CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Colloque Gouvernance Sécurité des Systèmes d'Information

Agence Régionale de Santé - PACA

Marseille, 7 juin 2011

Pascal LOINTIER
Président du CLUSIF

Menaces Informatiques et Pratiques de Sécurité, enquête 2010

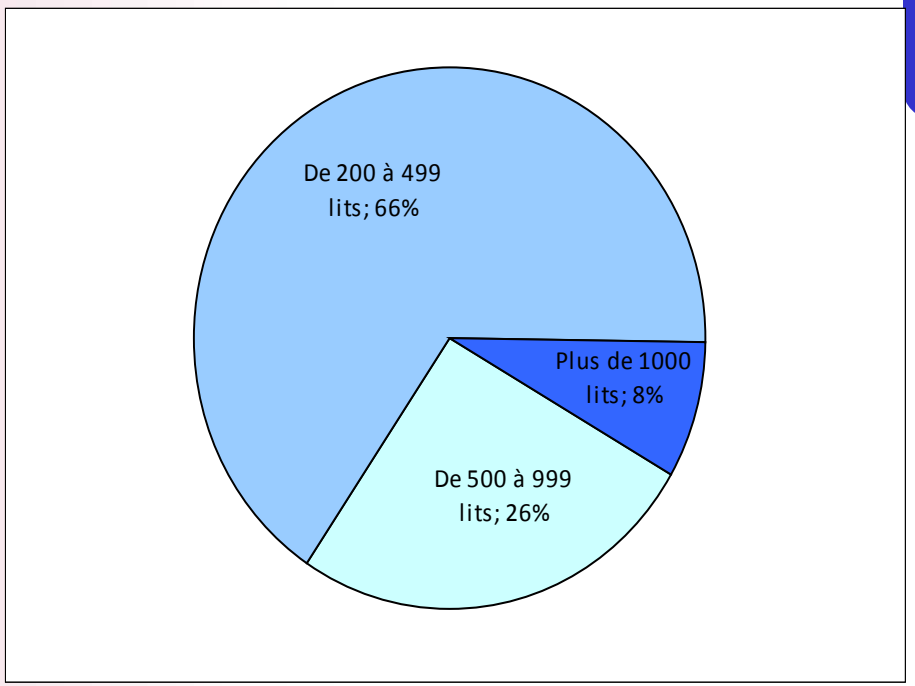
Enquête sur les entreprises (>200 salariés), les hôpitaux, les internautes

- Questionnaires spécifiques
- Collecte des données non biaisée, par un organisme spécialisé (GMV Conseil)
- Groupe d'experts pour analyse et/ou commentaires

Les hôpitaux – Présentation de l'échantillon

Enquête réalisée auprès des hôpitaux publics de plus de 200 lits en France (~ 500)

151 hôpitaux y ont répondu : 30% des hôpitaux publics de plus de 200 lits



Enquête 2006 : cible différente: hôpitaux de moins de 200 lits inclus (66% du panel)

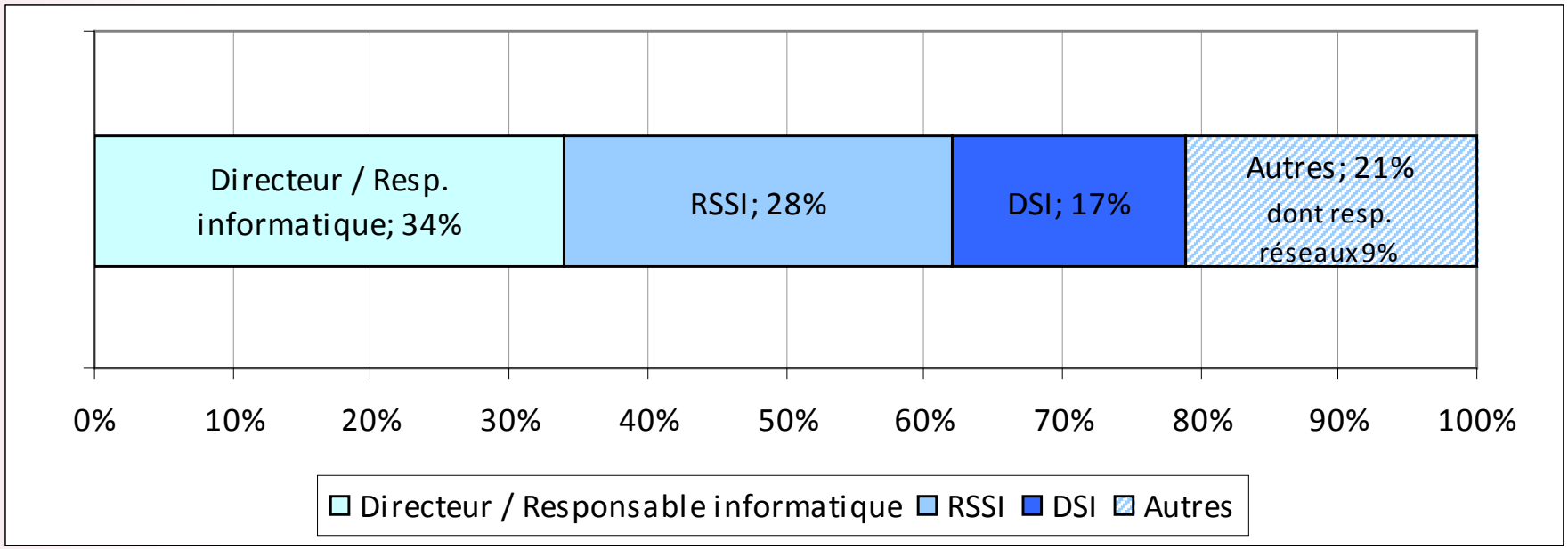
Personne ciblée: RSSI ou à défaut le responsable informatique ou toute autre personne ayant cette question en charge

Interlocuteur en charge de la sécurité

- Directeur (ou responsable) Informatique : un tiers des cas.
- DSI : 17 % des cas.
- RSSI (cible prioritaire) : n'a pu être joint que dans 28 % des cas.

51%

Souvent, pas de RSSI identifié, ni en tant qu'individu ni en tant que fonction.



Le budget informatique serait-il une information confidentielle ?

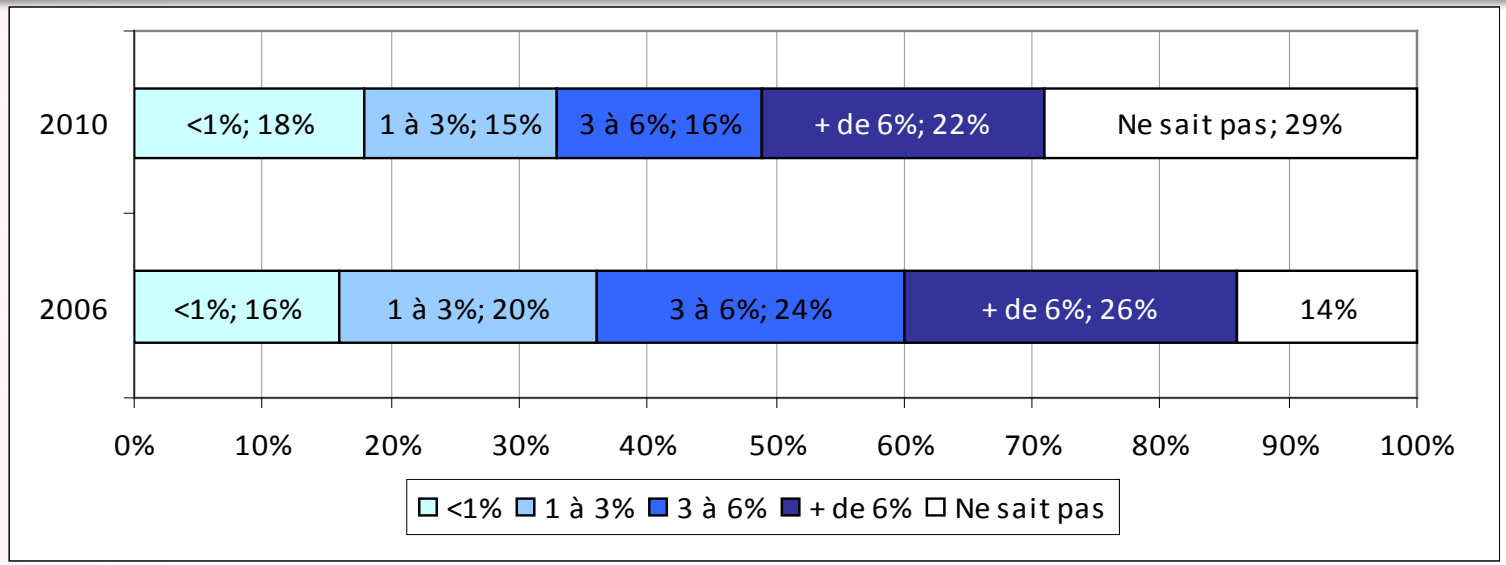
Moyenne	1 015 k€
Minimum	7 k€
Maximum	12 000 k€

Budget informatique : pas toujours connu ou diffusable (70 % de réponses)

Dans les hôpitaux une partie des investissements informatiques est faite directement dans les services.

Capacité à identifier le budget sécurité dans le budget IT global: a fortement diminué

La part du budget informatique consacrée à la sécurité à diminué



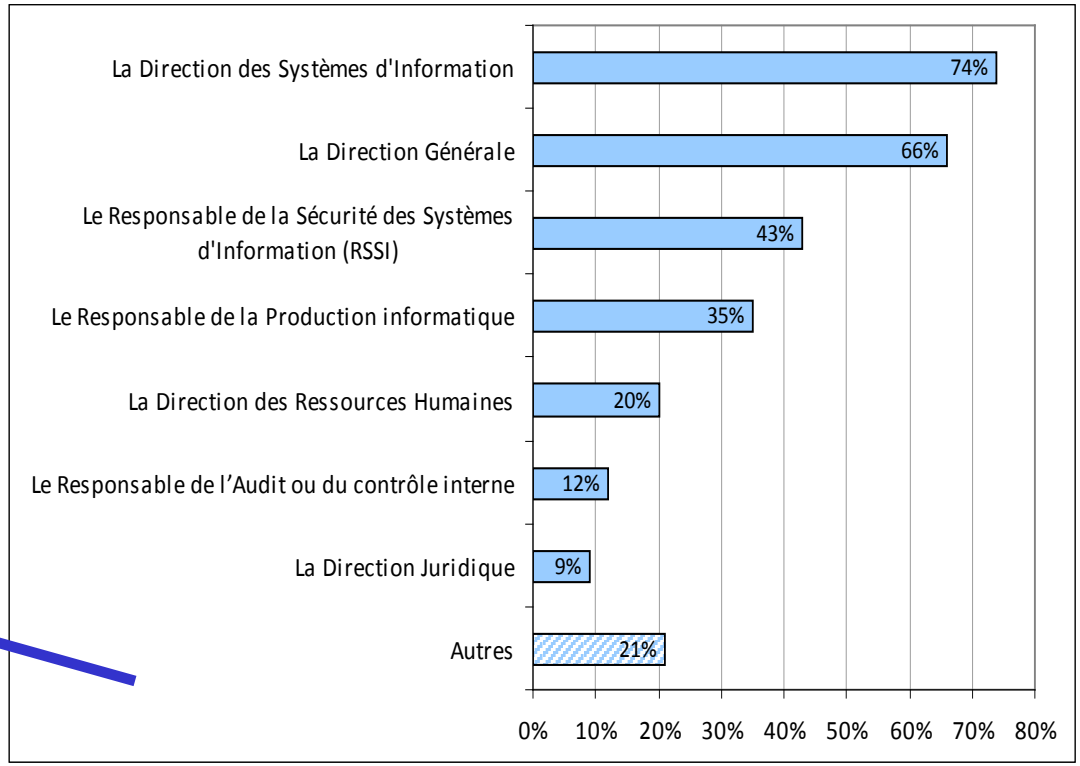
Politique de Sécurité : préoccupation de la Gouvernance des hôpitaux

Tendance : lier l'élaboration de la Politique de sécurité à l'analyse de risques

- 63% des hôpitaux ont formalisé leur Politique de Sécurité (55% en 2006)
- Sa mise à jour date de moins de deux ans pour 75% des hôpitaux

La Direction Générale soutient cette Politique à 94% (99% en 2006).

Contributeurs à l'élaboration de la politique de sécurité



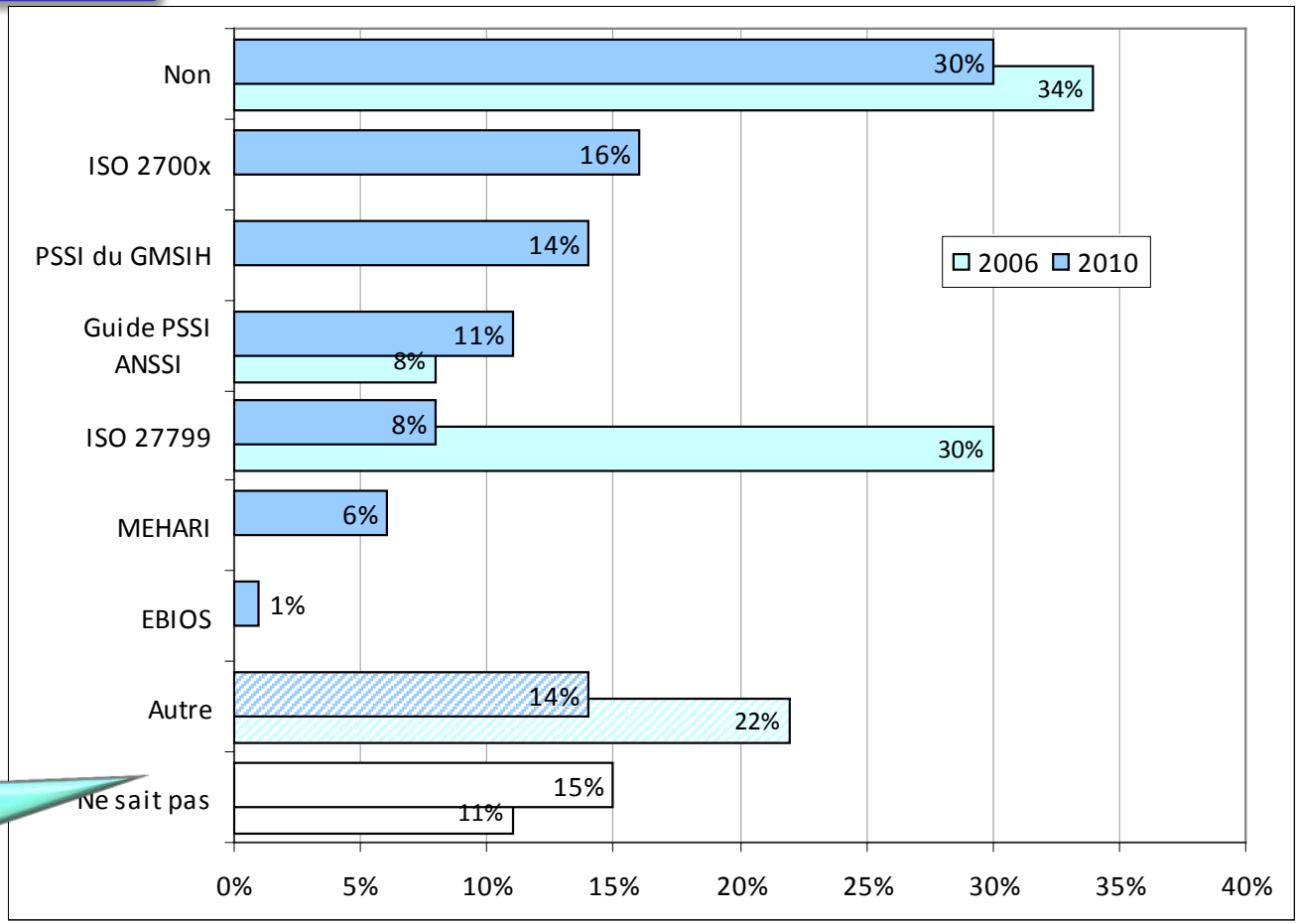
L'utilisation de modèles se précise sans s'étendre

Les hôpitaux s'appuient sur des normes (2700x, 27799, etc.) pour élaborer leur Politique de Sécurité : **55%, en progression**

Normes utilisées plus variées, plus ciblées

- ISO 27000 : 16%
- GMSIH : 14%
- ANSSI : 11%
- ISO 27799 : 8%
- MEHARI : 6%

Quelle norme de sécurité avez-vous utilisée ?



Organisation et moyens

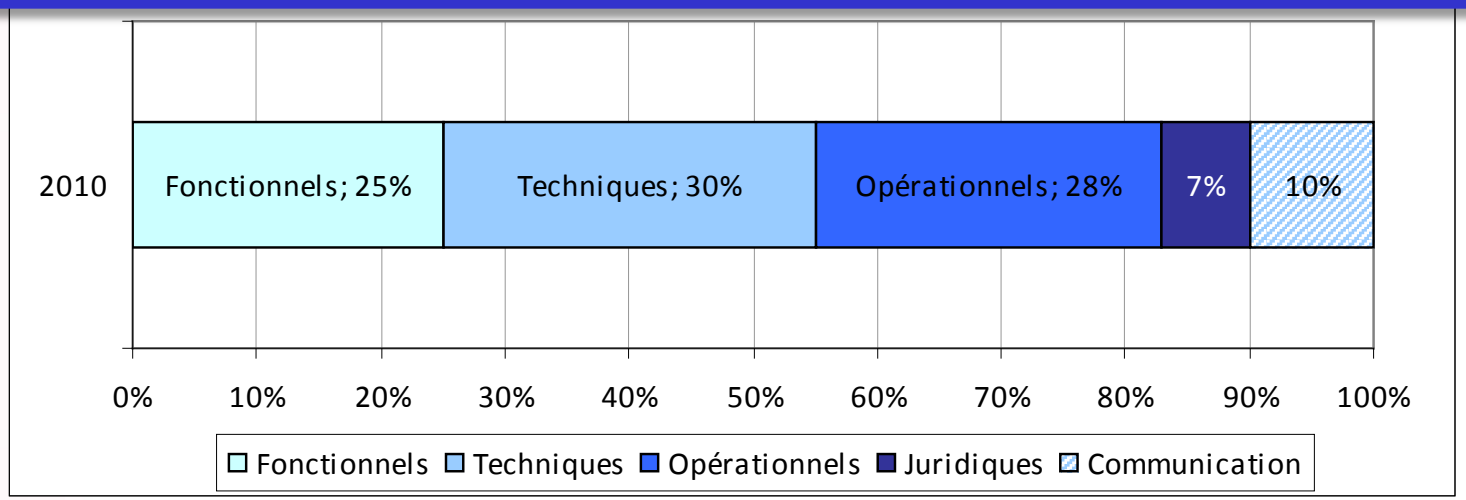
La fonction de RSSI s'impose peu à peu : identifiée et attribuée 37% (27% en 2006)

Elle est moins assurée par une personne dédiée : 23% en 2010 (41% en 2006)

Les RSSI sont de plus en plus rattachés au DSI : 36% en 2010 (32% en 2006)

Séparation des fonctions entre la DIM (Direction de l'informatique médicale) et la DSI : explique que le dossier patient papier ne soit pas considéré comme du ressort du RSSI

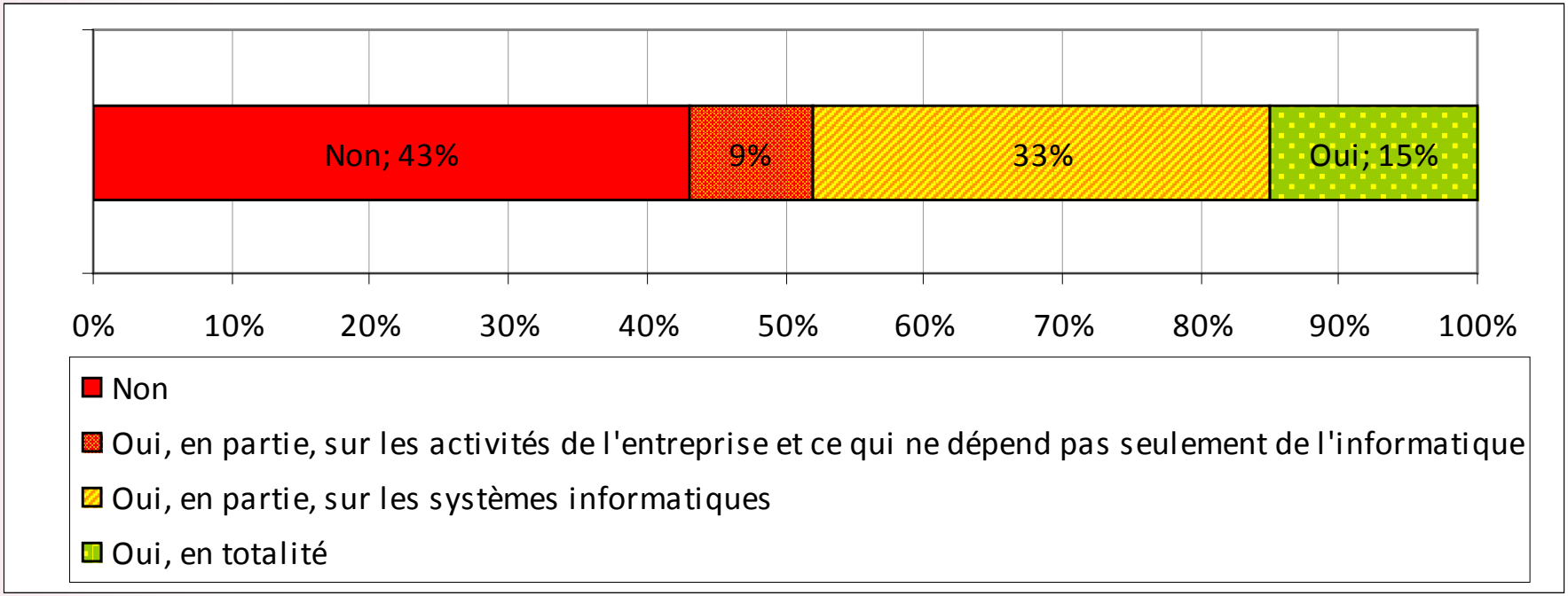
Les fonctions opérationnelles et techniques représentent l'activité principale du RSSI



Inventaire des informations: encore à développer

57% des hôpitaux a procédé à l'inventaire de ses informations en 2009

Classement des informations: réalisé par 48% des hôpitaux, selon les critères de confidentialité (82%), de Disponibilité (62%) et d'Intégrité (48%) ou Autres



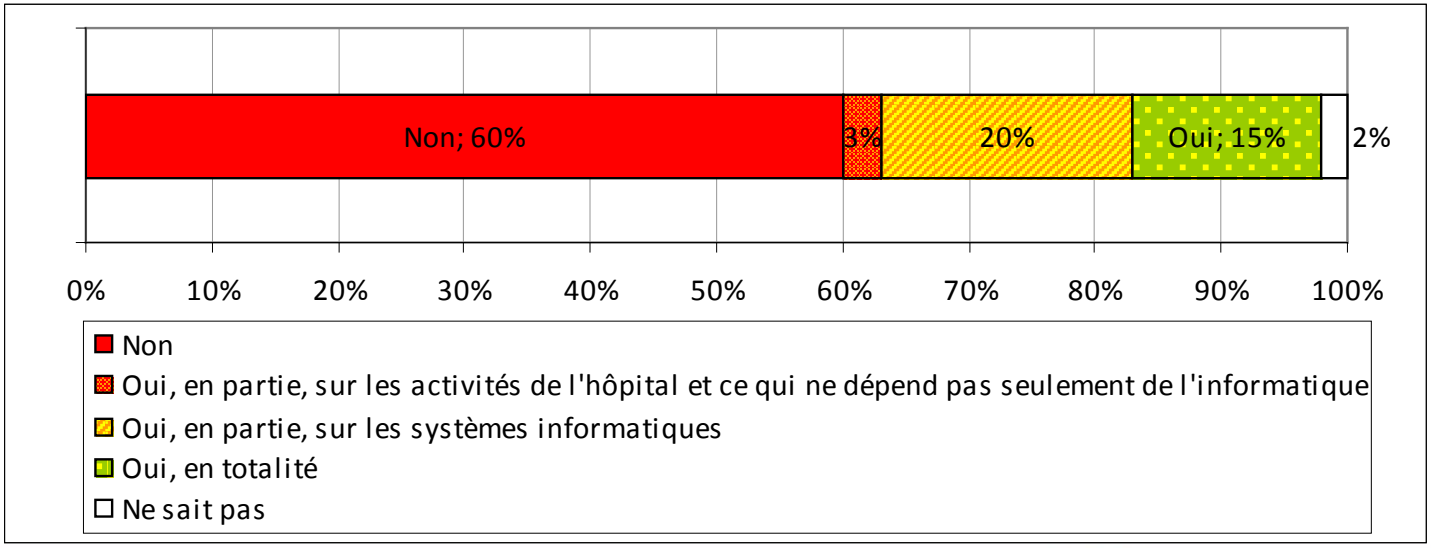
L'analyse de risques s'impose peu à peu aux hôpitaux

Les analyses de risque menées en 2010 se sont traduites par des plans d'actions de manière plus systématique

Le Responsable Sécurité est clairement reconnu comme le porteur de cette activité : 43% en 2010 contre 35% en 2008

Mais 60% des hôpitaux ne font aucune analyse de risques

Avez-vous réalisé une Analyse des Risques ?



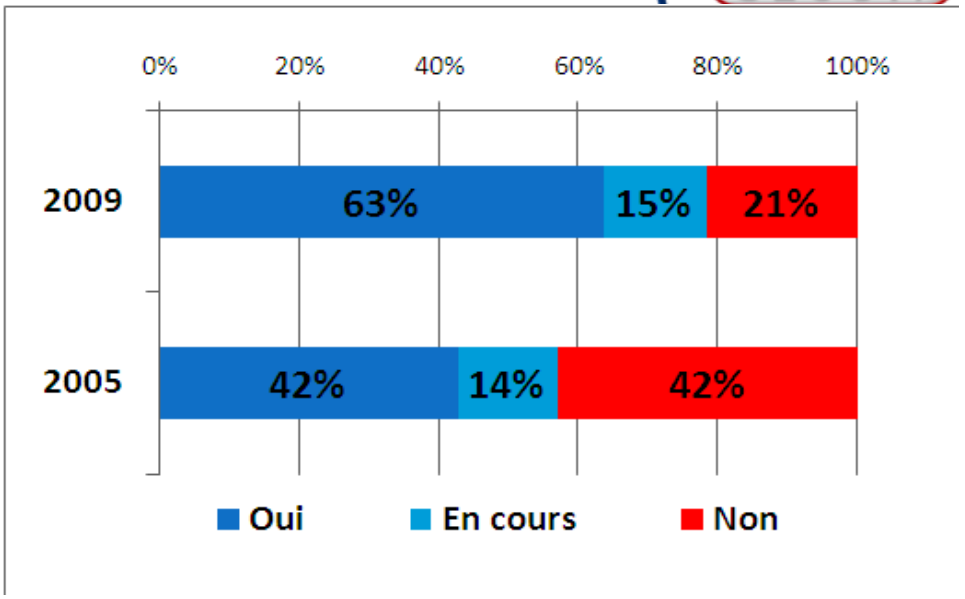
78 % : en quatre ans, les hôpitaux ont adopté les chartes de sécurité !

Diffusion plus large

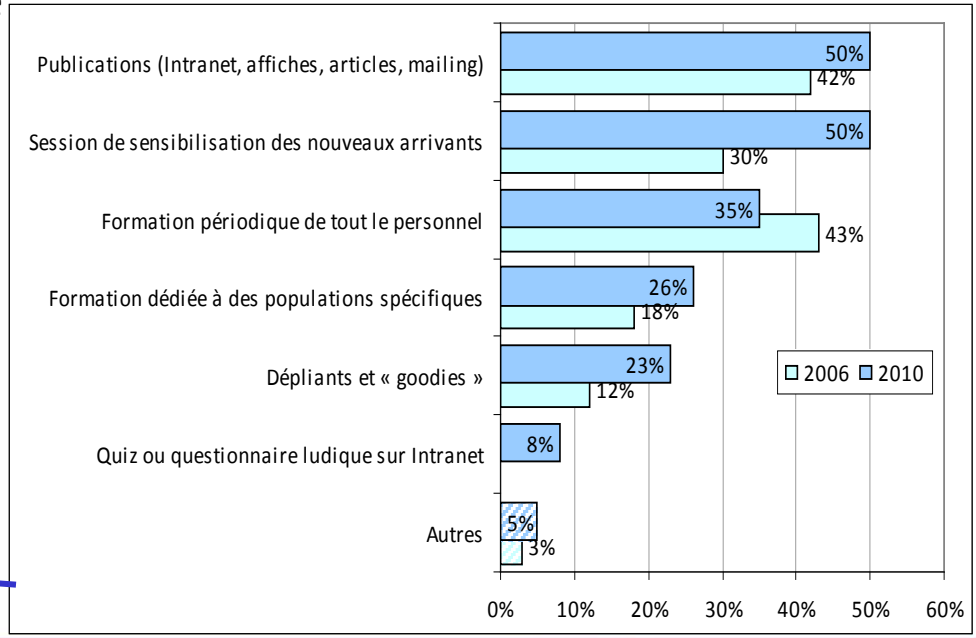
Signée par tous les salariés dans plus de la moitié des établissements.

Devient un outil de management: des sanctions disciplinaires sont prévues dans le règlement intérieur.

Progrès attendus: sensibilisation des salariés à la sécurité de l'information. Dans les deux-tiers des établissements, il n'existe aucun programme de sensibilisation.



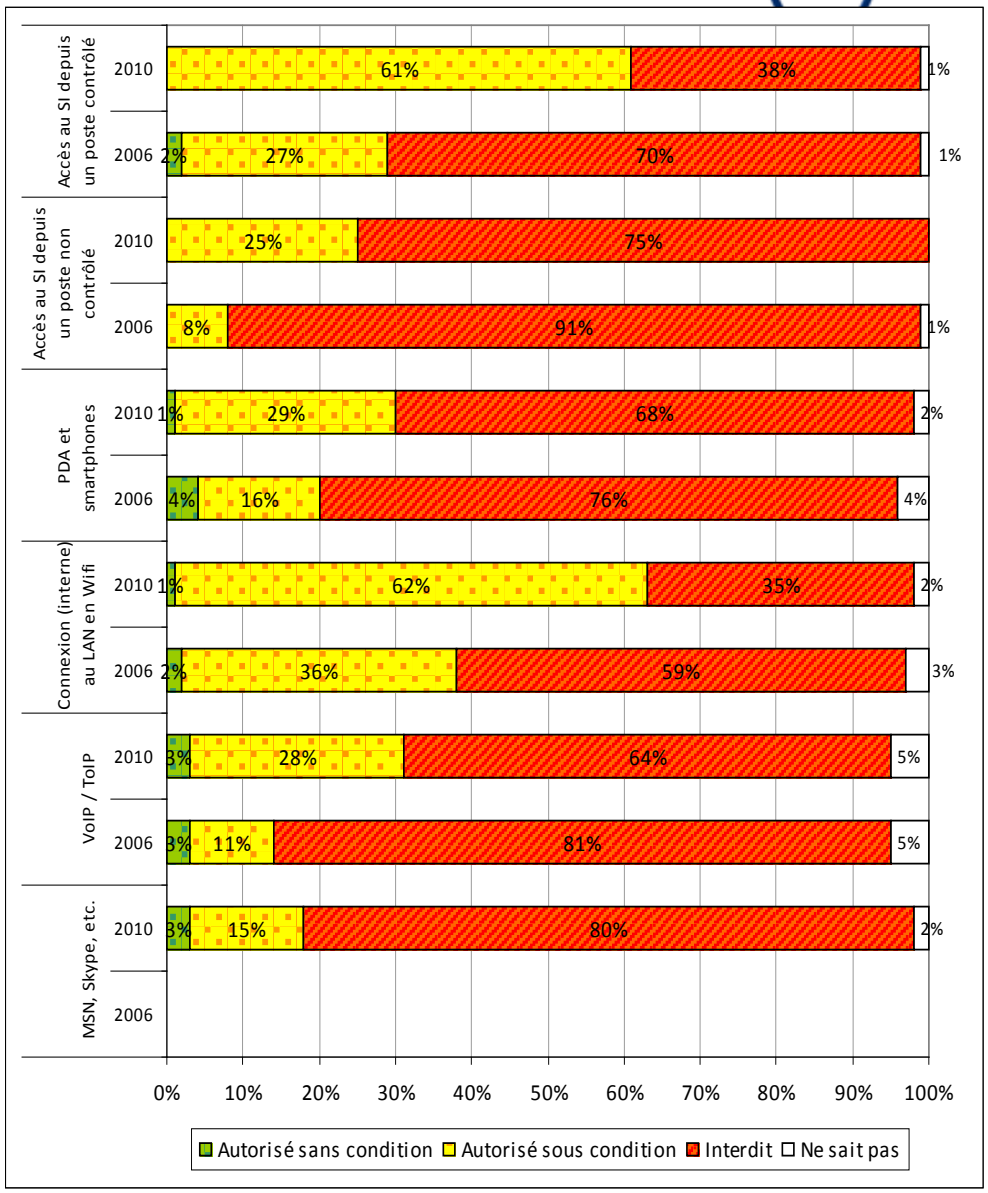
Moyens utilisés pour assurer la sensibilisation



Sécurité liée aux nouvelles technologies : diminution de leur interdiction pure et simple

Les hôpitaux moins permissifs que les entreprises dans l'utilisation des nouvelles technologies

- Accès à partir de postes de travail non maîtrisés en augmentation mais largement interdit
- Les réseaux sans fil prennent de plus en plus d'ampleur
- L'usage de la téléphonie sur IP s'étend (presque triplée en 4 ans)
- Les hôpitaux ne résistent pas au nomadisme



Lutte antivirale : la démarche de sécurisation est la même pour entreprises et hôpitaux

Utilisation du chiffrement des données utilisateur : **inférieure de 10% aux** entreprises

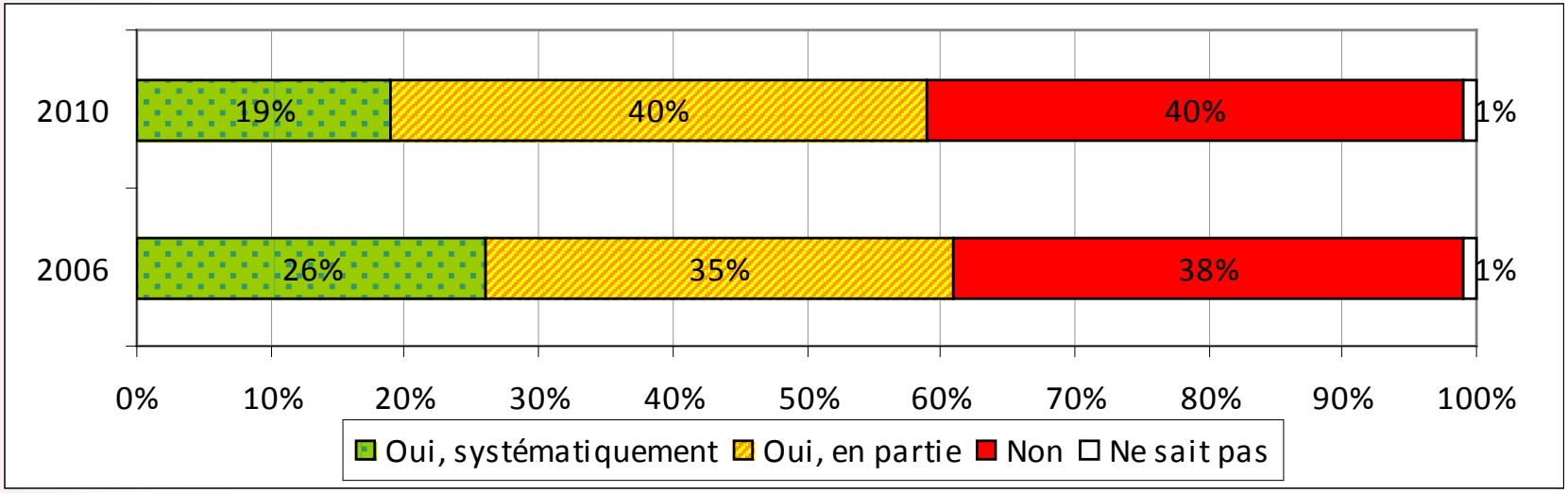
Majorité des machines chiffrées = ordinateurs fixes : démarche plus axée sur la confidentialité des données que sur le vol d'équipements portables.

Moins d'infogérance dans les hôpitaux

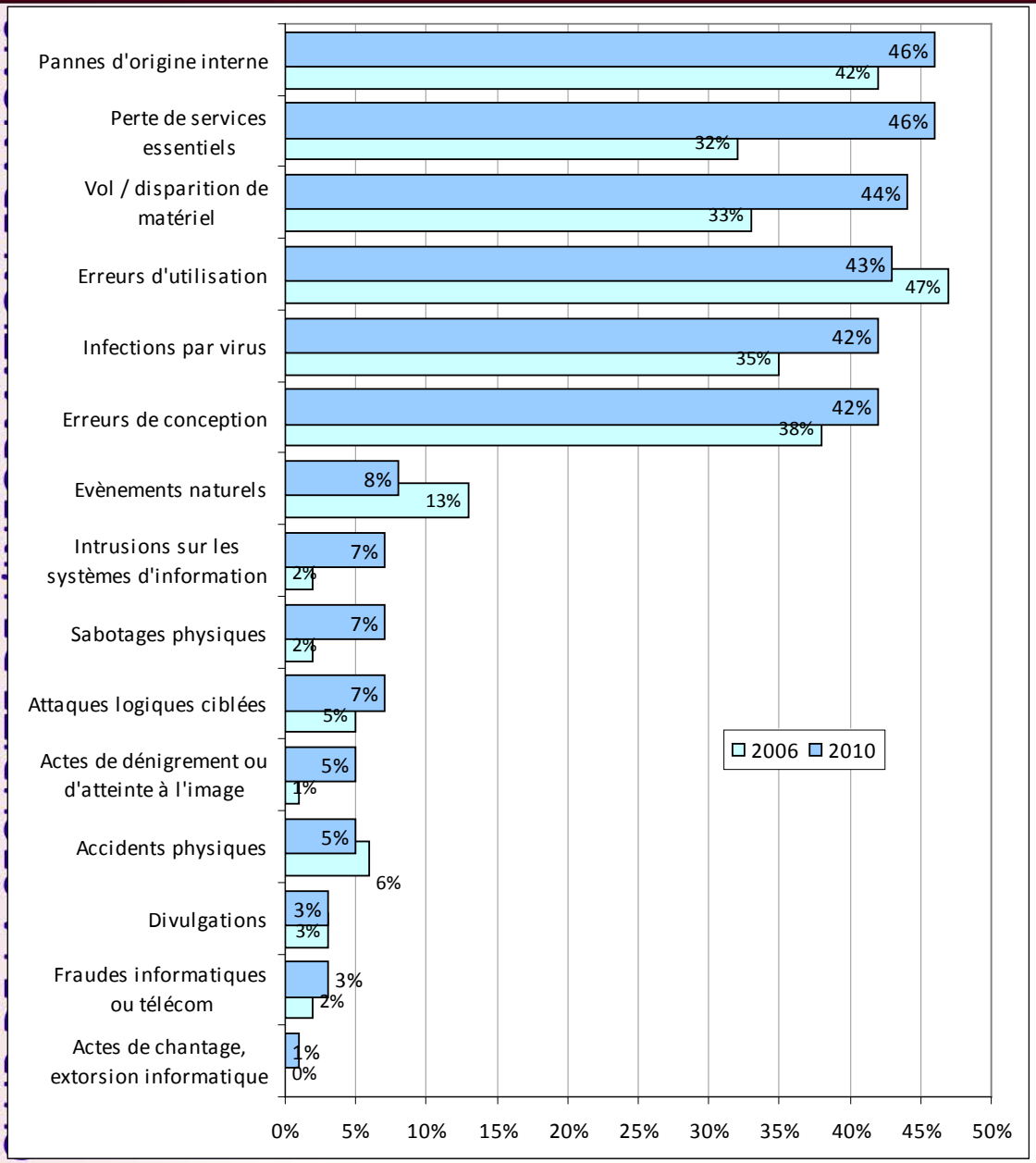
26%, soit une diminution de 11% depuis la précédente étude

Un contrôle de la sécurité limité des contrats d'infogérance : les hôpitaux sont plus nombreux en 2009 à exercer leur droit de regard sur les prestations associées via des audits de sécurité au moins ponctuels, mais ce chiffre (31%) reste faible

Veille sur les vulnérabilités: stagne et reste insuffisante : 59% seulement des hôpitaux s'y consacrent



- Progrès modéré dans la mise en place de procédures de gestion des correctifs
- Déploiement des correctifs de plus en plus formalisés :
  - 47% des hôpitaux, contre 34% en 2006
- Déploiement des correctifs en moins de 3 jours (urgence) : 80%



Les incidents de sécurité mieux détectés par les hôpitaux

Forte augmentation de la perte de services essentiels (augmentation de la taille des hôpitaux, Conficker)

Progression de plus d'un tiers des vols de matériels informatiques et de télécommunications

(accueil quotidien du public, développement outils nomades)

Baisse des causes accidentelles , hausse des causes malveillantes

CNIL : 94% des hôpitaux estiment être en conformité totale ou sur les traitements les plus sensibles !

Mise en place d'un Correspondant Informatique et Liberté progresse nettement : faite ou décidée dans 43% des hôpitaux (37% en 2006).

31% ignorent que leur hôpital est soumis à des lois /règlementations spécifiques en matière de sécurité des informations !

Le profil du répondant est-il en cause, ou sa sensibilisation aux aspects juridiques ?

Tableaux de bord: copie blanche ?

7% des hôpitaux ont des tableaux de bord de suivi de la Sécurité informatique

Aucune progression depuis 2006

1ères conclusions

Progressions constatées

Politique de sécurité: formalisation, mise à jour, soutien

Utilisation accrue de ISO 2700x et PSSI du GMSIH

Nombre de RSSI

Chartes de sécurité

Sécurité des nouvelles technologies

SSO, authentification forte

Détection incidents

Conformité CNIL

Opportunités d'amélioration

Inventaires et classement des informations

Analyses de risques

Sensibilisation du personnel

Contrôle de l'infogérance

Gestion des accès , droits, mots de passe

Veille sur les vulnérabilités

Résorption de l'impact des incidents

Plans de Continuité

Gestion de crise

Connaissance des lois/règlementations sécurité

Audits de sécurité

Tableaux de bord

Points de vigilance

Focus (légitime) sur la protection de la donnée (divulgation (DLP)) mais…

- Propagation du virus Conficker (*via* port USB)
- Paralysie des services hospitaliers londoniens (virus *via* messagerie)

Services Généraux sur IP (Internet Protocol, pas Identifiant Patient ☺)

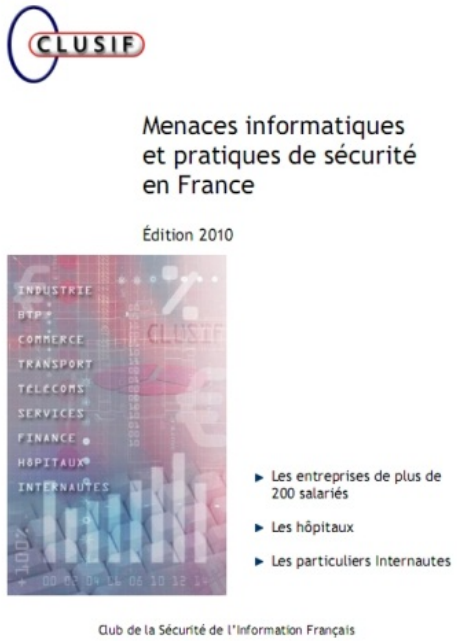
- Electricité, ventilation (HVAC), badges sans contact, serrures, vidéo-surveillance…

Hacking du biomédical… plus seulement les accès de télémaintenance (e.g. imagerie) mais aussi les équipements embarqués…sur l'individu

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

www.clusif.asso.fr

(libre téléchargement)



Prochaine conférence CLUSIF :

« Gestion des incidents »

16 juin - CNA, Paris