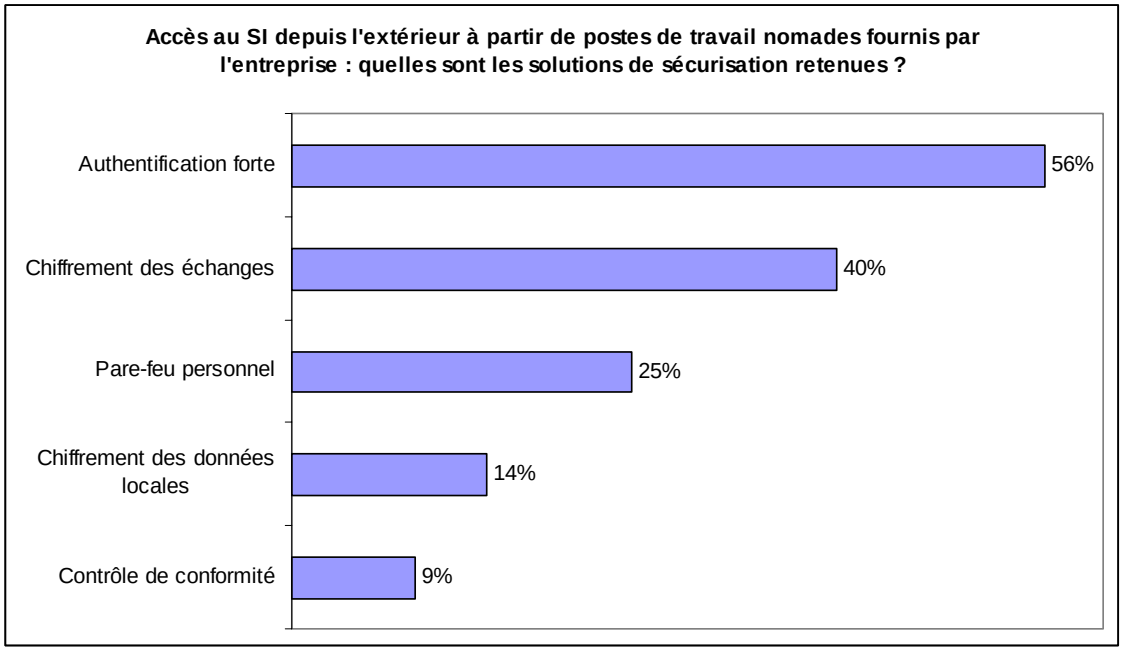

Figure 15 : technologies de sécurisation des accès nomades depuis des postes maîtrisés

La problématique de protection du terminal semble être couverte de façon moins exhaustive puisque malgré l'occurrence régulière de vols ou pertes (au 4ème rang des incidents cités dans cette enquête), 14 % des entreprises seulement utilisent le chiffrement des données locales, ce qui reste très faible. On sait pourtant que nombre d'informations importantes se trouvent dans les fichiers locaux et les données de messagerie des dirigeants.

Si l'on examine le cas spécifique des *smartphones*, il apparaît que les solutions de sécurité sont très peu déployées : 19 % seulement des *smartphones* sont équipés d'antivirus. Si les virus recensés sur ces plates-formes restent encore peu nombreux, il ne faut pas oublier que ce sont des ordinateurs connectés à part entière et que leur diffusion en forte augmentation devrait en toute logique attirer une attention de plus en plus grande de la part des créateurs de programmes malveillants.

La mobilité interne (Wifi) progresse

L'utilisation du Wifi en entreprise progresse : il était interdit par 55 % des entreprises en 2006 contre 44 % en 2008. Le besoin de mobilité au sein de l'entreprise est réel, et si par le passé la technologie a montré des faiblesses de sécurité, les évolutions de la norme permettent dorénavant de mettre en place des points d'accès suffisamment sécurisés mettant en œuvre des systèmes d'authentification et de chiffrement solides, mais nécessitant tout de même une bonne rigueur dans la définition de l'architecture et le déploiement. C'est d'ailleurs en s'appuyant sur ces mécanismes (70 % utilisent une authentification renforcée et 43 % le chiffrement des échanges) que les entreprises déploient progressivement ces solutions.

La VoIP[5] et la ToIP[5] : un déploiement inéluctable

Ce sujet est celui qui montre à la fois la plus grande stabilité entre 2006 et 2008 (puisque les chiffres sont quasi identiques) et les plus importantes prévisions d'équipement pour 2008 avec 21 % des entreprises non équipées envisageant un projet.

La ToIP est un cas à part, puisqu'il s'agit en général d'une nouvelle responsabilité attribuée aux DSI, la téléphonie étant historiquement gérée par les services généraux. Ce nouveau domaine est accompagné d'attentes fortes d'un point de vue « disponibilité » de la part des utilisateurs. Elle apporte aussi son lot de contraintes, notamment en termes de sécurisation.

Technologies de protection et de gestion des vulnérabilités

Des nouvelles technologies de sécurité qui peinent à s'imposer

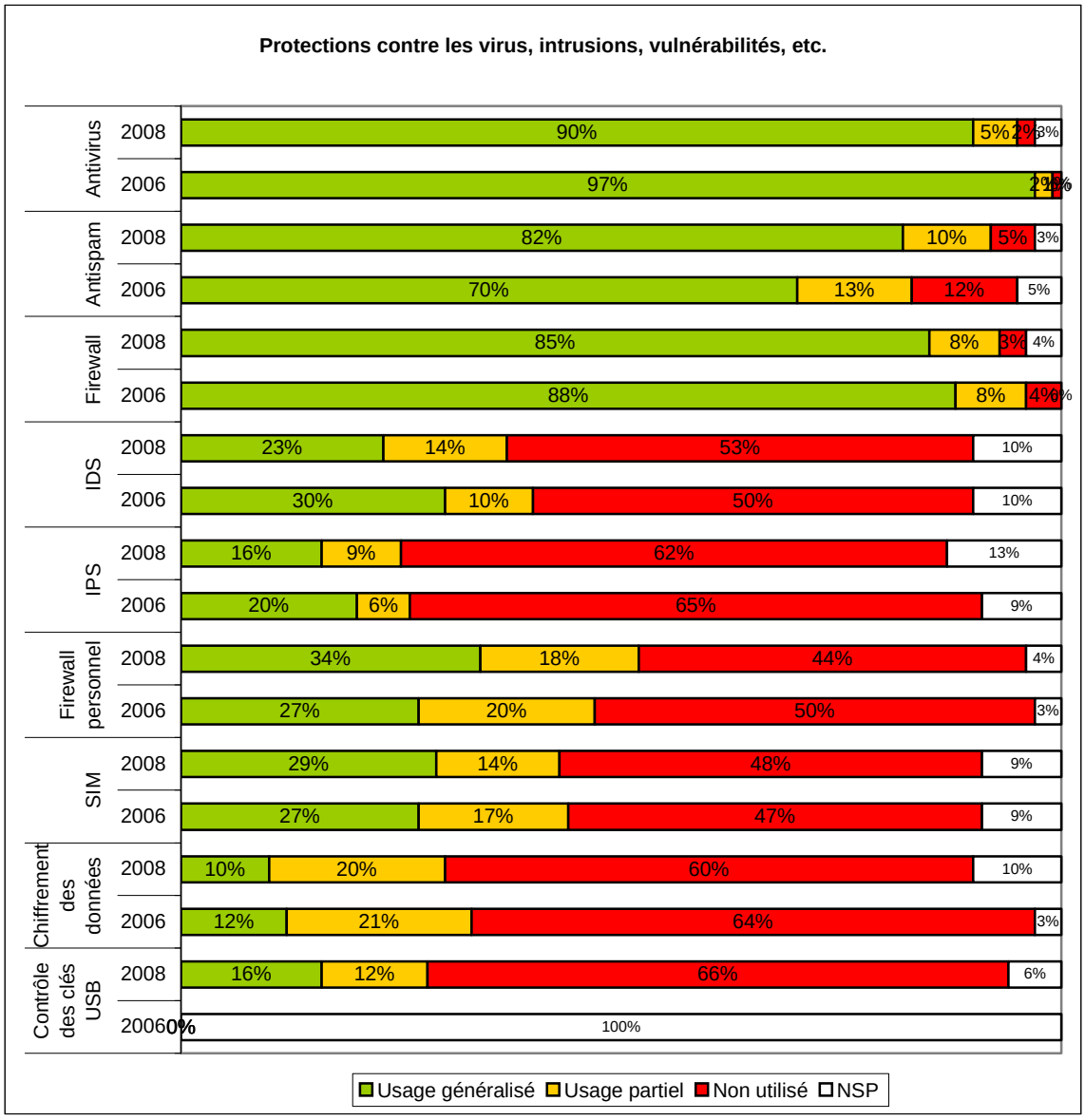

Figure 16 : technologies de sécurité / lutte antivirale, anti-intrusion, gestion des vulnérabilités

[5] Voir glossaire

Les anti-virus et firewalls font déjà l'objet d'une utilisation systématique et sont donc un fait acquis : il faut les deux, partout, comme des serrures aux portes. Pourtant les attaques virales restent encore régulières (30 % des entreprises ont été victimes d'incidents de ce type au cours de l'année 2007), sans doute lié entre autres à des problématiques de mise à jour sur certaines installations.

Les logiciels antispam suivent, eux, une forte progression pour se rapprocher rapidement d'une utilisation quasi-systématique, ce qui est logique eu égard à la nécessité de ce type d'outil (en 2007, plus de 96 % du trafic de messagerie est constitué de spam[6]).

L'usage des IDS et IPS reste stable, voir légèrement en régression. Il est vrai que les IDS nécessitent une bonne expertise et du temps pour être utilisés à bon escient, et que les fonctions IPS étant de plus en plus intégrées aux nouvelles générations de firewalls, l'achat de boîtiers spécifiques se justifie moins.

La mise en place de SIM[7] reste complexe à aborder du fait de la multiplicité des sources d'événements et de journaux. Pourtant ces outils sont indispensables à la bonne surveillance des systèmes et sont aussi la base de possibles systèmes d'alertes (en cas, par exemple, de détection d'activité anormale sur un type d'évènement particulier). Ce sont les plus grandes entreprises qui prévoient le plus de projets de mise en place pour 2008 (10 %), ce qui montre que ce sujet reste une préoccupation réelle.

La sécurisation du poste de travail est un sujet en progression, on le voit dans les stratégies « produit » des éditeurs puisque la plupart proposent désormais des suites complètes dans leur gamme entreprise, comprenant antivirus, firewall, gestion des ports, etc. On le voit également dans les résultats de l'enquête où l'usage du firewall personnel progresse globalement. Ce dernier est aujourd'hui plus systématiquement utilisé dans le cadre des ordinateurs portables, ce qui est bien entendu indispensable dès lors qu'on l'utilise pour se connecter à des réseaux ouverts.

Le chiffrement des données ne progresse pas. Il est vrai que si les outils de chiffrement sont assez aisés à déployer sur des parcs de portables pour adresser les problèmes de perte ou de vol, ils sont beaucoup plus compliqués à mettre en place dès lors que l'on veut chiffrer des données partagées : nécessité d'une démarche de classification des informations et de processus organisationnels formalisés pour gérer les clés de chiffrement et les droits d'accès aux données chiffrées.

[6] Source : *Panorama des menaces emails - France 2007*, SECUSERVE (4 janvier 2008)
[7] Voir glossaire

Thème 11 : Contrôle des accès logiques

Le contrôle des accès logiques est envisagé sous trois aspects :

- les moyens d'authentification forte pouvant être utilisés,
- la manière de gérer et mettre en œuvre les droits d'accès des utilisateurs,
- les systèmes de contrôle d'accès centralisés et d'authentification unique (*Single Sign-On*).

On constate que ces technologies restent peu déployées, et surtout que la situation ne semble pas avoir évoluée en deux ans, puisque les résultats 2008 sont presque identiques à ceux de 2006. 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.

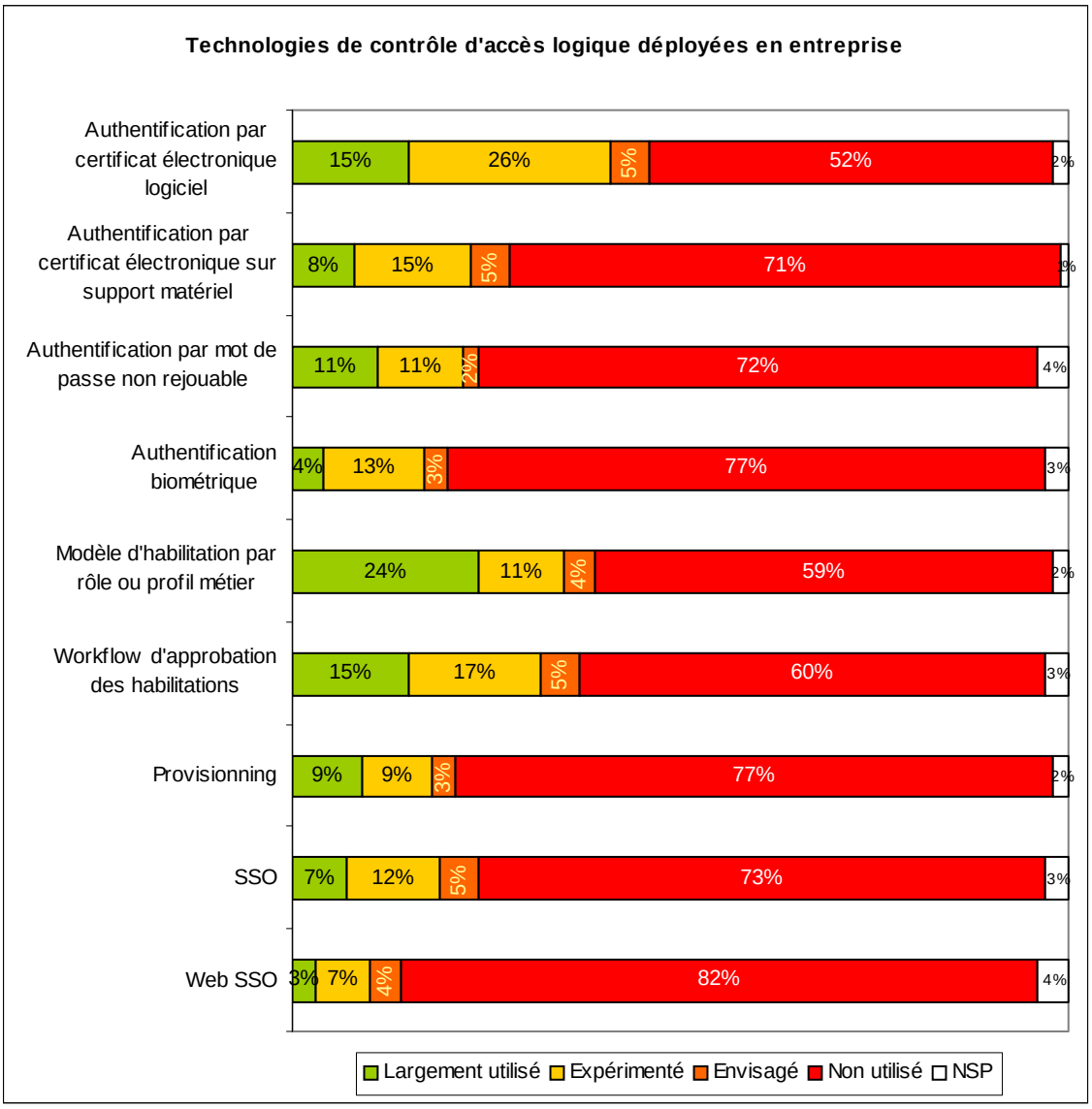

Figure 17 : technologies de contrôle d'accès logique déployées en entreprise

Légère percée de la biométrie, progrès 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 2008, on constate cependant une légère percée de la biométrie : 4 % des entreprises se sont mises à l'utiliser largement au cours des deux dernières années et 8 % de plus sont en cours d'expérimentation.

L'utilisation des certificats sur support logiciel, solution arrivant en tête en 2006, se confirme cette année encore et même se renforce légèrement (5 % des entreprises en plus les ont largement adopté, avec un volume constant d'entreprises en cours d'expérimentation), même si nous sommes encore loin d'une adoption massive puisque la moitié des entreprises n'envisagent toujours pas de passer le pas.

Les autres technologies d'authentification forte ne montrent pas d'évolution notable.

De manière surprenante, 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 19 % à utiliser largement des certificats logiciels, et 15 % des certificats sur support matériel (carte à puce, clé USB cryptographique, etc.), contre respectivement 14 % et 9 % sur l'ensemble des entreprises.

Les secteurs financiers et des services témoignent comme dans d'autres domaines d'une avance sur les autres secteurs d'activité : leader sur le déploiement des dispositifs d'authentification forte, il n'y a que pour la biométrie où un autre secteur (transports et télécoms) envisage davantage d'étudier cette solution.

Gestion des habilitations : des progrès timides

Les modèles de gestion des habilitations n'ont pas évolué en deux 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.

Par contre, il semble que celles qui ont mis en place un tel modèle en 2006 aient poursuivi leur logique en renforçant leurs outils de gestion : dans un premier temps, par la mise en place en cours d'un *workflow* de validation des habilitations (+ 6 % pour l'expérimentation, mais le nombre de *workflow* largement utilisés reste identique), voire pour les plus avancées par la mise d'un système de distribution automatique des droits (*provisioning*), avec là aussi + 6 % en cours d'expérimentation, pour un nombre de dispositifs pleinement opérationnels stables.

Le faible nombre d'entreprises envisageant de renforcer leur gestion des habilitations en 2008 est surprenant, puisque les évolutions légales et réglementaires (Loi sur la Sécurité Financière, Sarbanes-Oxley, etc.) tendent à augmenter le niveau d'exigence en matière de traçabilité et de maîtrise des droits d'accès.

Contrôle d'accès et SSO : les grandes entreprises l'expérimentent

Les dispositifs de *Single Sign-On* (SSO et Web SSO) peinent eux aussi à séduire les entreprises, avec toutefois une légère amélioration en perspective : si le nombre d'entreprise les ayant généralisés reste stable, on constate le doublement du nombre de celles les expérimentant en 2008, avec une forte avance des plus grandes entreprises. En effet, les expérimentations sont proportionnellement deux fois plus nombreuses dans la tranche des plus de 1000 salariés que dans les autres tranches. Mais plus des trois-quarts des entreprises n'envisagent toujours pas de telles solutions, qui apportent pourtant un réel confort aux utilisateurs, facilitant ainsi le respect de politiques de mots de passe plus strictes.

Thème 12 : Acquisition, développement et maintenance

Veille et gestion des vulnérabilités : une situation qui se stabilise

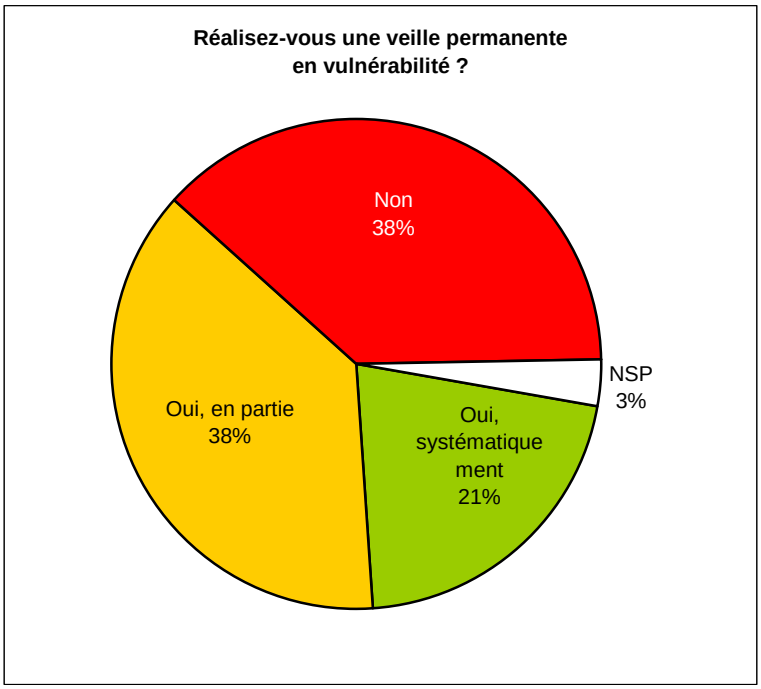

Figure 18 : réalisation d'une veille permanente en vulnérabilité

59 % des entreprises disent réaliser une veille systématique ou partielle sur les nouvelles failles de sécurité et sur les nouvelles attaques. Les grandes entreprises déclarent plus souvent réaliser une veille systématique, c'est-à-dire couvrant très largement le périmètre de leurs environnements techniques. Ce chiffre reste à peu près stable par rapport à 2006. Les entreprises n'ont globalement pas renforcé leur vigilance vis-à-vis des menaces.

Maintenance et déploiement de correctifs de sécurité : une meilleure automatisation

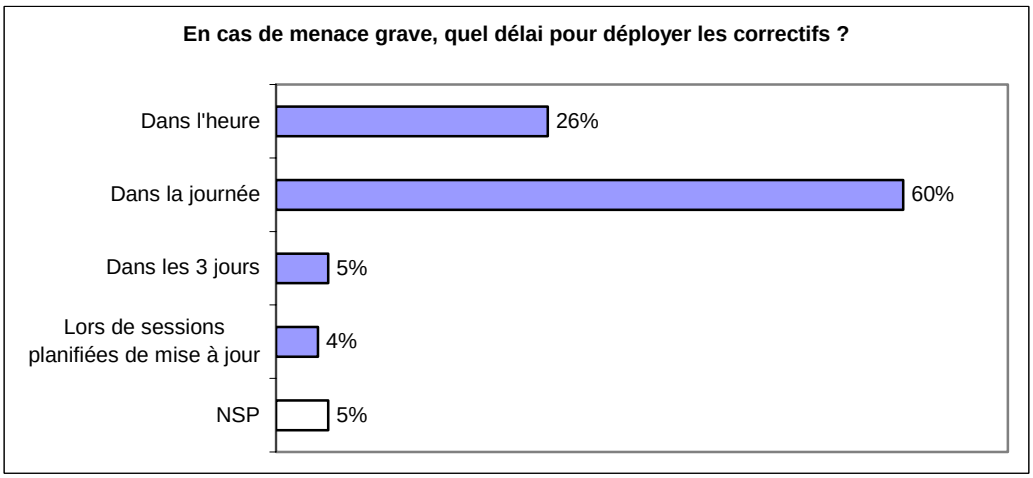

Figure 19 : délai de déploiement des correctifs

Près de la moitié des entreprises formalisent les procédures de déploiement des correctifs. À noter que les entreprises de plus de 1000 salariés sont les plus avancées en matière de formalisation.

Parmi celles qui ont mis en place des procédures de déploiement des correctifs, 86 % des entreprises réalisent les déploiements de leurs correctifs en moins d'une journée, ce qui représente une progression de près de 10 % entre 2006 et 2008. L'utilisation des dispositifs de déploiement automatique semble donc progresser significativement, en tout cas pour ce qui concerne les environnements « poste de travail ». Le CLUSIF constate en effet que si la pratique de déploiement des correctifs est maintenant assez courante pour les postes de travail, elle reste peu répandue pour les environnements serveurs.

Thème 13 : Gestion des incidents - sinistralité

Faible évolution dans le suivi des incidents de sécurité

La proportion des entreprises interrogées ne disposant pas d'une équipe consacrée à la gestion des incidents de sécurité d'origine malveillante est toujours très proche de 60 %, comme en 2006. Pour les entreprises qui assurent un suivi, un tiers possèdent une cellule dédiée à la sécurité. Pour les deux tiers restants, une cellule existe mais elle traite également d'autres fonctions d'exploitation.

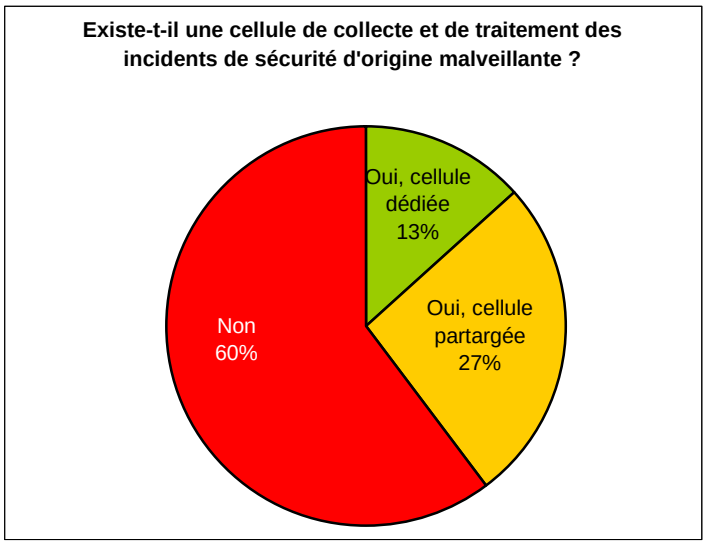

Figure 20 : cellules de collecte et de traitement des incidents d'origine malveillante

Les entreprises rechignent toujours à déposer des plaintes…

Le taux de dépôt de plainte est quant à lui absolument stable, aux alentours de 5 % des entreprises interrogées, alors que l'on constate que nombre d'entre elles ont rencontré des incidents méritant vraisemblablement des suites judiciaires. Les différentes interventions des autorités, notamment la Gendarmerie Nationale, la Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information (BEFTI), la Direction de la Surveillance du territoire (DST) et l'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC) et campagnes de sensibilisation effectuées en 2007 auprès des RSSI n'ont pas encore réussi à convaincre totalement et beaucoup d'affaires restent cachées.

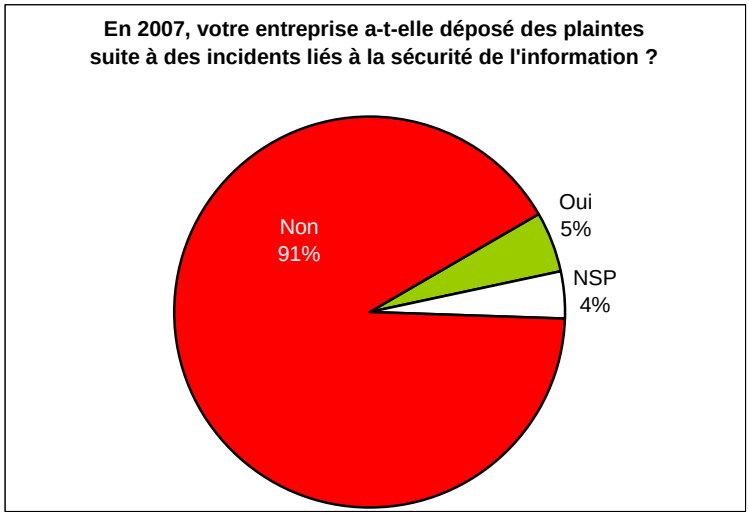

Figure 21 : dépôts de plaintes des entreprises

… mais 56 % des RSSI constatent au moins un incident

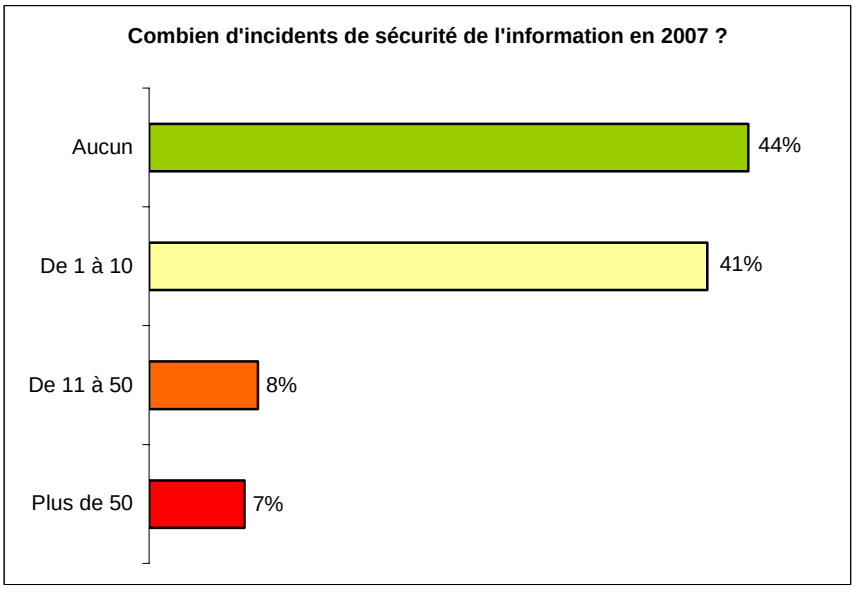

Figure 22 : nombre d'incidents de sécurité recensés en 2007 par les entreprises

Évaluation des impacts financiers : moins d'une entreprise sur trois !

Dernier constat, en cohérence avec le piteux tableau déjà dressé, seulement 28 % des entreprises procèdent à une évaluation de l'impact financier des incidents de sécurité. Toutefois, on note une petite évolution positive de ce taux (de 24 % à 28 % entre 2006 et 2008), on ne peut donc que souhaiter que cette tendance se confirme dans les deux prochaines années.

Financement des sinistres par l'assurance : dans 15 % des cas seulement !

Par ailleurs, l'impact financier des sinistres n'est pas résorbé (dans 41 % des cas) ou n'est pas identifié (25 %) alors qu'un transfert financier est possible vers l'assurance (seulement 15 % dans notre enquête) ou par l'octroi d'un emprunt bancaire (dans 0,5 %).

Peu de variations dans les typologies d'incidents de sécurité rencontrées

Par rapport à 2006, il n'y a pas de grosse évolution dans les types d'incidents rapportés, même si l'on peut noter une baisse des incidences de vols ou disparitions de matériels et des infections par des virus. On note une évolution des divulgations d'information et des attaques ciblées (+50 %), dont il faudra certainement suivre les évolutions dans les années à venir.

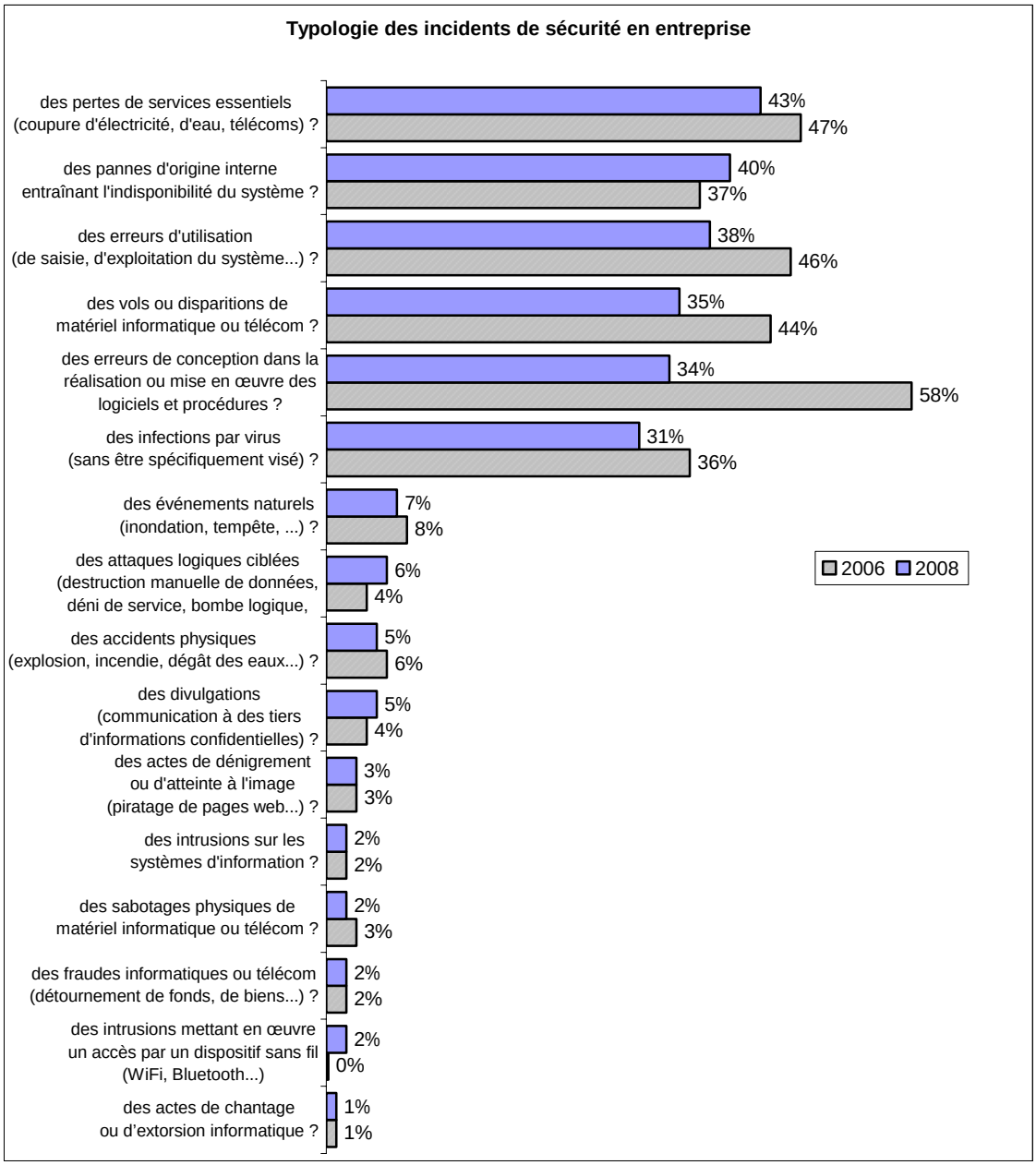

Figure 23 : typologie des incidents de sécurité en entreprise

Thème 14 : Gestion de la continuité d'activité

Gestion de la continuité de l'activité : de grandes inégalités dans la maîtrise du processus

Bien que la dépendance de l'activité de l'entreprise vis-à-vis de son informatique soit un fait acquis, nous constatons de grandes inégalités dans la maîtrise de la gestion de la continuité d'activité. 40 % des entreprises n'ont toujours pas mis en place un processus de gestion de la continuité d'activité. Un peu plus d'un quart d'entre elles (28 %) toutes tailles confondues estiment avoir mis en place un processus de continuité d'activité couvrant l'ensemble de leurs activités critiques.

De manière générale, plus les entreprises sont petites, moins elles ont mis en place un processus de gestion de la continuité. Ceci résulte sans doute d'une fausse perception de la complexité et du coût de mise en œuvre d'un plan de continuité.

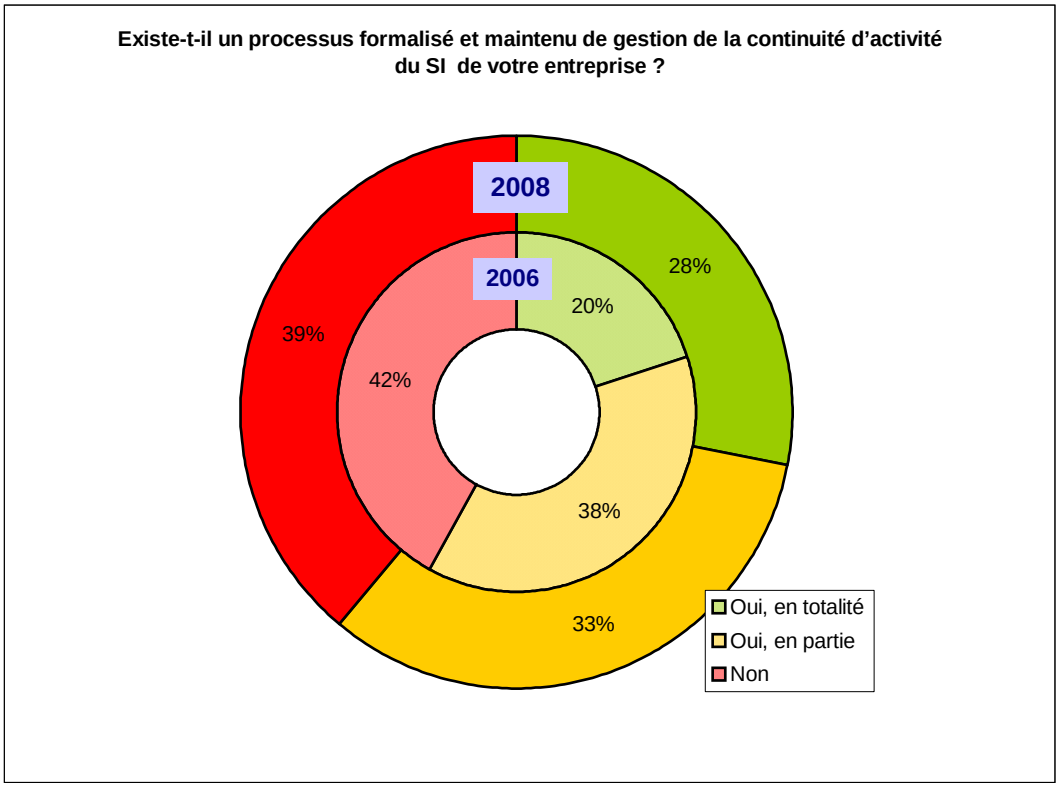

Figure 24 : mise en place d'un processus de gestion de la continuité d'activité du SI

La maintenance : un effort nécessaire

Les entreprises qui disposent d'un processus de continuité semblent avoir bien compris la nécessité de garantir le « maintien en condition opérationnelle » de ce processus : seulement moins de 10 % ne teste pas et ne mettent pas régulièrement à jour leur plan de continuité d'activités. À l'opposé, et c'est rassurant, 72 % d'entre-elles réalisent au moins un test par an.

Si les processus de continuité d'activité mis en place traitent majoritairement l'aspect informatique (sauvegarde des données, secours informatique), les processus de gestion de crise et de continuité d'activité métier restent à développer dans de très nombreux cas.

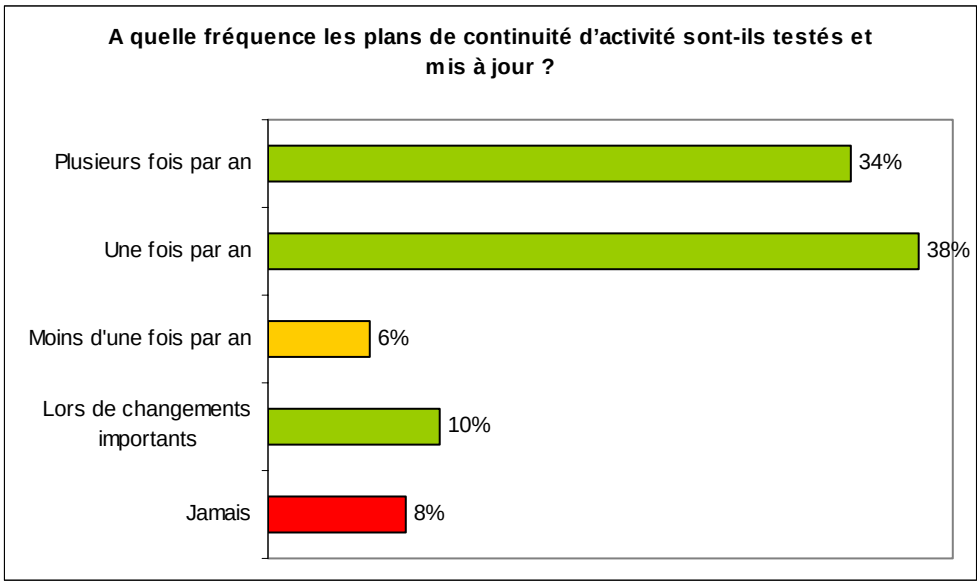

Figure 25 : fréquence des tests des plans de continuité d'activité

Secours informatique : les sauvegardes restent l'outil principal

Afin de palier à des sinistres majeurs la solution la plus fréquemment utilisée reste les moyens de sauvegarde dits « classiques » : près de 80 % des entreprises utilisent cette solution. Mais très souvent, nous constatons qu'un travail de fond reste à réaliser pour s'assurer que le plan de sauvegardes intègre bien l'externalisation régulière des supports, en phase avec les enjeux pour l'entreprise en cas d'impact majeur sur ses activités critiques. Nous rencontrons malheureusement encore trop souvent des entreprises qui, certes réalisent des sauvegardes, mais laissent les supports/médias dans la salle informatique. En cas de sinistre, la perte est alors totale pour les entreprises.

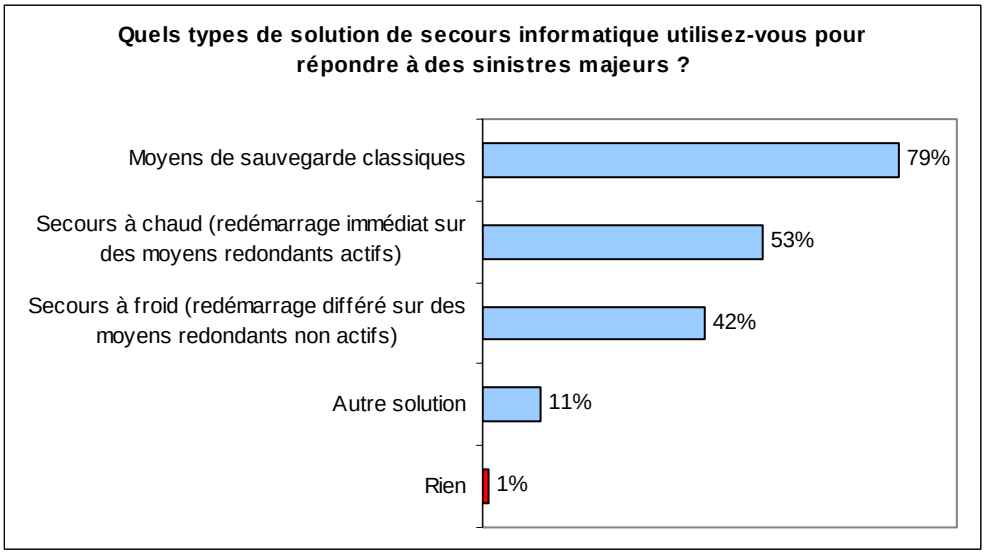

Figure 26 : solutions de secours informatique

Tous les chiffres de l'étude 2008 dans le domaine de la continuité d'activité sont assez comparables à ceux de l'étude réalisée en 2006. La gestion de la continuité continue donc sa trop lente progression malgré la pression réglementaire dans certains secteurs et le développement global de la gestion des risques au sein des entreprises.

Thème 15 : Conformité

Ce thème aborde les éléments liés à la conformité, à travers 3 sujets :

- le respect des exigences de la **Loi Informatique et Libertés**,
- le contrôle des niveaux de sécurité à travers les **audits**,
- le suivi des niveaux de sécurité grâce aux **tableaux de bord** de sécurité.

1/ Les obligations liées à la loi informatique et libertés

Toujours autant d'entreprises non conformes aux exigences de la loi informatique et libertés

Le pourcentage d'entreprises qui déclarent respecter les exigences de la loi informatique et libertés n'évolue pas par rapport à l'étude menée en 2006. Un tiers d'entre elles estiment ne pas être en totale conformité. Le développement notable des correspondants informatique et libertés devrait faire évoluer ce chiffre positivement dans les années à venir.

Le correspondant informatique et libertés – une prise en compte plus précise

En effet, 25 % des entreprises déclarent avoir mis en place un correspondant informatique et libertés (CIL), soit environ 1500 entreprises. Cette année, les réponses des entreprises interrogées sont donc particulièrement compatibles avec les données officielles fournies par la CNIL : au 20 août 2007, celle-ci indique que 1450 organismes avaient désigné un correspondant informatique et libertés. Très récemment (mai 2008), la CNIL a annoncé que 2376 CIL étaient déjà nommés en France. La vision de la mission donnée par la loi de 2004 au correspondant informatique et libertés s'est donc précisée.

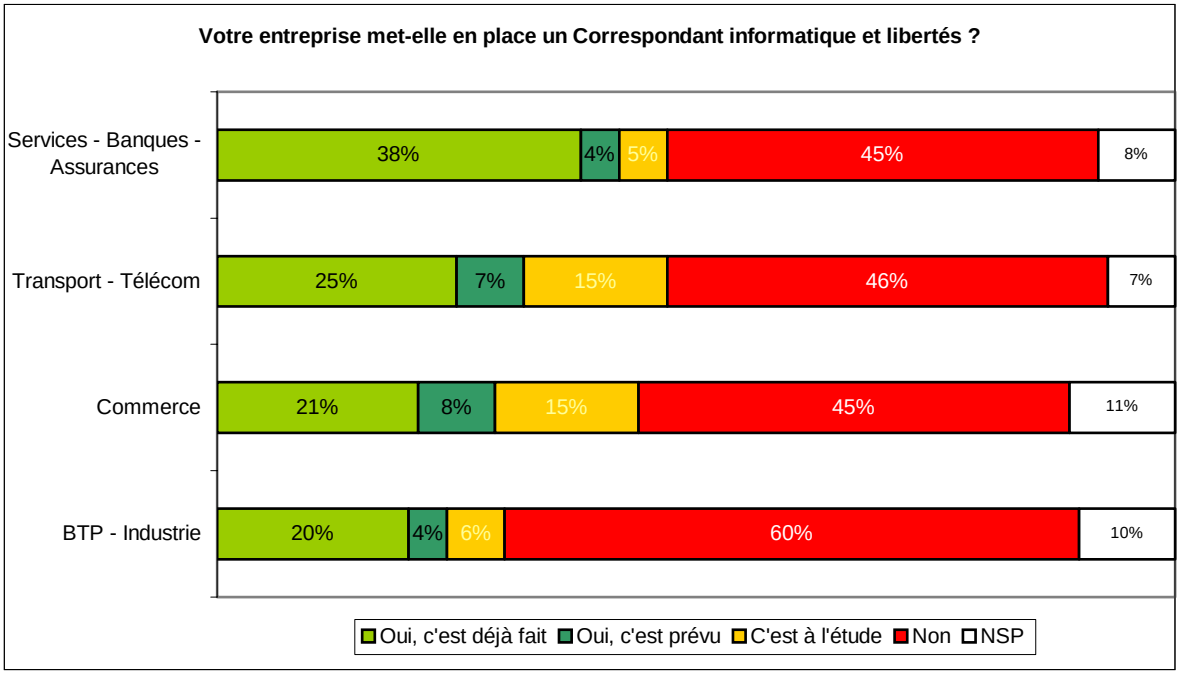

Figure 27 : correspondant informatique et libertés en entreprise, par secteur d'activité

2/ Les audits

35 % des entreprises ne mènent jamais d'audit de sécurité

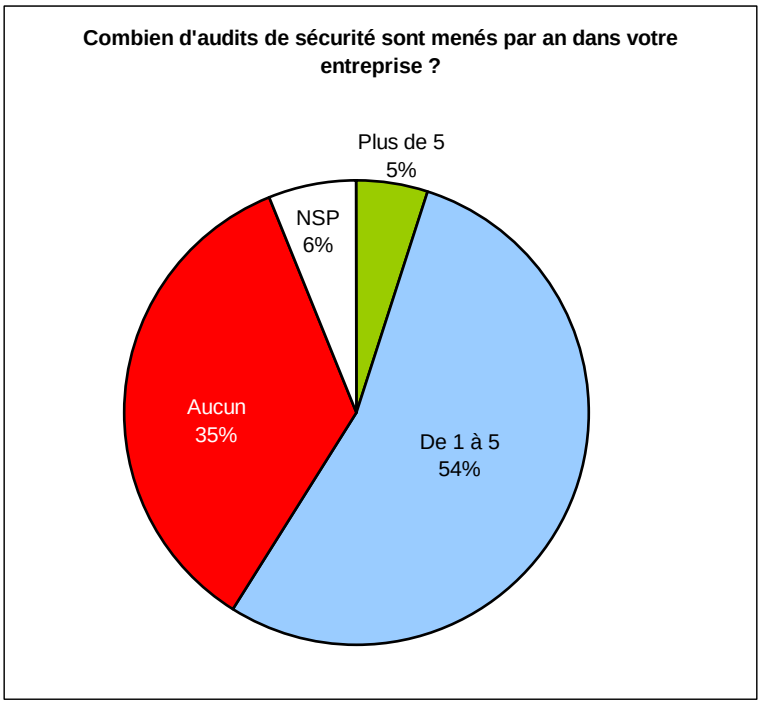

Figure 28 : nombre d'audits de sécurité menés sur un an

Le nombre d'entreprises qui réalisent au moins un audit (59 %) est en légère régression par rapport à 2006 (69 %) où l'on avait noté un bond spectaculaire. Seules les grandes entreprises (plus de 1000 salariés) progressent puisque 82 % d'entre elles réalisent au moins un audit par an, contre 75 % en 2006. Dans ces dernières, la pratique de l'audit devient très systématique.

Ces audits sont plus d'une fois sur deux (56 %) motivés par la politique interne qui énonce une obligation d'audit, ou bien des exigences contractuelles ou réglementaires.

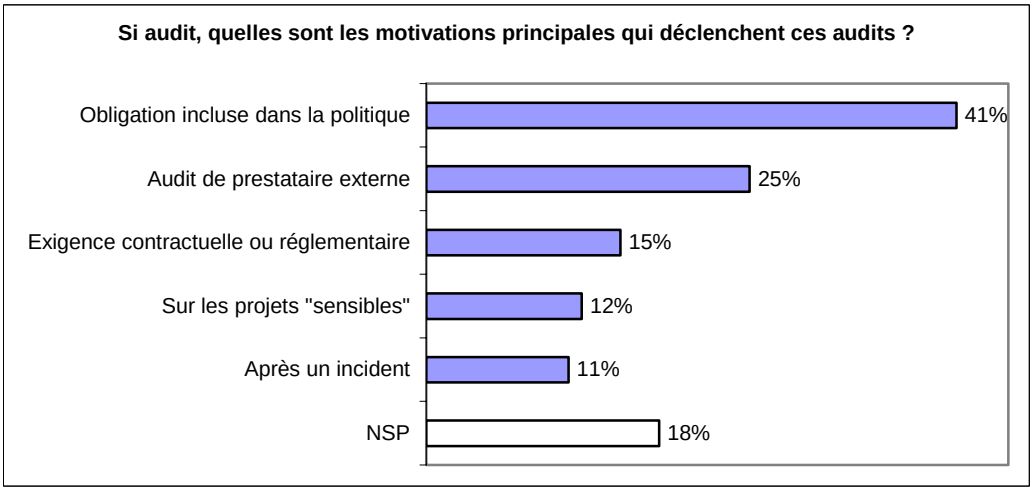

Figure 29 : motivations des audits de sécurité

A noter que la part d'audits de prestataires externes est en forte augmentation par rapport à 2006 (25 % au lieu de 12 %). Cette évolution semble assez naturelle dans un contexte où les entreprises externalisent de manière plus fréquente l'exploitation de tout ou partie de leur informatique.

3/ Les tableaux de bord de sécurité

Plus de 75 % des entreprises ne mesurent pas leur niveau de sécurité régulièrement

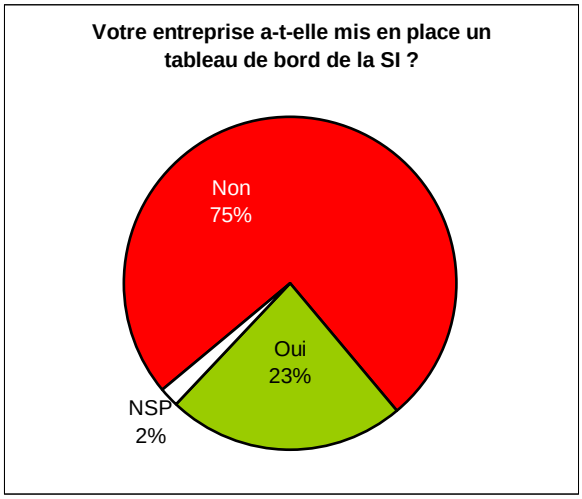

Figure 30 : mise en place de tableaux de bord en entreprise

On note cependant une nette augmentation des entreprises qui le diffusent à leur direction générale (52 % contre 28 % il y a deux ans).

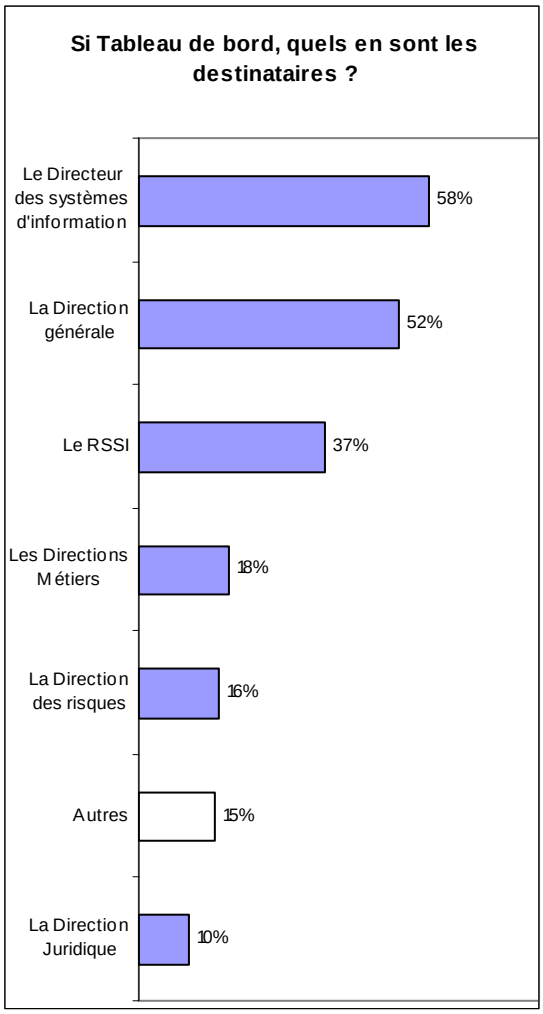

Figure 31 : destinataires du tableau de bord

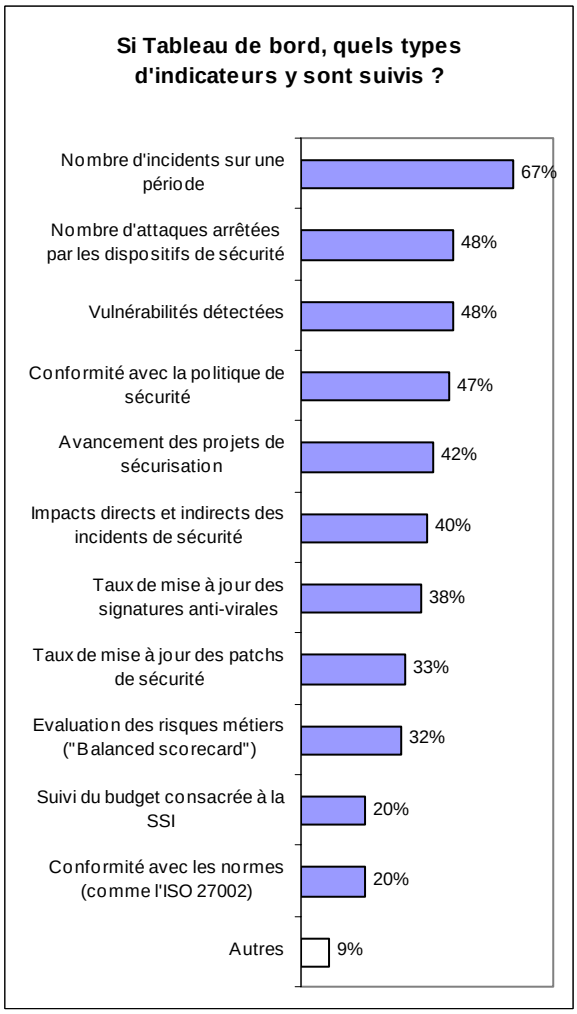

Figure 32 : indicateurs suivis dans les tableaux de bord

Les indicateurs inclus dans le tableau de bord restent majoritairement techniques. Les thèmes les plus importants en matière de pilotage (évaluation des risques, avancement des projets, suivi du budget…) sont peu usités.

Collectivités locales

- Présentation de l'échantillon
- Dépendance à l'informatique des collectivités
- Moyens consacrés à la sécurité de l'information par les collectivités
- 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 10 : Gestion des opérations et des communications
- Thème 11 : Contrôle des accès
- Thème 12 : Acquisition, développement et maintenance
- Thème 13 : Gestion des incidents - sinistralité
- Thème 14 : Gestion de la continuité d'activité
- Thème 15 : Conformité

Les Collectivités locales

Présentation de l'échantillon

Cette année encore, le CLUSIF s'est intéressé au secteur public. La cible de l'enquête 2006 a été élargie et ne se cantonne plus aux seules mairies importantes. L'échantillon interrogé s'établit comme suit:

- les mairies de plus de 30 000 habitants ;
- les communautés d'agglomérations de plus de 50 000 habitants ;
- les communautés de communes de plus de 20 000 habitants ;
- les conseils généraux ;
- les conseils régionaux.

Pour construire l'échantillon interrogé, la méthode des quotas a, ici encore, été utilisée. Un redressement a également été effectué de manière à ce que la répartition par catégorie des répondants corresponde parfaitement avec la réalité des collectivités françaises.

	Réalisé par le CLUSIF	**%**	redressement	**Données nationales**
Mairies	79	40,7 %	➔	34 %
Communautés de communes	27	13,9 %	➔	32 %
Communautés d'agglomération	42	21,6 %	➔	20 %
Conseils généraux	41	21,1 %	➔	11 %
Conseil régionaux	5	2,6 %	➔	3 %
Total	**194**	**100 %**		**100 %**

Figure 33 : échantillon des collectivités locales interrogées et redressement effectué

L'enquête a été réalisée entre le 24 janvier et le 10 mars 2008, essentiellement par téléphone (seulement 8 questionnaires complets par Internet). L'interlocuteur recherché en priorité était le RSSI ou FSSI mais une fois sur deux c'est le responsable informatique qui a répondu à l'enquête.

Les entretiens téléphoniques ont duré en moyenne 29 minutes et, sur 10 interlocuteurs contactés, environ seulement 2 ont accepté de répondre complètement au questionnaire. Donc pour obtenir 194 questionnaires complets, environ 1000 collectivités toutes catégories confondues ont été contactées au moins une fois.

Dépendance à l'informatique des collectivités

Le système d'information stratégique pour les collectivités

L'enquête confirme que l'informatique est perçue comme stratégique par une large majorité des collectivités, mais moins largement qu'en entreprise : 68 % contre 73 % d'entre elles ne pourraient tolérer une indisponibilité de moins de 24h de leurs outils informatiques. Ce nombre plonge à 59 % pour les conseils généraux ou régionaux.

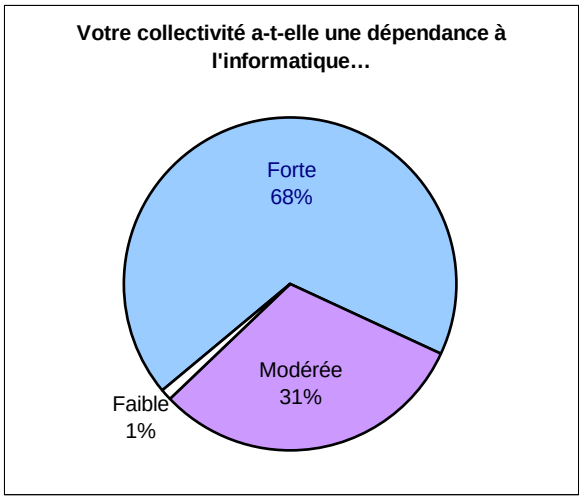

Figure 34 : dépendance des collectivités locales à l'informatique

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

Un budget informatique moyen de 1,5 million d'euros

Plus d'une collectivité sur deux de notre échantillon a accepté de révéler le montant de son budget informatique annuel, comprenant les dépenses d'investissement et de fonctionnement. A la même question, les entreprises ne sont que 25 % à accepter de répondre. Les responsables des collectivités connaissent-ils mieux leur budget informatique que les entreprises ou appliquent-ils une politique de transparence inconnue dans le privé ?

	MAIRIE	COMMUNAUTE DE COMMUNES	COMMUNAUTE D'AGGLOMERATIONS	CONSEIL GENERAL / REGIONAL
Budget informatique moyen	680 000 €	1 850 000 €	500 000 €	3 800 000 €

Figure 35 : budget informatique moyen par type de collectivité locale

Le budget informatique moyen est de 1,5 million d'euros mais ce chiffre cache une grande disparité. En effet, la majorité (53 %) des collectivités ont un budget inférieur à 500 000 €.

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

Les budgets alloués à la sécurité semblent en tout cas un peu mieux identifiés que dans le privé : 26 % des personnes interrogées ne savent pas quantifier leur budget sécurité, contre 31 % dans le privé. Les tendances ne sont pas nettes, même si les régions, départements et communautés de communes ont un budget sécurité plutôt en-dessous des 6 % du budget informatique. Quant aux villes, on trouve tout le spectre possible. La gestion de la sécurité est donc très liée à la politique locale.

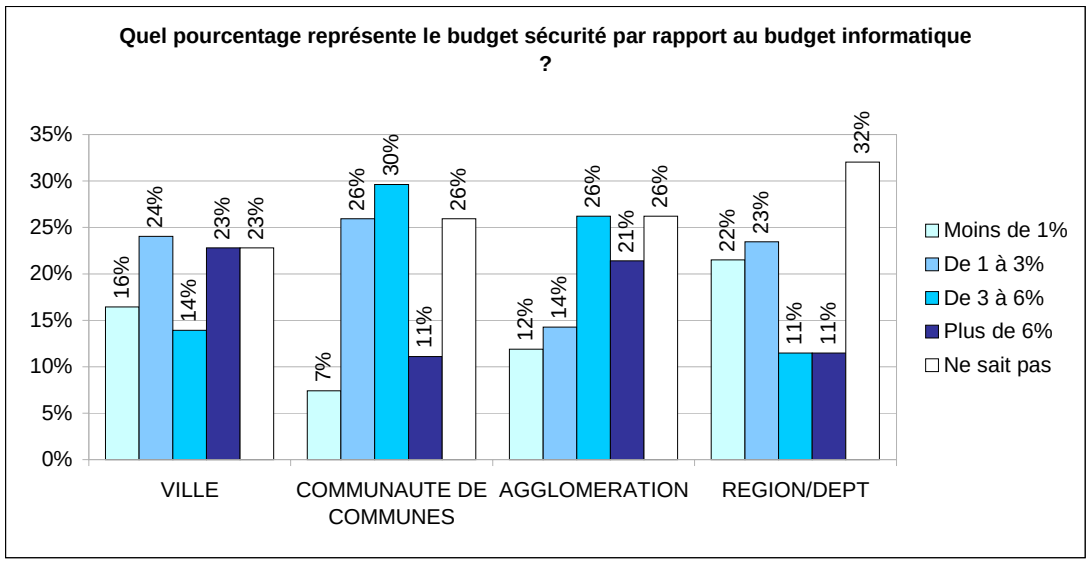

Figure 36 : part du budget informatique alloué à la sécurité dans les collectivités

En termes d'évolution, les budgets sécurité du public sont plus attentistes que dans le privé : 49 % étant constants en moyenne contre 43 % pour les entreprises. La lanterne rouge étant décernée aux villes : pour 55 %, le budget sécurité n'évolue pas. Là encore, la complexification des systèmes et leur ouverture sur l'extérieur ne se traduit donc pas en termes financiers. Les régions et départements au contraire investissent sensiblement dans la sécurité, avec une seconde place pour les communautés de communes.

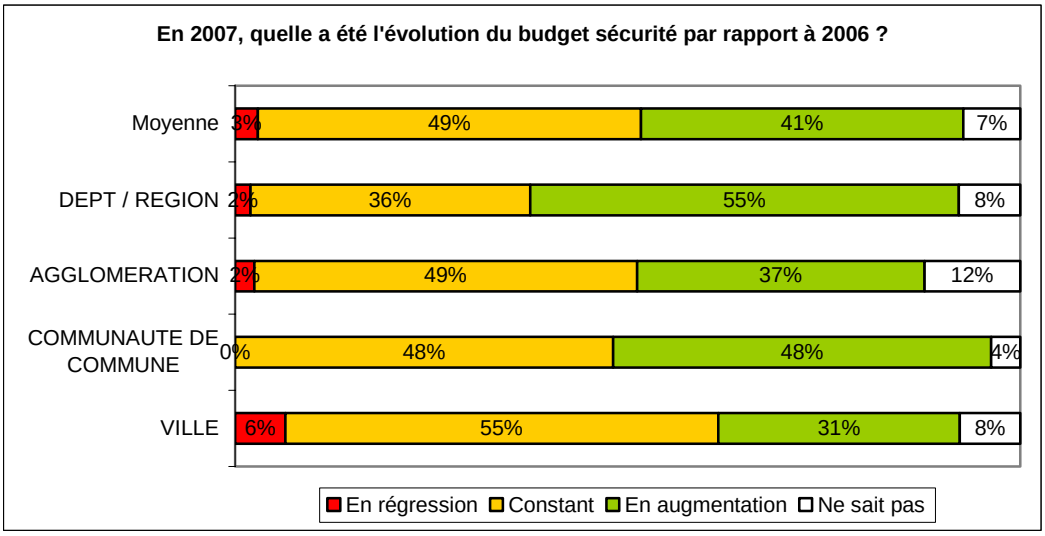

Figure 37 : évolution des budgets selon les types de collectivités

La recherche des freins à la conduite des missions de sécurité montre que le problème principal dans le ressenti des collectivités est le **manque de budget**. En effet, c'est la raison citée en frein premier presque 1 fois sur 2.

Les RSSI dans les collectivités souffrent également d'un manque d'entrain de la part de la hiérarchie, des utilisateurs et des services qui sont perçus une fois sur deux comme premier ou deuxième handicap. Ce manque d'implication du personnel est à relier au constat que nous faisons plus loin dans ce rapport concernant les immenses progrès à faire en sensibilisation du personnel des collectivités.

Le manque de personnel qualifié est cité comme troisième frein majeur. A vrai dire, il est rarement cité comme raison première (par 20 % des RSSI seulement) mais c'est la raison la plus souvent citée comme frein secondaire (34 %), en général après le manque de budget ou la réticence des utilisateurs.

Étonnamment, les contraintes organisationnelles dont se plaignent en premier lieu les RSSI des entreprises ne concernent que peu les collectivités.

Enfin, comme dans le privé cette fois, la DSI est une alliée du RSSI des collectivités.

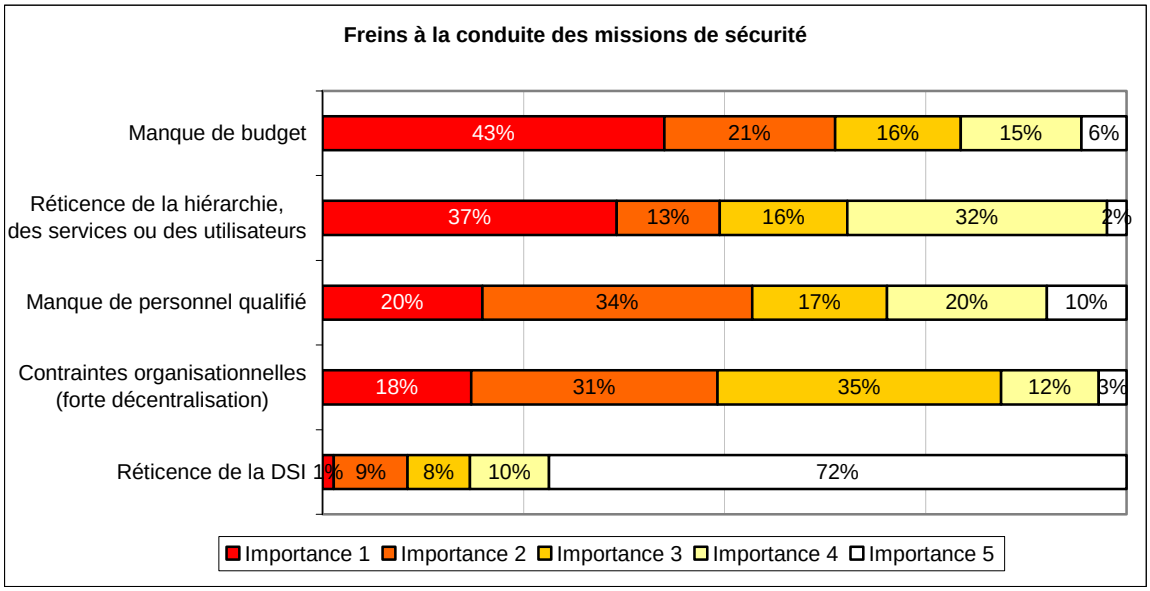

Figure 38 : freins à la conduite des missions de sécurité

En conclusion, les insuffisantes budgétaires, le manque de collaboration du personnel (ou leur manque de sensibilité aux enjeux de la sécurité de l'information) compliquent la tâche du RSSI dans les collectivités. Même si les directions des systèmes d'information soutiennent largement les projets, les moyens ne sont pas donnés et les complications inhérentes paraissent compliquées à surmonter.

Thème 5 : Politique de sécurité

Une sensibilité encore relative des collectivités à la formalisation de leur politique de sécurité de l'information (PSI)

Malgré une forte dépendance perçue à l'informatique, les collectivités semblent en retard dans la formalisation de leur PSI. Seulement 1 collectivité sur 3 l'a formalisée mais avec un soutien « en totalité » de la hiérarchie dans 70 % des cas ou « en partie » dans 22 % des cas.

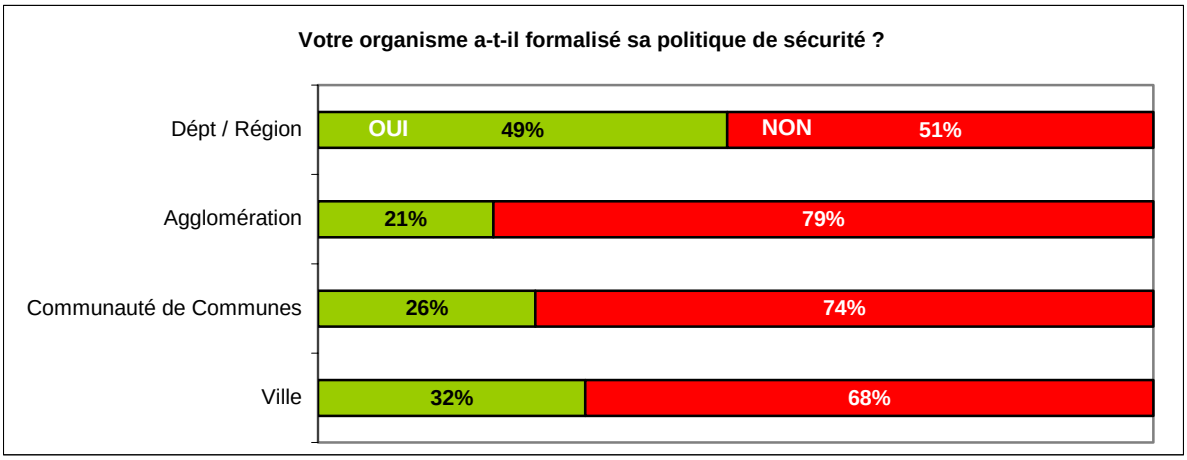

Figure 39 : existence d'une politique sécurité en fonction du type de collectivité

Une PSI essentiellement aux mains des informaticiens

L'élaboration de la PSI résulte très majoritairement du travail des informaticiens (95 %) et peu des autres acteurs de la collectivité (RSSI = 30 %, DRH = 22 %, etc.) de sorte que toutes les menaces et tous les risques ont pu ne pas être pris en compte.

Une PSI qui ne s'appuie que très minoritairement sur des normes exhaustives

Seulement 44 % des mairies qui ont formalisé leur politique de sécurité de l'information l'ont fait en se référant à des normes exhaustives telles que l'ISO 2700x ou le guide PSSI[8] de la Direction Centrale de la Sécurité des SI (DCSSI). Enfin, 15 % disent utiliser un autre cadre méthodologique : pourtant aucun autre cadre formel n'existe aujourd'hui pour les collectivités !...

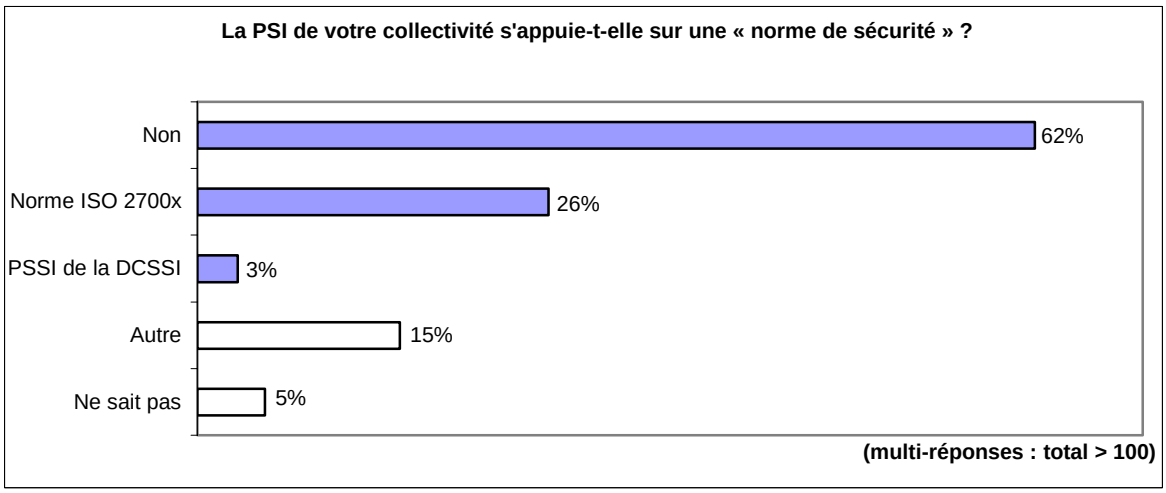

Figure 40 : appui de la PSI des collectivités sur une « norme » de sécurité

[8] Voir glossaire

Thème 6 : Organisation de la sécurité et moyens

Le RSSI, une fonction encore trop peu identifiée

Seulement 22 % des collectivités ont identifié clairement la fonction RSSI dans leur organisation. Ces résultats sont relativement proches de ceux de l'enquête précédente. Pour autant, seules 6 % des collectivités ont dévolu un rôle à temps plein à leur RSSI.

Dans les autres cas, on retrouve le DSI (37 %) ou bien le responsable informatique (31 %) pour endosser les responsabilités du RSSI. Apparaît également le consultant externe (pour 5 % des cas).

Par ailleurs, les collectivités sont en retard sur les entreprises dans la désignation d'un RSSI (37 % des entreprises le font contre seulement 22 % des collectivités).

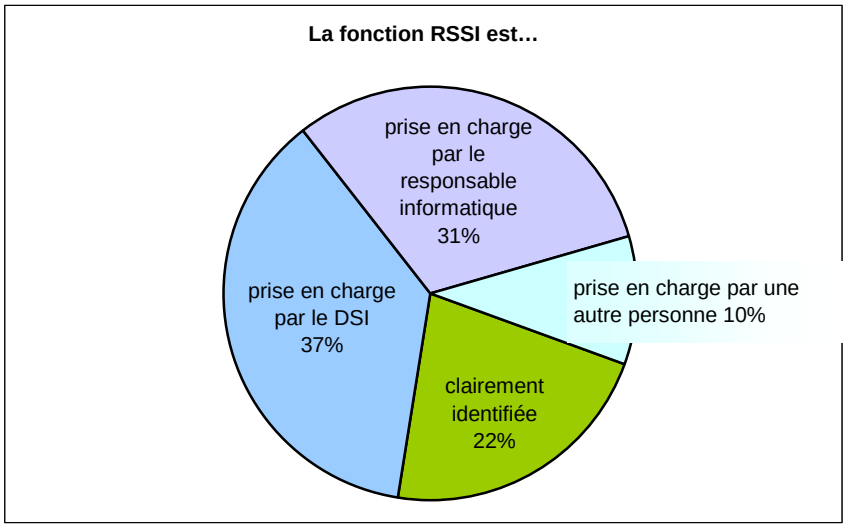

Figure 41 : identification de la fonction de RSSI

Le RSSI, un rattachement à la Direction des Systèmes d'Information

La tendance depuis la précédente enquête s'est encore accentuée puisque dans 61 % des cas, le Responsable de la Sécurité des Systèmes d'Information est rattaché à la Direction des Systèmes d'Information. On peut cependant noter qu'un petit nombre de collectivités ont directement rattaché le RSSI à l'élu (ou à son cabinet) de plus haut niveau. Ces collectivités marquent ainsi une volonté forte de protection des biens immatériels, même si elles restent encore rares.

La démarche entamée côté entreprises, rattachement à la Direction Générale, tarde à se concrétiser dans les collectivités.

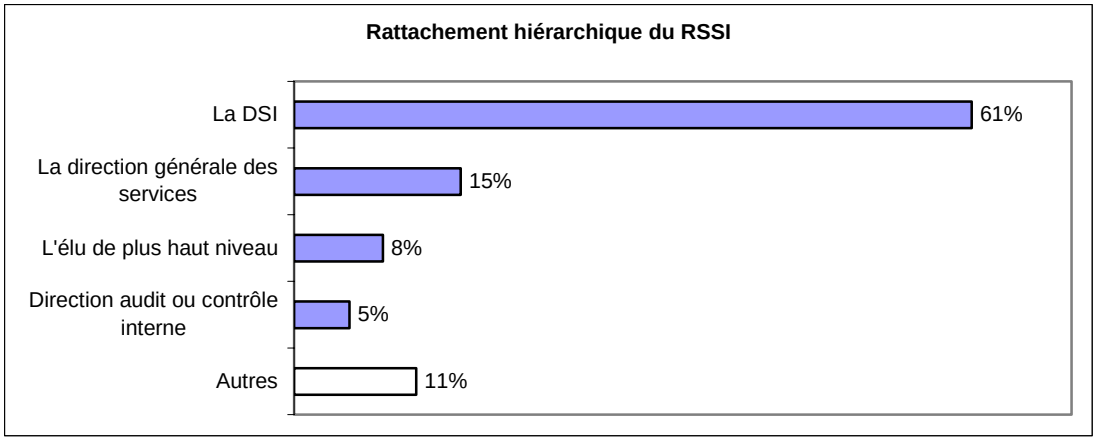

Figure 42 : rattachement hiérarchique du RSSI dans les collectivités

Le RSSI : une fonction équilibrée entre l'opérationnel, le technique et le fonctionnel

Le RSSI voit son rôle réparti en 3 tiers quasiment équivalents. Cette répartition est classique et comparable à ce qu'on trouve ailleurs.

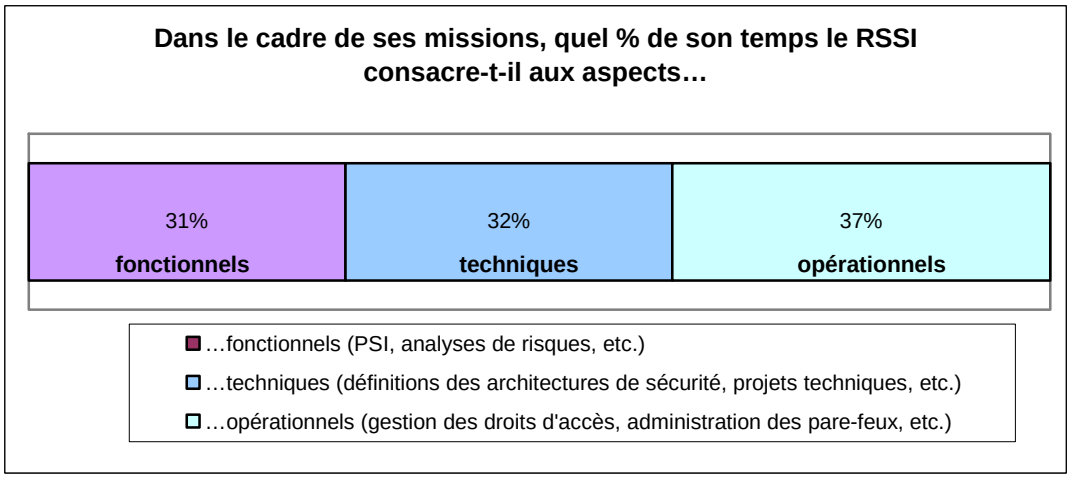

Figure 43 : répartition des missions du RSSI

Les effectifs dédiés en permanence à la sécurité des systèmes d'information sont rares

Près de la moitié des collectivités n'ont pas d'équipe sécurité permanente. Pour les autres, cette équipe dépasse rarement 2 personnes. Les effectifs dédiés à la sécurité sont donc souvent de très petite taille, ce qui est généralement aussi le cas pour la taille de l'ensemble de l'équipe informatique.

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

Des collectivités moins « orientées risques » que les entreprises

42 % des collectivités ont réalisé une analyse globale, au moins partielle, des risques liés à la sécurité du SI, et un plan d'action a été argumenté et défini sur cette base pour 53 % d'entre elles.

Mais seulement 16 % des collectivités déclarent que l'analyse des risques couvre l'ensemble du périmètre de leur système d'information, et donc un niveau de maturité moins élevé que dans les entreprises.

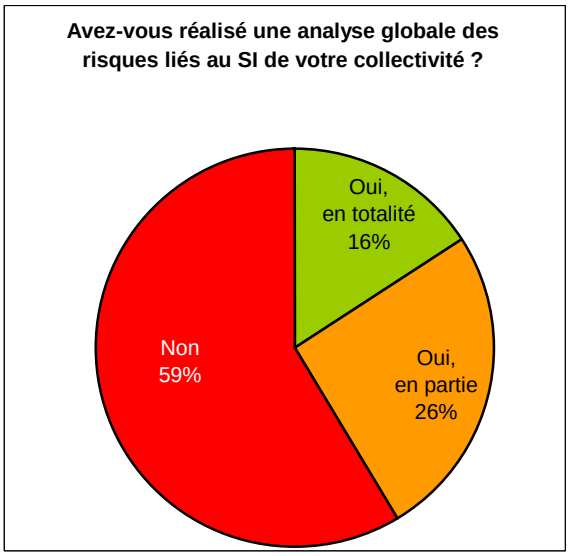

Figure 44 : analyse des risques réalisée par les collectivités

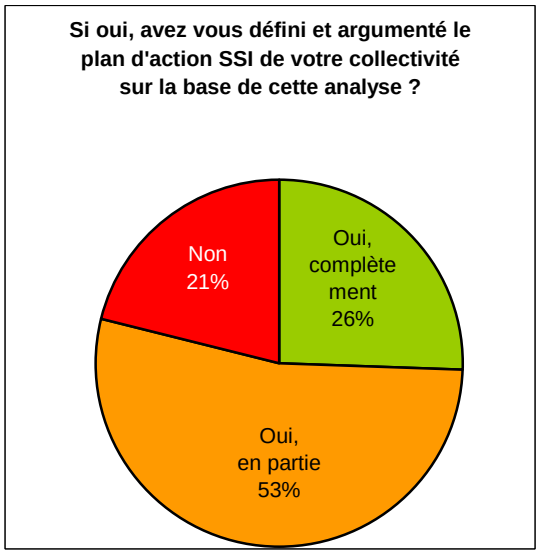

Figure 45 : processus d'amélioration de la sécurité du SI pour les collectivités

En revanche, la prise en compte de la sécurité dans les projets est plus fréquente, puisque 75 % des collectivités réalise des analyses de risques projet, dont 36 % de manière systématique.

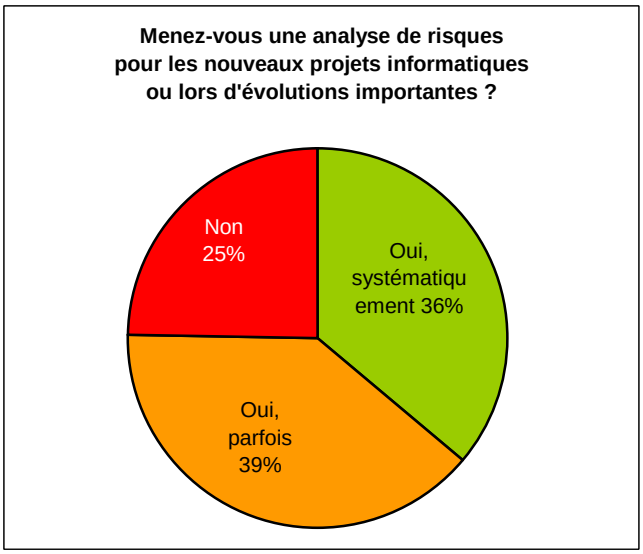

Figure 46 : prise en compte des risques dans les projets

Les principaux acteurs dans l'identification des risques de sécurité sont :

- le RSSI (32 %),
- le chef de projet informatique (13 %),
- le propriétaire d'un actif ou le maître d'ouvrage (6 %),
- autre ou indéterminé dans la moitié des cas.

La culture « risque » est très peu courante au niveau des responsables métiers ou maîtres d'ouvrage. Le RSSI est le responsable le plus souvent cité, mais dans seulement un tiers des cas, ce qui tendrait à confirmer qu'il ne s'agit généralement pas d'une analyse formelle s'appuyant sur une méthode dédiée demandant une certaine expérience et des compétences spécifiques.

Thème 8 : Sécurité liée aux Ressources Humaines

Par rapport aux entreprises, les chartes sécurité sont moins répandues puisque 41 % seulement des collectivités se sont dotées d'un tel document. Ces chartes sont généralement communiquées aux instances représentant le personnel. En revanche, et c'est une différence sensible par rapport aux entreprises, les sanctions disciplinaires sont beaucoup moins intégrées dans les chartes : seulement un tiers des collectivités les intègrent dans le règlement intérieur contre, rappelons-le, 56 % des entreprises qui disposent d'une charte.

Dans les collectivités, les chartes sont probablement davantage édictées pour se conformer à des usages réglementaires que pour devenir un élément important de la politique de sécurité de l'information, même si la proportion de chartes en cours d'élaboration est très significative (18 % des collectivités). La dissociation entre les principes édictés dans une charte et la sanction du non respect de ces principes fait douter de l'efficacité des chartes de sécurité dans les collectivités.

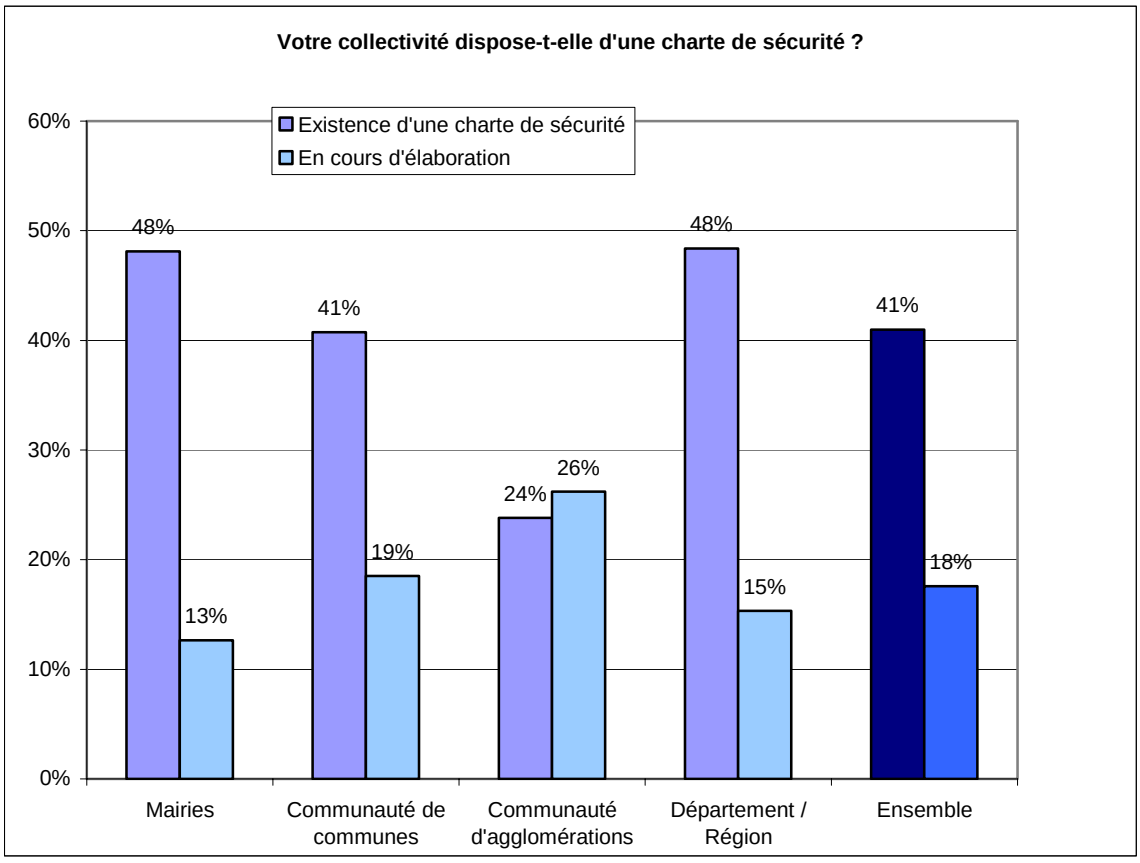

Figure 47 : existence d'une charte de sécurité

Pour ce qui concerne la sensibilisation des utilisateurs, des progrès majeurs restent à faire : seules 23 % des collectivités ont lancé des actions dans ce domaine et 10 % en préparent. Comme conséquence de ces mauvais chiffres, il ne faut pas s'étonner du manque d'implication du personnel dans le suivi de la politique de sécurité et que le RSSI ressente la réticence des utilisateurs et des services comme frein majeur dans la conduite de ses missions !

En matière de moyens, on retrouve la hiérarchie classique des outils : publications, sessions de sensibilisation et formation. Mais les impacts de ces actions ne sont pas mesurés dans près de neuf collectivités sur dix.

L'utilisateur du système d'information est le dernier rempart qui le protège des menaces qui peuvent peser sur lui. Ne pas l'impliquer dans la politique de sécurité revient à se priver d'un allié précieux.

Thème 10 : Gestion des opérations et des communications

Des collectivités plus frileuses vis-à-vis des nouvelles technologies que les entreprises

Le graphique ci-dessous donne des indications sur l'usage des nouvelles technologies, et en particulier des technologies de mobilité, au sein des collectivités.

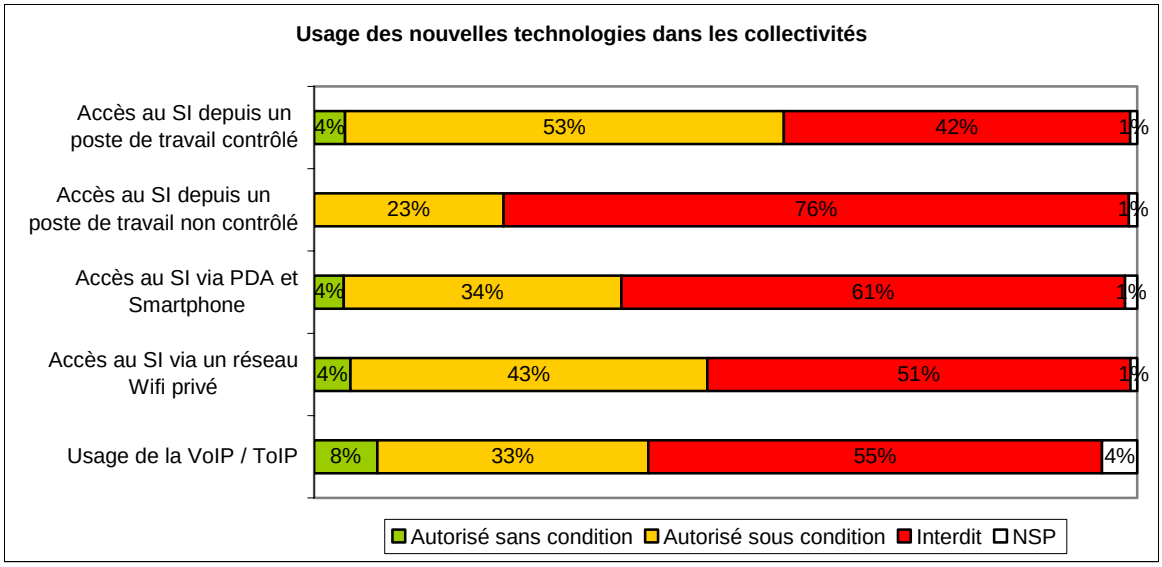

Figure 48 : mobilité et accès au SI dans les collectivités

Les accès extérieurs depuis les portables sont moins développés dans les collectivités que dans les entreprises (42 % d'interdiction contre 13 %) sauf dans le cas des conseils régionaux et généraux ou au contraire l'usage est quasi généralisé avec seulement 11 % d'interdiction. La même différence entre les conseils généraux et régionaux et les autres collectivités locales se retrouve au niveau des accès depuis des postes de travail non identifiés. L'usage des PDA et *smartphone* est, lui, à peu près du même niveau.

Concernant la téléphonie IP, la différence est importante entre entreprises et collectivités, plus particulièrement les conseils généraux et régionaux. Ceux-ci sont seulement 35 % à interdire la VoIP et la ToIP, alors que leurs confrères des communes et agglomérations sont beaucoup plus proches du monde des entreprises.

En synthèse on observe un déploiement plus important des nouvelles technologies au sein des conseils généraux et régionaux, avec notamment une ouverture à la mobilité externe et à la ToIP supérieure au niveau moyen d'équipement constaté sur l'ensemble des acteurs interrogés, entreprises et collectivités confondues.

Pour ce qui concerne la protection des accès nomades, les collectivités utilisent globalement les mêmes types de technologies que les entreprises avec quelques différences notables sur le niveau de cette utilisation : l'authentification forte est plus répandue dans les entreprises (56 % dans les entreprises contre 40 % dans les collectivités), de même que les pare-feu personnels (25 % contre 16 %). A l'inverse, les outils de chiffrement des données locales sont plus répandus dans les collectivités (29 % contre 14 %).

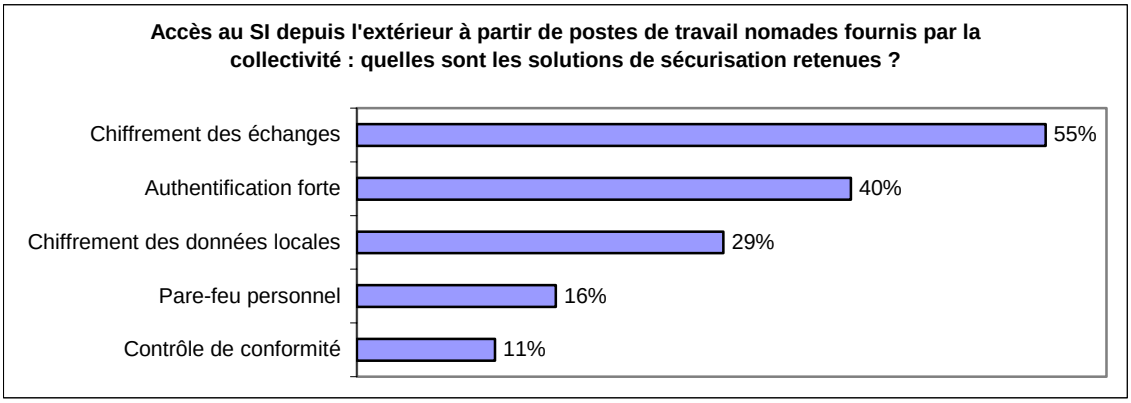

Figure 49 : sécurisation des accès au SI via des postes nomades fournis par les collectivités

Un niveau d'équipement correct pour les technologies de sécurité « de base »

Les collectivités disposent d'un bon niveau d'équipement pour les technologies de sécurité les plus classiques : antivirus, antispam et pare-feu réseau. Ce niveau d'équipement est plus en retrait que les entreprises pour des outils comme le firewall personnel, les IDS ou les IPS. Une donnée surprenante : les collectivités utilisent pour un tiers d'entre elle des solutions de gestion des journaux (Security Information Manager – SIM).

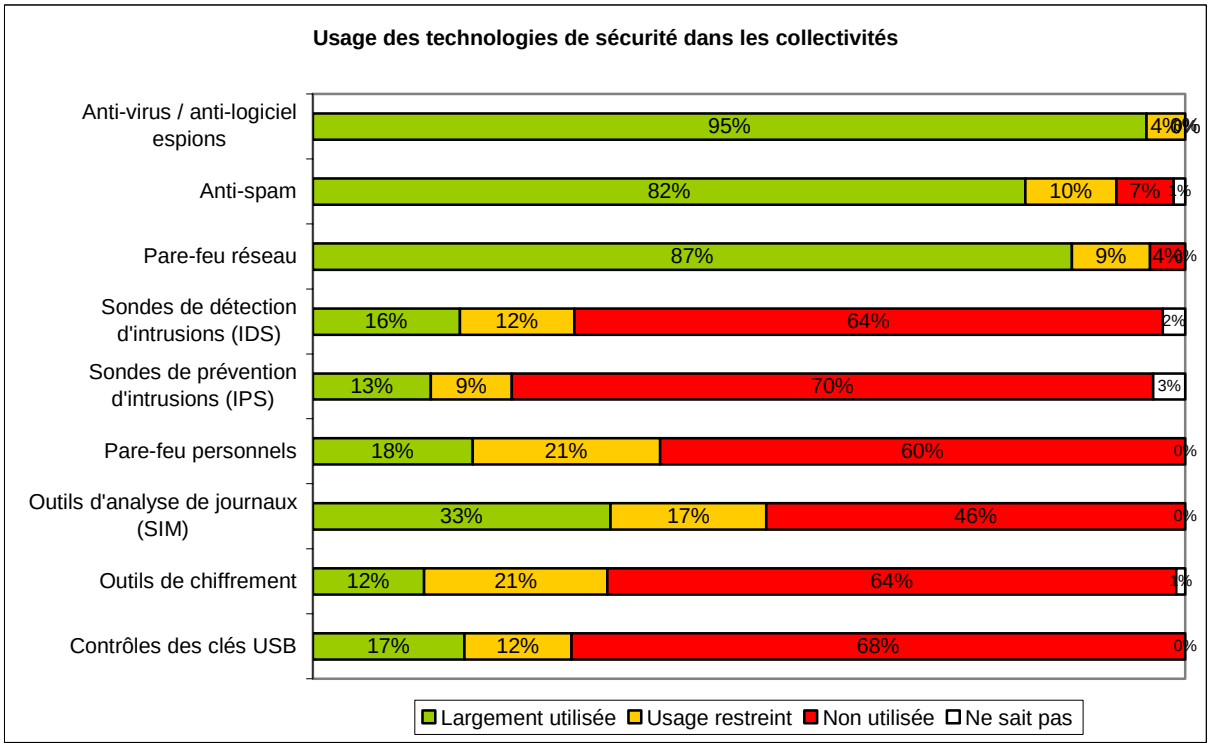

Figure 50 : technologies de sécurité utilisées dans les collectivités

Thème 11 : Contrôle des accès

Le contrôle des accès logiques est envisagé sous trois aspects :

- les moyens d'authentification forte pouvant être utilisés,
- la manière de gérer et mettre en œuvre les droits d'accès des utilisateurs,
- les systèmes de contrôle d'accès centralisés et d'authentification unique (Single Sign-On).

Afin de comparer avec la situation 2006, qui ne prenait en compte que les municipalités, deux graphiques sont proposés : l'ensemble des collectivités territoriales, puis les mairies uniquement.

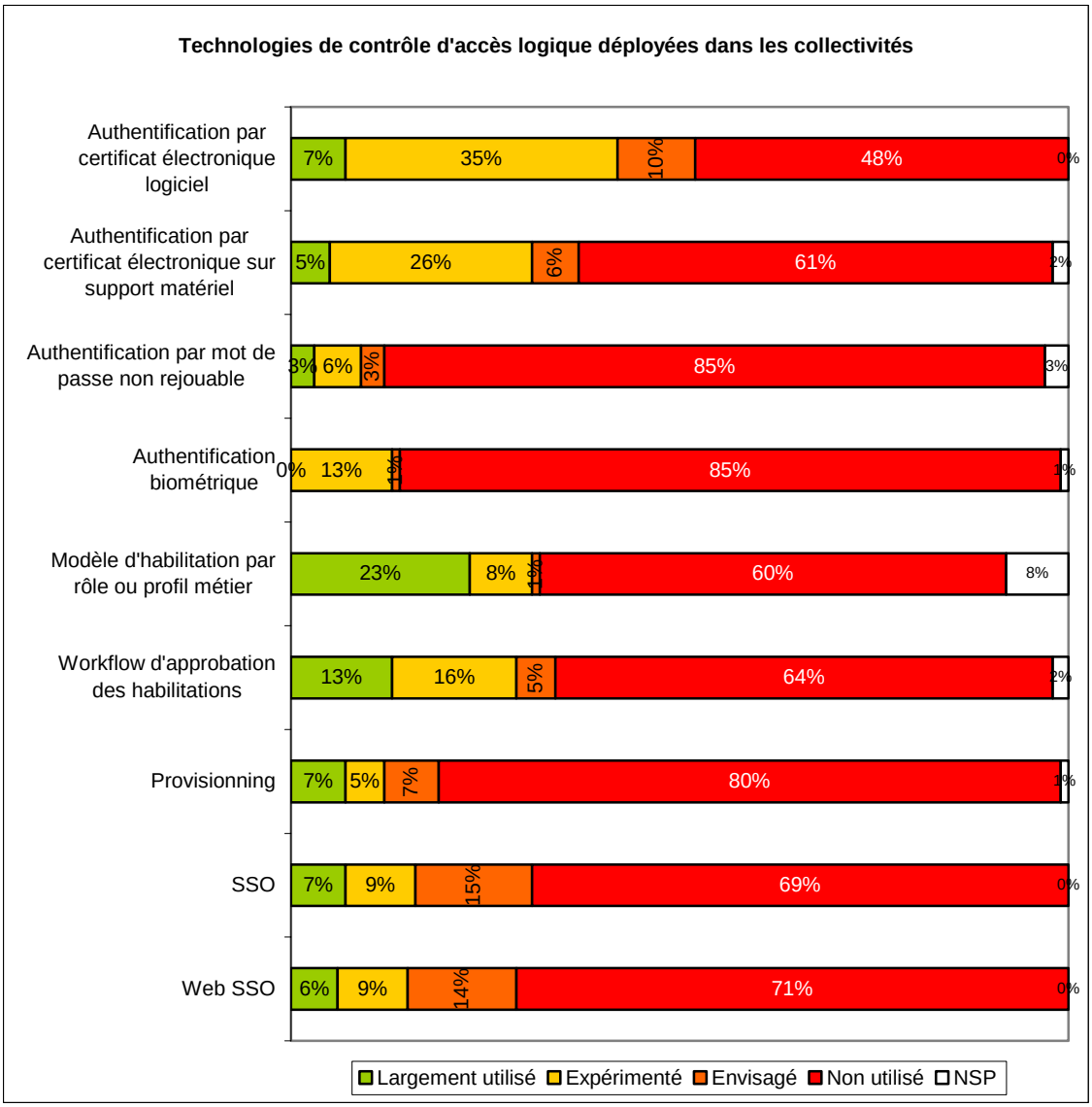

Figure 51 : technologies de contrôle d'accès logique utilisées dans les collectivités

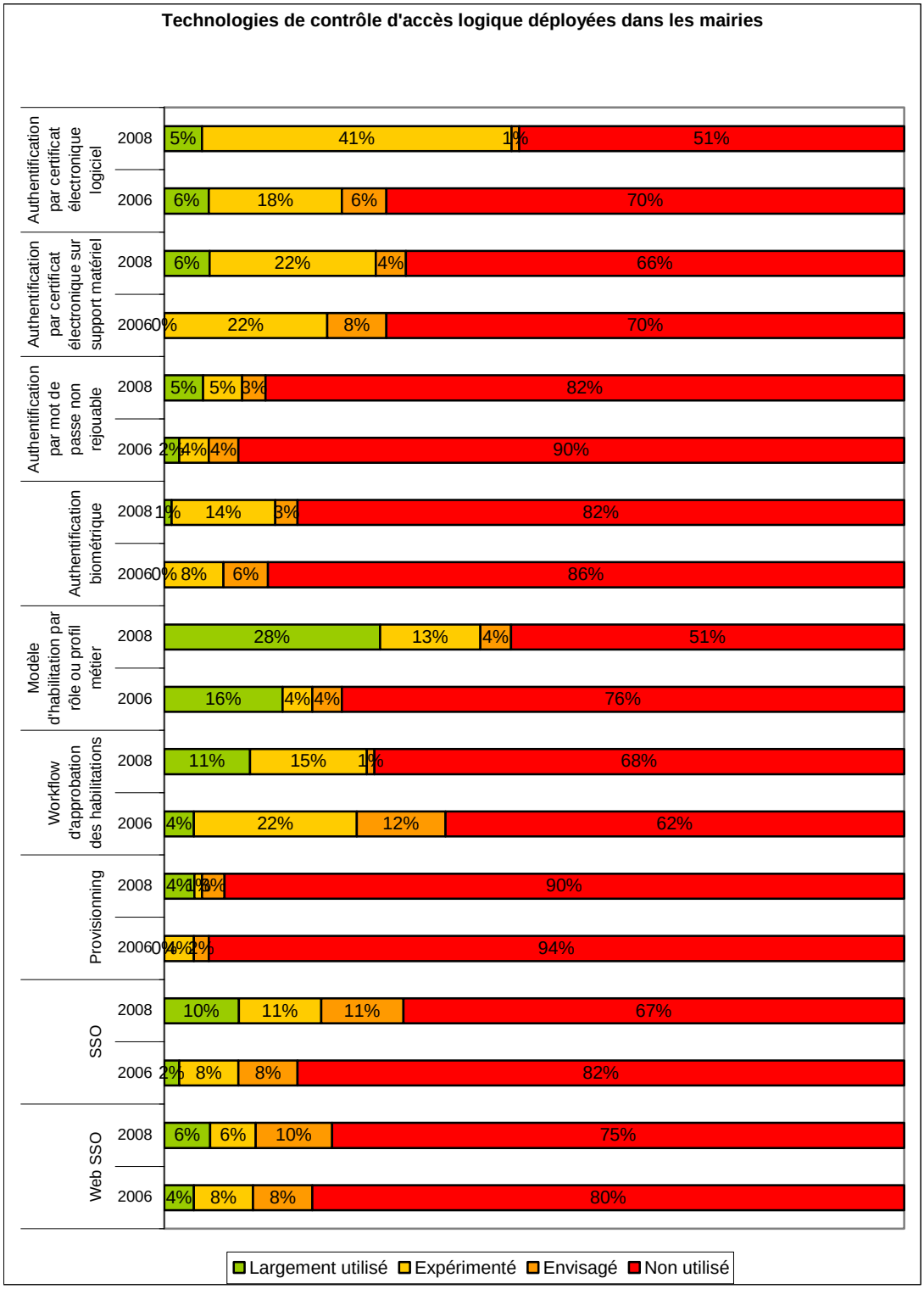

Figure 52 : technologies de contrôle d'accès logique utilisées dans les mairies, en 2008 et 2006

Authentification forte par certificat : un regain d'intérêt dans les mairies

L'authentification forte connaît le succès auprès des collectivités, en tout cas sous la forme de certificats, le plus souvent sur support logiciel, mais aussi sur support matériel. La biométrie commence à intéresser, alors que les calculatrices à mots de passe non *rejouables* ne suscitent guère l'intérêt.

A l'inverse des entreprises, on constate une grande différence par rapport au constat effectué en 2006 sur les mairies. La situation n'a pas fondamentalement changé pour ce qui est des certificats sur support matériel, mais les autres moyens d'authentification forte ont eux connu une progression visible : une mairie sur quatre s'est nouvellement convertie aux certificats sur support logiciel. On note aussi un léger gain d'intérêt pour la biométrie, tout du moins en expérimentation ou en déploiement partiel.

On constate enfin une forte disparité selon le type de collectivité : les mairies semblent privilégier les certificats logiciels, alors que les régions et départements recourent beaucoup plus fréquemment aux autres technologies.

Gestion des habilitations : des progrès dans les mairies

Alors que seules quatre collectivités sur 10 ont mis en place une gestion des droits par rôle ou profil métier, ou du moins souhaitent le faire, on constate néanmoins que ce modèle progresse, puisque c'est près d'une mairie supplémentaire sur quatre qui a fait ce choix au cours des deux dernières années.

La mise en œuvre d'un modèle RBAC s'accompagne logiquement d'un *workflow* de validation des habilitations : le nombre de mairies ayant initié ou généralisé un tel dispositif a augmenté depuis 2006 dans les mêmes proportions que celles ayant choisi une gestion des droit par profil métier. Par contre, les systèmes de *provisioning*, totalement inexistant en 2006, ne suscitent qu'à peine plus d'intérêt aujourd'hui.

Contrôle d'accès centralisé : avantage aux régions et départements

Les systèmes de contrôle Web et SSO, utilisés ou expérimentés par seule une mairie sur 10 en 2006, ont connu une progression notable, puisque cette proportion a doublé en deux ans, et qu'une mairie sur 10 envisage d'en déployer un sur 2008.

Les régions et départements ont là encore une nette avance sur les autres collectivités territoriales : les deux-tiers d'entre eux ont déjà sauté le pas du SSO, et la moitié pour le Web SSO. Par contre, les communautés de commune ou d'agglomération sont très frileuses face à ces technologies : trois communautés d'agglomérations sur quatre, et 4 communautés de communes sur cinq n'envisagent pas de s'en pourvoir.

Thème 12 : Acquisition, développement et maintenance

Veille et gestion des vulnérabilités : une situation qui se stabilise

Les chiffres sont homogènes par rapport aux entreprises. 61 % des collectivités réalisent une activité de veille sur les vulnérabilités.

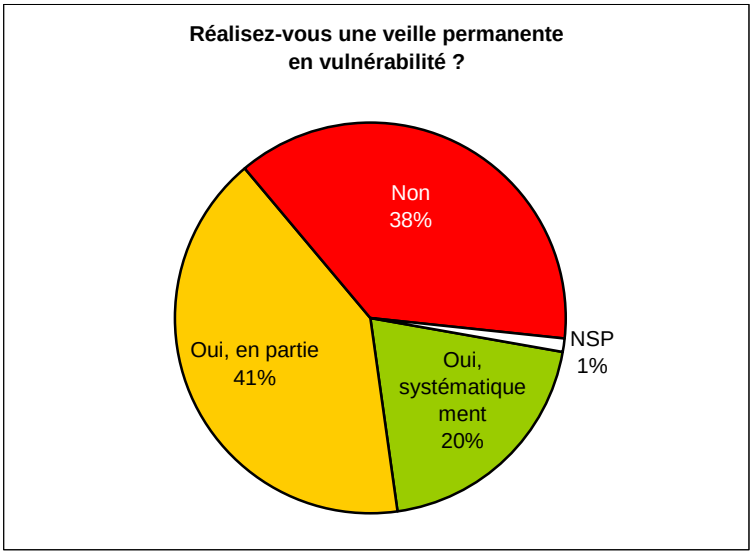

Figure 53 : réalisation d'une veille permanente en vulnérabilité dans les collectivités

Maintenance et déploiement de correctifs de sécurité

Plus de la moitié des collectivités formalisent les procédures de déploiement des correctifs.

Parmi celles qui ont mis en place des procédures de déploiement des correctifs, 84 % des collectivités réalisent les déploiements de leurs correctifs « poste de travail » en moins d'une journée, ce qui montre que le délai de déploiement des correctifs dans les collectivités locales est assez similaire à celui des entreprises. Ici aussi, force est de constater que si la pratique de déploiement des correctifs est maintenant assez courante pour les postes de travail, elle reste peu répandue pour les environnements serveurs.

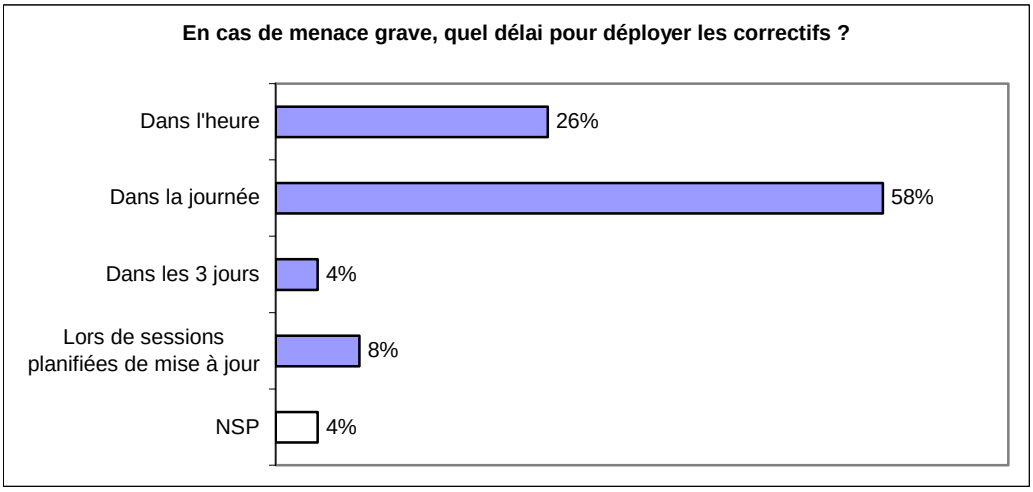

Figure 54 : délai de déploiement des correctifs dans les collectivités

Thème 13 : Gestion des incidents - sinistralité

Une prise en compte balbutiante des incidents de sécurité

Les collectivités ont encore, à l'instar des entreprises, une gestion peu organisée des incidents avec dans un peu plus d'un quart de celles interrogées une cellule dédiée (6 %) ou participant (20 %) à la gestion de ces incidents.

Cela conduit 5 % des collectivités seulement à déposer plainte pour des incidents de sécurité alors que, par exemple, 38 % d'entre elles déclarent avoir subi des vols ou disparitions de matériels informatiques. Autre conséquence plus inquiétante encore : seules 7 % des collectivités déclarent effectuer une évaluation financière des incidents qu'elles subissent.

On note sur ces points une forte disparité en fonction du type de collectivités. Ainsi régions et départements déclarent à 19 % avoir porté plainte pour des incidents de sécurité au cours de l'année.

Une vision contrastée des incidents

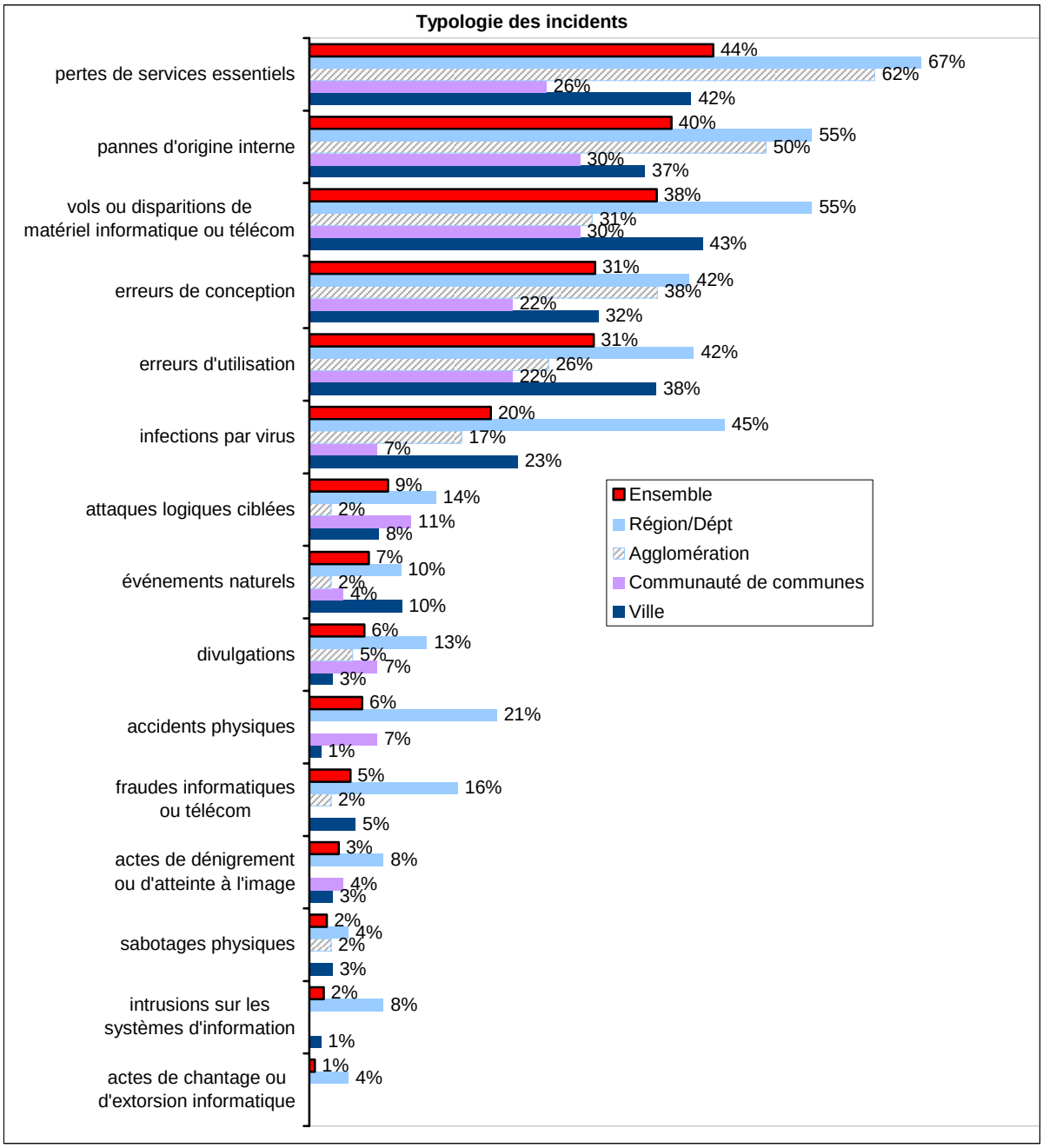

Figure 55 : typologie des incidents pour les collectivités

Les vols ou disparitions de matériels informatiques sont toujours une cause importante de sinistralité. Et les intrusions sur les systèmes d'information (1 à 8 %) et autres fraudes (2 à 16 %) atteignent des niveaux non négligeables.

Une collectivité sur 5 touchée par les virus

Parmi les 20 % ayant subi une infection virale, 13 % ont une origine interne et 24 % ont une origine indéterminée.

De l'aveu même des RSSI, l'impact de ces infections n'est pas négligeable une fois sur cinq environ.

Lorsque les collectivités sont victimes d'infections virales, elles le sont en moyenne 11 fois, certaines l'ayant été plus de 100 fois…

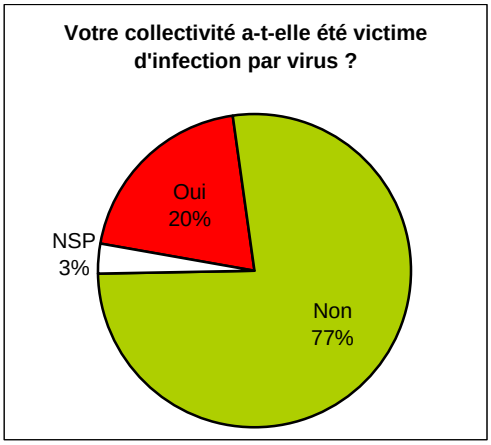

Figure 56 : taux d'infection par virus dans les collectivités

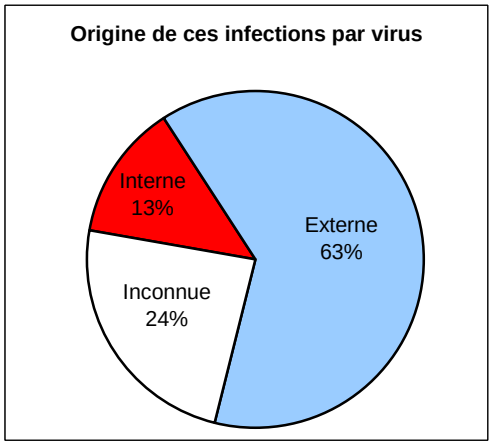

Figure 57 : origine des infections virales pour les collectivités

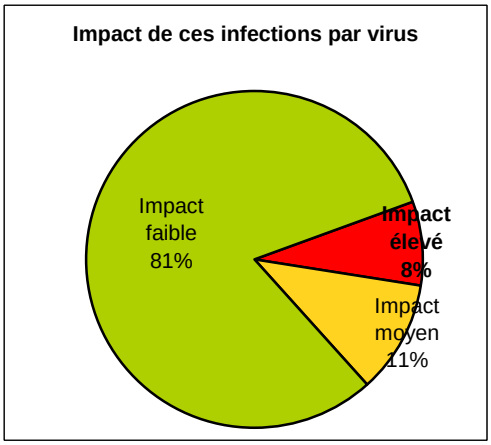

Figure 58 : impact des infections virales pour les collectivités

60 % des collectivités touchées …

Bien qu'il n'y ait pas de cellule de collecte et de traitement des incidents au sein des collectivités, plus d'un RSSI sur deux estime avoir subi des sinistres l'année passée. 7 % d'entre eux en recensent même plus de 50 et certains plus de… 400 !

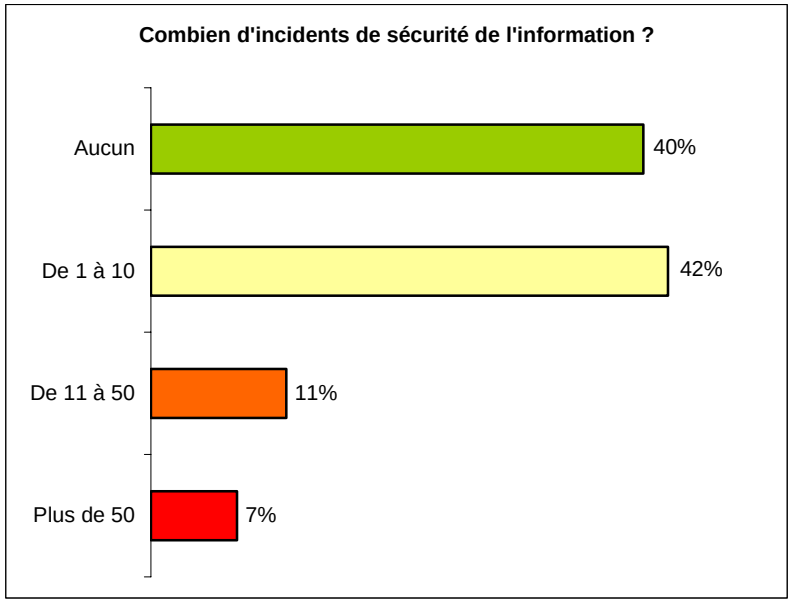

Figure 59 : nombre d'incidents de sécurité recensés l'an dernier par les collectivités

… pour un bilan peu flatteur

La conclusion est que si 60 % des collectivités confessent des incidents, 74 % ne sont pas organisées pour collecter et traiter ces événements, 95 % ne déposent jamais de plainte et 93 % n'évaluent même pas l'impact financier de ces incidents.

Thème 14 : Gestion de la continuité d'activité

Gestion de la continuité de l'activité : en légère progression mais il reste beaucoup à faire

Là où les entreprises sont 61 % à avoir formalisé totalement ou en partie un processus de gestion de la continuité, les collectivités ne sont que 38 %. Autrement dit, cela signifie qu'il y a encore près des 2/3 d'entre elles qui n'ont aucune solution de reprise après incident majeur.

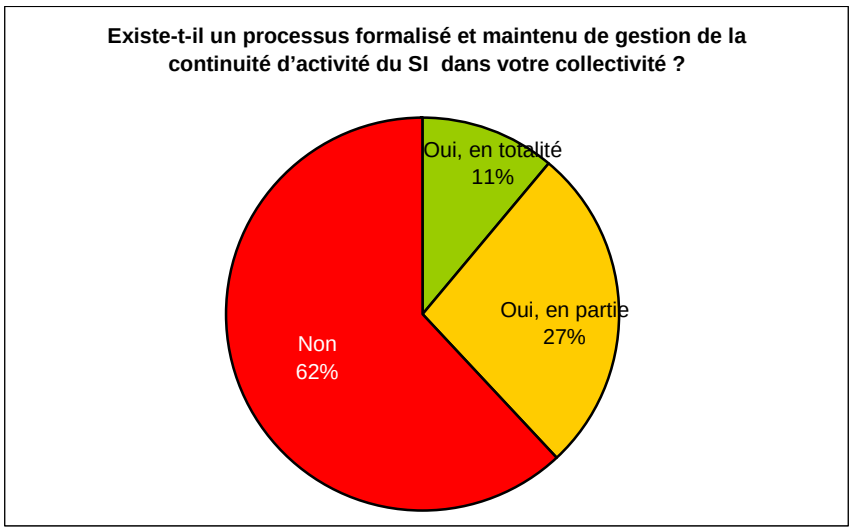

Figure 60 : existence d'un processus formalisé de gestion de la continuité d'activité du SI

Le constat est terrible mais il est atténué par une nette tendance à l'amélioration que l'on constate en s'intéressant aux mairies. Lors de notre précédente enquête en 2006, 72 % des mairies de plus de 30 000 habitants n'avaient pas de PCA, aujourd'hui ce chiffre chute à 61 %.

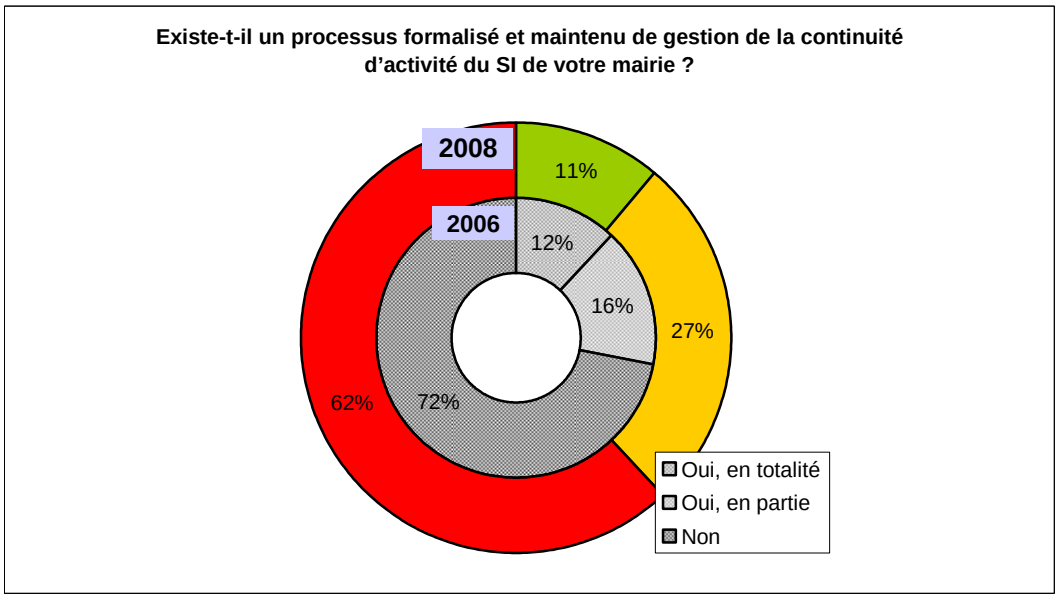

Figure 61 : PCA dans les mairies de plus de 30 000 habitants, en 2008 et 2006

On peut espérer que ces améliorations concernent les collectivités dans leur ensemble et que cette tendance positive va continuer et s'amplifier. Ici encore, le travail de sensibilisation des organisations professionnelles et des associations comme le CLUSIF n'est pas terminé.

La maintenance : décalage important avec le monde des entreprises

56 % des collectivités disposant d'un plan de continuité réalisent au moins une fois par an des tests et des mises à jour. Seules 11 % d'entre elles déclarent réaliser des tests multiples chaque année, ce qui est très inférieur par rapport aux chiffres rencontrés dans les entreprises (38 %).

Et pourtant, une solution de continuité qui n'est pas testée de manière régulière présente de forts risques de ne pas être opérationnelle le jour où elle sera enclenchée suite à un sinistre…

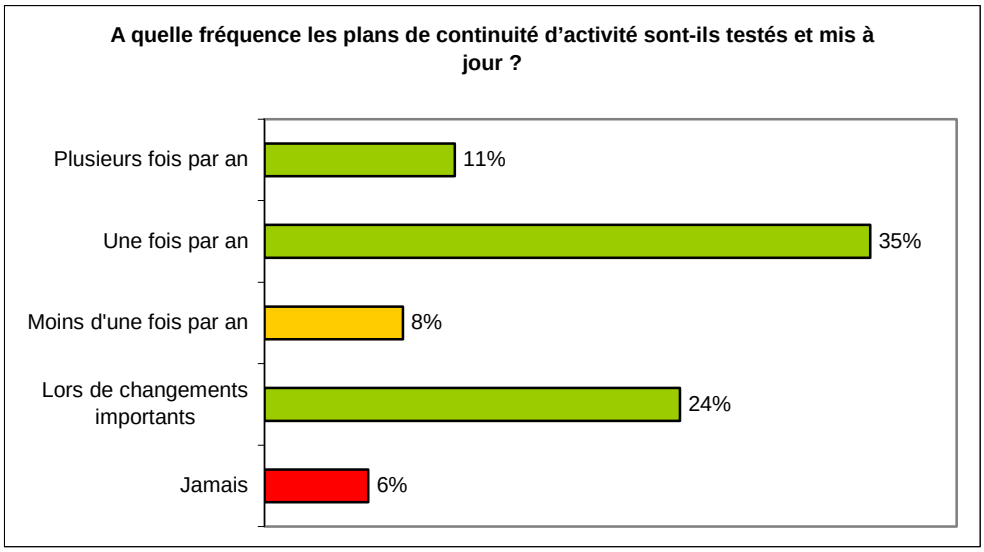

Figure 62 : tests et mise à jour des plans de continuité d'activité

On constate également que les collectivités attendent et/ou profitent de changements importants pour tester les plans de continuité (24 % d'entre-elles) alors que dans le monde des entreprises, seules 10 % d'entre-elles le font dans les mêmes circonstances.

Secours informatique : les sauvegardes plébiscitées

Les résultats présentés pour les solutions de secours sont également légèrement différents entre le secteur privé et le secteur public. Plus de 9 collectivités sur 10 utilisent des moyens de sauvegardes classiques contre 79 % en entreprises.

Il est à noter que les tendances et résultats sont sensiblement identiques en proportion si on compare ceux des Villes, des communautés, des agglomérations ou enfin des régions.

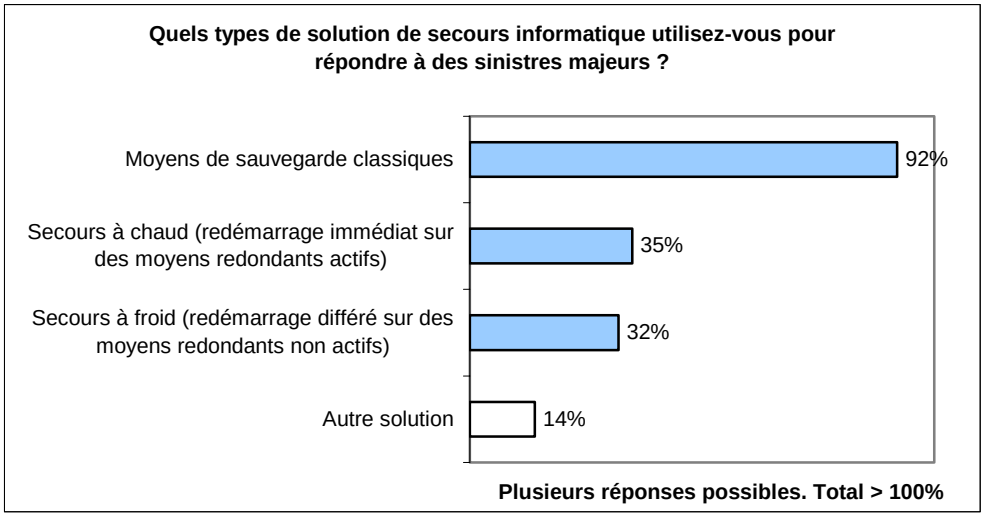

Figure 63 : solutions de secours informatique

Il apparaît clairement que le marché des collectivités manque encore de moyens. En effet, la grande majorité d'entre-elles (92 %) n'utilisent toujours que des moyens de sauvegardes classiques contre 79 % pour les entreprises.

Les technologies éprouvées de secours à chaud / à froid sont beaucoup plus présentes dans les entreprises (53 % / 42 %) par rapport aux collectivités (35 / 32 %).

Thème 15 : Conformité

Ce thème aborde les éléments liés à la conformité, à travers 3 sujets :

- le respect des exigences de la **Loi Informatique et Libertés**,
- le contrôle des niveaux de sécurité à travers les **audits**,
- le suivi des niveaux de sécurité grâce aux **tableaux de bord** de sécurité.

1/ Les obligations liées à la Loi Informatique et Libertés

Des collectivités plus en avance que les entreprises

La situation des collectivités vis-à-vis de la Loi Informatique et Liberté n'est pas parfaite, même si elle est légèrement meilleure que celle des entreprises (69 % de conformité totale, contre 64 % pour les entreprises). Dans les mairies, cette situation semble toutefois s'être dégradée (69 % de conformité totale, contre 84 % en 2006).

Par ailleurs, 30 % des collectivités déclarent avoir nommé un CIL, contre 25 % pour les entreprises. Là encore les mairies sont en recul par rapport à 2006, mais nous pouvons certainement supposer que ces résultats sont plus proches de la réalité, la notion de Correspondant Informatique et Liberté s'étant largement précisée en 2 ans.

2/ Les audits de sécurité

Une pratique de l'audit insuffisante

Plus de 40 % des collectivités mènent un audit au moins une fois par an, alors que 56 % n'en mènent pas du tout.

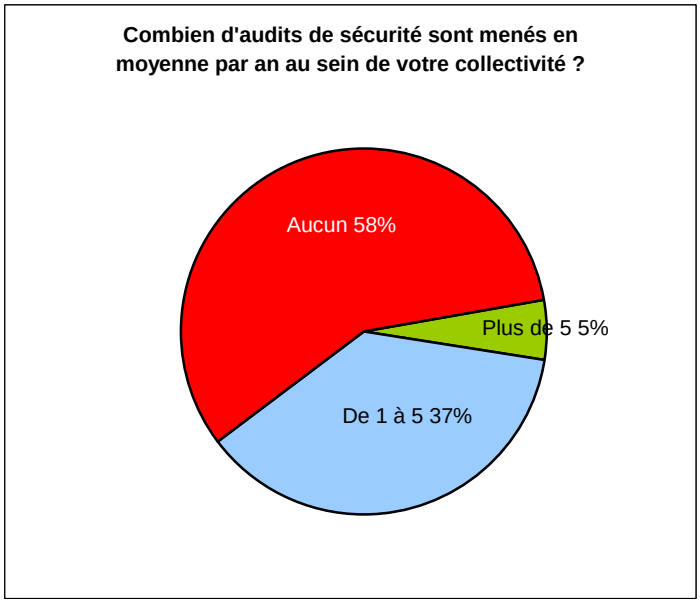

Figure 64 : nombre d'audits de sécurité menés par an par les collectivités

Le chiffre de 41 % est en nette régression par rapport à 2006 (à périmètre constant, c'est-à-dire en ne considérant seulement que les mairies, 42 % contre 56 %, il y a deux ans).

Les audits réalisés traitent plus souvent des aspects techniques (vérifications de configuration technique, tests d'intrusion) que des aspects organisationnels.

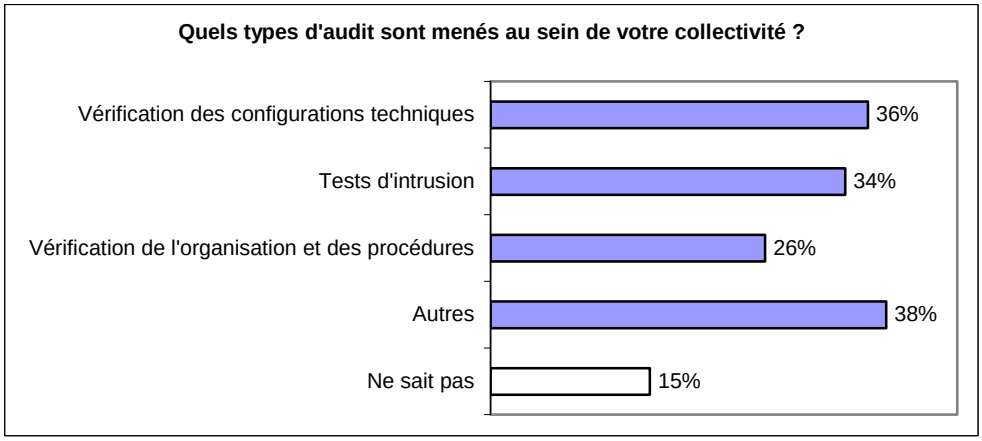

Figure 65 : types d'audits de sécurité

Ces audits sont une fois sur trois motivés par la politique interne ou des exigences contractuelles ou réglementaires. L'audit de prestataires externes semble nettement moins répandu que dans les entreprises.

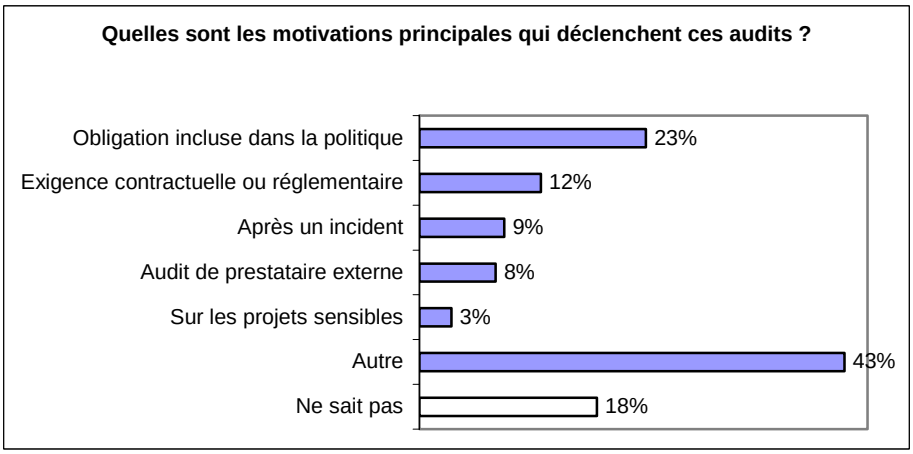

Figure 66 : déclenchement des audits

3/ Les tableaux de bord de sécurité

10 % seulement des collectivités ont mis en place un tableau de bord. Le tableau de bord de la sécurité de l'information ne s'impose toujours pas et reste très marginalement employé. Les indicateurs inclus dans ces tableaux de bord restent majoritairement techniques.

Internautes

- Partie 1 : Profil de l'internaute
- Partie 2 : Les usages d'Internet
- Partie 3 : Perception des menaces et des risques
- Partie 4 : Moyens et comportements de sécurité
- Conclusion

Les Internautes

A travers cette étude, le CLUSIF a souhaité caractériser la population des internautes français, connaître les usages d'Internet par cette population et surtout évaluer leur perception de la menace informatique, des risques et l'interroger sur ses pratiques de sécurité.

Partie 1 : Profil de l'internaute

Constitution de l'échantillon

Le CLUSIF s'est adressé pour l'occasion à un institut spécialiste des enquêtes d'opinion, Harris Interactive, qui a réalisé cette étude intégralement par Internet. L'échantillon est constitué de 1139 personnes issues d'un panel de 700 000. L'importance de ce panel garantit la présence de tous les profils d'internaute. Sa constitution autour d'une signalétique précise a de plus permis de constituer un échantillon structuré représentant précisément la réalité de la population des internautes français en termes de CSP[9], âge, sexe, région, type d'agglomération, etc. En dernière correction, des redressements mineurs ont pu être faits afin que les réponses soient directement transposables à la réalité de la population française.

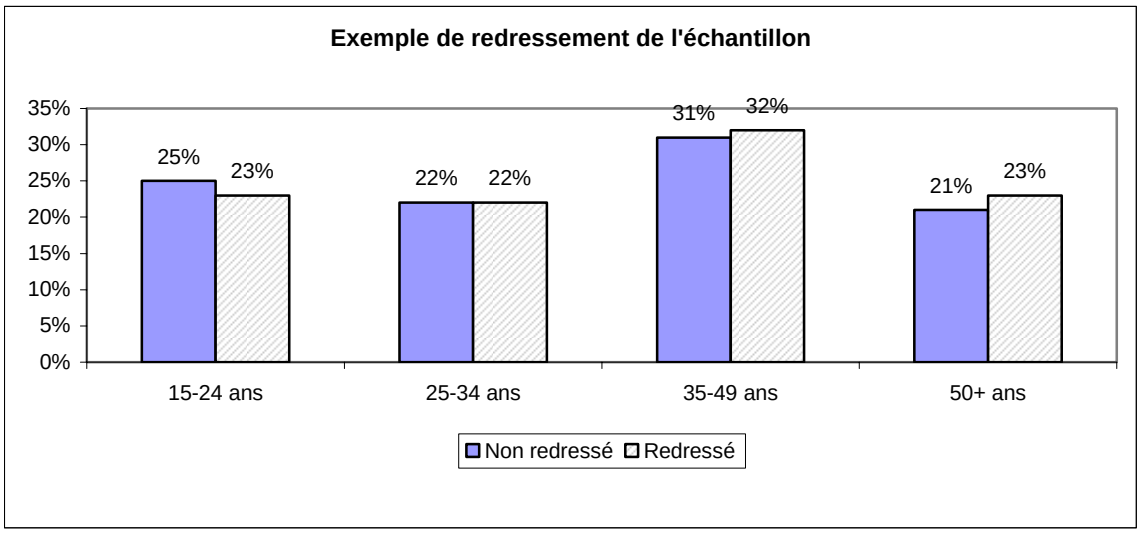

Figure 67 : exemple de redressement effectué sur l'échantillon

Comme on peut le voir ci-dessus, l'échantillon CLUSIF comportait 25 % de 15-24 ans alors que la moyenne nationale est de 23 %. Pour coller au mieux à la réalité, les réponses à l'enquête subissent donc un post-traitement visant à pondérer chaque tranche d'âge au plus juste.

[9] Voir glossaire

Un ou deux ordinateurs par foyer

Rappelons que l'enquête concerne seulement les foyers qui sont connectés à Internet. L'inventaire du matériel informatique familial fait apparaître les caractéristiques suivantes.

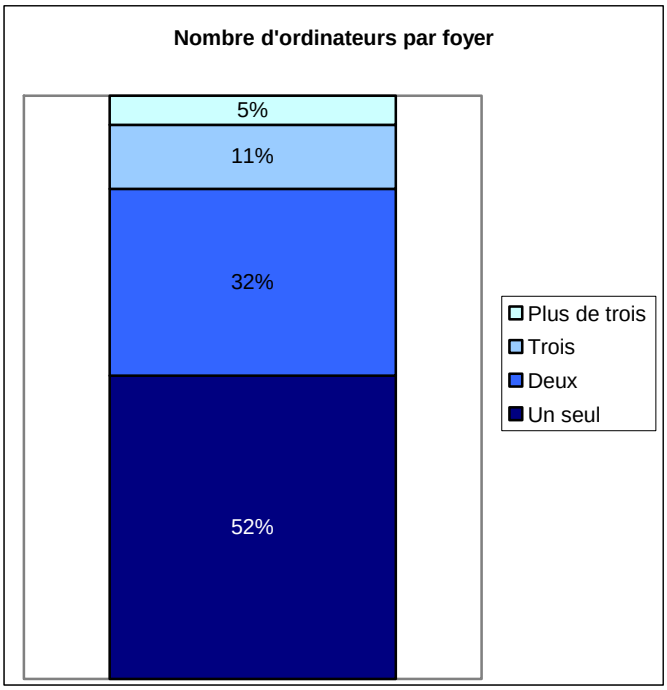

Figure 68 : nombre d'ordinateurs par foyer

52 % des foyers ont un seul ordinateur (moyenne nationale) :

- 48 % dans la catégorie CSP+[10]
- 57 % dans la catégorie CSP-
- 58 % chez les 25-34 ans
- 54 % chez les plus de 50 ans

16 % des foyers ont 3 ordinateurs ou plus (Moyenne nationale).

- 20 % dans la catégorie CSP+
- 11 % dans la catégorie CSP-
- 20 % chez les 35-49 ans

Le taux d'équipement montre relativement peu de disparités selon les zones géographiques et les catégories socioprofessionnelles.

Un parc informatique plutôt récent

Ces ordinateurs sont acquis depuis moins de 3 ans pour près de 60 % des foyers : le parc d'équipement peut donc être considéré comme assez récent compte tenu de la maturité des technologies des ordinateurs personnels.

Parmi les foyers qui disposent de 2 ordinateurs ou plus, 80 % ont au moins deux postes raccordés à Internet.

Wifi en majorité

51 % des foyers en sont équipés (moyenne nationale), avec des pointes :

- 59 % des foyers dans l'agglomération parisienne.
- 60 % des foyers avec des jeunes 15-24 ans.
- 61 % dans les foyers CSP+, où le relais vers un téléviseur peut être déterminant.

L'utilisation majoritaire du Wifi est imputable à la progression très rapide de l'équipement en « box triple play » (Internet-TV-téléphone) et au parc récent (comme exposé au paragraphe précédent) notamment des ordinateurs portables, tous ces équipements ayant des connexions Wifi incorporées.

Les français se donnent les moyens de leurs envies : des ordinateurs neufs sans fil pour surfer en toute liberté.

[10] Voir glossaire

L'ordinateur personnel est un ordinateur familial…

Comme on peut s'y attendre, au sein de la famille, l'ordinateur est partagé entre les différents membres qui la constituent, et ce, dans trois quarts des cas. En effet, seuls 26 % des ordinateurs sont mono-utilisateurs.

En moyenne, l'ordinateur familial est utilisé par **2,4 utilisateurs**.

… mais utilisé professionnellement à 33 %

Les particuliers déclarent faire un usage uniquement personnel de leur ordinateur familial dans 66 % des cas. 33 % en ont un usage mixte (professionnel et personnel).

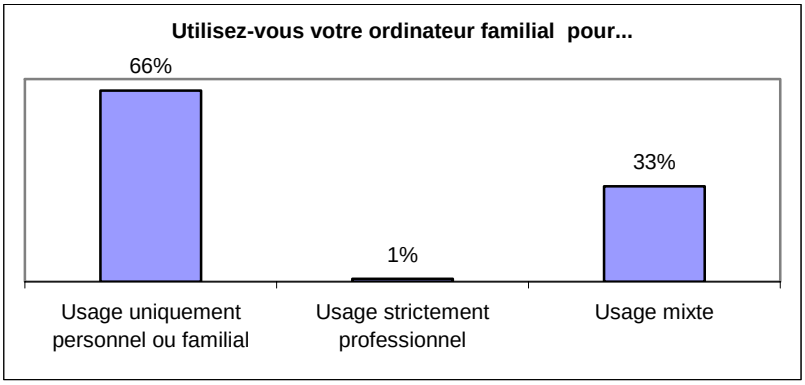

Figure 69 : types d'usage de l'ordinateur familial

L'usage mixte est dominant pour les professions suivantes :

- 80 % Artisans, commerçants, chefs d'entreprise (<10 salariés),
- 66 % Professions libérales et assimilés,
- 60 % Cadres de la fonction publique, professions intellectuelles et artistiques,
- 59 % Étudiants, lycéens, collégiens, apprentis.

40 % des cadres d'entreprises travaillent à la maison

Parmi les différentes catégories socioprofessionnelles, celle des cadres d'entreprises mérite une attention particulière, du moins du point de vue du CLUSIF. En effet, 40 % de ces cadres affirment utiliser leur ordinateur personnel pour travailler et donc manipuler des données de leur entreprise, parfois confidentielles ou sensibles, et ce dans un environnement informatique totalement non maîtrisé par le RSSI. Le constat de cette pratique « mixte » doit amener les responsables de la sécurité des systèmes d'information à s'interroger sur les risques qu'elle induit et les protections qu'elle rend nécessaires. Il faudrait également savoir s'il est réaliste d'interdire les utilisations dites « mixtes » où s'il n'est pas plus profitable pour l'entreprise de les tolérer, voire de les favoriser, tout en développant les actions de sensibilisation et les outils de protections appropriés.

L'ordinateur plébiscité pour les photos

Les usages d'un ordinateur familial sont variés et importants, en particulier pour stocker et manipuler :

- des photos ou des vidéos personnelles pour 97 % d'entre eux,
- des documents personnels (courriers, comptabilités, ..) pour 88 %,
- des documents professionnels ou de travail (études) pour 49 % (avec une pointe (72 %) chez les 15-24 ans et un taux faible (31 %) chez les 50 ans et plus, probablement moins habitués à l'outil informatique).

Partie 2 : Les usages d'Internet

80 % des utilisateurs sont connectés en permanence à Internet

80 % des sondés déclarent être connectés à Internet en permanence ou presque, c'est à dire dès que leur poste est allumé.

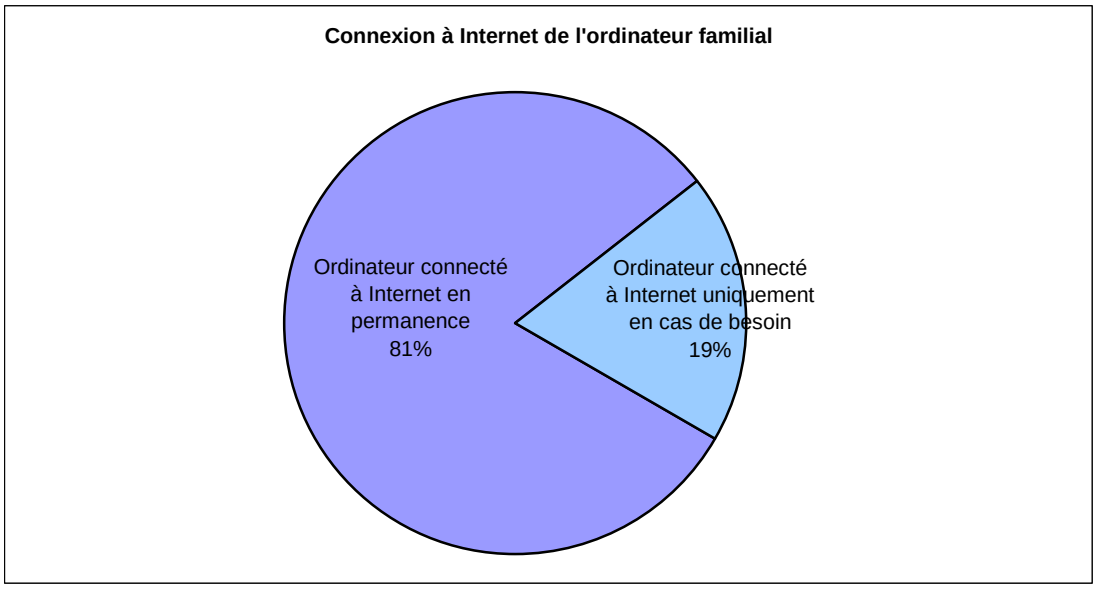

Figure 70 : temps de connexion à Internet

A noter que la généralisation des accès ADSL augmente le temps d'exposition aux risques sans que l'internaute en ait la conscience explicite.

FAI différents selon les zones d'habitat

Trois fournisseurs d'accès à Internet (FAI) dominent le marché, dans l'ordre : Wanadoo/Orange (35 %), Neuf (26 %) et Free (24 %), avec des répartitions très différentes selon les zones d'habitat.
En effet, Wanadoo/Orange est le FAI de 53 % des habitants des zones rurales mais de seulement 18 % des franciliens. En ce qui concerne Free, la règle s'inverse (11 % des ruraux utilisent Free contre 38 % des parisiens).

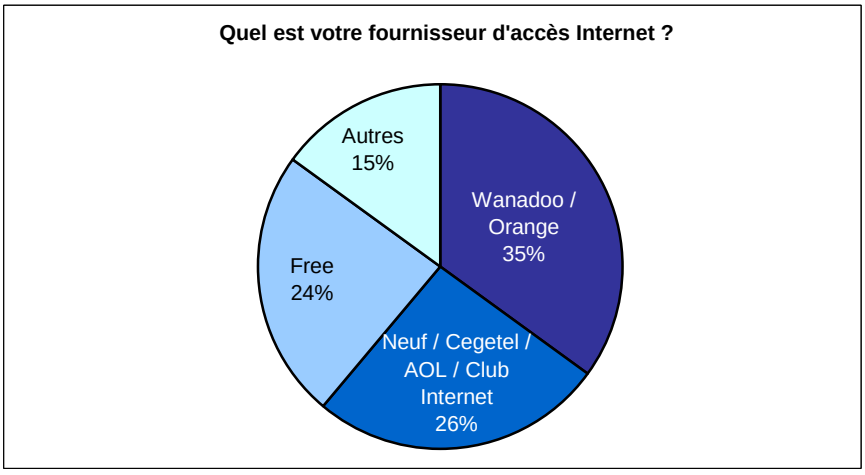

Figure 71 : parts de marché des FAI

D'autre part, le raccordement par câble représente aujourd'hui une part négligeable du marché sauf en agglomération parisienne où il atteint juste 10 % des foyers connectés.

Les usages des internautes sont foisonnants et diversifiés

La quasi totalité des particuliers déclarent utiliser Internet pour la navigation et la messagerie (> 97 %).

Les usages suivants sont pratiqués « souvent » et « très souvent » par la moitié des internautes :

- dialoguer avec une messagerie instantanée : 55 % (19 % ne le font jamais) ;
- effectuer des opérations bancaires : 51 % (23 % ne le font jamais) ;
- payer des achats en ligne : 52 % (10 % ne le font jamais) ;
- faire des démarches administratives : 49 % (déclarer ses impôts, faire ses déclarations *chèque emploi service universel*, inscrire son enfant à la cantine scolaire par exemple).

La fréquence d'utilisation d'Internet pour les actions suivantes est moindre (de 35 % à 15 % dans l'ordre décroissant) pour :

- les ventes aux enchères ou entre particuliers,
- les jeux en ligne,
- la téléphonie sur Internet,
- la communication avec une webcam,
- la tenue d'un blog.

Moins de 10 % des internautes déclarent faire une utilisation fréquente pour :

- communiquer sur des réseaux sociaux,
- télécharger des logiciels,
- utiliser des réseaux de rencontres ou amicaux.

Enfin, et même si un internaute sur 3 fait un usage mixte (professionnel et personnel) de son ordinateur personnel, cette utilisation professionnelle est assez rarement synonyme de connexion au réseau de l'entreprise depuis le domicile :

- 10 % seulement des internautes qui travaillent (hors inactifs donc) déclarent se connecter souvent ou très souvent à leur entreprise,
- 10 % s'y connectent parfois,
- 80 % ne s'y connectent pas.

Téléchargements légaux, téléchargements illégaux

Lorsqu'on interroge l'homme de la rue sur sa pratique d'activités illégales, il faut nécessairement s'attendre à de la « sous-déclaration ». Le CLUSIF s'est tout de même laissé tenter par l'expérience et les résultats obtenus sont… à prendre avec précaution et difficiles à commenter.

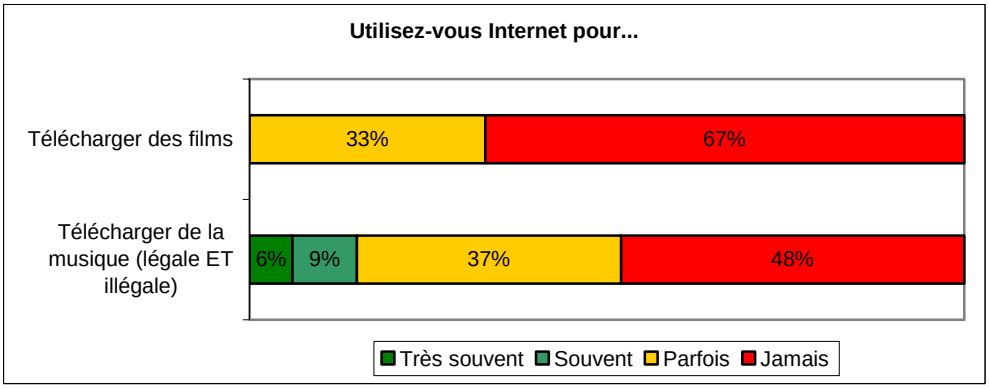

Figure 72 : habitudes de téléchargement de musique et films

Un internaute sur quatre paie sur Internet sans aucune condition

Pour les personnes qui effectuent des achats sur Internet (environ 92 % des internautes le font) :

- 24 % le font sans condition particulière.
- 76 % vérifient une ou plusieurs de ces conditions avant de payer en ligne :
  - le site « semble » sécurisé (cadenas, https:, etc.),
  - le site est connu (marque ou enseigne réputées),
  - l'emploi de techniques spécifiques (PayPal™, e-Carte Bleue, etc.).

Les internautes semblent donc vigilants dès qu'il s'agit de protéger leurs intérêts financiers personnels mais sont-ils vraiment bien informés ? La question qui suit semble prouver que non ! En effet, 86 % des interrogés ignorent que leur cybermarchand (ou son intermédiaire bancaire) a le droit de conserver le numéro de carte bancaire dans son système d'information. Est-ce que les 14 % d'internautes mieux informés connaissent les immenses affaires de divulgations de numéros de cartes bancaires en cours ici ou là ? Nous ne le savons pas mais la majorité de « ceux qui savent » déplorent (à 60 %) que leur précieux numéro soit conservé.

Partie 3 : Perception des menaces et des risques

Assez peu de problèmes de sécurité subis par les internautes

Les problèmes de sécurité que les internautes rapportent avoir rencontrés dans les 18 derniers mois s'établissent comme suit :

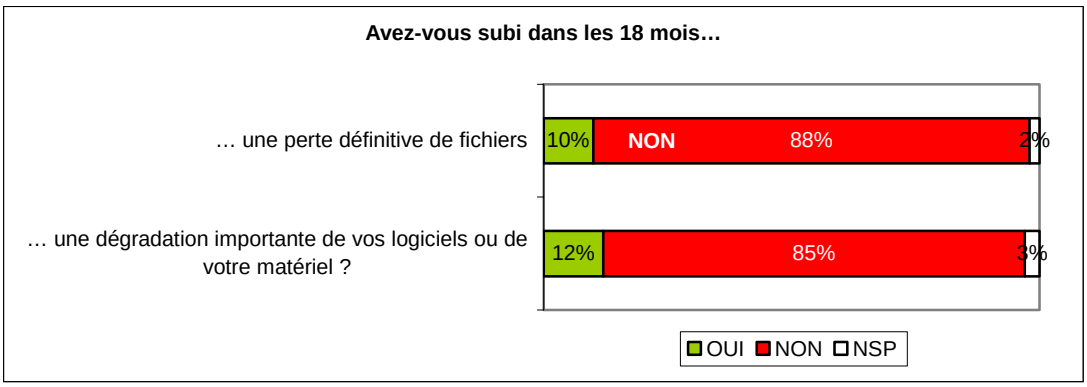

Figure 73 : incidents de sécurité subis par les internautes dans les 18 mois

Selon la nature du problème, 10 à 12 % de la population interrogée déclare avoir eu des problèmes de sécurité au cours des 18 derniers mois.

La sensibilité à la sécurité est aussi le fruit de l'expérience !

Une fraction significative des internautes exprime une forte inquiétude vis-à-vis des menaces et des risques induits par l'utilisation d'Internet :

- 13 % des internautes se déclarent très inquiets au sujet de la protection de leur vie privée.
- 25 % craignent fortement pour leurs fichiers ou leur matériel.

Ces niveaux d'inquiétude sont doublés lorsqu'une perte de fichiers ou une dégradation est intervenue dans les 18 mois précédents.

Mais concernant l'évolution de la menace et des risques, il ne se dégage pas d'opinion sur une quelconque tendance pour la période à venir :

- 20 % pensent que les risques sont en baisse ou forte baisse,
- 21 % qu'ils sont en hausse, éventuellement très forte.

Vie privée : des internautes vigilants mais peu organisés

60 % des internautes pensent qu'Internet peut mettre en danger « un peu » ou « beaucoup » leur vie privée.

La plupart ont bien compris les nuisances qu'ils pourraient subir lorsqu'ils fournissent des informations personnelles sur Internet :

- 19 % d'entre eux ne remplissent jamais les formulaires de collecte de données,
- 75 % le font seulement lorsqu'ils ont des critères (qu'ils jugent) objectifs de confiance dans le site qui les interroge,
- 6 % répondent systématiquement, sans aucune condition.

Les moins méfiants sont les jeunes (15-24 ans) qui répondent beaucoup plus facilement aux questionnaires. Des programmes[11] de sensibilisation initiés par des associations ou les pouvoirs publics témoignent du phénomène.

Si, globalement, ils se méfient de l'exploitation des informations qu'ils fournissent dans les formulaires, les internautes appréhendent par contre peu les risques pour leur vie privée liés à :

- un wifi non sécurisé : 42 % n'y voient pas de risques,
- au vol du support de leurs données (ordinateur ou clé USB) : pour 56 %, les risques induits sont nuls ou peu importants.

Pourtant les particuliers n'utilisent que très peu le chiffrement local de leurs données : moins d'une personne sur dix.

Pour la protection de leurs données personnelles et de leur vie privée, nous ne pouvons donc pour l'heure que constater un sérieux décalage entre les intentions et les pratiques des internautes. Aux associations, pouvoirs publics et médias de faire progresser la prise de conscience de la globalité des risques possibles.

[11] Lire la fiche technique « Protection des enfants » sur le site « Portail de la sécurité informatique » du Secrétariat Général de la Défense Nationale, Direction centrale de la sécurité des systèmes d'information (SGDN/DCSSI), à l'adresse http://www.securite-informatique.gouv.fr/gp_article201.html.

Les menaces virales viennent toujours en tête des préoccupations

La figure ci-dessous présente les menaces qui sont identifiées ou perçues par les internautes. Ces menaces sont classées par ordre d'importance décroissante. Les craintes dominantes restent encore les attaques virales ou par spyware.

Figure 74 : menaces par ordre d'importance, selon les internautes

Cette figure synthétise les menaces jugées comme faisant peser des risques « très importants » et « importants » sur l'informatique familiale. A l'opposé, les menaces suivantes sont jugées comme représentant un « risque nul » :

- Le vol de l'ordinateur ou d'une clé USB par 20 % des internautes interrogés,
- Les erreurs de manipulation par 15 %,
- Les pannes de courant par 15 %,
- Le piratage de leur Wifi à 11 %.

Les hommes relativisent plus que les femmes

Il est notable que les femmes qualifient beaucoup plus facilement que les hommes comme « très important » les risques potentiellement induits par les menaces que nous avons citées, sauf pour un unique cas, le vol.

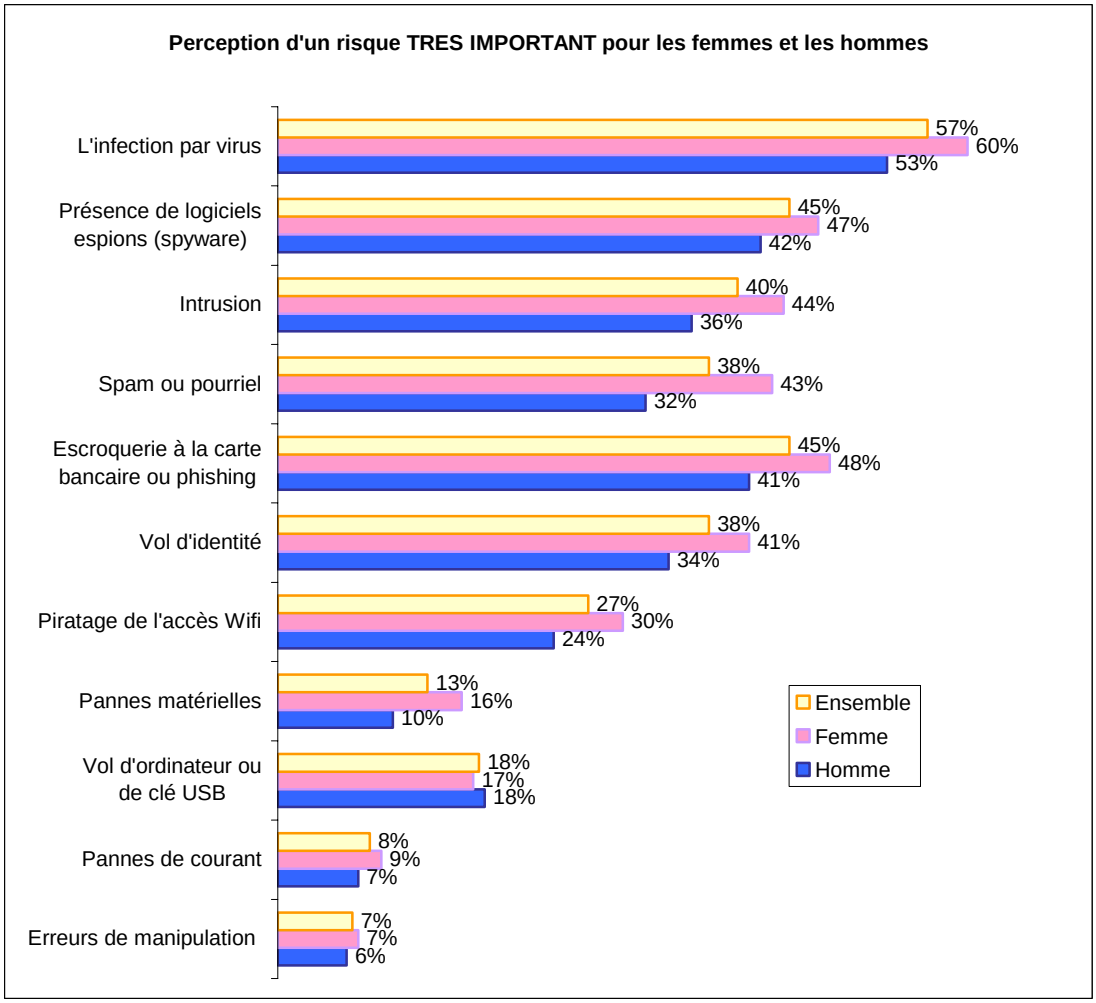

Figure 75 : différence de perception des risques selon le sexe

De grosses lacunes dans la compréhension des situations à risque

De la même façon, pour les internautes interrogés sur les comportements et les situations à risque, l'absence de protections vis-à-vis des menaces virales arrive logiquement en première place.

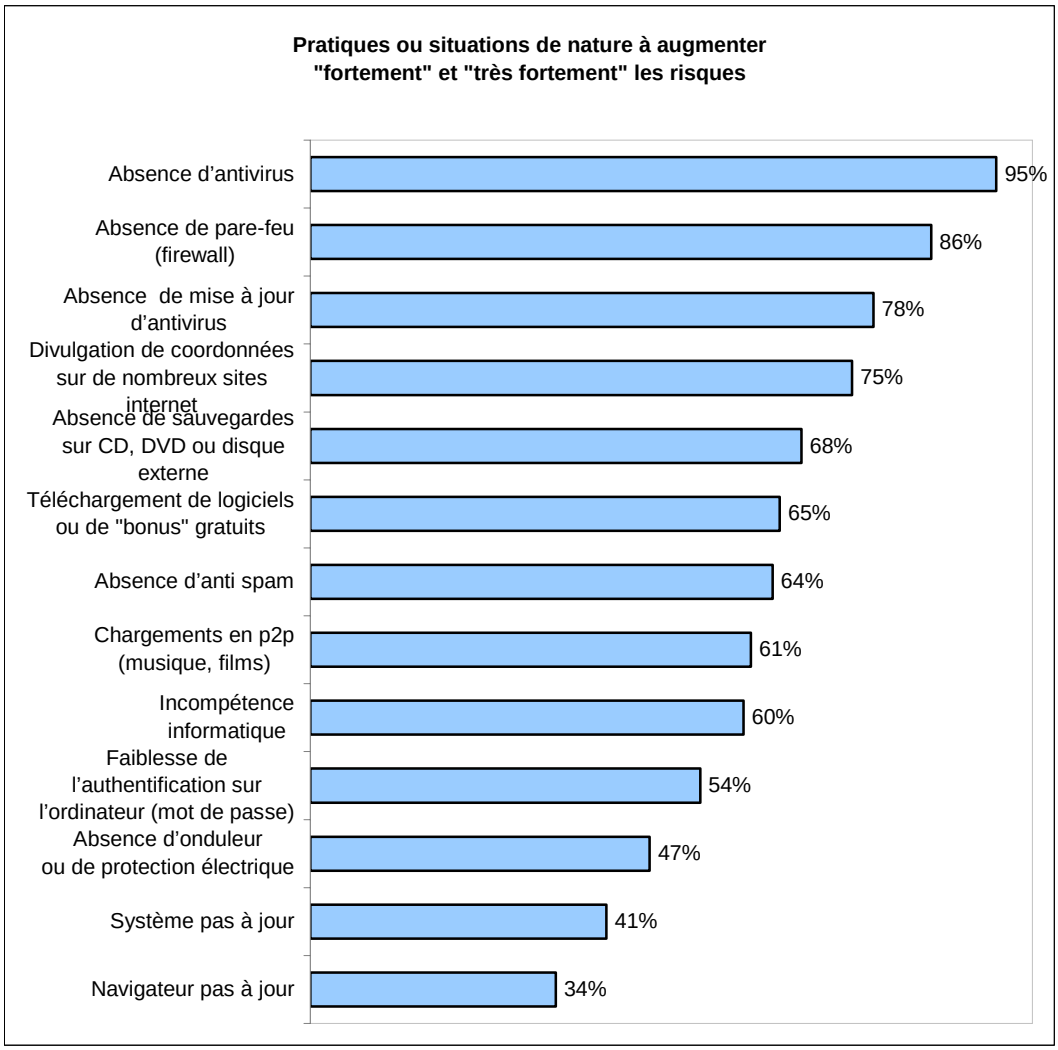

Figure 76 : pratiques et situations jugées à risque par les internautes

Il faut noter le besoin d'éducation et de sensibilisation aux bonnes pratiques des utilisateurs qui considèrent majoritairement que ne pas mettre à jour leurs systèmes et navigateurs n'augmente pas fortement les risques, alors qu'en pratique, c'est primordial. Un système d'exploitation pas à jour, même doté d'un antivirus, sera la plupart du temps vulnérable aux attaques externes.

Partie 4 : Moyens et comportements de sécurité

Les internautes utilisent sans surprise des moyens de protection « classiques »

Compte tenu des risques ressentis les internautes utilisent, sans surprise, des moyens de protection « classiques » en rapport avec les niveaux de menace ressentis.

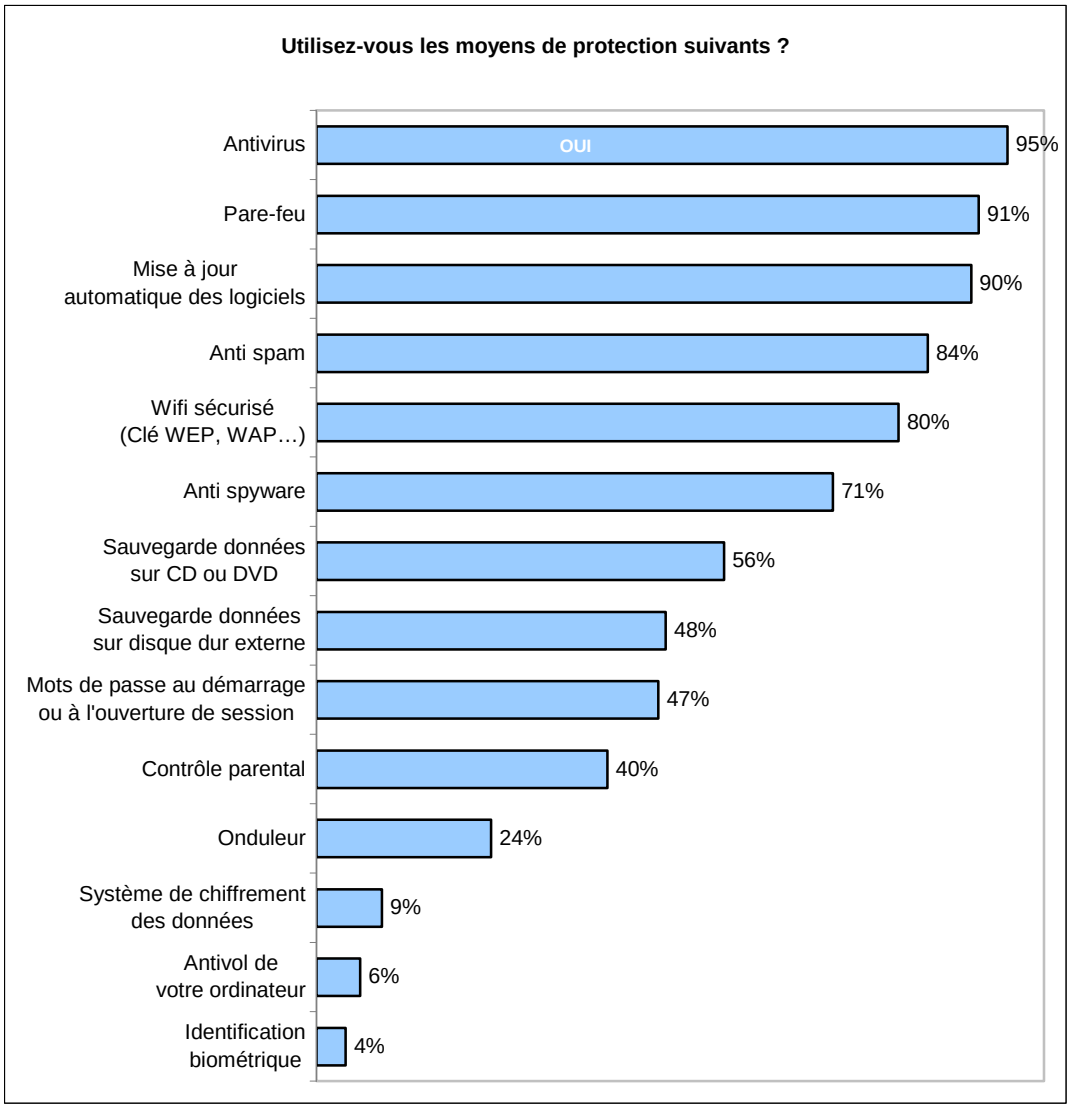

Figure 77 : moyens de protection utilisés par les internautes

Sur les ordinateurs des internautes, les outils de protection contre les menaces Internet sont très présents, en particulier l'antivirus et le pare-feu. De plus :

- 90 % utilisent des mises à jour automatiques des logiciels sensibles ainsi que du système et du navigateur. On doit s'en féliciter même si l'on peut s'en étonner au regard des 54 % d'internautes estimant qu'un système d'exploitation obsolète n'augmente pas du tout (17 %) ou faiblement (37 %) les risques et les 60 % pensant la même chose des navigateurs Internet non mis à jour.
- 84 % pensent avoir un antispam.
- 80 % affirment que leur connexion Wifi est sécurisée.
- 71 % utilisent un anti-spyware.

Coût de la protection et mises à jour automatiques

Dans la hiérarchie des moyens de protection, l'enquête indique une certaine corrélation entre le taux d'équipement et deux éléments : la gratuité et l'automatisation.

Côté gratuité, la plupart des moyens de protection les plus utilisés selon notre enquête sont gratuits, inclus sans supplément de coût dans le système d'exploitation livré avec l'ordinateur ou facilement téléchargeables auprès des éditeurs ou de sites spécialisés. De même, les mises à jour automatiques, réalisées pour 90 % des internautes interrogés (systèmes d'exploitation, antivirus, navigateurs…) ne nécessitent, par définition, pas d'effort particulier de la part de l'internaute.

A l'inverse l'utilisation des outils de sécurité impliquant un acte d'achat et/ou un effort de la part de l'internaute pour comprendre les risques et juger de l'équilibre entre dépense et prise de risque, est moins répandue. Il s'agit toutefois de risques statistiquement moins fréquents (protection électrique, chiffrement, biométrie, antivols, etc.) que les virus et les spywares.

Un contre exemple, et de taille : l'antivirus. En regard de la menace ressentie et des risques attendus (perception parfois issue d'une expérience personnelle malheureuse), les internautes investissent dans des abonnements de mise à jour d'antivirus.

Conclusion

Notre enquête montre que les internautes sont globalement peu inquiets des menaces induites par leur utilisation d'Internet : seulement 25 % d'entre eux craignent fortement pour la protection de leurs données ou de leur matériel, et 94 % d'entre eux se sentent « plutôt ou totalement » en sécurité lorsqu'ils utilisent leur ordinateur familial sur Internet.

Ce constat paraît surprenant alors que l'actualité montre que les menaces ne faiblissent pas et sont toujours plus ingénieuses. Si les internautes se pensent en relative sécurité, c'est certainement grâce la présence d'un arsenal défensif qui paraît effectivement assez développé (usage large de l'antivirus, de l'anti-spyware et du pare-feu personnel). Pourtant, rien ne nous permet d'affirmer que ces outils sont correctement utilisés et paramétrés. Cette situation pourrait se dégrader dans l'avenir, les jeunes internautes paraissant moins précautionneux dans l'usage de leur identité sur Internet et dans l'usage du téléchargement de logiciels. Nul doute donc que les actions de sensibilisation voire de formation devront être plus largement développées à l'avenir.

Annexe


TELECOMS
TRANSPORTS
BTP
COMMERCE
SERVICES
INDUSTRIE
COLLECTIVITES PUBLIQUES
98
99
00
01
02

Annexe

Glossaire[12]

Terme	Définition
CSP	Catégorie socioprofessionnelle. Caractérisation de la population active française en classes et professions, établie par l'INSEE. Voir http://www.insee.fr/fr/nom_def_met/nomenclatures/prof_cat_soc/pages/pcs.htm.
DSI	Directeur des Systèmes d'Information
ISO 27002	Norme internationale constituant un « guide de bonnes pratiques » en matière de sécurité de l'information (anciennement ISO 17799:2005).
MEHARI	Méthode d'analyse des risques, développée par le CLUSIF. Voir http://www.clusif.asso.fr/mehari/.
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*.
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. Voir http://www.ssi.gouv.fr/fr/confiance/pssi.html.
RSSI	Responsable Sécurité des Systèmes d'Information.

[12] 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
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
30, rue Pierre Sémard
75009 Paris
✆ 01 53 25 08 80
clusif@clusif.asso.fr

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