



Politiques de sécurité des systèmes d'information et sinistralité en France

Bilan de l'année 2005



Edition 2006

- ▶ Les entreprises de plus de 200 salariés
- ▶ Zoom sur les mairies
- ▶ Zoom sur les hôpitaux

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
Mme CHAMBON Catherine	MINISTERE DE L'INTERIEUR
M. DELIN Hubert	DEUTSCHE BANK AG PARIS
L.C. FERRY Joël	GENDARMERIE NATIONALE
C.E. FREYSSINET Eric	GENDARMERIE NATIONALE
M. GRATIOLET François	HAPSIS
M. GUERIN Olivier	CLUSIF
M. HAMON Bruno	EXEDIS
M. HIRSCHMANN Michel	CREDIT DU NORD
M. JONCHERES Thibaud	DATALAB
M. JOURDAIN Benoît	HORUS INFORMATION ET TECHNOLOGIE
M. MARECHAL Laurent	HAPSIS
M. MARTINEZ Frédéric	ALCATEL-CIT
M. ROSE Philippe	CIO
M. ROULE Jean-Louis	Consultant indépendant
M. SAGHROUNE Serge	ACCOR
M. VERGELY Axel	SUNGARD

Le CLUSIF remercie aussi vivement les représentants des entreprises, mairies et hôpitaux qui ont bien voulu participer à cette enquête.

Enquête statistique réalisée pour le CLUSIF par le cabinet GMV Conseil.

Editorial

A travers cette nouvelle enquête 2005 sur les politiques de sécurité et la sinistralité informatique, le CLUSIF a souhaité réaliser un bilan approfondi des pratiques en matière de sécurité de l'information en France. Cette enquête se veut être une référence de par la taille et la représentativité des échantillons d'entreprises, de mairies et d'hôpitaux interrogés. Elle est se veut par ailleurs très complète puisqu'elle passe en revue un large panel de thèmes relatifs à la sécurité des SI.

A l'heure où la sécurité de l'information reste sous les feux de l'actualité (multiplication des vols de données, attaques logiques (virus, phishing...) qui poursuivent leur développement...) tous les acteurs ont-ils pris conscience des risques et mis en œuvre en conséquences les mesures qui s'imposent ?

En réponse à cette question, nous dressons un constat mitigé.

Certes tous les acteurs interrogés ressentent bien que les Systèmes d'Information deviennent critiques pour leur activité. Certes des progrès très importants ont été enregistrés depuis notre enquête précédente, publiée en 2004, notamment en matière de formalisation des chartes de sécurité, en matière de recensement des actifs clés, de conduite d'analyse de risques ou d'actions d'audits et de contrôle.

Mais les approches restent encore souvent partielles. Les budgets n'augmentent pas si vite que l'on pourrait l'imaginer, et les projets piétinent encore. Au-delà de la prise de conscience qui semble bien réelle, la professionnalisation des pratiques n'est pas encore la règle loin de là : la veille sur les menaces est partielle, les plans de continuité d'activité, quand ils existent, ne sont pas toujours testés, et les tableaux de bord sont encore quasi inexistant.

Pourtant, notre enquête montre bien que les incidents et les malveillances existent et sont bien réels, avec une présence toujours active des attaques virales, un développement du vol de matériel, et surtout des problèmes de divulgation d'information, des attaques logiques ciblées ou des fraudes en quantités non négligeables.

Le travail de sensibilisation doit donc être poursuivi, de même que la mise en place de systèmes complets de gestion de la sécurité de l'information, basés sur des normes reconnues telles que l'ISO 17799 et l'ISO 27001. En effet, c'est en démontrant sa rigueur et son professionnalisme que la « communauté des sachants » de la sécurité convaincra progressivement les décideurs d'investir plus dans ce domaine.

Le CLUSIF continuera à y contribuer comme il l'a toujours fait.

Laurent BELLEFIN
Pour le Groupe de Travail « Enquête Politique
de Sécurité et sinistralité informatique »

Sommaire

Méthodologie	9
Les Entreprises	12
Présentation de l'échantillon	12
Dépendance à l'informatique des entreprises de plus de 200 salariés	12
Moyens consacrés à la sécurité de l'information par les entreprises	13
Thème 5 : Politique de sécurité	15
Thème 6 : Organisation de la sécurité et moyens	16
Thème 7 : Gestion des actifs et identification des risques	16
Thème 8 : Sécurité des ressources humaines (charte, sensibilisation)	18
Thème 10 : Gestion des communications et des opérations	19
Sécurisation des nouvelles technologies	19
Lutte anti-virale, protection contre les intrusions et gestion des vulnérabilités	20
Sécurité et infogérance de services d'exploitation	20
Thème 11 : Contrôle des accès	21
Thème 12 : Acquisition, développement et maintenance	22
Veille et gestion des vulnérabilités : une pratique qui se généralise	22
Maintenance et déploiement de correctifs de sécurité : une industrialisation partielle	22
Thème 13 : Gestion des incidents de sécurité	23
Thème 14 : Gestion de la continuité	25
Thème 15 : Conformité (CNIL, audits, tableaux de bord)	28
CNIL	28
Audits	29
Tableaux de bord	30
Les Mairies	32
Présentation de l'échantillon	32
Dépendance à l'informatique des mairies	32
Moyens consacrés à la sécurité de l'information par les mairies	32
Thème 5 : Politique de sécurité	34
Thème 6 : Organisation de la sécurité et moyens	34
Thème 7 : Gestion des actifs et identification des risques	36
Thème 8 : Sécurité des ressources humaines (charte, sensibilisation)	36
Thème 10 : Gestion des communications et des opérations	37
Sécurisation des nouvelles technologies	37
Lutte anti-virale, protection contre les intrusions et gestion des vulnérabilités	37
Sécurité et infogérance de services d'exploitation	37
Thème 11 : Contrôle des accès	38
Thème 12 : Acquisition, développement et maintenance	38
Thème 13 : Gestion des incidents de sécurité	38
Thème 14 : Gestion de la continuité	40
Thème 15 : Conformité (CNIL, audits, tableaux de bord)	40
CNIL	40
Audits	41
Les Hôpitaux	44
Présentation de l'échantillon	44
Dépendance à l'informatique des hôpitaux publics	44
Moyens consacrés à la sécurité de l'information par les hôpitaux publics	44
Thème 5 : Politique de sécurité	46
Thème 6 : Organisation de la sécurité et moyens	47
Thème 7 : Gestion des actifs et identification des risques	47
Thème 8 : Sécurité des ressources humaines (charte, sensibilisation)	48
Thème 10 : Gestion des communications et des opérations	49
Sécurisation des nouvelles technologies	49

Lutte anti-virale, protection contre les intrusions et gestion des vulnérabilités.....	49
Sécurité et infogérance de services d'exploitation.....	49
Thème 11 : Contrôle des accès.....	50
Thème 12 : Acquisition, développement et maintenance.....	50
Thème 13 : Gestion des incidents de sécurité.....	50
Thème 14 : Gestion de la continuité.....	51
Thème 15 : Conformité (CNIL, audits, tableaux de bord).....	52
CNIL.....	52
Audit.....	52
Annexe.....	56
Quelques rappels de définitions utiles.....	56

Index des graphiques

Graphique 1 : Dépendance des entreprises vis-à-vis de l'informatique.....	13
Graphique 2 : Part du budget sécurité dans le budget informatique des entreprises.....	14
Graphique 3 : Evolution du budget sécurité des entreprises.....	14
Graphique 4 : Existence d'une Politique Sécurité en fonction de la taille de l'entreprise.....	15
Graphique 5 : Actifs inventoriés en entreprise.....	17
Graphique 6 : Existence d'une charte de sécurité, selon la taille des entreprises.....	18
Graphique 7 : Moyens utilisés pour assurer la sensibilisation du personnel des entreprises.....	19
Graphique 8 : Sécurisation des nouvelles technologies en entreprise.....	19
Graphique 9 : Technologies de contrôle d'accès au système d'information en entreprises...	21
Graphique 10 : Veille permanente en vulnérabilités en entreprise.....	22
Graphique 11 : Gestion des vulnérabilités en entreprise.....	23
Graphique 12 : Typologie des incidents de sécurité en entreprise.....	24
Graphique 13 : Plan de continuité d'activité d'entreprise.....	25
Graphique 14 : Fréquence de test et de mise à jour des plans de continuité d'activité en entreprise.....	26
Graphique 15 : Types de solution de secours informatique en entreprise.....	26
Graphique 16 : Mise en place de correspondants CNIL par secteur d'activité en entreprise..	28
Graphique 17 : Nombre d'audits sécurité en 2005 dans l'entreprise.....	29
Graphique 18 : Motivations principales des audits sécurité en entreprise.....	29
Graphique 19 : Mise en place des tableaux de bord de sécurité en entreprise.....	30
Graphique 20 : Destinataires du tableau de bord de sécurité en entreprise.....	30
Graphique 21 : Dépendance des mairies vis-à-vis de l'informatique.....	32
Graphique 22 : Pourcentage du budget sécurité dans le budget informatique des mairies..	33
Graphique 23 : Evolution du budget sécurité des mairies.....	33
Graphique 24 : Soutien de la Politique de sécurité de l'information.....	34
Graphique 25 : La mission de Responsable de la Sécurité des Systèmes d'Information (RSSI) dans les mairies.....	35
Graphique 26 : Le RSSI, une fonction équilibrée entre l'opérationnel, le technique et le fonctionnel.....	35
Graphique 27 : Charte de sécurité à destination du personnel des mairies.....	36
Graphique 28 : Communication de la charte sécurité au personnel des mairies.....	36
Graphique 29 : Les moyens utilisés pour assurer la sensibilisation du personnel des mairies.....	37
Graphique 30 : Technologies de contrôle d'accès au système d'information dans les mairies	38
Graphique 31 : Typologie des incidents de sécurité dans les mairies.....	39
Graphique 32 : Plan de continuité d'activité des mairies.....	40
Graphique 33 : Nombre d'audits sécurité en 2005 dans les mairies.....	41
Graphique 34 : Motivations principales des audits sécurité dans les mairies.....	41
Graphique 35 : Pourcentage du budget sécurité dans le budget informatique des hôpitaux	45
Graphique 36 : Evolution du budget sécurité des hôpitaux.....	45

Graphique 37 : La Politique de sécurité de l'information dans les hôpitaux.....	46
Graphique 38 : La mission de Responsable de la Sécurité des Systèmes d'Information (RSSI) dans les hôpitaux.....	47
Graphique 39 : Charte de sécurité à destination du personnel des hôpitaux.....	48
Graphique 40 : Communication de la charte sécurité au personnel des hôpitaux	48
Graphique 41 : Outils de sensibilisation du personnel des hôpitaux	49
Graphique 42 : Typologie des incidents de sécurité dans les hôpitaux	50
Graphique 43 : Plan de continuité d'activité des hôpitaux.....	51
Graphique 44 : Mise en place des CIL dans les hôpitaux publics	52
Graphique 45 : Nombre d'audits sécurité en 2005 dans les hôpitaux.....	53

Méthodologie

L'enquête du CLUSIF sur les politiques de sécurité du système d'information et la sinistralité informatique en France en 2005 a été réalisée via des entretiens téléphoniques au cours des mois de février et mars 2006. Ces entretiens ont été menés par le cabinet spécialisé GMV Conseil, sur la base d'un questionnaire élaboré par le CLUSIF.

Ce questionnaire a été construit en reprenant les différents thèmes de la norme ISO 17799:2005, norme qui décrit les différents items à couvrir dans le domaine de la sécurité des systèmes d'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 : Gestion des actifs et identification des risques
- 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 côté.

Trois cibles ont été retenues pour cette enquête :

- Les entreprises de plus de 200 salariés : 400 entreprises de cette catégorie ont répondu à cette enquête.
- Les mairies des communes de plus de 30 000 habitants : 50 mairies ont accepté de répondre à cette enquête.
- Les hôpitaux publics : 186 établissements de tailles diverses ont répondu à cette enquête.

Les entités interrogées ont été choisies « au hasard » par GMV Conseil. A noter par exemple que le fichier des adhérents du CLUSIF n'a pas été utilisé, ce qui aurait pu impacter les résultats de l'enquête, les adhérents du CLUSIF étant par nature déjà sensibilisés à la sécurité de l'information.

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



- ▶ Moyens informatiques 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 : Gestion des actifs et identification des risques
- ▶ 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)

Les Entreprises

Présentation de l'échantillon

400 entreprises ont répondu à la sollicitation du CLUSIF, soit environ 7% des entreprises de plus de 200 salariés.

- 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	8	4	2	14	4%	→	6%
COMMERCE	19	9	7	35	9%	→	17%
INDUSTRIE	118	48	30	196	49%	→	43%
SERVICES	71	28	28	127	32%	→	25%
TRANSPORTS— TELECOMS	16	6	6	28	7%	→	9%
Total	232	95	73	400			
Total en %	58%	24%	18%				

↓ ↓ ↓

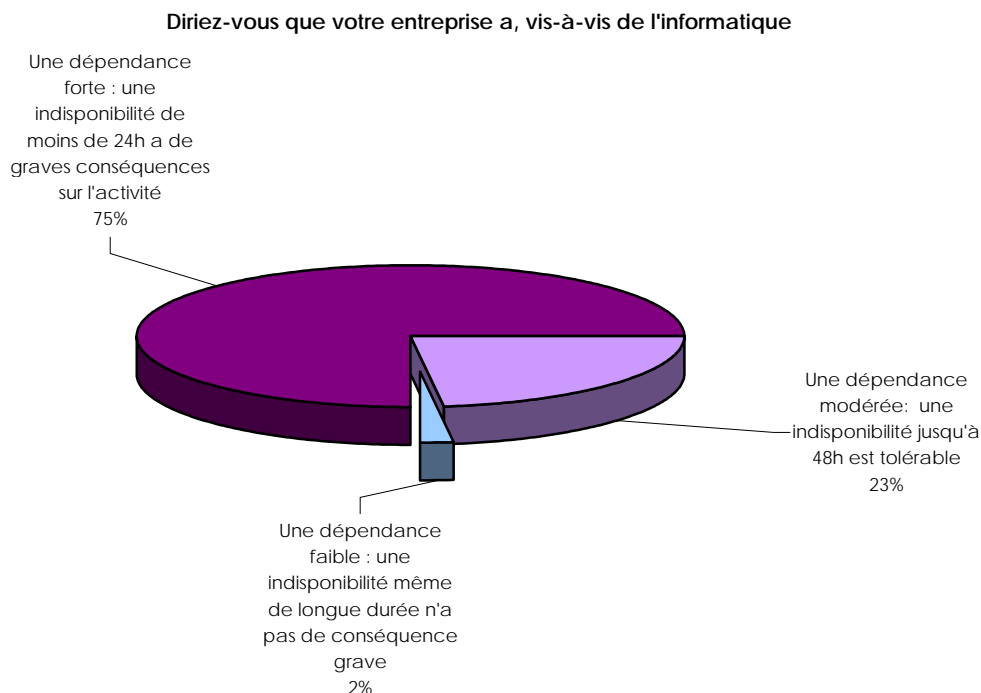
Données INSEE	66%	19%	15%
---------------	-----	-----	-----

Au sein de chaque entreprise, nous avons cherché à interroger en priorité le Responsable de la Sécurité des Systèmes d'Information (pour 28 % des entreprises interrogées), ou à défaut, en particulier dans les plus petites entreprises de notre échantillon, le responsable informatique (pour 44 % des entreprises interrogées).

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

Le système d'information est bien devenu l'épine dorsale des entreprises

La dépendance perçue par les entreprises vis-à-vis de leur informatique se stabilise et semble avoir trouvé un point d'équilibre à un niveau élevé, puisque 98% des entreprises avouent une dépendance modérée ou forte. Seules 2% d'entre elles indiquent une dépendance faible. Même si cette dépendance est ressentie plus fortement dans les grandes entreprises de plus de 1000 salariés, les écarts restent faibles avec les plus petites entreprises de notre échantillon.



Graphique 1 : Dépendance des entreprises vis-à-vis de l'informatique

L'industrie maintenant aussi dépendante à l'informatique que les autres secteurs.

C'est le secteur du BTP qui reste le moins dépendant à une défaillance de l'informatique (52% seulement avouent une dépendance forte). Les entreprises du secteur industrie ont rejoint les entreprises du secteur des services ou du transport et des télécoms, ce qui démontre bien la place de plus en plus cruciale de l'informatique dans cette activité.

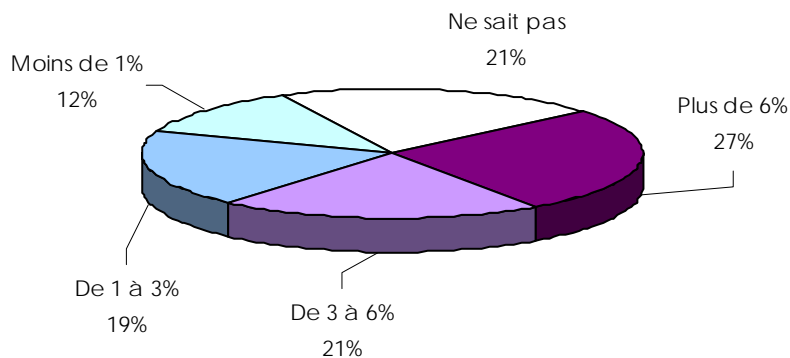
Moyens consacrés à la sécurité de l'information par les entreprises

Un budget sécurité dont le périmètre semble encore mal cerné.

Le niveau de dépense des entreprises en matière de sécurité de l'information semble encore très hétérogène. De plus, une part significative des entreprises (21 %) ne semble pas identifier ou mesurer cette dépense. Cela révélerait-il un manque de communication sur le sujet ? Ou bien plutôt le fait que ce budget n'ait pas encore une définition très claire et un périmètre bien délimité ? C'est plutôt cette dernière interprétation qui semble à privilégier. Des progrès semblent donc nécessaires dans ce domaine : la maîtrise du budget est une composante indispensable à une bonne gestion des risques, dans une optique de mise en œuvre de moyens proportionnés aux enjeux.

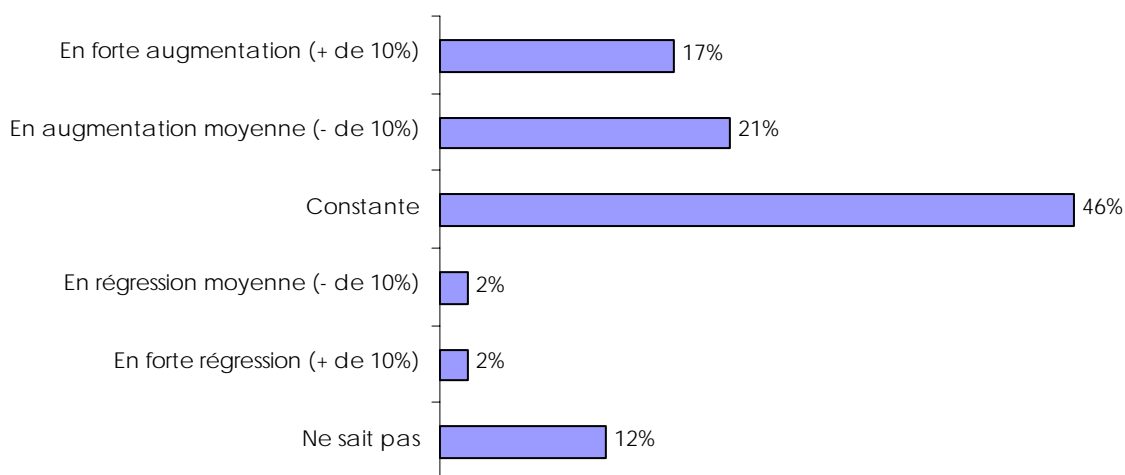
Reste que la tendance est bien à la hausse de ces budgets pour 38 % des entreprises, ou à une stabilisation pour 46 % d'entre elles.

Quel pourcentage représente le budget sécurité par rapport au budget informatique total en 2005 ?



Graphique 2 : Part du budget sécurité dans le budget informatique des entreprises

Quelle est l'évolution du budget sécurité par rapport à l'année 2005 ?



Graphique 3 : Evolution du budget sécurité des entreprises

Difficile de faire passer un projet sécurité dans l'entreprise ?

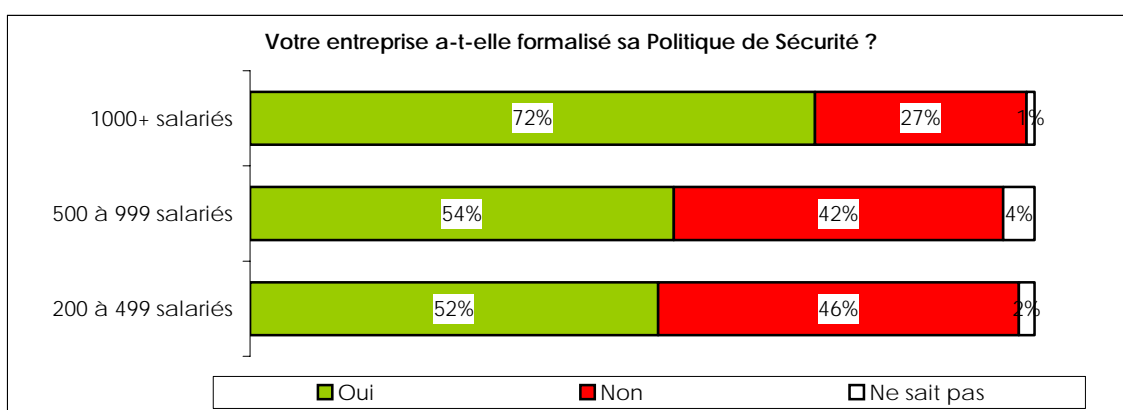
Pour les entreprises de plus de 200 salariés, les freins à la conduite des missions de sécurité sont dans un ordre décroissant le manque de budget (37%), le manque de personnel qualifié (25%), les contraintes organisationnelles (20%) et les réticences diverses (20%). Il est manifeste que dans l'entreprise soumise à des contraintes de productivité et de rentabilité de plus en plus forte, les projets sécurité ont encore du mal à justifier un retour sur investissement suffisant pour être mis en œuvre. La valorisation des impacts des incidents potentiels et l'évaluation des risques opérationnels liés à l'informatique n'ont pas encore fait complètement leur chemin. Jusqu'au jour où la survenance d'un sinistre démontre par l'exemple le coût d'un arrêt non sollicité...

Thème 5 : Politique de sécurité

La mise en œuvre d'une PSI – Politique de Sécurité de l'Information - est une étape importante dans la mise en place des règles de bonne gouvernance du SI en entreprise. Les analyses de risques réalisées dans les entreprises et le soutien de plus en plus fréquent de la direction générale dans la mise en application d'une politique de sécurité démontrent bien la volonté de se doter d'une vraie culture de la sécurité des systèmes d'information.

Un net progrès dans la formalisation des politiques de sécurité de l'information...

56% des entreprises sont dotées d'une PSI. Dans 71% des cas, cette PSI est soutenue explicitement par la Direction Générale de l'entreprise. Même si ce sont bien les grandes entreprises qui sont les plus avancées, les progrès sont globalement très nets. Le travail des RSSI ainsi que des associations professionnelles commence à porter leurs fruits.



Graphique 4 : Existence d'une Politique Sécurité en fonction de la taille de l'entreprise

...mais une utilisation encore assez restreinte des normes du domaine

En revanche, pour le moment, seules 48% des entreprises s'appuient sur une norme ou une méthode pour formaliser cette PSI. 29% des entreprises utilisent pour cela la norme ISO 17799, qui s'impose bien progressivement comme la référence en la matière. Des progrès sont donc encore possibles, l'intérêt d'une telle norme étant notamment de garantir la complétude des thèmes traités par la PSI, et pourquoi pas, dans le futur, viser une certification des entreprises, telle que cela est pratiqué dans le domaine de la qualité.

La pression réglementaire continue, déclenchée notamment par les scandales liés à la mauvaise gestion de certaines entreprises, et les incidents fréquents et largement médiatisés concernant par exemple la divulgation d'informations confidentielles, vont continuer à pousser les entreprises à mettre en place des règles de gouvernance plus strictes en matière de sécurité de l'information. Reste aux RSSI à bien se positionner pour faire valoir la valeur ajoutée de la sécurité de l'information en entreprise.

Thème 6 : Organisation de la sécurité et moyens

Le RSSI, une responsabilité trop peu identifiée et attribuée

La sécurité de l'information n'est pas formellement définie et attribuée à un RSSI pour 58% des entreprises étudiées. Dans ce cas, elle est assurée à 84% directement par le DSI lui-même ou par du personnel au sein des domaines informatique et/ou réseaux ; dans les 15% restants, ce rôle est assuré par des responsables de haut niveau (jusqu'au DG) ou transversaux (finance, contrôle interne,...).

La prégnance de la DSI est plus forte dans les secteurs du commerce et du service (vers 90%), médiane pour l'industrie et plus faible (vers 60%) pour le BTP et Transport/télécoms.

La présence de RSSI identifié est de 41% en moyenne et croît régulièrement avec la taille de l'entreprise :

- 33% des entreprises pour un effectif de 200 à 400 personnes,
- 46% entre 400 et 1000 personnes,
- 72% au-delà de 1000 personnes.

Le RSSI, une fonction très souvent assumée à temps partiel

L'existence du poste de RSSI n'implique sa prise en charge de manière exclusive que pour 50 à 60% des entreprises tous secteurs et toutes tailles confondus, les RSSI devant combiner leur fonction avec d'autres missions, en particulier liées à la DSI.

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

Le poste de RSSI est rattaché à la Direction Générale dans 39% des cas. Sinon, il sera rattaché au DSI lui-même (41%), à la production informatique (3%), et exceptionnellement à la Direction des risques (1%) ou à la sûreté générale (1%). L'évolution vers une relative indépendance du RSSI par rapport aux fonctions informatiques semble se poursuivre, mais sans être très rapide.

Le RSSI est souvent un homme seul

Il n'y a pas d'équipe assignée en permanence à la sécurité de l'information dans 11% des entreprises en moyenne. S'il y a une équipe permanente dédiée à la sécurité, elle comprend 1 à 2 personnes pour 63% des entreprises, 3 à 5 personnes pour 19% des cas et ne dépasse 5 personnes que dans 5 % des cas.

Une quasi-constance de cet effectif est observée quelle que soit la taille des entreprises, le seul fait notable est cependant que le RSSI est moins souvent seul au-delà de 1000 salariés (6% des entreprises au lieu de 13% en dessous de 1000 salariés).

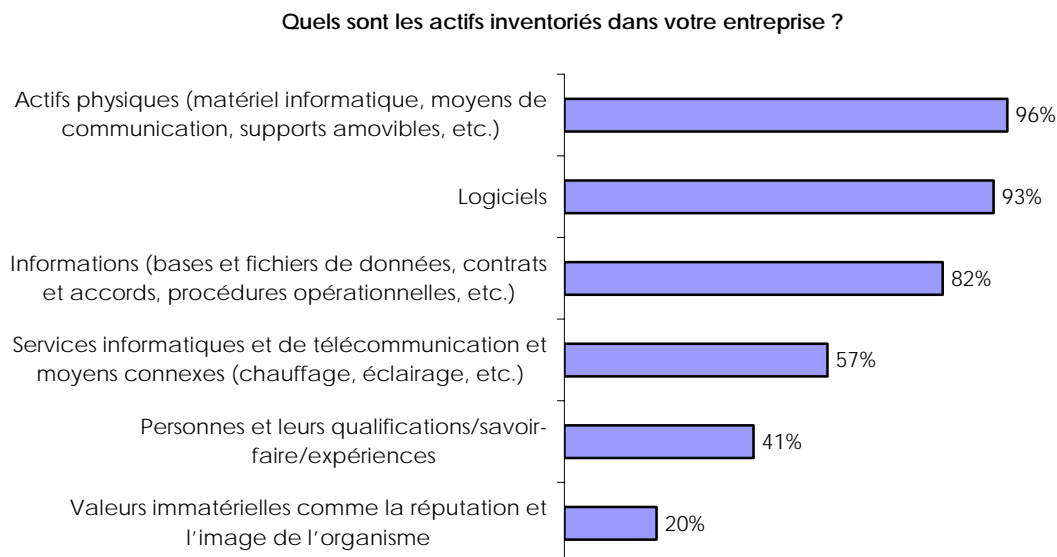
Thème 7 : Gestion des actifs et identification des risques

La gestion des risques liés au Système d'Information (SI) d'un organisme consiste schématiquement en la réalisation, puis le maintien à jour

- de l'inventaire [V] des actifs [I] relatifs à ce système d'information et de l'expression des besoins de sécurité [II] de ces actifs,
- de l'analyse des risques pesant sur ces actifs,
- du traitement de ces risques, afin de les réduire et les rendre acceptables.

Un inventaire partiel des actifs entraîne une identification partielle des risques.

Seule la moitié des entreprises interrogées ont réalisé un inventaire total des actifs relatifs à leur SI et un tiers un inventaire partiel. De plus, cet inventaire porte essentiellement sur les actifs physiques (96%), les logiciels (93%) et les bases et fichiers de données (82%).



Graphique 5 : Actifs inventoriés en entreprise

L'inventaire des actifs relatifs au SI étant une composante nécessaire à la gestion des risques, cela signifie qu'au moins une entreprise sur deux n'est pas en mesure d'identifier l'ensemble des risques qui pèsent sur son SI.

La classification des actifs sous la responsabilité de ses propriétaires reste à systématiser.

La classification (ou l'expression des besoins de sécurité) des actifs inventoriés est principalement réalisée, soit par le RSSI (39%), ou le propriétaire de chaque actif (24%), ou le chef de projet informatique / réseau (23%). Il est à noter que si le propriétaire d'un actif [X] peut déléguer la classification de cet actif, il reste néanmoins responsable de cette classification.

Le nombre de nouveaux projets informatiques prenant en considération la sécurité au plus tôt constitue un résultat encourageant.

Concernant les nouveaux projets informatiques, 3 entreprises sur 4 réalisent l'expression des besoins de sécurité et l'analyse des risques dès la phase de conception au moins pour les projets jugés "sensibles". Seulement la moitié de ces entreprises le font pour tous les projets. Ce chiffre démontre un grand progrès dans l'appréciation des risques informatiques.

La gestion des risques, un grand choix de méthodes.

Ces quelques résultats montrent que les fondements de la gestion des risques liés au SI sont ignorés par plus d'une entreprise sur deux. Il existe pourtant de nombreuses méthodes permettant de classer les actifs et d'apprécier et traiter les risques relatifs à la sécurité du SI. Citons, par exemple, parmi les méthodes les plus utilisées en France, MEHARI [VIII] et EBIOS [III]. L'utilisation de l'une ou l'autre de ces méthodes peut de plus s'inscrire dans une démarche plus large de management de la sécurité de l'information comme spécifiée par l'ISO/IEC 27001:2005 [VII] par exemple.

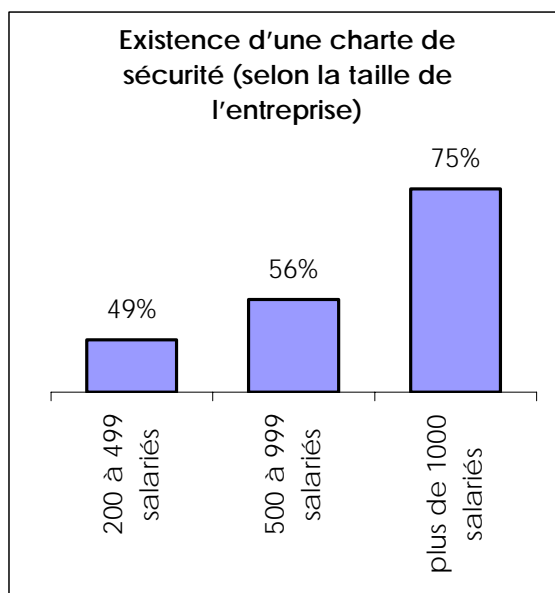
Thème 8 : Sécurité des ressources humaines (charte, sensibilisation)

Chartes de sécurité : un passage obligé

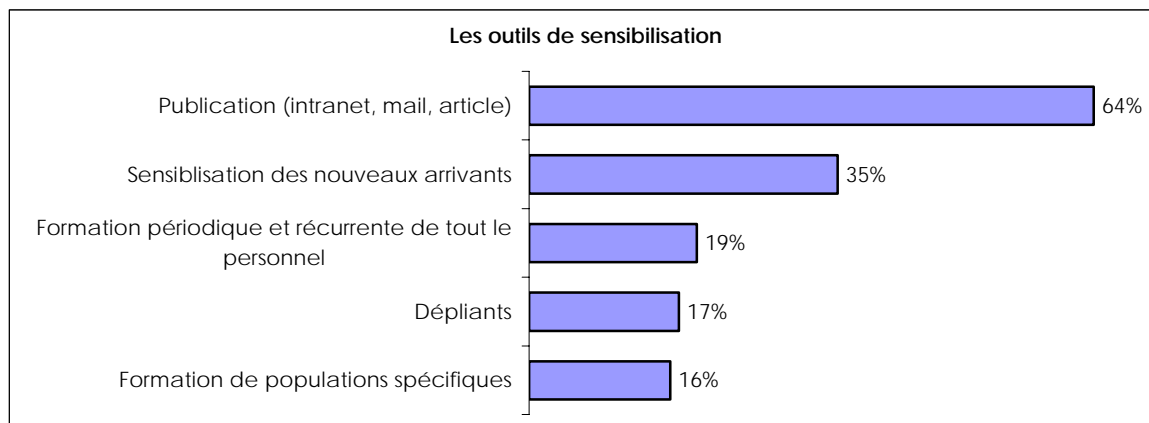
La proportion des entreprises dotées d'une charte sécurité atteint 55%. Elle est plus élevée pour les entreprises de services (66%) par rapport aux secteurs du commerce, de l'industrie et des transports/télécoms. On observe également un effet de taille d'entreprise : entre les PME de moins de 500 salariés et les grandes entreprises de plus de mille collaborateurs, l'écart atteint vingt cinq points. Ce décalage tient à l'importance des ressources mises en œuvre et à la maturité des politiques de sécurité dans les grandes organisations.

Il s'exprime également dans la mise en œuvre de programmes de sensibilisation : un tiers des entreprises de moins de 500 salariés disposent de telles programmes, mais la moitié de celles de plus de mille salariés (37% en moyenne pour l'ensemble des entreprises). Les moyens les plus répandus restent la publication (sur l'intranet, par mailing, affiches ou articles), à 64%, et les sessions de sensibilisation pour les nouveaux arrivants. Hélas, l'impact de cet effort de sensibilisation n'est guère mesuré (par seulement 23% des entreprises), surtout dans les PME (18%).

En revanche, une fois que les chartes sont mises en œuvre, le critère de la taille de l'entreprise ou du secteur économique semble beaucoup moins discriminant. On peut interpréter cette situation comme le signe que lorsque les bonnes pratiques sont intériorisées dans une organisation, elles sont appliquées largement. Ainsi, la consultation des instances représentant le personnel, la communication aux collaborateurs ou encore l'annexion aux contrats de travail ne dépendent pas de la taille de l'entreprise ni de son secteur. On note toutefois que la consultation des représentants du personnel est moins fréquente dans les entreprises de moins de 500 salariés.



Graphique 6 : Existence d'une charte de sécurité, selon la taille des entreprises



Graphique 7 : Moyens utilisés pour assurer la sensibilisation du personnel des entreprises

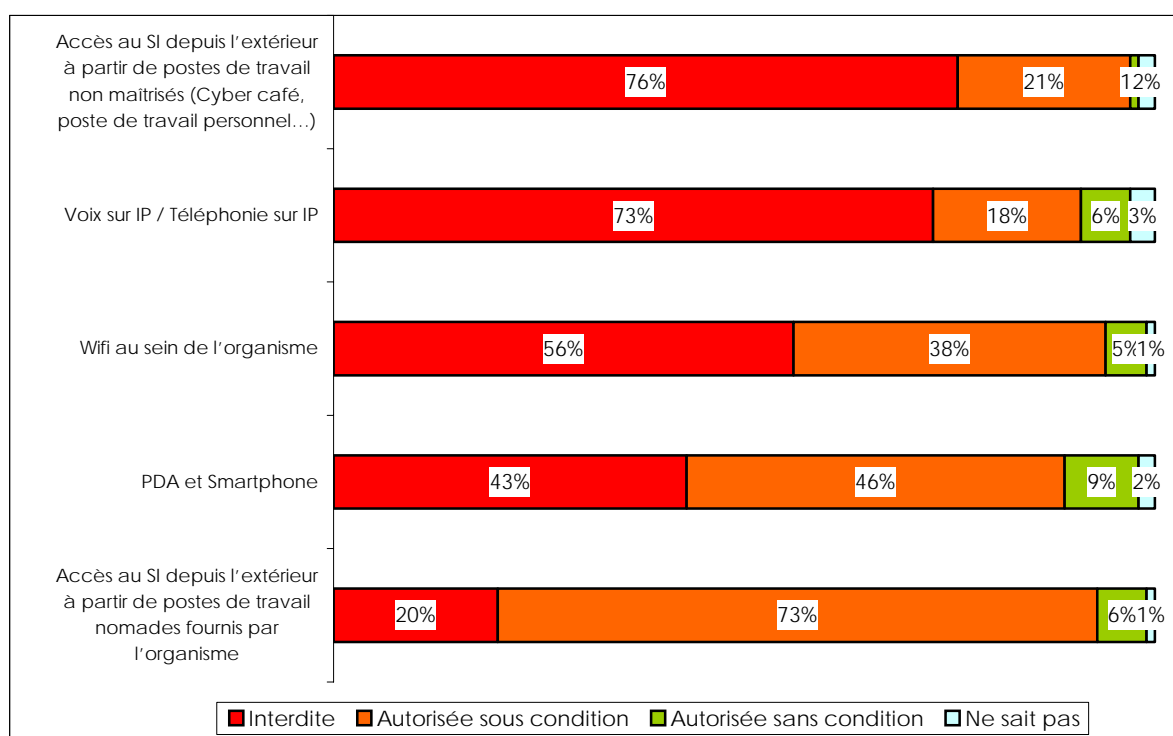
Thème 10 : Gestion des communications et des opérations

Sécurisation des nouvelles technologies

Une forte volonté de contrôle

L'interdiction des nouvelles technologies qui induisent des risques pour la sécurité semble être encore souvent la méthode retenue pour se prémunir de ces risques dans les entreprises :

- 76 % interdisent l'accès (webmail, extranet) à partir d'un poste non maîtrisé,
- 73 % « interdisent la voix sur IP »
- 56 % interdisent le wifi
- 43 % (disent ou souhaitent ...) interdire PDA et smartphones
- 20 % interdisent l'accès au SI en situation de mobilité, même avec un poste contrôlé



Graphique 8 : Sécurisation des nouvelles technologies en entreprise

Une position de fermeté qui ne sera pas facile à maintenir

Une portion très importante des sondés affiche une position qui est ou sera difficile à tenir face au déploiement de nouvelles technologies : tout d'abord, certaines sont appréciées des utilisateurs finaux, comme la voix sur IP (via autocom ou via Skype™, par exemple), ou encore le webmail, le wifi, ou les assistants personnels. Une opposition formelle et continue sera ressentie comme un frein à l'innovation. D'autre part, dans un certain nombre de cas, l'interdiction s'avère très difficile à faire appliquer sur le plan technique (cas de Skype™ ou des PDA ...). Le RSSI devra donc s'efforcer de proposer des règles et des solutions permettant de contenir les risques, et de sensibiliser les utilisateurs aux bonnes pratiques à adopter dans l'utilisation de ces technologies.

Des mises en gardes pas toujours en rapport avec les incidents constatés

Enfin, en cas de demande d'arbitrage, attention aux statistiques d'incidents (cf. plus bas) qui ne viennent pas à l'appui de la position du RSSI : pour l'instant, les incidents officiellement recensés font très peu appel aux nouvelles technologies ...

Ainsi, puisque l'on constate que le vol de portables est l'une des conséquences notables de la progression de certains usages (ici l'accès depuis l'extérieur), est-il logique que les conditions de cet usage soient à 53% basées sur l'authentification forte, à 39% sur le chiffrement des échanges, mais à seulement 19% sur le chiffrement des données locales ?

Si la situation n'évolue pas, et que les mesures d'interdiction nécessitent un investissement pour être appliquées, il risque d'y avoir rapidement divergence entre les intentions et les faits.

Lutte anti-virale, protection contre les intrusions et gestion des vulnérabilités

Un déploiement très progressif des nouvelles technologies de sécurité

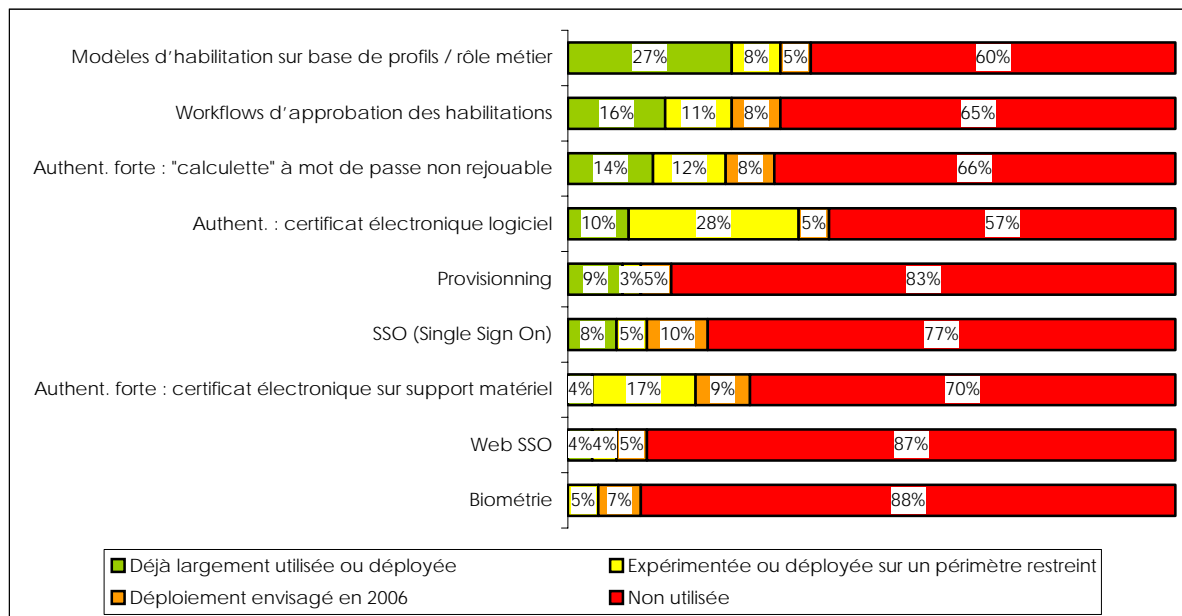
Les outils de sécurité les plus connus, les plus présents sur les PC des particuliers ou dans les points de connexion à Internet sont aujourd'hui déployés de façon massive en entreprise : antivirus à 97%, pare-feu à 88 %, anti-spam à 70 %. En revanche, les solutions de nouvelle génération plus complexes, plus innovantes ou plus récentes, telles que IDS / IPS / SIM, ou outils de chiffrements et pare-feu personnels connaissent un déploiement beaucoup plus progressif. Ce deuxième groupe de solutions n'est adopté que par 15 à 29% des sondés, et ne sera pas utilisé à court terme par 47 à 64 % des sondés. Un cas particulier à retenir : le pare-feu personnel, « rejeté » à 50 % est encore couramment (96%) associé aux postes portables.

Sécurité et infogérance de services d'exploitation

Des contrats plutôt bien surveillés

Lorsque les entreprises externalisent une partie de l'exploitation de leur SI (cas d'un gros quart d'entre elles) ces contrats sont plutôt régulièrement suivis (65 %) et audités (50 %) sous l'angle de la sécurité.

Thème 11 : Contrôle des accès



Graphique 9 : Technologies de contrôle d'accès au système d'information en entreprises

Des technologies encore peu déployées...

Le contrôle des accès logiques, qui est un élément crucial en matière de sécurité de l'information, semble encore en être à ses balbutiements. Le sujet progresse, mais le déploiement des technologies prend du temps. Dans ce domaine, les efforts des entreprises ont principalement porté sur le renforcement des moyens d'authentification. La biométrie reste pour l'instant très en retrait et surtout utilisée en sécurité physique : les entreprises semblent encore peu rassurées par la technologie, et freinées par son coût élevé.

En revanche, nous constatons une montée en puissance des certificats électroniques logiciels (38 % : les téléprocédures administratives y sont sûrement pour beaucoup) et des « calculatrices » à mot de passe non jouable (26%). Pour autant, ces chiffres semblent faibles au regard des risques générés par le développement rapide du nomadisme et des applications extranet. Même si les entreprises hésitent encore à ouvrir leur SI (cf. le thème 10), elles le font encore souvent sans prendre les précautions nécessaires.

Enfin, on est au stade des tous premiers déploiements pour les technologies de SSO ou de provisionning (création automatique des comptes et des droits), sachant que dans les entreprises de plus de 1000 salariés, ces sujets donnent lieu à des réflexions et à des projets de manière plus soutenue en 2006.

...mais la volonté de rationaliser les modèles et les processus

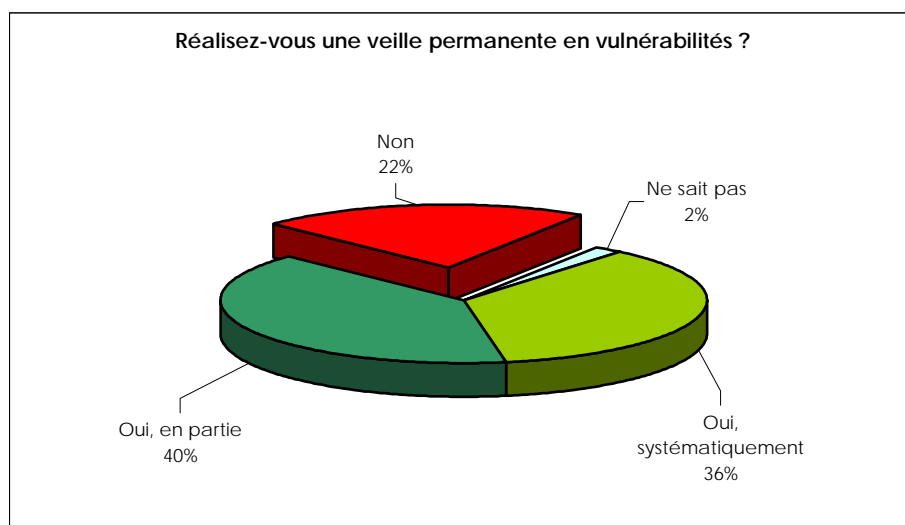
Côté progression, il est positif et rassurant de constater le développement significatif des modèles d'habilitation reposant sur les profils métiers et non pas directement sur les identités des personnes : ce type de modèle est généralisé par 27% des entreprises et utilisé en partie par 8% d'entre elles. Cette approche, formalisée notamment par le modèle RBAC (Role Based Access Control), semble bien être la seule qui va permettre progressivement de rationaliser des processus de gestion des droits de plus en plus complexes et de plus en plus pénalisants tant pour la sécurité que pour la qualité de service.

Les utilisateurs ne tolèrent plus de longs délais d'attribution des habilitations, et la sécurité ne peut pas se permettre l'existence de comptes orphelins ou l'attribution de droits injustifiés. Ce point souligne d'ailleurs l'importance des aspects processus et gestion du changement organisationnel dans tous les projets de gestion des identités et des accès.

Thème 12 : Acquisition, développement et maintenance

Veille et gestion des vulnérabilités : une pratique qui se généralise

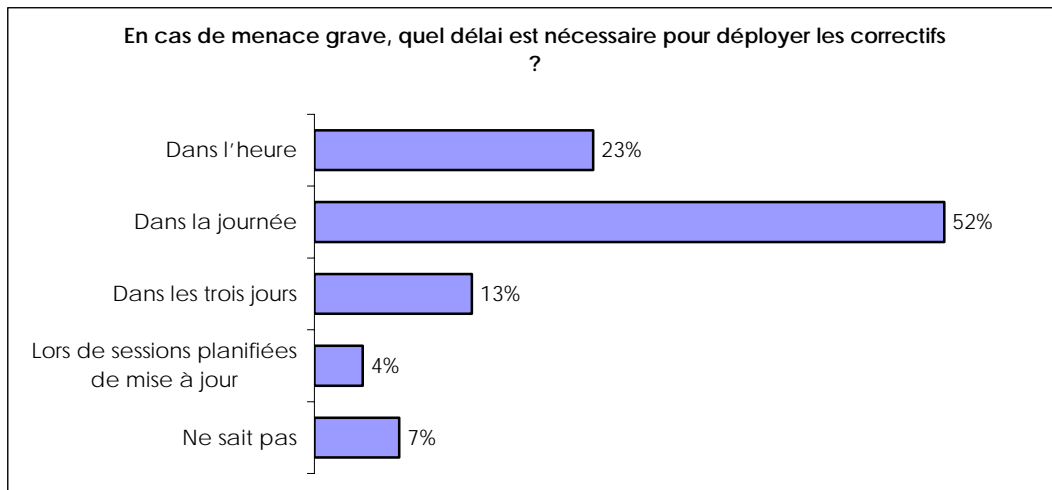
Près de 3 entreprises sur 4 disent réaliser systématiquement ou en partie une veille sur les nouvelles failles de sécurité découvertes et sur les nouvelles attaques.



Graphique 10 : Veille permanente en vulnérabilités en entreprise

Maintenance et déploiement de correctifs de sécurité : une industrialisation partielle

Toutefois, 42% reconnaissent ne pas avoir formalisé les procédures de déploiement associées (de « patch management »). Pour les près de 6 entreprises sur 10 qui l'ont fait, le résultat revendiqué est que le délai nécessaire au déploiement du correctif de sécurité ne dépasse pas une journée pour 3 entreprises sur 4. A noter que les grandes entreprises sont plus avancées (75% des entreprises de plus de 1000 salariés ont formalisé les procédures de déploiement de correctifs). A noter que ce résultat, que nous qualifierons d'optimiste par rapport à l'expérience des experts et à d'autres enquêtes, répond à une situation de « menace grave ».



Graphique 11 : Gestion des vulnérabilités en entreprise

Thème 13 : Gestion des incidents de sécurité

Un suivi encore faible des incidents de sécurité

A 58%, les entreprises interrogées n'ont pas d'équipe dédiée à la collecte et au traitement des incidents de sécurité, proportion qui varie de 63% dans les entreprises de 200 à 500 salariés à 39% dans les entreprises de plus de 1000 salariés.

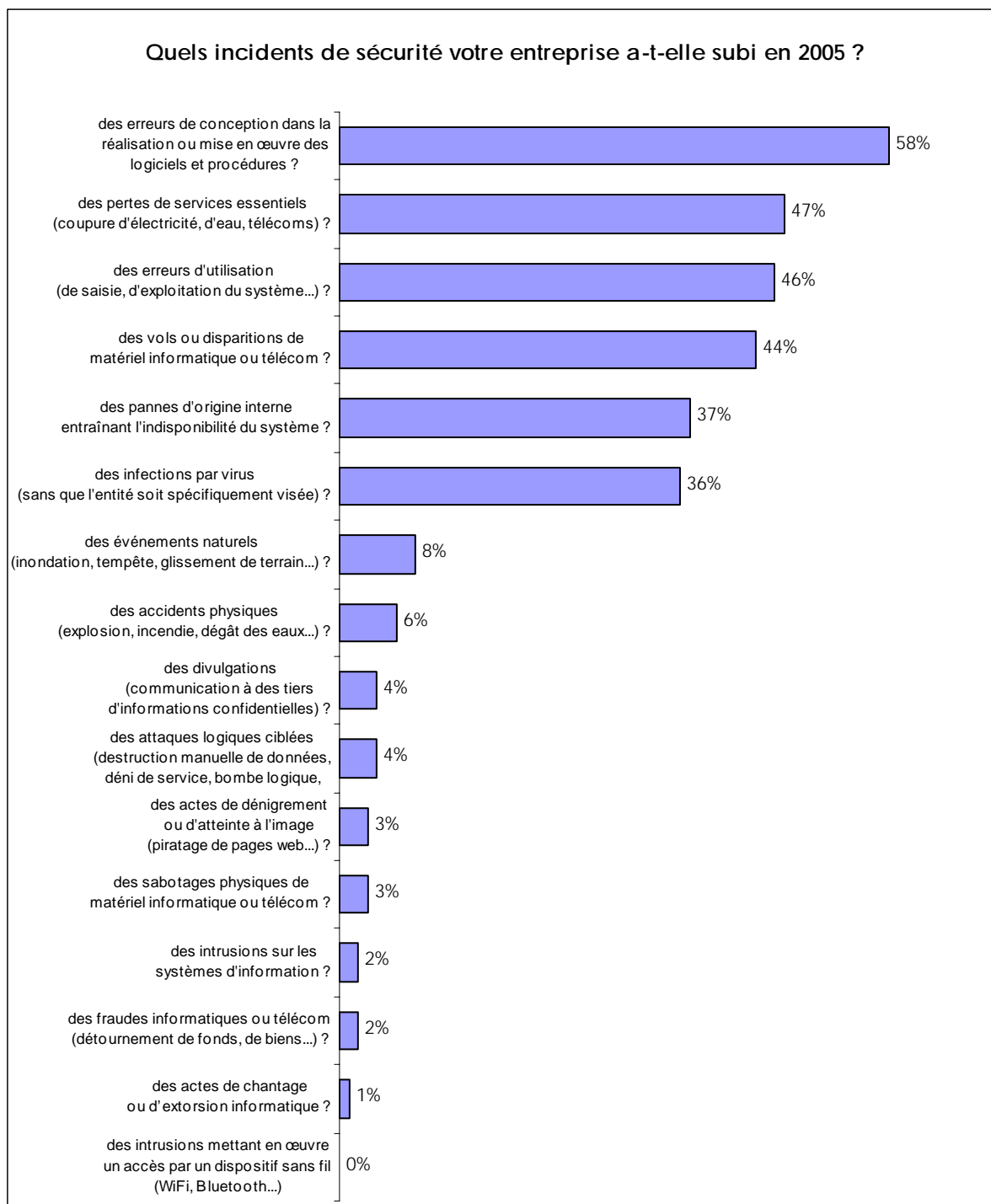
Cette absence d'outil de mesure précis de l'impact des incidents de sécurité se confirme par un taux faible (24%) d'entreprises qui procèdent à une évaluation financière de l'impact des incidents de sécurité. Cette notion n'a pas évolué depuis notre dernière étude publiée en 2004.

Malveillance informatique : un phénomène bien réel

Outre les incidents liés à des causes fortuites qui restent, et c'est heureux, les plus importants en quantité, la malveillance ou la négligence sont bien réellement présentes, et ceci même si les pourcentages des incidents liés à des malveillances peuvent paraître faibles au premier abord. Si on les cumule et si on les extrapole sur l'ensemble des entreprises, le nombre d'incidents constatés est significatif !

Vols et pertes de matériels à un niveau inquiétant

Les incidents liés à des infections par virus constituent toujours un problème important pour les entreprises consultées (36%), mais on note une progression inquiétante – quoique logique – des problèmes de vols ou de pertes de matériels par rapport aux chiffres relevés par le CLUSIF pour l'année 2003 : sur la tranche 200 à 499 salariés, étudiée en 2003 et en 2005, la proportion des PME ayant constaté au moins un vol est passée de 6% à 37%. Cette proportion atteint son maximum à 65% pour les entreprises de plus de 1000 salariés. La grande pénétration des outils nomades (PDA, ordinateurs portables) explique certainement ce constat.



Graphique 12 : Typologie des incidents de sécurité en entreprise

Enfin, les dépôts de plaintes sont encore rares : malgré l'ampleur des problèmes rencontrés, 5% des entreprises ont porté plainte suite à des incidents liés à la sécurité informatique en 2005.

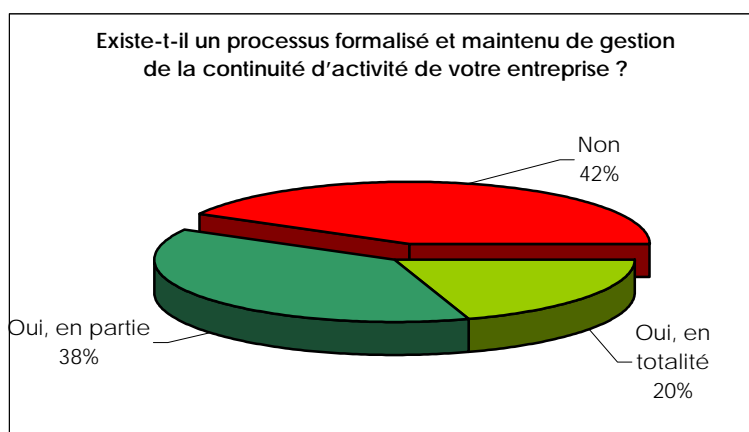
Thème 14 : Gestion de la continuité

Une grande disparité dans la maîtrise du processus

Si la dépendance vis-à-vis de l'informatique est largement reconnue par les entreprises interrogées, force est de constater que de grandes disparités subsistent dans la maîtrise de la gestion de la continuité d'activité.

Alors que la quasi-totalité des entreprises, tous secteurs d'activité confondus, et quel que soit le nombre de personnes, déclarent une dépendance forte vis-à-vis de l'informatique, plus de 40% des entreprises n'ont toujours pas mis en place un processus de gestion de la continuité d'activité ; nous pouvons constater que moins les entreprises ont de salariés, plus l'absence de processus de continuité est forte. Une explication de l'absence de processus peut être une surestimation de la complexité et du coût de mise en œuvre d'un plan de continuité.

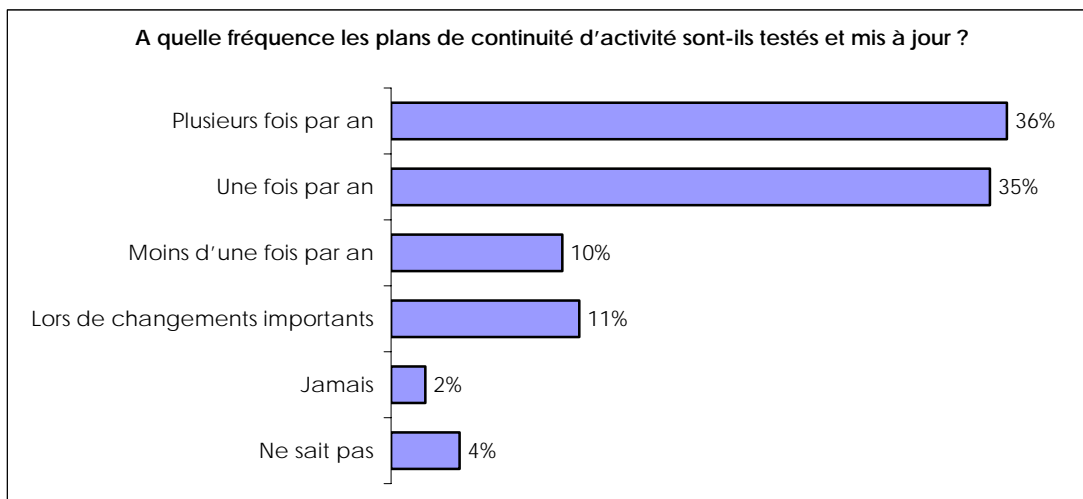
Par ailleurs, si les processus de continuité d'activité mis en place intègrent majoritairement l'aspect informatique (sauvegarde des données, secours informatique), les processus de gestion de crise et de continuité d'activité métiers restent à développer dans de très nombreux cas.



Graphique 13 : Plan de continuité d'activité d'entreprise

La maintenance : un enjeu fort

Les entreprises, qui ont mis en place un processus formalisé de gestion de la continuité d'activité de leur système d'information, ont conscience que la maintenance de ce processus est un enjeu vital. Les tests constituent un temps fort de la maintenance ; 2/3 des entreprises concernées déclarent en réaliser régulièrement (au moins une fois par an). En revanche, les processus de maintenance mis en place, notamment les tests réalisés, restent de nature très diverses et ne sont donc pas forcément un révélateur de bon fonctionnement des moyens de continuité mis en place.



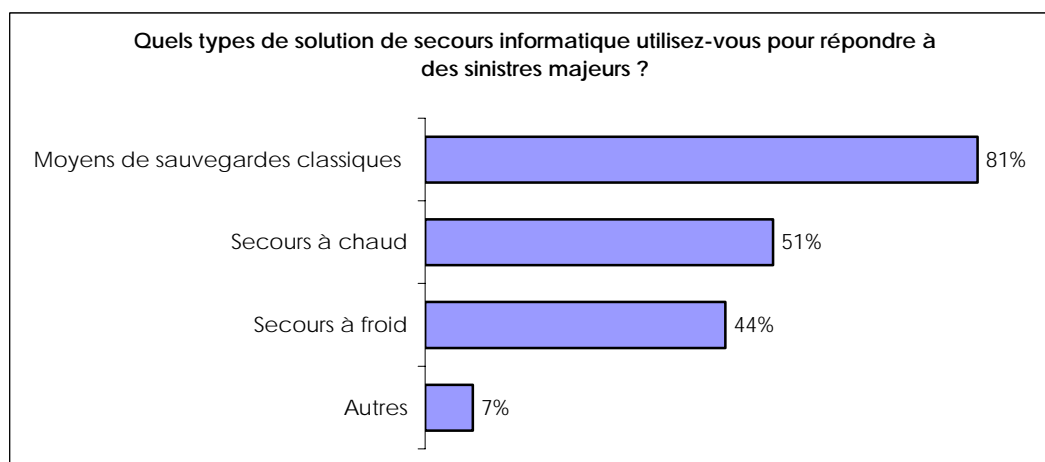
Graphique 14 : Fréquence de test et de mise à jour des plans de continuité d'activité en entreprise

Etat des lieux du secours informatique

Il apparaît clairement que le marché tend à réduire les délais de reprise et la perte de données informatiques acceptée par les entreprises. Cette tendance a certainement pu être facilitée par l'innovation dans les outils de secours proposés, ainsi que par les prix pratiqués à la baisse par les fournisseurs de solutions.

Si la grande majorité des entreprises interrogées déclare réaliser des sauvegardes en « bon père de famille », en utilisant des moyens « classiques », base de tout secours possible suite à une perte de données, 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.

De même, si le recours à des moyens de secours semble se généraliser (51% des entreprises utilisent des moyens de secours à chaud, 44% à froid), il n'est pas sûr que la solution de secours informatique mise en place consiste en un véritable recueil des procédures de reprise de l'architecture de secours, retenue par l'entreprise, sur des moyens externalisés par rapport au site des moyens de production.



Graphique 15 : Types de solution de secours informatique en entreprise

Une amélioration prévisible de la gestion de la continuité d'activité

On peut penser que, globalement, ces résultats vont sensiblement s'améliorer dans les années à venir, et ce en raison d'au moins 3 phénomènes :

- un courant réglementaire de plus en plus fort : obligation légale ou réglementaire pour une partie des entreprises (directement pour les entreprises du secteur financier par le règlement CRBF 97-02 modifié par le règlement 2004-02, indirectement pour les entreprises soumises à la Loi française de Sécurité Financière ou à loi américaine dite Sarbanes-Oxley),
- le développement de la gestion globale des risques,
- le facteur commercial différenciateur dans le cadre d'entreprises devant répondre à des appels d'offres.

Thème 15 : Conformité (CNIL, audits, tableaux de bord)

CNIL

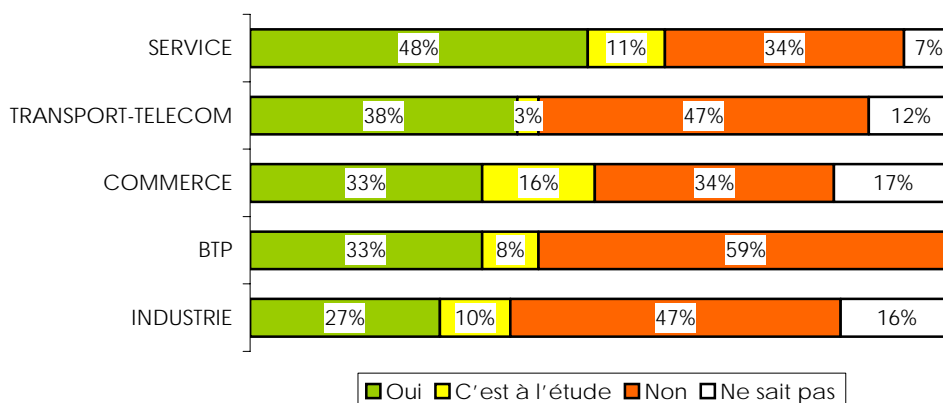
30% d'entreprises non conformes aux exigences de la CNIL

70% des entreprises déclarent estimer être en conformité avec les obligations de la loi informatique et libertés (ce qui en laisse tout de même 30% où la situation est incertaine). Cela reste d'ailleurs assez constant que l'on classe les entreprises par leur nombre de salariés ou par secteur d'activité.

Le correspondant CNIL : un dispositif encore mal compris

Le dispositif du correspondant CNIL, mis en place suite à la modification de la loi informatique et libertés en août 2004, et le décret d'application correspondant d'octobre 2005, est en revanche compris de façon encore très variable par les entreprises. D'emblée, on constate que les réponses fournies par les entreprises interrogées ne correspondent pas au bilan effectué récemment par la CNIL qui a annoncé connaître 79 correspondants informatique et liberté dans 190 organisations différentes au 22 mars 2006, à comparer aux 24% d'entreprises qui déclarent l'avoir mis en place (ce qui correspondrait à plus de 1000 entreprises).

Votre entreprise met-elle en place un Correspondant Informatique & Liberté ?



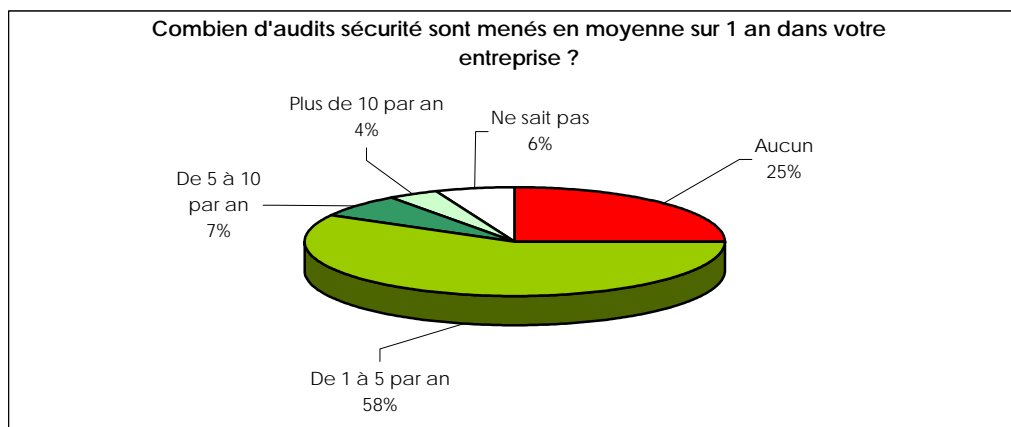
Graphique 16 : Mise en place de correspondants CNIL par secteur d'activité en entreprise

La mise en place récente de ce dispositif explique certainement la confusion existant encore dans l'esprit des personnes ayant répondu au questionnaire, qui ont très certainement (pour la plupart de ceux qui ont répondu oui) chargé depuis de nombreuses années une personne du suivi des dossiers de déclaration CNIL, ce que semble confirmer la comparaison sur ce point par secteurs d'activité (voir Graphique 16), où les entreprises des secteurs les plus concernés par ces déclarations arrivent en tête. Il sera intéressant d'observer ces proportions relatives dans les années à venir où la désignation d'un correspondant CNIL – qui peut être un spécialiste extérieur à l'entreprise – aura aussi un gros intérêt pour les entreprises qui font peu de déclarations de bases de données nominatives.

Audits

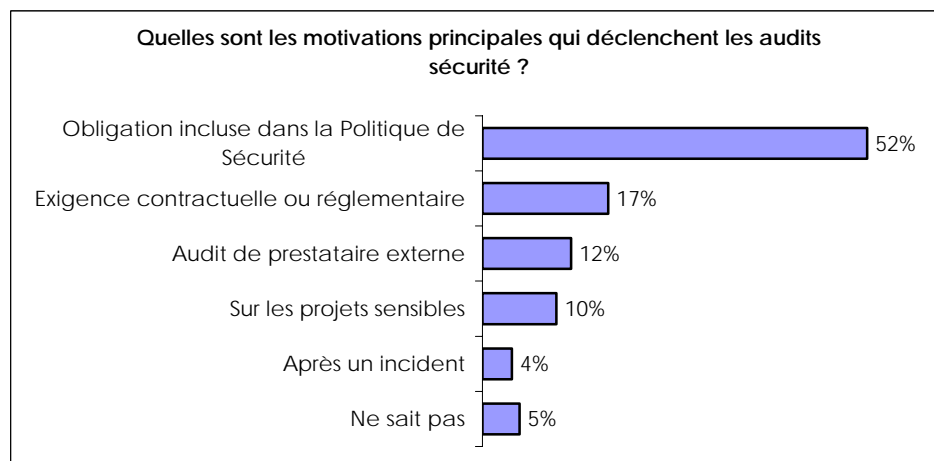
Une forte progression du contrôle et de l'audit

Les audits commencent à devenir une composante culturelle des entreprises françaises puisque 69% d'entre elles ont eu au moins un audit de sécurité dans l'année qui s'est écoulée. Une progression spectaculaire puisqu'en 2003, seulement 44 % des entreprises de moins de 500 salariés avaient recours aux audits, en 2005 elles sont 67% à les pratiquer au moins une fois par an !



Graphique 17 : Nombre d'audits sécurité en 2005 dans l'entreprise

Une fois sur deux ces audits ont été motivés par une obligation incluse dans la politique de sécurité de l'entreprise. Ce qui signifie que pour une grande majorité de celles qui ont formalisé leur Politique de Sécurité, les entreprises voient la nécessité de contrôler son implémentation.

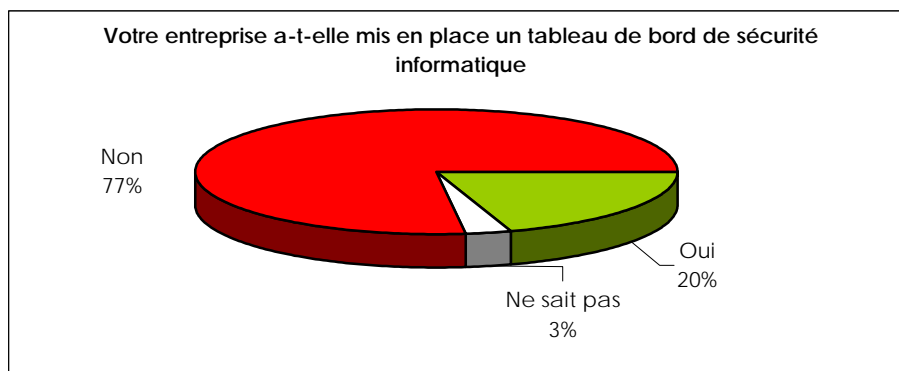


Graphique 18 : Motivations principales des audits sécurité en entreprise

A noter que seuls 12% des ces audits concernent la vérification d'un prestataire externe. Le contrôle a donc pour cible majoritaire les processus et systèmes internes. Il semble donc encore une fois que les différentes lois et réglementations (SOx, LSF, CRBF...) imposant un renforcement des contrôles internes ne soient pas étrangères à cette forte augmentation.

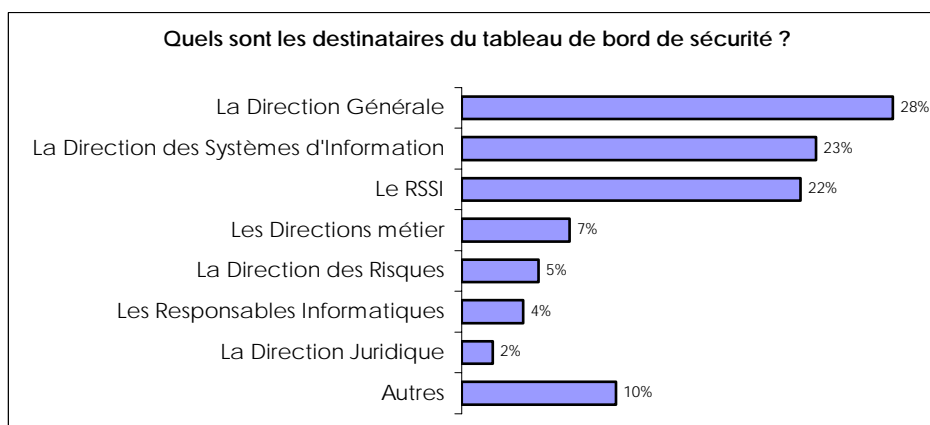
Tableaux de bord.

Ce sujet, véritable antienne des réunions entre RSSI, ne s'impose toujours pas. En effet, seulement 20% des entreprises ont mis en place un tableau de bord.



Graphique 19 : Mise en place des tableaux de bord de sécurité en entreprise

Un des aiguillons des RSSI dans ce domaine semble être la direction générale, mais il apparaît clairement que ces initiatives restent encore confinées au niveau des organes pilotant le Système d'Information (à 51%).



Graphique 20 : Destinataires du tableau de bord de sécurité en entreprise

Les indicateurs retenus dans ces tableaux de bord sont essentiellement, d'une part le respect des politiques et l'avancement des projets de sécurisation, et d'autre part les incidents et vulnérabilités, ce qui explique que leur diffusion soit limitée à ces organes. La difficulté reste donc de générer des indicateurs de risque pertinents pour les directions métier.

Mairies



- ▶ Moyens informatiques des mairies de plus de 30 000 habitants
- ▶ Moyens consacrés à la sécurité de l'information par les mairies
- ▶ Thème 5 : Politique de sécurité
- ▶ Thème 6 : Organisation de la sécurité et moyens
- ▶ Thème 7 : Gestion des actifs et identification des risques
- ▶ Thème 8 : Sécurité des ressources humaines (charte, sensibilisation)
- ▶ Thème 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)

Les Mairies

Présentation de l'échantillon

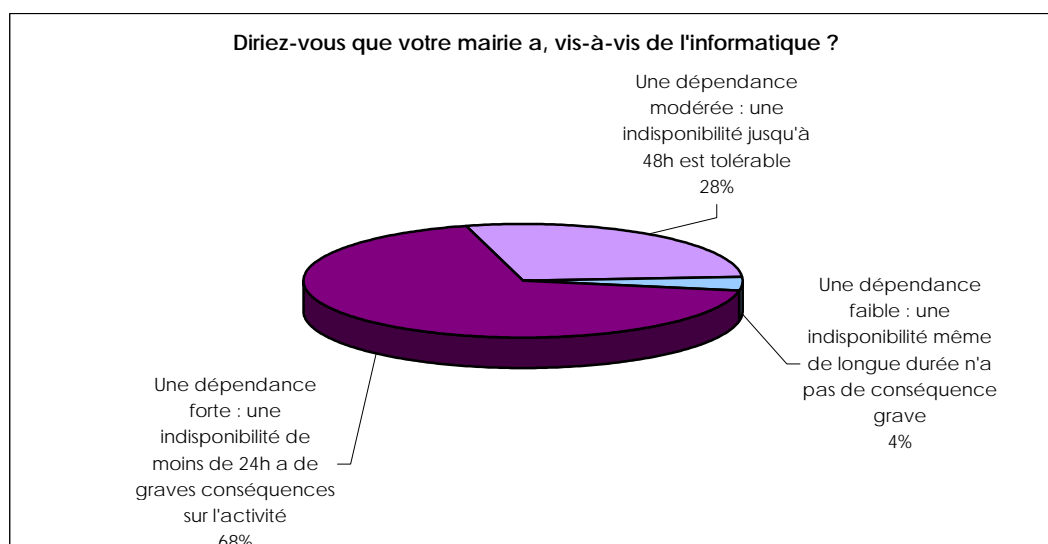
50 mairies de communes de plus de 30 000 habitants ont répondu à la sollicitation du CLUSIF, soit environ 15% des mairies de cette catégorie.

Au sein de chaque mairie, nous avons cherché à interroger en priorité le Responsable de la Sécurité des Systèmes d'Information (pour 10 % des mairies interrogées) ou le Fonctionnaire de la Sécurité des Systèmes d'Information (FSSI) (pour 8% des mairies), fonction équivalente au RSSI et qui est mise en place progressivement dans les administrations et services publics. A défaut, c'est le responsable informatique (pour 24 % des mairies interrogées) ou le responsable réseau (pour 24% des mairies interrogées) qui ont été contactés.

Dépendance à l'informatique des mairies

Les mairies aussi dépendantes de l'informatique que les entreprises

Comme dans de nombreuses autres administrations et entreprises, l'informatique est devenue pour les mairies un outil de travail essentiel. La défaillance de l'informatique pèse lourd sur l'activité de la mairie. Le pourcentage semble avoir augmenté par rapport à notre étude de 2003, même si cette dernière ciblait plus largement les collectivités territoriales.

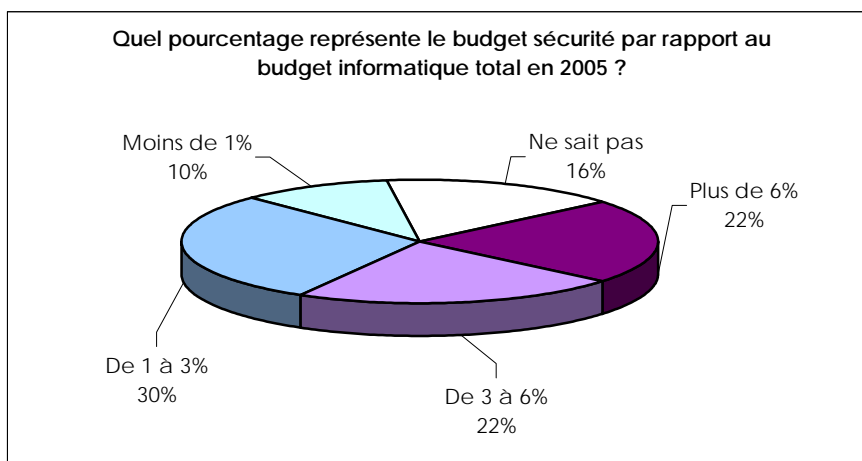


Graphique 21 : Dépendance des mairies vis-à-vis de l'informatique

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

44% des mairies de plus de 30 000 habitants déclarent utiliser plus de 3% de leur budget informatique pour la sécurité, la moitié d'entre elles se situant au-dessus de 6%.

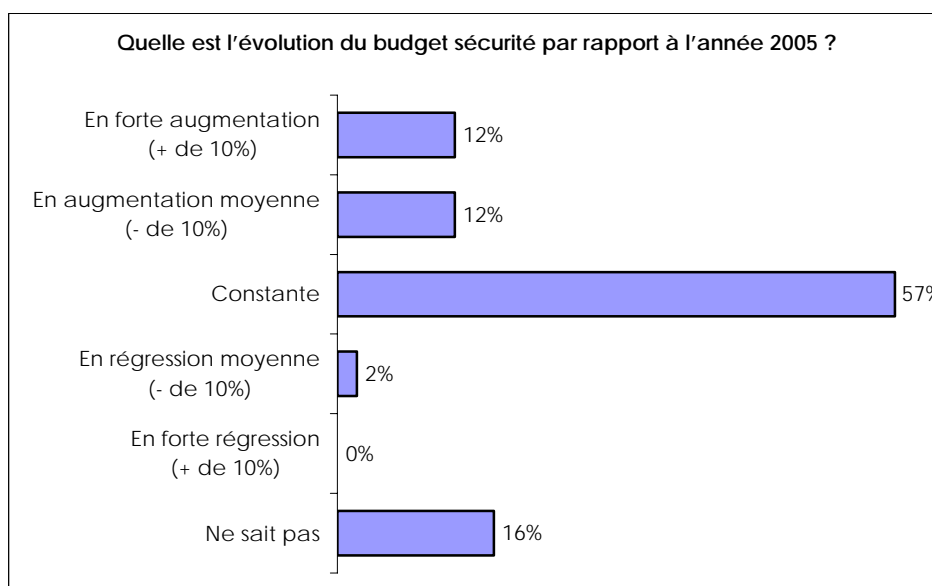
Ces chiffres sont donc tout aussi honorables que dans les entreprises. Pourtant, les mairies françaises ne sont pas au niveau d'investissement de leurs homologues à l'étranger.



Graphique 22 : Pourcentage du budget sécurité dans le budget informatique des mairies

Un budget sécurité stable ou en hausse...

Le budget sécurité est stable par rapport à l'année précédente pour 57% des mairies, en augmentation moyenne pour 12% des mairies, enfin en forte augmentation pour 12%. Globalement, pour 80% des mairies qui maintiennent ou augmentent ce budget, la sécurité est perçue comme un enjeu primordial. 2% seulement des mairies avouent un léger recul du budget sécurité.



Graphique 23 : Evolution du budget sécurité des mairies

... qui reste un frein aux investissements sécurité

Malgré ce constat, 42% des mairies indiquent qu'un manque de budget freine la conduite des missions de sécurité, tandis que 25% avouent une lacune dans les compétences de leur personnel sur le sujet, et 22% de fortes contraintes organisationnelles.

Thème 5 : Politique de sécurité

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

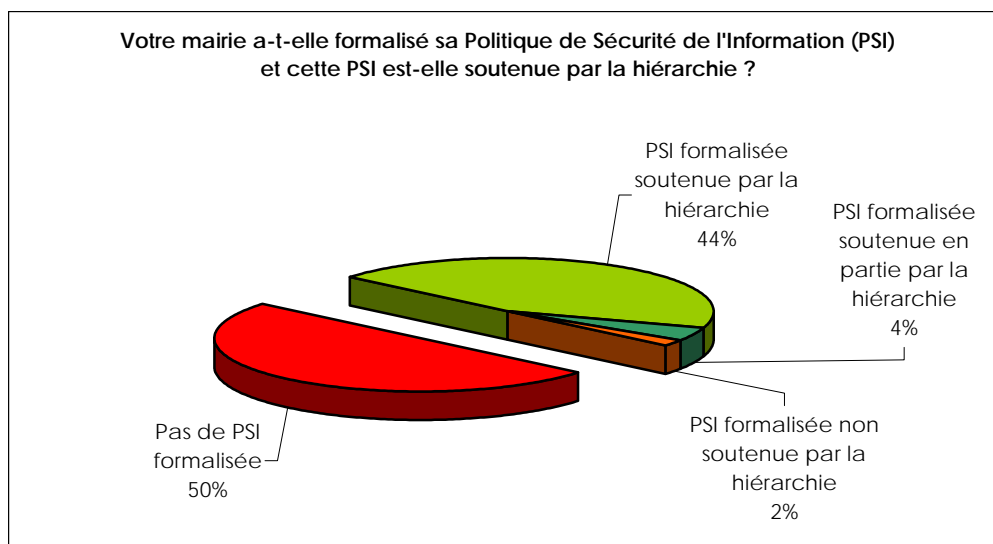
Malgré une forte dépendance perçue à l'informatique, les mairies semblent en retard dans la formalisation de leur politique de sécurité de l'information. Seulement 1 mairie sur 2 a formalisé sa politique de sécurité de l'information (PSI) mais avec un fort soutien de la hiérarchie dans la plupart des cas (88% des cas).

Une PSI essentiellement aux mains des informaticiens

L'élaboration de la PSI résulte très majoritairement du travail des informaticiens mais pas des autres acteurs de la collectivité 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 40% des mairies qui ont formalisé leur politique de sécurité de l'information l'ont fait en se référant à des normes exhaustives telle que l'ISO 17799 ou le guide PSSI de la Direction Centrale de la Sécurité des SI (DCSSI).



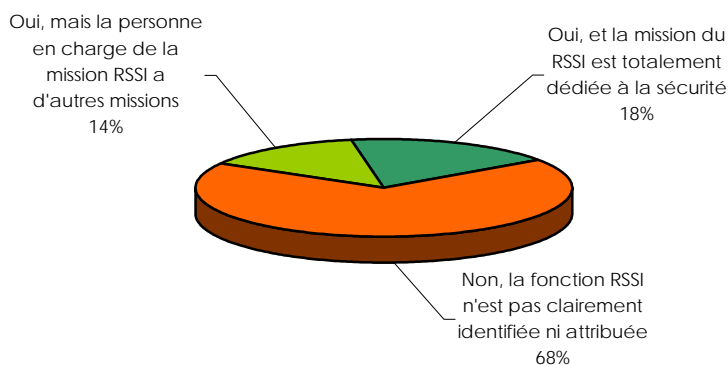
Graphique 24 : Soutien de la Politique de sécurité de l'information

Thème 6 : Organisation de la sécurité et moyens

Le RSSI, une fonction encore trop peu identifiée

Dans presque 7 cas sur 10, la fonction de RSSI n'est pas identifiée. Seulement 1 mairie sur 5 a confié à un agent à plein temps la fonction de RSSI. Moins d'1 sur 5 ont confié les missions du RSSI à un autre agent, qui exerce dans une très grande majorité des cas un métier en relation directe avec les systèmes d'information.

La fonction RSSI est-elle clairement identifiée ? Si oui, la personne en charge de la mission RSSI est-elle dédiée à cette mission ?



Graphique 25 : La mission de Responsable de la Sécurité des Systèmes d'Information (RSSI) dans les mairies

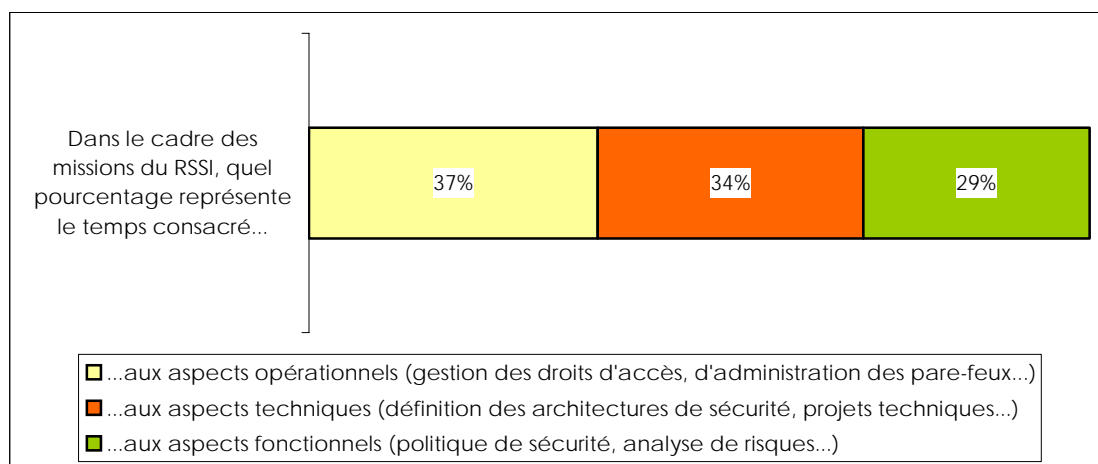
Le RSSI, un rattachement à la direction des systèmes d'information

1 fois sur 2, le RSSI est rattaché à la direction des systèmes d'information (DSI) et 1 fois sur 3 au directeur général des services. Dans ce dernier cas, ce rattachement est un signe fort de l'importance de la mission de RSSI pour la collectivité.

Le rattachement du RSSI à la DSI montre simplement que cette mission est déléguée par le directeur général des services.

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

Le RSSI consacre toutefois une part très légèrement supérieure de son activité aux aspects opérationnels.



Graphique 26 : Le RSSI, une fonction équilibrée entre l'opérationnel, le technique et le fonctionnel

Des effectifs dédiés en permanence à la sécurité des systèmes d'information

L'équipe permanente dédiée à la sécurité ne dépasse pas 5 personnes dans 96 % des cas.

- Près de 6 mairies sur 10 affectent 1 à 2 personnes à la sécurité de l'information,
- près de 4 mairies sur 10 affectent 3 à 5 personnes à cette même sécurité.

Même si la fonction de RSSI est encore peu diffusée dans les mairies, elles se donnent généralement les moyens d'exécuter correctement les missions liées à la sécurité tout en gérant au mieux les coûts inévitables engendrés par celle-ci.

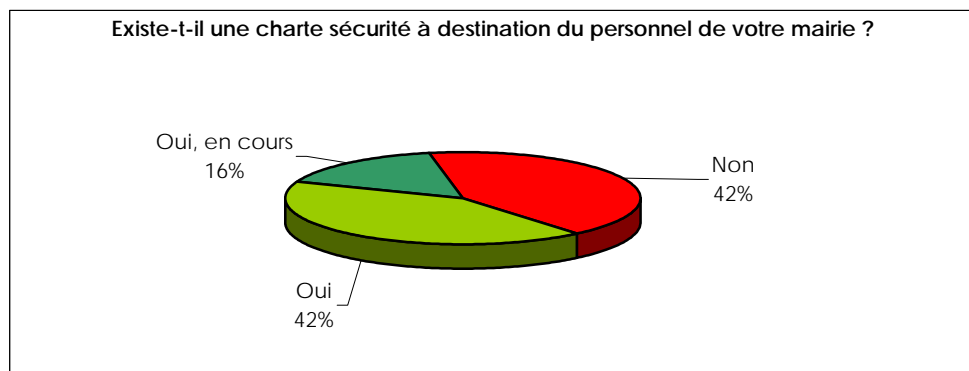
Thème 7 : Gestion des actifs et identification des risques

Les résultats de l'enquête relatifs à la gestion des risques concernant les mairies sont sensiblement identiques à ceux concernant les entreprises (cf. Thème 7 : Gestion des actifs et identification des risques des entreprises, page 16).

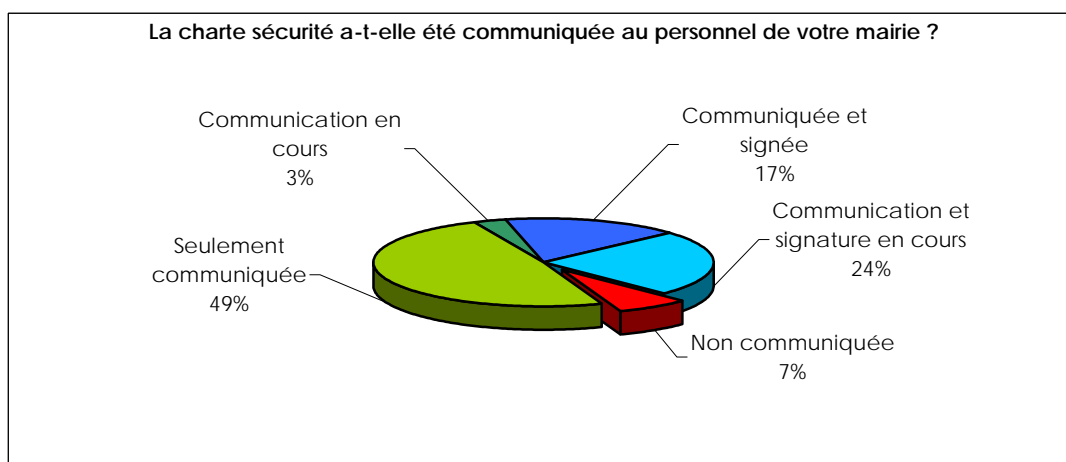
Thème 8 : Sécurité des ressources humaines (charte, sensibilisation)

Un déficit de communication et de sensibilisation

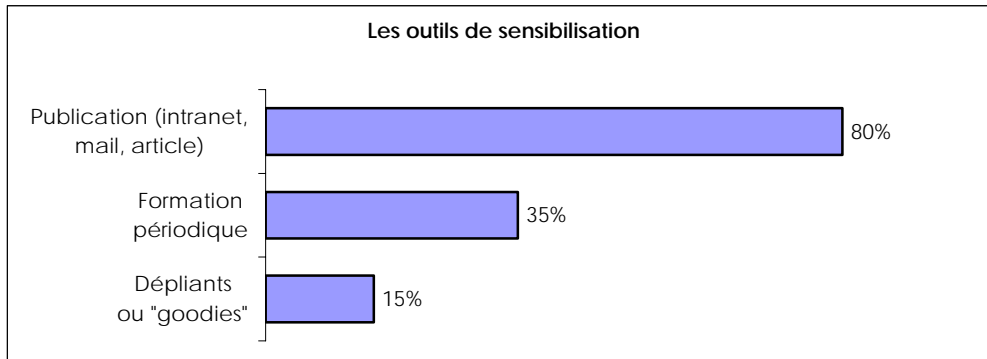
Les chartes de sécurité ne sont pas encore répandues dans la majorité des mairies de plus de 30 000 habitants : quatre sur dix ont élaboré un tel document. Dans un cas sur deux, elles font l'objet d'une communication aux utilisateurs du système d'information. Le constat d'un déficit dans le domaine de la communication autour de la sécurité de l'information est renforcé par la fréquence relativement faible des programmes de sensibilisation. On ne les retrouve que dans un tiers des mairies, essentiellement par des publications (dans 80% des cas). L'impact de ces programmes n'est mesuré que dans une mairie sur cinq qui les a mis en œuvre.



Graphique 27 : Chartes de sécurité à destination du personnel des mairies



Graphique 28 : Communication de la charte sécurité au personnel des mairies



Graphique 29 : Les moyens utilisés pour assurer la sensibilisation du personnel des mairies

Thème 10 : Gestion des communications et des opérations

Sécurisation des nouvelles technologies

Une forte volonté de contrôle, en particulier des accès externes

Comme dans les entreprises, l'interdiction des nouvelles technologies qui induisent des risques pour la sécurité semble être encore souvent la méthode retenue pour se prémunir de ces risques :

- 84 % interdisent l'accès (webmail, extranet) à partir d'un poste non maîtrisé,
- 60 % « interdisent la voix sur IP »
- 58 % interdisent le wifi
- 50 % interdisent l'accès au SI en situation de mobilité, même avec un poste contrôlé
- 46 % (disent ou souhaitent ...) interdire PDA et smartphones

A noter que les mairies sont encore plus méfiantes que les entreprises à l'égard des accès « externes ». Les remarques déjà faites pour les entreprises concernant l'image négative (frein à l'innovation) et la capacité réelle à implémenter de telles restrictions restent valables. Ces interdictions sont d'autant plus surprenantes que, parallèlement, l'accès en ligne des citoyens à des interfaces de l'Administration électronique ou à des formulaires en ligne se développe rapidement.

Lutte anti-virale, protection contre les intrusions et gestion des vulnérabilités

Les mairies présentent des réponses globalement semblables à celles des entreprises.

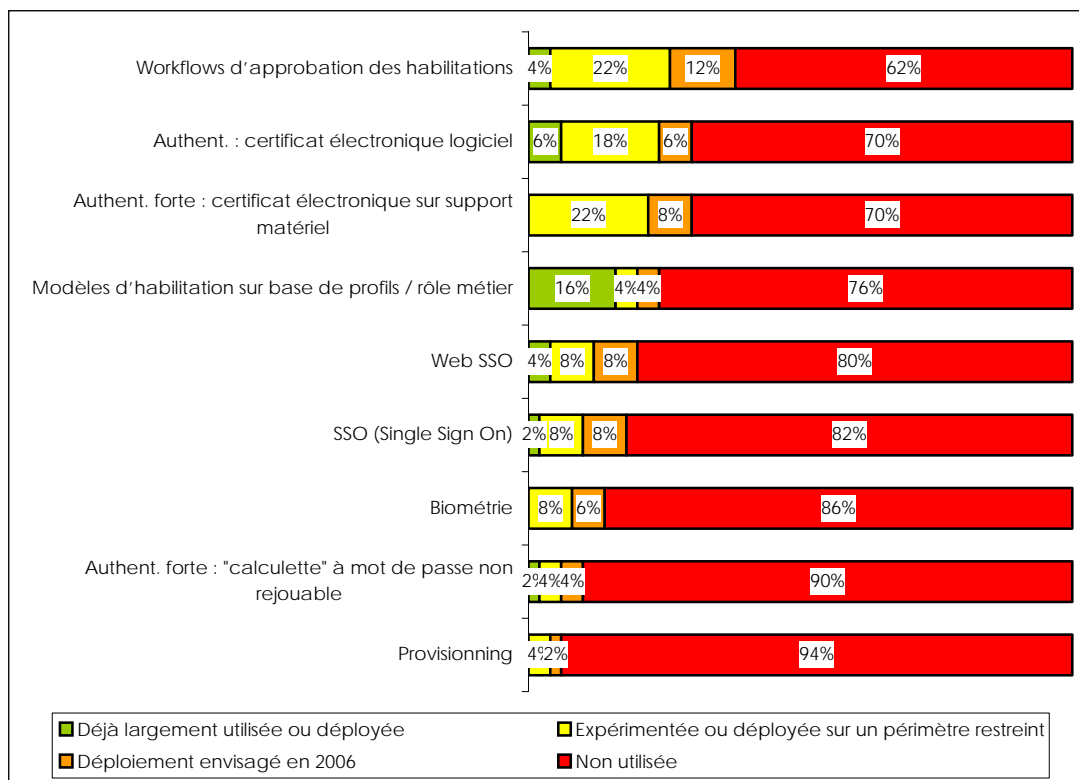
Sécurité et infogérance de services d'exploitation

Des services peu externalisés, mais aussi peu contrôlés

Alors qu'on aurait pu supposer des contraintes budgétaires entraînant un recours fréquent à la sous-traitance, les mairies ne disent externaliser qu'en partie l'exploitation de leur système d'information (12%), et ces services probablement peu stratégiques sont finalement peu contrôlés (17%).

Thème 11 : Contrôle des accès

Le constat dans les mairies est le même que pour les entreprises dans le domaine des technologies de contrôle des accès logiques au système d'information. Ces technologies restent encore très peu déployées. En revanche, les mairies sont largement en retard pour ce qui relève de l'optimisation des processus de gestion des droits et des accès.



Graphique 30 : Technologies de contrôle d'accès au système d'information dans les mairies

Thème 12 : Acquisition, développement et maintenance

Pas de divergence profonde des chiffres comparés à ceux des entreprises.

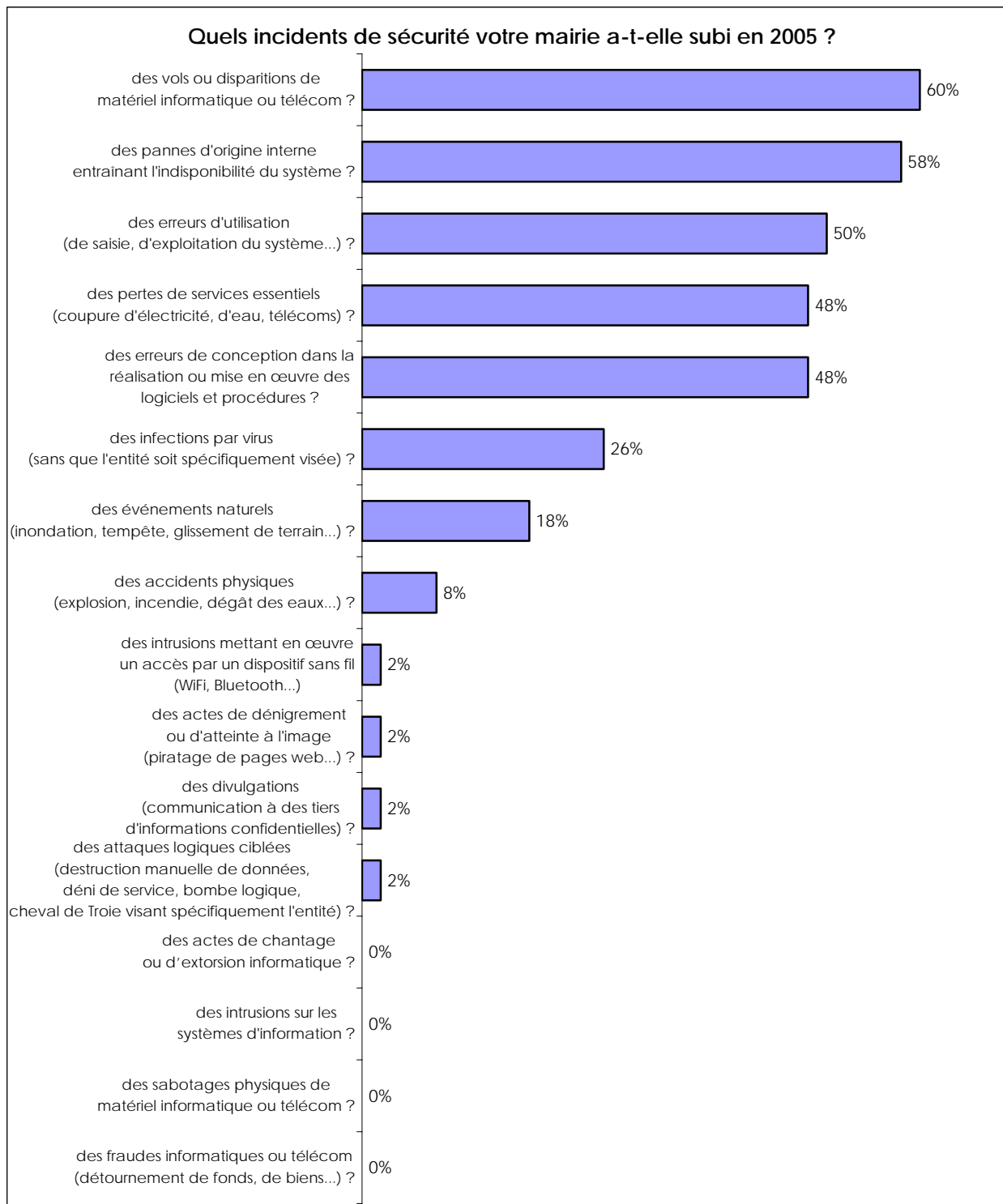
Thème 13 : Gestion des incidents de sécurité

Les mairies de plus de 30 000 habitants ont assez peu souvent mis en place une cellule dédiée à la sécurité informatique (30% d'entre elles), en totale cohérence avec l'identification d'un RSSI au sein de ces structures territoriales.

L'impact financier des incidents de sécurité est peu souvent évalué (12% des mairies concernées), ce qui semble particulièrement surprenant avec la première place prise parmi les incidents de sécurité par les vols ou disparitions de matériels informatique ou de télécommunications (60% des mairies, donc devant les pannes ou erreurs d'utilisation). Ces vols ou disparitions sont d'ailleurs la plupart du temps (pour 60% des mairies concernées) d'origine inconnue.

On note que les infections par virus sont rapportées par seulement 26% des mairies consultées, mais demeurent un problème important.

Au regard de ces chiffres, il est surprenant que seulement 4% d'entre elles déclarent avoir porté plainte suite à un incident de sécurité.

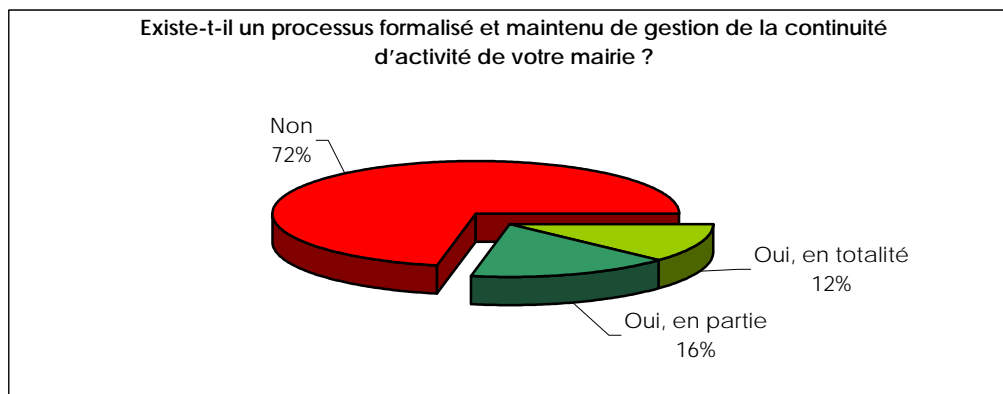


Graphique 31 : Typologie des incidents de sécurité dans les mairies

Thème 14 : Gestion de la continuité

Un processus peu appréhendé par les mairies

Moins d'une mairie sur 3 déclare avoir mis en place, au moins partiellement, un processus formalisé et maintenu de gestion de la continuité d'activité du système d'information ; soit 72% des mairies déclarent ne s'être dotées d'aucun processus de gestion de la continuité d'activité.



Graphique 32 : Plan de continuité d'activité des mairies

De surcroît, parmi les mairies qui ont mis en place un processus de gestion de la continuité, il faut noter que seulement 57% procèdent à des tests et des mises à jour sur une base annuelle. Il est important de souligner qu'une solution de continuité qui n'est pas testée régulièrement a de fortes chances de ne pas être opérationnelle au moment où elle sera déployée suite à un sinistre.

Etat des lieux du secours informatique

Si la grande majorité des mairies interrogées déclare réaliser des sauvegardes en « bon père de famille », en utilisant des moyens « classiques », base de tout secours possible suite à une perte de données, 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 la mairie en cas d'impact majeur sur ses activités critiques.

De même, si le recours à des moyens de secours semble se généraliser (50% des mairies utilisent des moyens de secours à chaud, 44% à froid), il n'est pas sûr que la solution de secours informatique mise en place consiste en un véritable recueil des procédures de reprise de l'architecture de secours retenue par la mairie, sur des moyens externalisés par rapport au site des moyens de production.

Thème 15 : Conformité (CNIL, audits, tableaux de bord)

CNIL

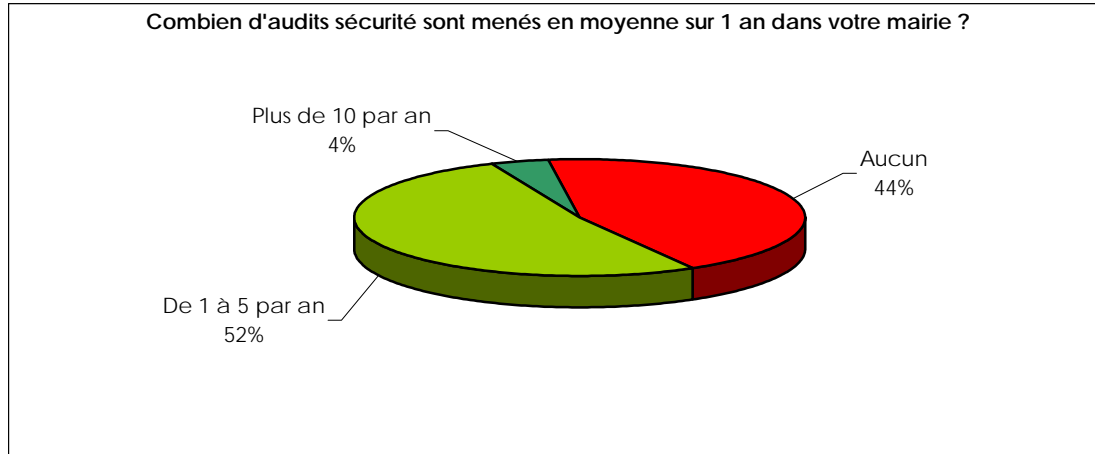
84% des mairies conformes aux exigences de la CNIL

84% des mairies déclarent estimer être en conformité avec les obligations de la loi informatique et libertés, ce qui est un bon score, bien meilleur que celui des entreprises. C'est assez heureux puisque les mairies manipulent de plus en plus d'informations personnelles informatisées (état civil, listes électorales...).

Audits

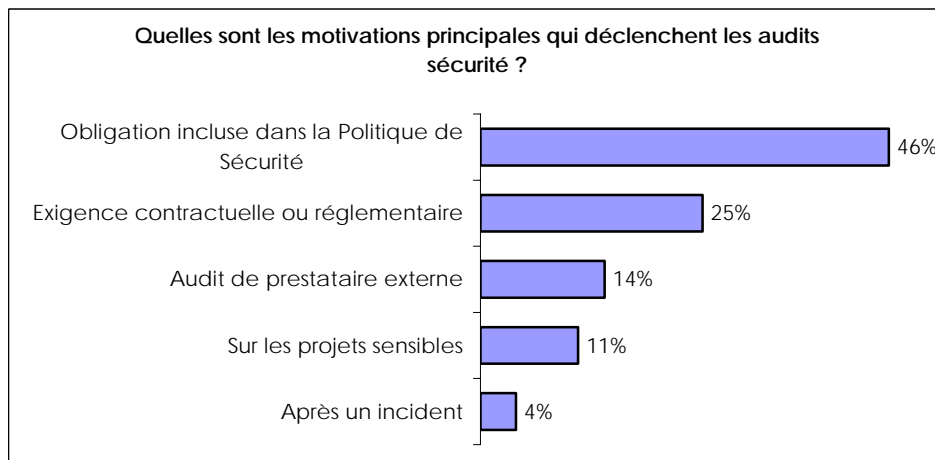
Un contrôle encore timide

56% des mairies de plus de 30 000 habitants réalisent au moins un audit dans l'année. Les mairies semblent donc ne pas s'attacher autant au contrôle que les entreprises (69%).



Graphique 33 : Nombre d'audits sécurité en 2005 dans les mairies

Cette constatation est d'ailleurs confortée par le fait que moins de la moitié de ces audits sont motivés par une obligation incluse dans la Politique de Sécurité.



Graphique 34 : Motivations principales des audits sécurité dans les mairies

Par conséquent, si les entreprises ont mis en place, suite aux nombreux problèmes financiers de ces dernières années un contrôle interne assez important, cela ne semble pas encore être le cas pour les mairies.

Hôpitaux



- ▶ Moyens informatiques des hôpitaux publics
- ▶ Moyens consacrés à la sécurité de l'information par les hôpitaux publics
- ▶ Thème 5 : Politique de sécurité
- ▶ Thème 6 : Organisation de la sécurité et moyens
- ▶ Thème 7 : Gestion des actifs et identification des risques
- ▶ Thème 8 : Sécurité des ressources humaines (charte, sensibilisation)
- ▶ Thème 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)

Les Hôpitaux

Présentation de l'échantillon

186 établissements hospitaliers publics ont répondu à la sollicitation du CLUSIF, soit environ 17% des hôpitaux publics.

Au sein de cet échantillon, des établissements de taille variable sont représentés : 66% des hôpitaux interrogés disposent de moins de 200 lits, 22% de 200 à 500 lits et 12% plus de 500 lits.

Là encore, nous avons cherché à interroger en priorité le Responsable de la Sécurité des Systèmes d'Information (pour 8 % des hôpitaux interrogés). A défaut, c'est le responsable informatique (pour 61 % des hôpitaux interrogés) qui a été le plus souvent contacté.

Dépendance à l'informatique des hôpitaux publics

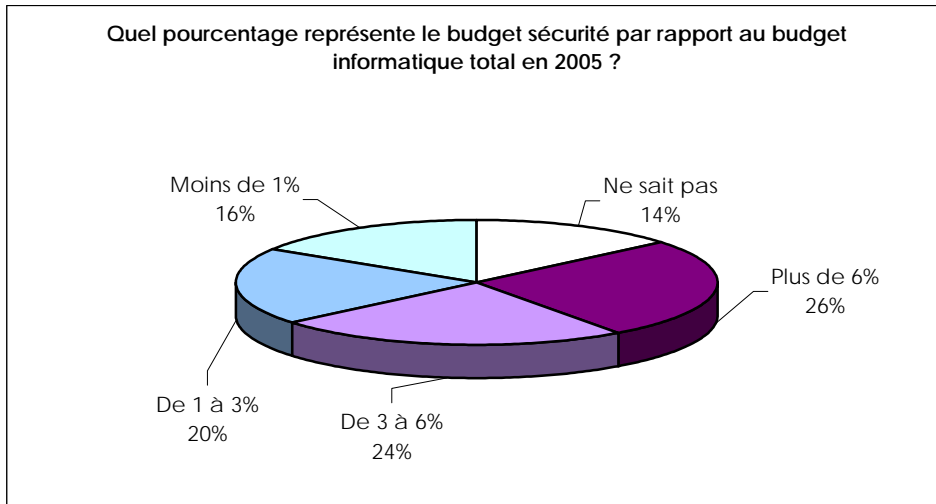
Forte dépendance à l'informatique dans les hôpitaux

33% des hôpitaux publics déclarent une dépendance faible ou modéré à l'informatique. Si l'on considère la taille des hôpitaux, la situation de dépendance augmente sensiblement entre les établissements de moins de 500 lits (61% en dépendance forte) et ceux de plus de 500 lits (86% en dépendance forte). L'informatique est présente aujourd'hui dans toutes les fonctions de l'hôpital :

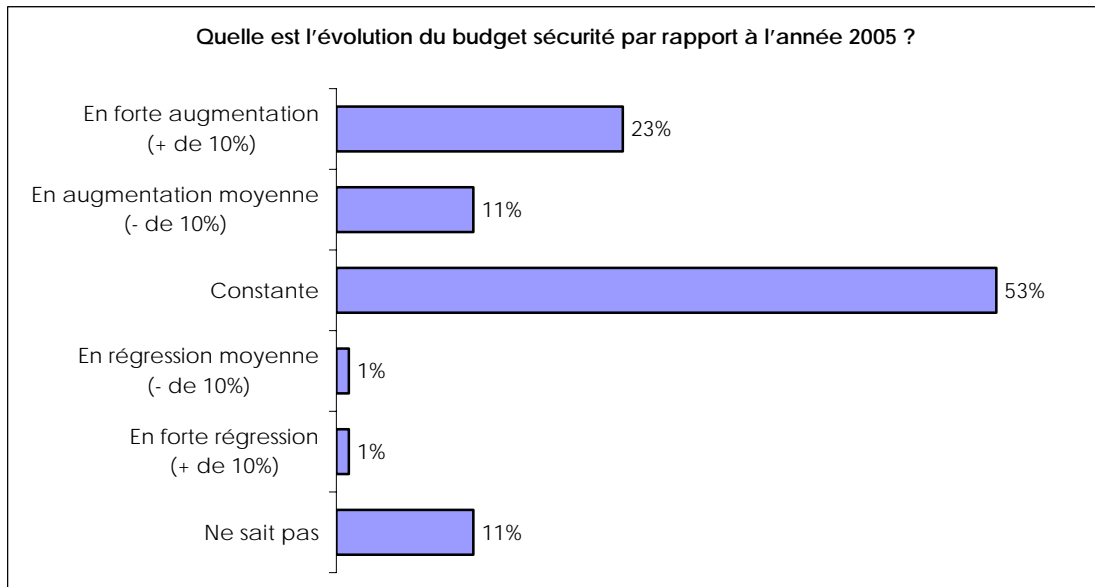
- Administratives ; paie, gestion du temps, facturation, gestion documentaire
- Pilotage ; entrée/sorties des patients, statistiques
- Médicale ; données concernant les patients (dossier médicaux, imagerie, examens...)

Moyens consacrés à la sécurité de l'information par les hôpitaux publics

La moitié exactement des hôpitaux publics consacrent plus de 3% de leur budget informatique à la sécurité. La part relative de budget allouée à la sécurité diminue avec la taille de l'établissement probablement avec le niveau de perception des risques.



Graphique 35 : Pourcentage du budget sécurité dans le budget informatique des hôpitaux



Graphique 36 : Evolution du budget sécurité des hôpitaux

Le budget : toujours le principal frein aux investissements pour la sécurité de l'information

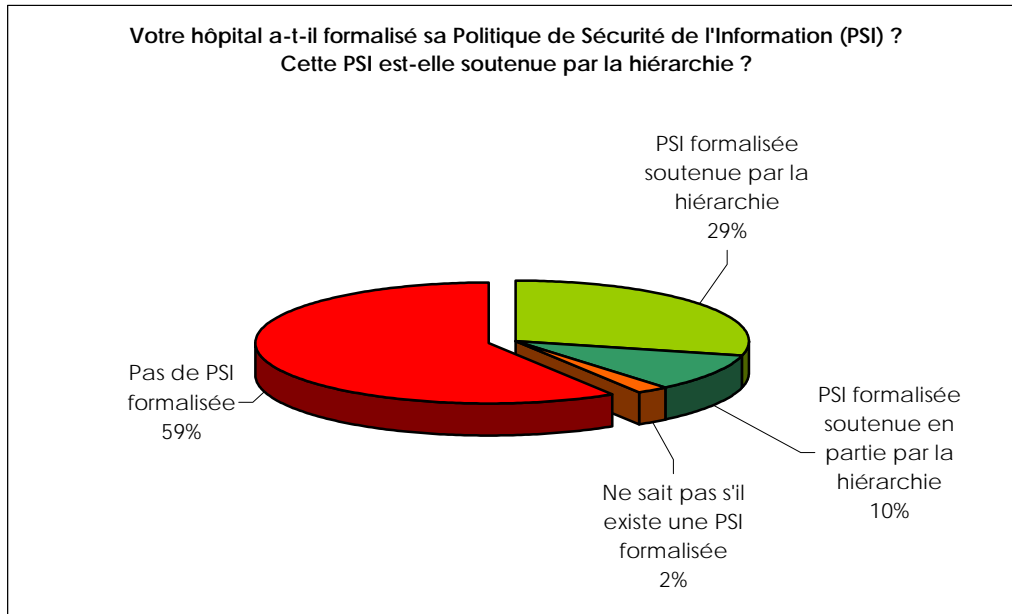
L'évolution de ce budget est à tendance stable pour la moitié des établissements, et en augmentation pour 34% d'entre eux. La sécurité est donc bien perçue aujourd'hui comme une nécessité absolue.

Lorsqu'on leur demande quel est le principal frein à la conduite des missions de sécurité, 40% répondent le manque de budget, 20% le manque de personnel qualifié, 20% les contraintes organisationnelles, 20% les réticences diverses. Seuls 3% des hôpitaux indiquent une réticence de la DSI sur ce sujet. Le caractère vital du budget sécurité de l'information est donc bien présent dans les esprits, mais insuffisamment budgété dans les hôpitaux.

Thème 5 : Politique de sécurité

Des politiques de sécurité encore rarement formalisées

2 hôpitaux sur 5 ont formalisé leur politique de sécurité de l'information. Les grands établissements se montrent plus réactifs dans ce domaine (1 établissement sur 2). Les hôpitaux sont donc très en retard dans ce domaine.



Graphique 37 : La Politique de sécurité de l'information dans les hôpitaux

Un engagement pas toujours dynamique des directions d'établissement

3 responsables d'établissement sur 4 soutiennent la PSI lorsqu'elle existe. Mais ce soutien est nettement plus marqué dans les petites structures (4 sur 5) que dans les moyennes et les grandes (un peu plus de 1 sur 2). Il est dès lors inversement proportionnel à l'importance de l'établissement.

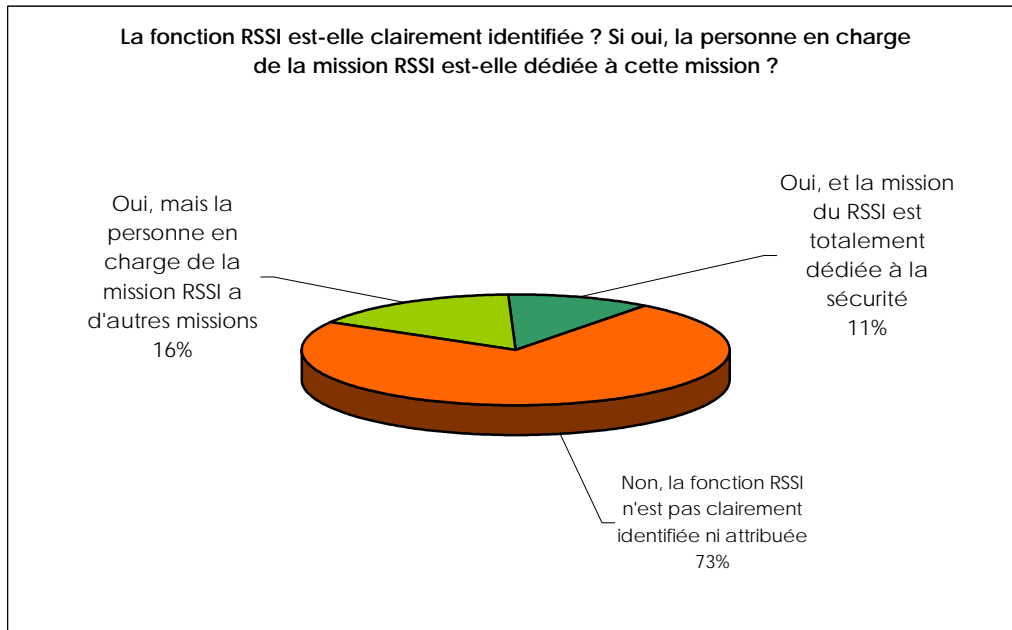
Une évaluation des menaces et des risques pas toujours efficiente

La direction d'établissement ainsi que les services gérant l'informatique ont largement participé à l'élaboration de la politique de sécurité. En revanche, les utilisateurs ont été associés d'une manière limitée de sorte que les menaces et les risques n'ont pas forcément été appréciés finement.

Une PSI qui s'appuie sur l'ISO 17799 dans 30% des cas.

Parmi les établissements ayant formalisé leur PSI, moins d'un établissement sur 2 a appuyé sa réflexion sur une norme exhaustive. Si l'ISO est la norme la plus utilisée, à noter aussi la référence à la méthode PSSI de la Direction Centrale de la Sécurité des SI (DCSSI) dans 8% des cas et aux recommandations du GNSIH (Groupement de Normalisation des SI Hospitaliers) dans 4% des cas.

Thème 6 : Organisation de la sécurité et moyens



Graphique 38 : La mission de Responsable de la Sécurité des Systèmes d'Information (RSSI) dans les hôpitaux

RSSI : une mission et une fonction à développer

La fonction RSSI est clairement identifiée dans seulement 1 hôpital sur 4 environ. En moyenne le RSSI est dédié à sa mission dans 2 cas sur 5, avec un score plus important (plus d'une fois sur 2) dans les structures moyennes et importantes. En revanche cette fonction est partagée 2 fois sur 3 dans les petites structures. Lorsque la fonction est partagée celle-ci échoit 1 fois sur 2 à des personnes qui n'ont pas forcément une culture informatique.

Un rattachement du RSSI qui varie en fonction de l'importance de l'établissement

Le RSSI est en moyenne 7 fois sur 10 directement rattaché à la direction de l'établissement. Toutefois les grandes structures rattachent 1 fois sur 3 ce responsable à la direction des systèmes d'information. Cette fonction est donc davantage placée sous le contrôle direct de la direction d'établissement dans les petites et moyennes structures, alors qu'elle est largement déléguée et souvent rattachée à l'informatique dans les structures importantes.

Des moyens pas toujours en adéquation avec les besoins de gestion de la sécurité de l'information

1 fois sur 4, quelle que soit l'importance de l'hôpital, il n'y a pas d'effectif dédié en permanence à la sécurité de l'information. Lorsqu'une équipe est mise en place, elle ne dépasse pas généralement 2 personnes. Dans les petites structures cet effectif se justifie facilement. Il est plus surprenant dans les gros établissements, même si dans 27 % des grands établissements de plus de 500 lits, ces équipes sont constituées de plus de 3 personnes

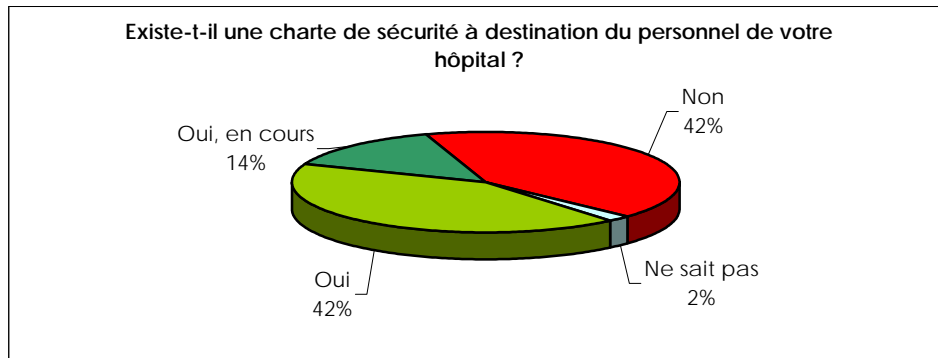
Thème 7 : Gestion des actifs et identification des risques

Les résultats de l'enquête relatifs à la gestion des risques concernant les hôpitaux sont sensiblement identiques à ceux concernant les entreprises (cf. Thème 7 : Gestion des actifs et identification des risques des entreprises, page 16).

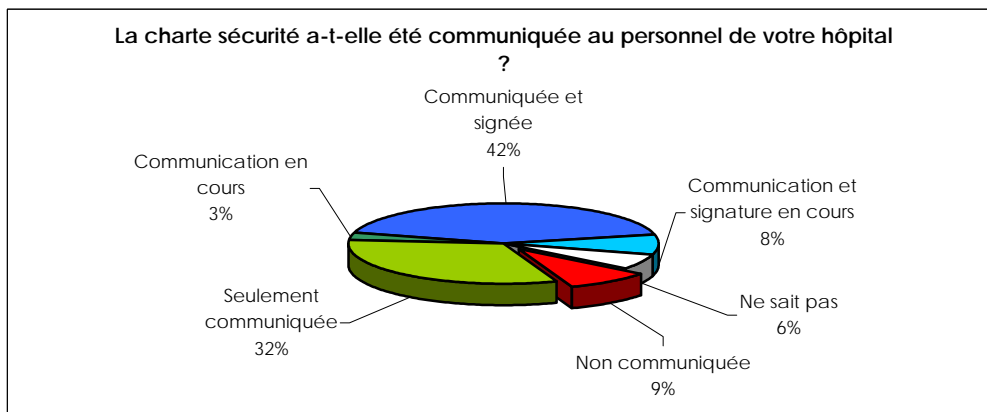
Thème 8 : Sécurité des ressources humaines (charte, sensibilisation)

Des chartes encore insuffisamment répandues

Seulement quatre hôpitaux sur dix disposent d'une charte de sécurité, proportion inférieure à celle des entreprises (55%, voir page 18), mais proche de celle des mairies. De même, lorsqu'elles existent, ces chartes sont moins fréquemment communiquées et signées par les collaborateurs.



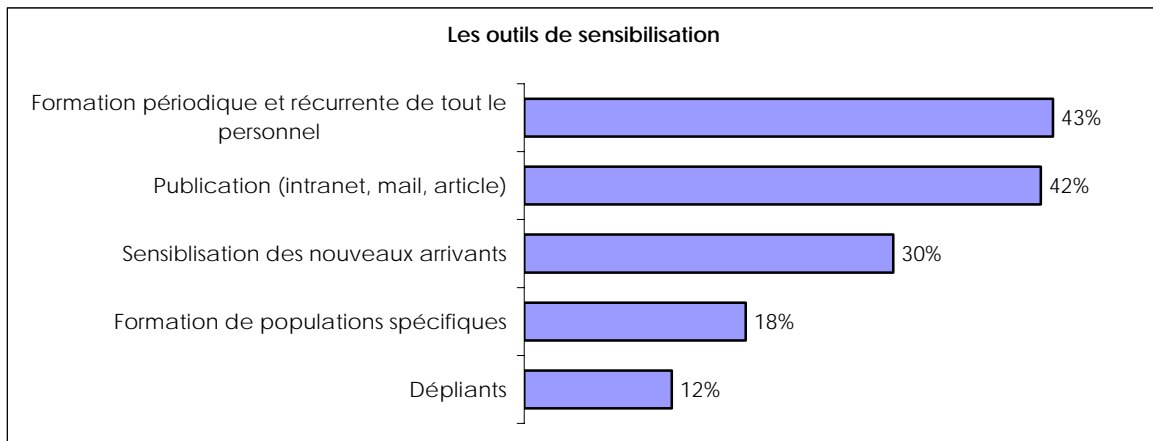
Graphique 39 : Charte de sécurité à destination du personnel des hôpitaux



Graphique 40 : Communication de la charte sécurité au personnel des hôpitaux

Un déficit de communication et de sensibilisation

Les hôpitaux accusent également un retard par rapport aux entreprises dans le domaine des programmes de sensibilisation à la sécurité. Ainsi, dans les deux tiers des hôpitaux, il n'existe aucune action de sensibilisation à la sécurité de l'information. Lorsqu'elles existent, elles se matérialisent le plus souvent (43%) par des formations périodiques et récurrentes de l'ensemble du personnel, ainsi que par la publication (sur l'intranet, par mail ou par des affiches). Plus encore que dans les entreprises, les effets de la sensibilisation ne sont pas mesurés de façon systématique (seulement 16% des hôpitaux ayant mis en œuvre de telles actions en étudient l'impact).



Graphique 41 : Outils de sensibilisation du personnel des hôpitaux

Thème 10 : Gestion des communications et des opérations

Sécurisation des nouvelles technologies

La sécurisation des nouvelles technologies passe d'abord par l'interdiction

Encore plus que dans les entreprises ou dans les mairies, l'interdiction des nouvelles technologies est très souvent choisie, avec le souhait de conserver une totale maîtrise du système d'information :

- 91 % interdisent l'accès (webmail, extranet) à partir d'un poste non maîtrisé,
- 81 % « interdisent la voix sur IP »
- 76 % (disent ou souhaitent ...) interdire PDA et smartphones
- 70 % interdisent l'accès au SI en situation de mobilité, même avec un poste contrôlé
- 59 % interdisent le wifi

Selon les technologies, les écarts avec les entreprises sont de 15 à 30 % de restrictions supplémentaires. On peut supposer que cette rigueur provient autant des risques de perturbations sur des appareils sensibles (rejet du Wifi à 59%, des PDA à 76%) que de la confidentialité des données manipulées (accès extérieurs interdits à 91% et 70%).

Lutte anti-virale, protection contre les intrusions et gestion des vulnérabilités

Sur ce thème, les hôpitaux présentent des réponses globalement semblables à celles des entreprises. A noter que la confidentialité des données échangées n'entraîne pas plus de déploiement de solutions de « chiffrement de données pour les utilisateurs » que dans la moyenne des entreprises : 10% y ont recours contre 15% dans les entreprises, 73% n'en déploient pas du tout contre 58% pour les entreprises.

Sécurité et infogérance de services d'exploitation

Une infogérance fréquente, mais avec un contrôle insuffisant de la sécurité

Les hôpitaux, qui externalisent assez fréquemment (plus du tiers externalise tout ou partie) suit ces contrats (45%) mais pas tellement sous l'angle de la sécurité (seuls 17% les audient, au moins ponctuellement).

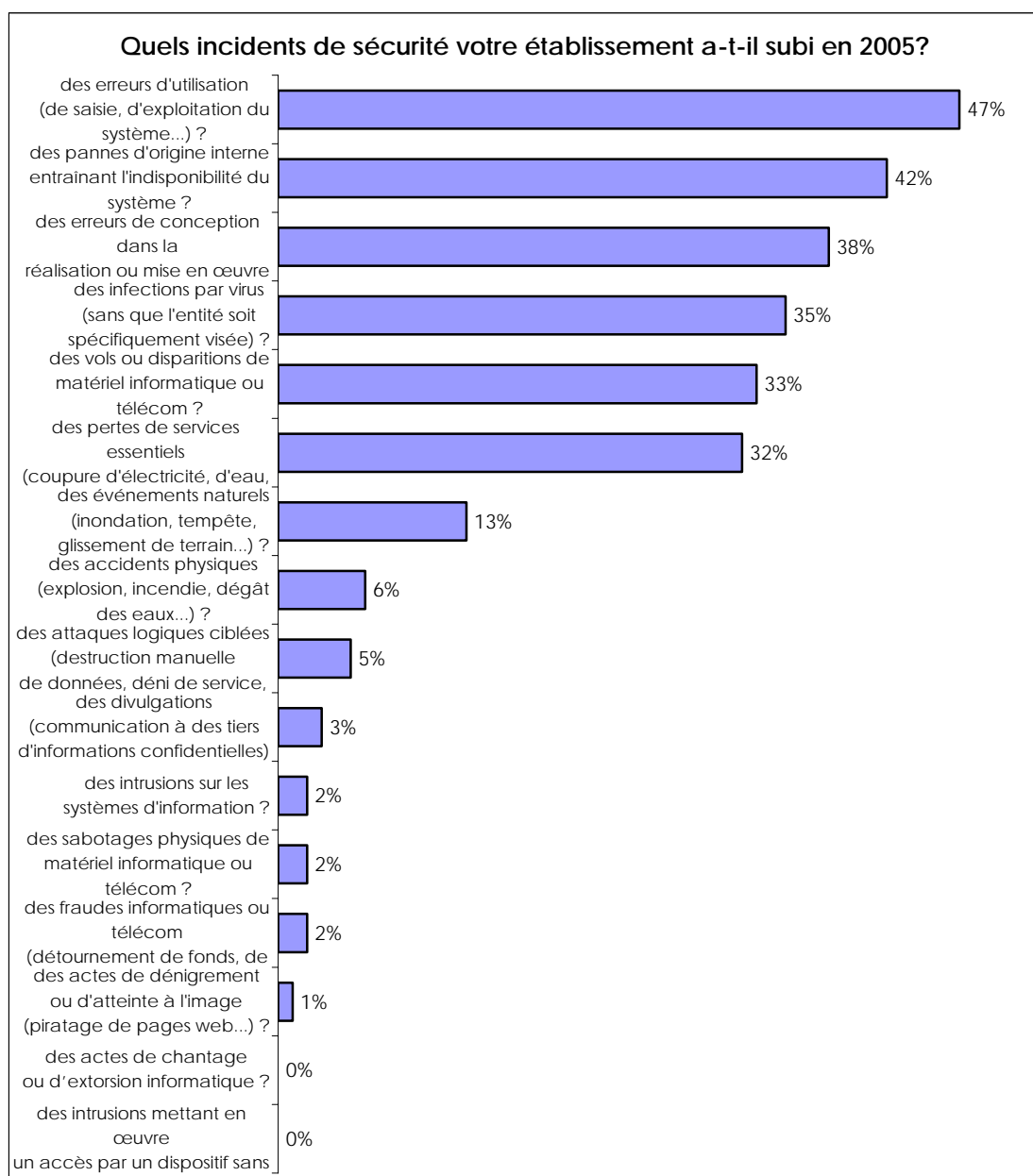
Thème 11 : Contrôle des accès

Le niveau d'utilisation des technologies de sécurisation des accès logiques au système d'information dans les hôpitaux reste faible : il se situe à un meilleur niveau que celui des mairies, mais inférieur à celui des entreprises.

Thème 12 : Acquisition, développement et maintenance

Les chiffres donnés par les hôpitaux sont très proches de ceux recensés dans les entreprises.

Thème 13 : Gestion des incidents de sécurité



Graphique 42 : Typologie des incidents de sécurité dans les hôpitaux

Un suivi des incidents qui reste à parfaire

Comme dans le cas des mairies, un nombre assez peu important d'hôpitaux (y compris parmi les gros établissements) possède une équipe dédiée à la sécurité informatique ou même une cellule chargée de cette mission (seulement 30% des établissements), ce qui semble coïncider avec la désignation d'un RSSI clairement identifié évoquée plus haut.

En cohérence avec la taille des établissements, l'impact financier des incidents de sécurité est plus souvent évalué dans les établissements de plus de 500 lits (23% contre 15% en moyenne dans l'ensemble des établissements), et cette proportion reste comparable à la proportion d'établissements qui déclarent disposer d'une équipe dédiée à la sécurité informatique.

Divulgaration, vols, mais aussi et toujours les virus...

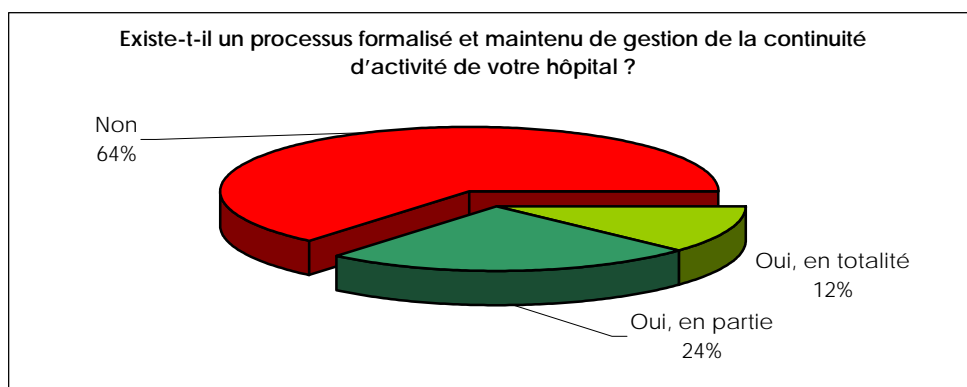
Parmi les incidents directement liés à des malveillances, les infections par des virus arrivent assez largement en tête et ce, quelle que soit la taille de l'hôpital (35% des hôpitaux sont touchés). Comme dans les autres échantillons, le vol de matériel existe en quantité non négligeable. On remarque aussi de façon assez inquiétante que 14% des établissements de plus de 500 lits font état de divulgations d'informations confidentielles.

Enfin, on note que le nombre de plaintes déposées effectivement pour des incidents liés à la sécurité de l'information reste très faible (2% des établissements), même si cela semble plus régulier dans les plus gros établissements.

Thème 14 : Gestion de la continuité

Un processus peu appréhendé par les hôpitaux

Si plus d'un tiers des hôpitaux déclarent avoir mis en place, au moins partiellement, un processus formalisé et maintenu de gestion de la continuité d'activité du système d'information, 64% des hôpitaux déclarent ne s'être doté d'aucun processus de gestion de la continuité d'activité.



Graphique 43 : Plan de continuité d'activité des hôpitaux

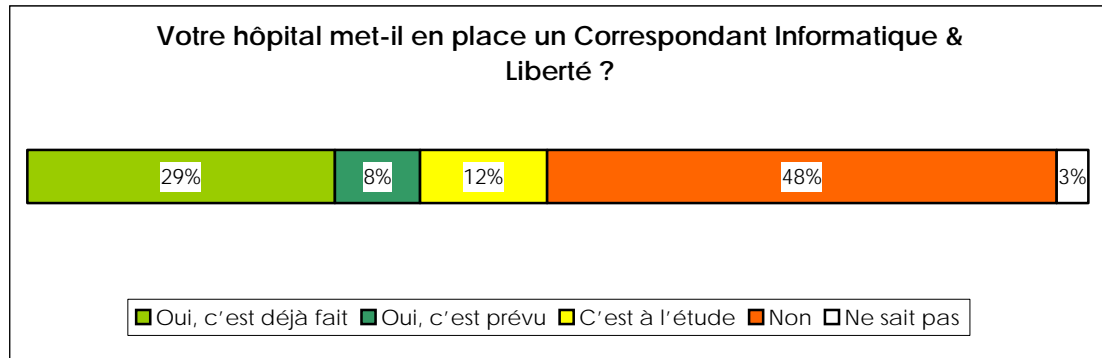
De surcroît, parmi les hôpitaux publics qui ont mis en place un processus de gestion de la continuité, il faut noter que seulement 41% procèdent à des tests et des mises à jour sur une base annuelle. Il est important de souligner qu'une solution de continuité qui n'est pas testée régulièrement a de fortes chances de ne pas être opérationnelle au moment où elle sera déployée suite à un sinistre.

Thème 15 : Conformité (CNIL, audits, tableaux de bord)

CNIL

Une conformité partielle aux exigences de la CNIL

70% des hôpitaux interrogés ont déclaré être en conformité avec les obligations CNIL, et 20% uniquement pour les traitements les plus sensibles. Cela laisse tout de même 10% d'établissements où la situation est incertaine, ce qui peut être inquiétant au regard du type de données traitées.



Graphique 44 : Mise en place des CIL dans les hôpitaux publics

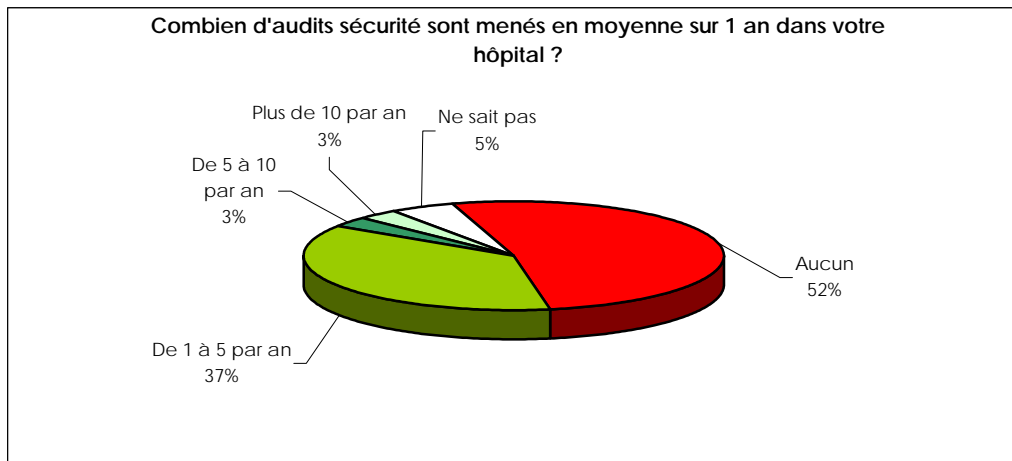
Le CIL encore mal compris

Le dispositif du correspondant CNIL, mis en place suite à la modification de la loi informatique et libertés en août 2004, et le décret d'application correspondant d'octobre 2005, est ressenti de façon assez similaire dans les différents établissements, quelle que soit leur taille. Sa mise en place récente explique la confusion qui doit exister entre ce nouveau dispositif et la désignation – certainement antérieure – pour 54 établissements d'une personne chargée de suivre ces problématiques, à comparer au nombre total d'organisations (190 entreprises et organisations de toute nature) pour laquelle la CNIL a reçu une déclaration de mise en place d'un tel correspondant au 22 mars 2006. Etant donnée la nature particulière des données traitées dans les établissements hospitaliers, il faudra suivre l'évolution de ce dispositif avec beaucoup d'attention dans les années à venir.

Audit

Le contrôle progresse mais n'est pas encore systématique

Seuls 43% des hôpitaux utilisent l'audit à des fins de contrôles. Si ce chiffre est peu élevé en comparaison de celui des mairies (56%) et très éloigné de celui des entreprises (69%), il faut quand même noter qu'il a progressé de façon significative depuis l'enquête CLUSIF 2003, où seuls 32% des hôpitaux y avaient recours.



Graphique 45 : Nombre d'audits sécurité en 2005 dans les hôpitaux

Par conséquent, si les entreprises ont déjà acquis la culture du contrôle interne cela ne semble pas encore être le cas pour les hôpitaux. Cependant la progression notable dans ce secteur semble indiquer une prise de conscience de la nécessité d'auditer régulièrement son système d'information.

Annexe



► Quelques rappels de définitions utiles

Annexe

Quelques rappels de définitions utiles

[I] Actifs

Le terme « Actifs » regroupe ici les biens de l'organisme, ainsi que les ressources humaines. Trois catégories d'actifs sont à considérer :

- les actifs gérés au travers du SI (informations et processus métier),
- les actifs techniques constituant le SI (logiciels, actifs physiques comme les matériels informatiques, les moyens de communication, etc.),
- les actifs relatifs à l'environnement du SI (personnes et bâtiments principalement).

[II] Besoins de sécurité

Il s'agit, principalement, des besoins de **D**isponibilité, **I**ntégrité, **C**onfidentialité et **P**reuve (DICP).

[III] EBIOS

Expression des **B**esoins et **I**dentification des **O**bjectifs de **S**écurité.

Méthode de gestion des risques relatifs à la sécurité des SI créée en 1995 et maintenue par la DCSSI.

[IV] Gestion des opérations : outils de sécurité

La lutte « anti-virale » regroupe les logiciels antivirus installés en coupure des passerelles de messagerie ou en résidant sur des serveurs et des postes. Les éditeurs ayant progressivement regroupé les fonctions dans des solutions convergées, la problématique anti-vers, chevaux de Troie, et spyware, et considérée comme liée.

Les outils de centralisations des journaux de sécurité (logs), liés à la problématique de SIM : Security Information Management, de Intrusion Detection System, ne prêtent pas à confusion.

[V] Inventaire des actifs

Selon l'ISO/IEC 17799:2005, l'inventaire des actifs comporte toutes les informations nécessaires pour faire face à un sinistre, en particulier le type de l'actif, son format, son emplacement, les informations relatives à sa sauvegarde et à la licence, ainsi que sa valeur pour l'organisme.

[VI] ISO/IEC 17799:2005

Norme internationale constituant un « guide de bonnes pratiques » en matière de sécurité de l'information.

[VII] ISO/IEC 27001:2005

Norme internationale spécifiant un **S**ystème de **M**anagement de la **S**écurité de l'**I**nformation (SMSI).

[VIII] Maintenance des SI, veille sur les vulnérabilités, application des correctifs

Les entreprises, par un processus de veille technologique ciblée, qu'il soit interne ou faisant appel à un prestataire, ce prestataire pouvant être une association, une société de services ou un éditeur, se doivent de surveiller l'apparition des failles et vulnérabilités dans leur parc.

Ces défauts (de programmation) facilitent les attaques et malveillances, et doivent être corrigées au plus vite, en général par l'application des recommandations ou des correctifs de l'éditeur. Le délai de réaction recouvre plusieurs temps, tout d'abord, le temps de

réaction de l'éditeur (unité : les semaines), puis le temps des tests de non-régression (unité : les jours) ou de validation des correctifs (patches) et enfin le temps de déploiement (unité : les heures).

[IX] MEHARI

Méthode Harmonisée d'Analyse des Risques.

Méthode de gestion des risques relatifs à la sécurité des SI maintenue par le CLUSIF.

[X] Outils de Communication, sécurisation des nouvelles technologies

De nombreuses nouvelles technologies liées à la mobilité ou à la migration de technologies plus traditionnelles vers IP accroissent l'exposition à la cybercriminalité.

Ainsi les technologies d'extranet, ou de messagerie unifiée, facilitent aussi bien le nomadisme (souhaité), que l'accès externe au système d'information (suspect).

Les messageries unifiées, ou leurs terminaux (smartphones, PDA) posent également des problèmes au moins de synchronisation avec le système d'information (ne serait-ce que par le carnet d'adresses).

Enfin la téléphonie sur IP est l'exemple type de l'usage qui inquiétait moins tant qu'il n'était pas IP (cas des autocom), et qui inquiète d'autant plus qu'il se charge d'une problématique d'outil « à installation spontanée » (cas de Skype™), problématique que l'on retrouve souvent pour ces nouvelles technologies (PDA, accès depuis le domicile) ou certains utilisateurs déploient eux-mêmes une solution qui n'a pas été soumise à la DSI ou au RSSI.

[XI] Propriétaire d'un actif

Selon l'ISO/IEC 17799:2005, le terme « propriétaire » identifie une personne ou une entité ayant accepté la responsabilité du contrôle de la production, de la mise au point, de la maintenance, de l'utilisation et de la protection des actifs. Ce terme ne signifie pas que la personne jouit à proprement parler de droits de propriété sur l'actif.



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