



Menaces informatiques  
et  
Pratiques de sécurité en France  
Édition 2010

17 juin 2010

# Enquête 2010

## Les Entreprises

**M. Lionel MOURER**

Directeur – Consultant Principal



## Les entreprises – présentation de l'échantillon

350 entreprises françaises de plus de 200 salariés ont été interrogées

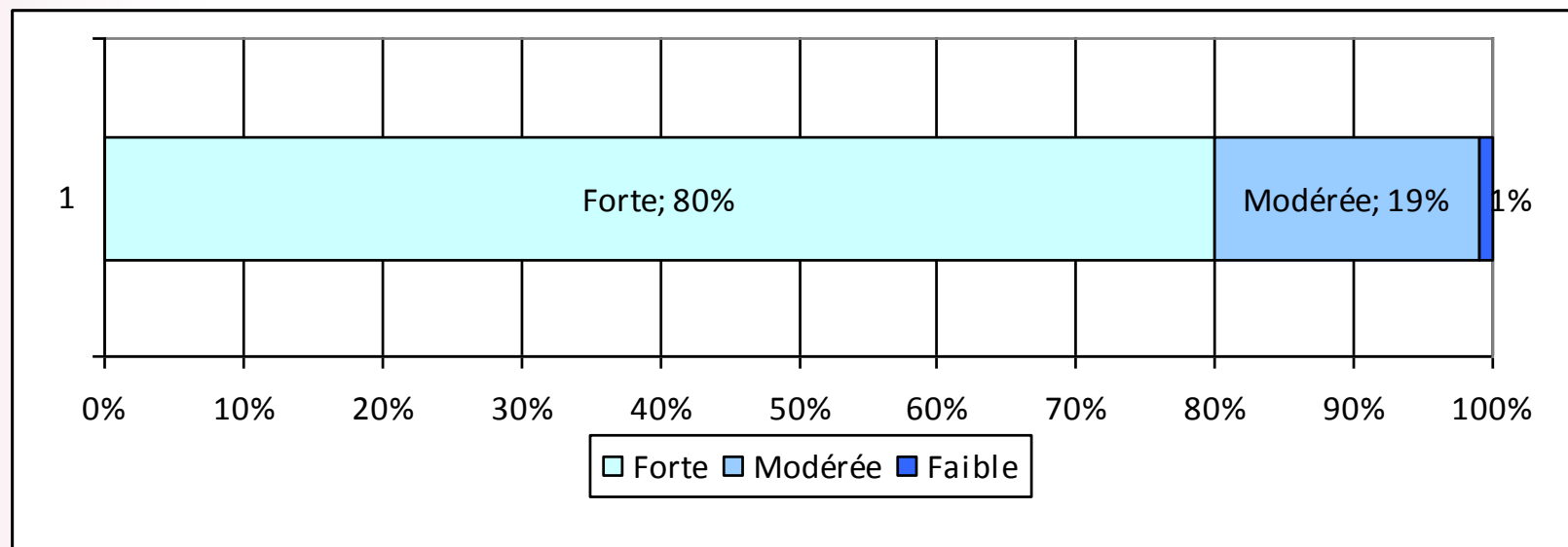
Les personnes interrogées

- des RSSI dans 29% des cas (40% pour les entreprises de + de 1 000 salariés)
- des responsables informatique dans 43% des cas

Les résultats sont redressés pour obtenir des chiffres représentatifs par secteur d'activité et/ou par taille

# Le Système d'Information : épine dorsale des entreprises

Diriez-vous que votre entreprise a, vis-à-vis de l'informatique, une dépendance ... ?

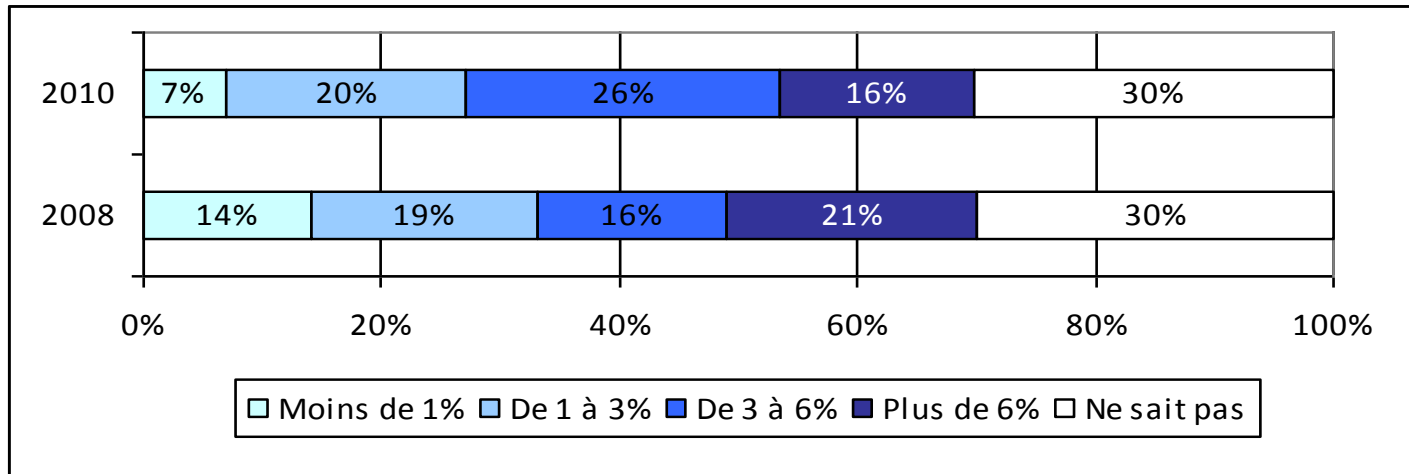


## Niveaux de dépendance

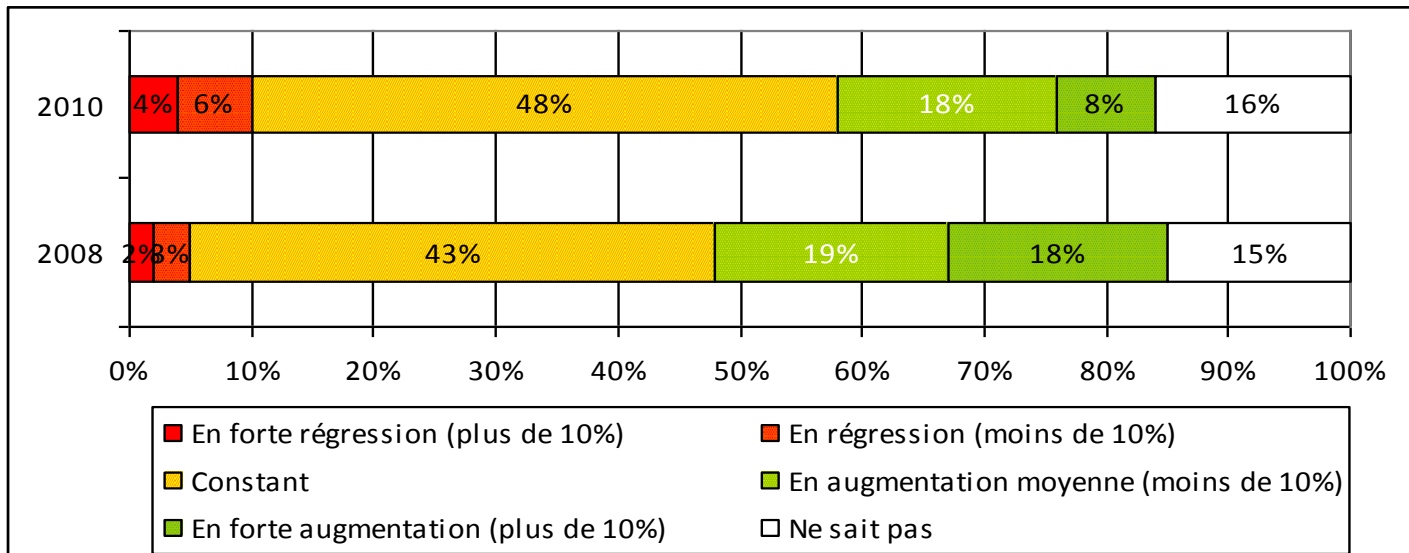
- **Forte** : une indisponibilité de moins de 24 heures a des conséquences graves
- **Modérée** : une indisponibilité jusqu'à 48 heures est tolérable
- **Faible** : une indisponibilité même de longue durée n'a pas de conséquence grave

# Un budget sécurité dont le périmètre semble encore mal cerné

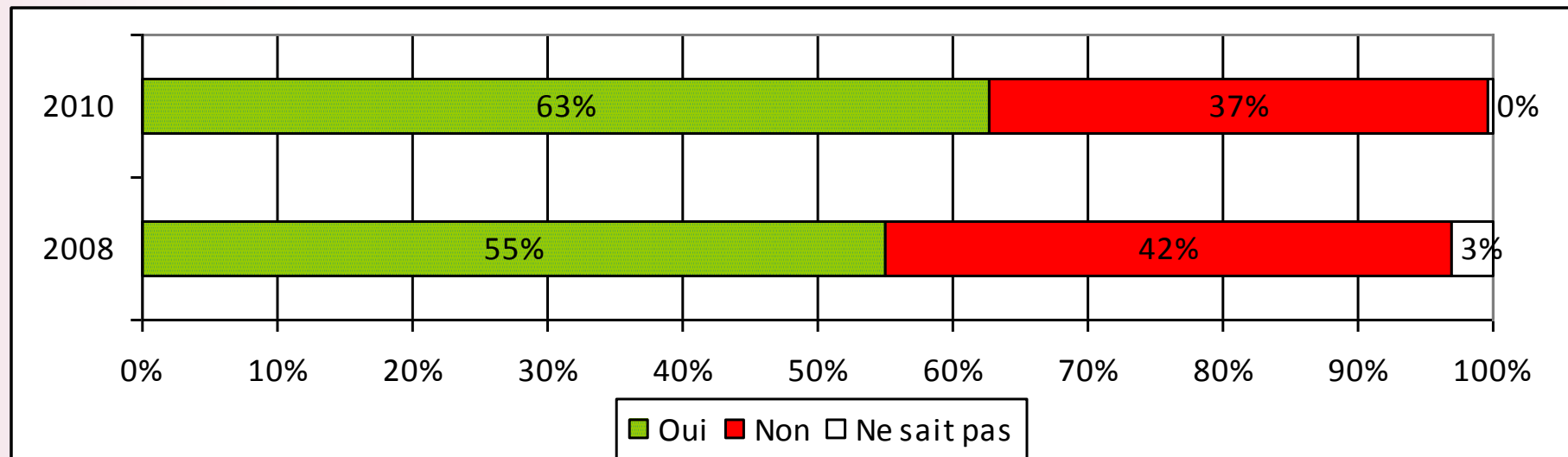
Quel pourcentage représente le budget sécurité par rapport au budget informatique total ?



Quelle a été l'évolution du budget sécurité par rapport à l'année précédente ?



## Des politiques de sécurité voulues par les Directions Générales



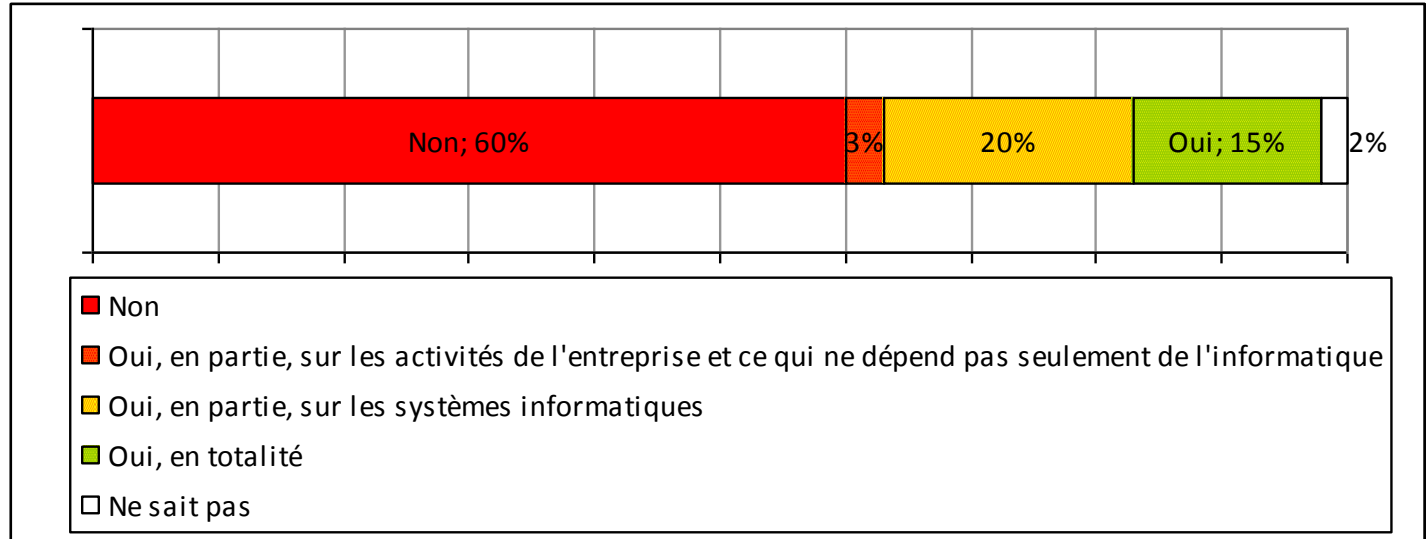
- 94% des politiques sont soutenues par la Direction Générale
  - mais cela ne suffit pas à leur mise en application !
- 52% seulement des politiques de sécurité s'inspirent d'une norme ou d'un standard sectoriel

## Organisation : un RSSI qui s'éloigne de la DG et qui dispose de moyens limités

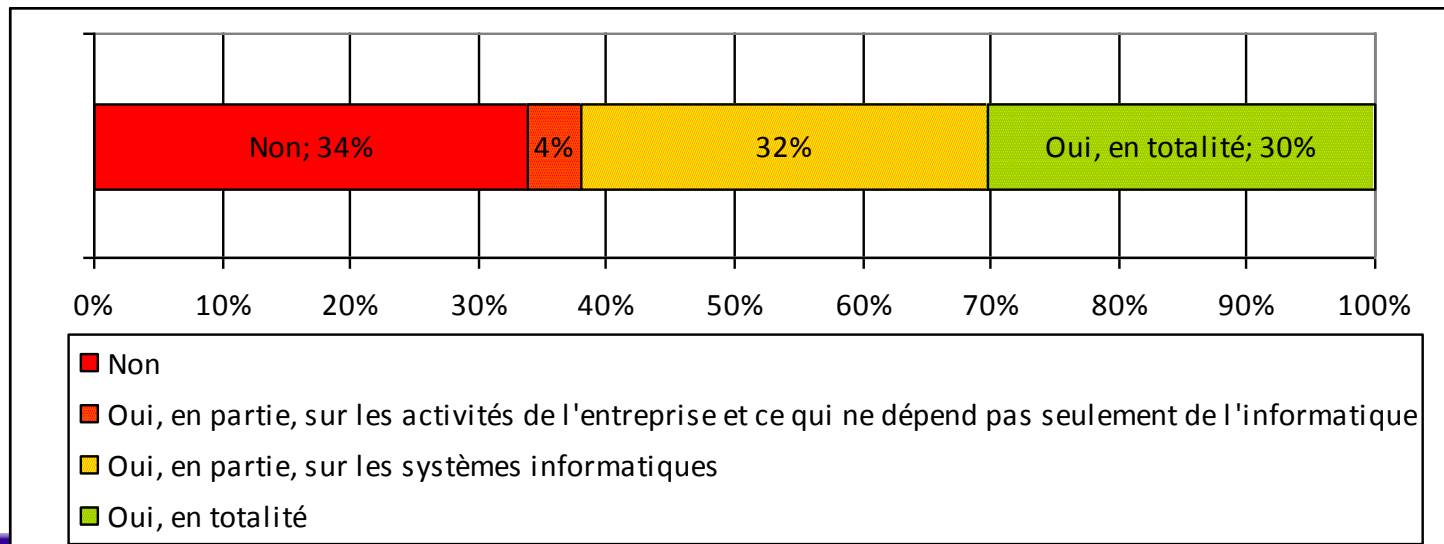
- 49% des entreprises seulement disposent d'une fonction RSSI clairement identifiée (+12% vs 2008)  
(16% à temps plein, 21% à temps partiel)
- Le RSSI est rattaché à la Direction Générale dans 34% des entreprises (-11% vs 2008)
- Il n'y a pas d'équipe sécurité dans 21% des entreprises et une équipe de 1 ou 2 personnes dans 61% des entreprises

# La notion de risque SI peine encore

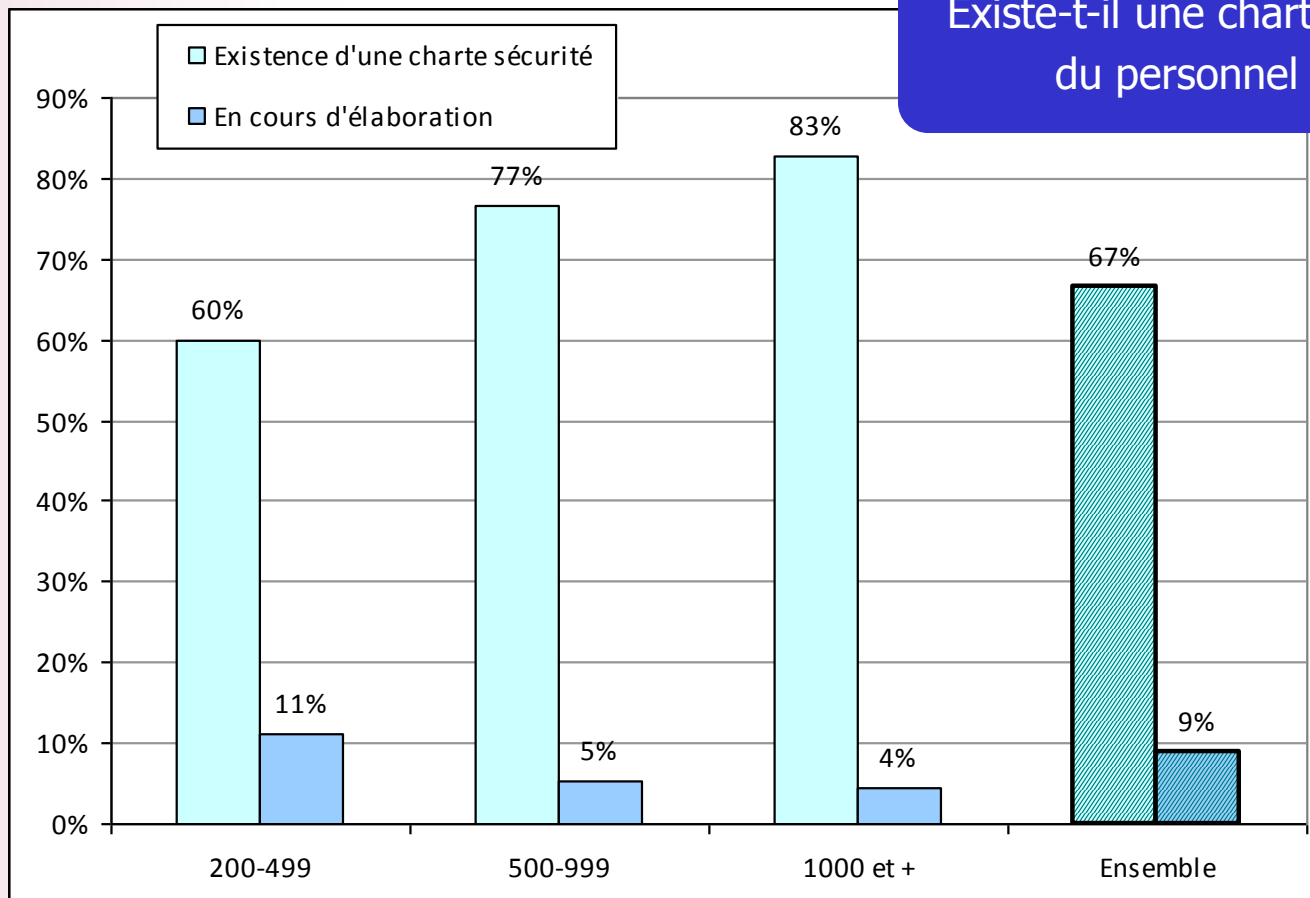
Avez-vous réalisé une analyse globale des risques liés à la sécurité du SI de votre entreprise ?



Avez-vous inventorié toutes les informations et leur avez-vous attribué un propriétaire ?



## Chartes de sécurité : un palier semble atteint

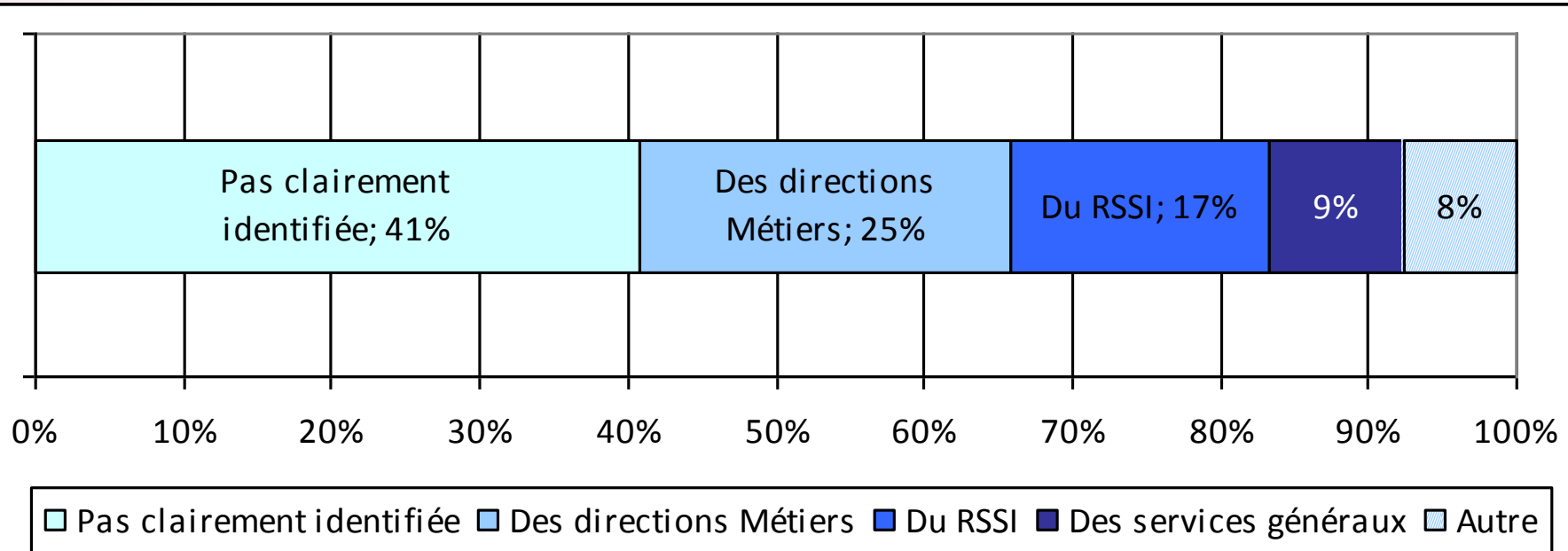


Existe-t-il une charte de sécurité à destination du personnel de votre entreprise ?

- Une charte présentée aux instances représentant le personnel dans 84% des cas
- Une charte qui précise des sanctions dans 53% des cas

# Sécurité des données « papier »

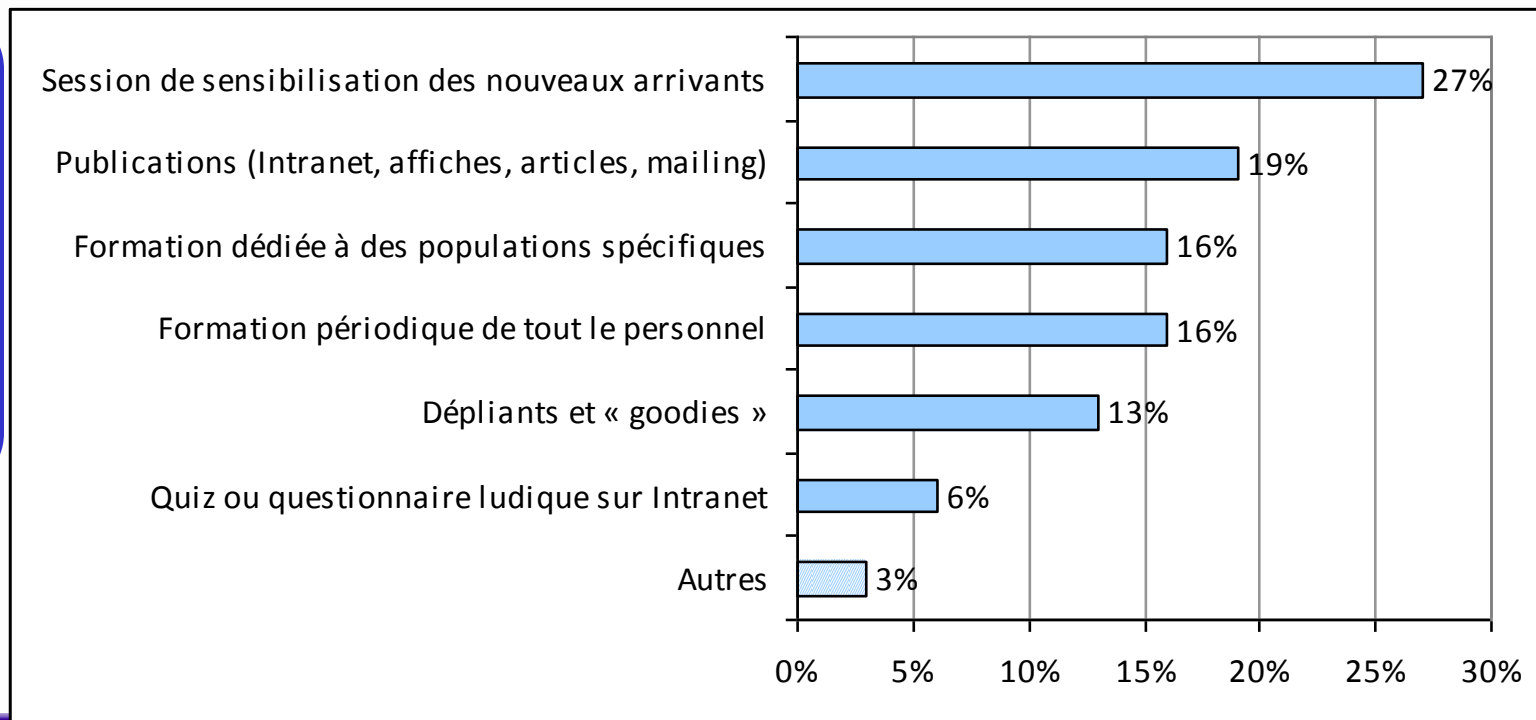
La sécurité physique des données sur papier est-elle de la responsabilité...



# Des actions de sensibilisation encore très partielles mais mieux contrôlées

- 32% des entreprises disposent d'un programme de sensibilisation à la sécurité de l'information (-3% vs 2008)
- L'impact de la sensibilisation est mesuré dans 37% des cas (+25% vs 2008)

Quels sont les moyens utilisés pour assurer la sensibilisation ?



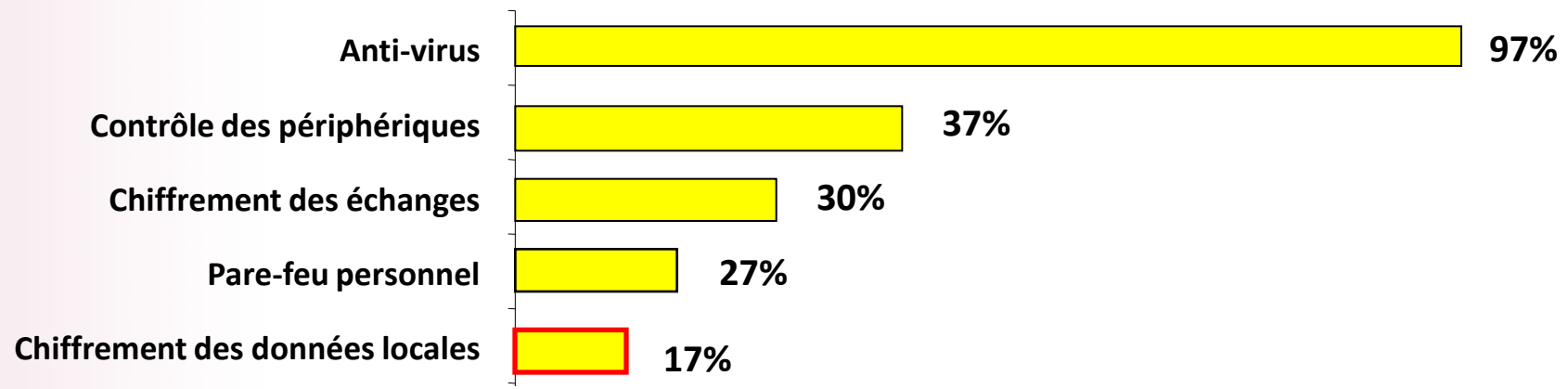
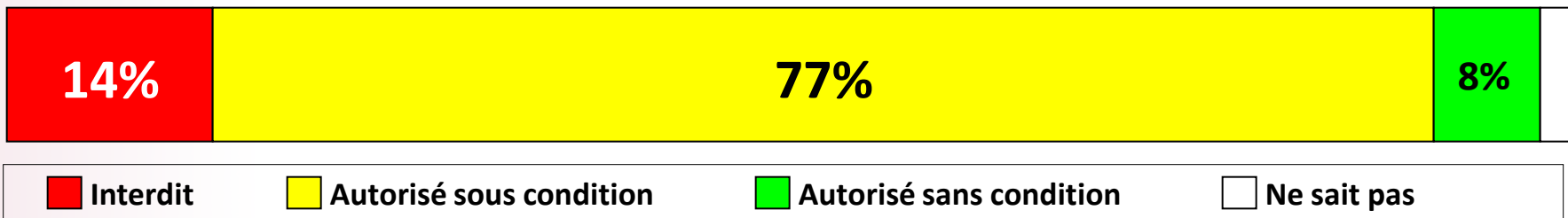
# Ouverture du SI et usage des nouvelles technologies : Smartphone et VoIP/ToIP progressent...

Technologie autorisée ou non autorisée dans votre politique de sécurité ?



# Des PC portables toujours peu protégés !

L'accès aux systèmes d'information à partir de poste de travail nomade est-il...

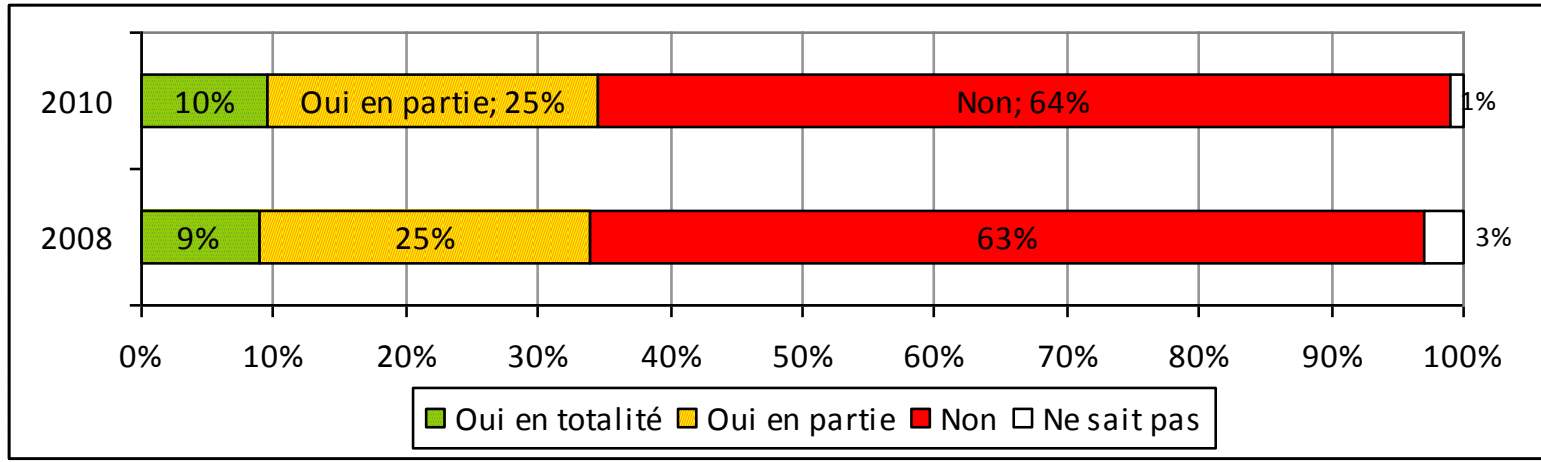


## Nouvelles technologies & Contrôle d'accès

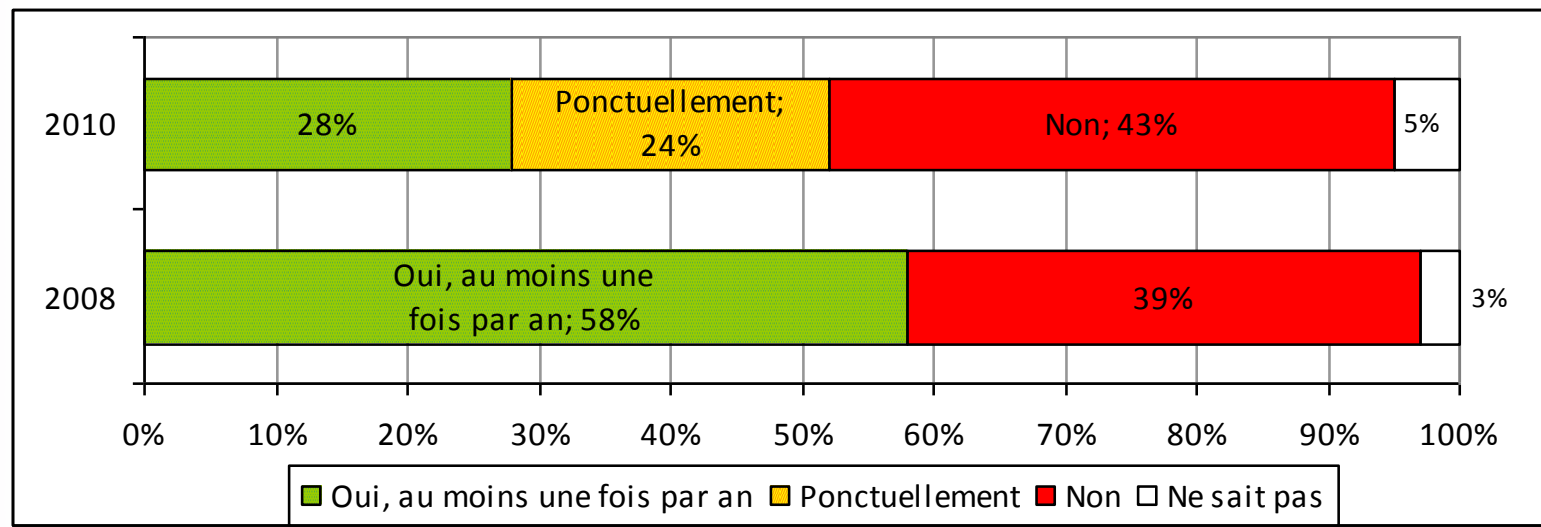
- Nouvelles technologies de sécurité : elles se diffusent lentement...
  - anti-virus, pare-feu et anti-spam font la course en tête (respectivement 97%, 95% et 91%)
  - IDS/IPS, technologies arrivées à maturité, progressent (34% et 27%, +11% vs 2008)
  - les technologies récentes (type NAC ou DLP) peinent à se déployer (respectivement 23% et 9%)
- Contrôle d'accès : stagnation globale, sauf...
  - SSO et Web-SSO décollent enfin (respectivement 21% et 8%, +14% et +5% vs 2008)

# Infogérance, SaaS, ASP : encore peu usitée, des progrès en suivi reste à faire...

Avez-vous placé tout ou partie de votre SI sous contrat d'infogérance ?

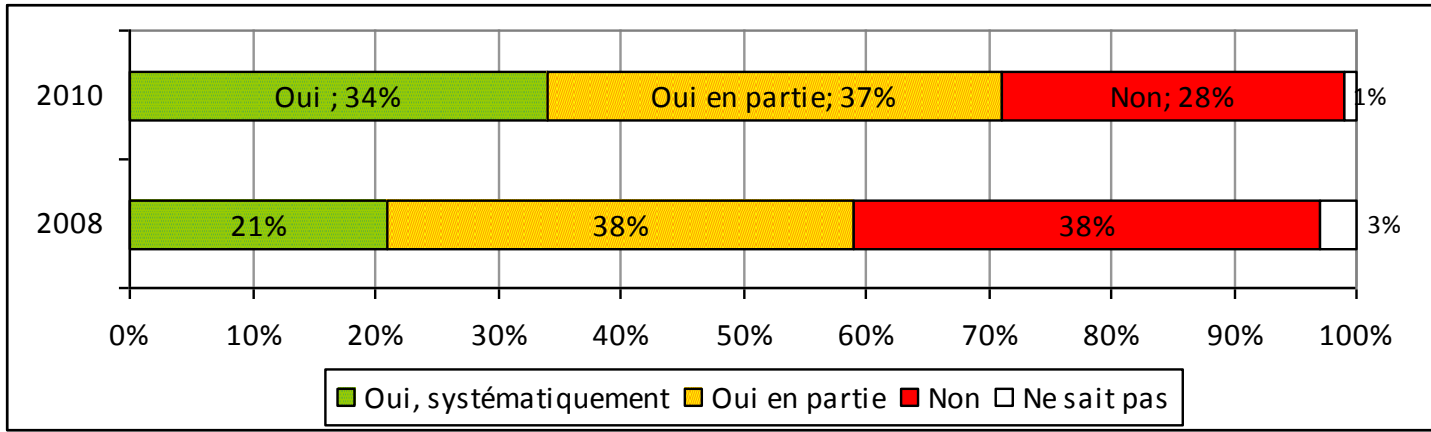


Effectuez-vous des audits sur cette infogérance ?

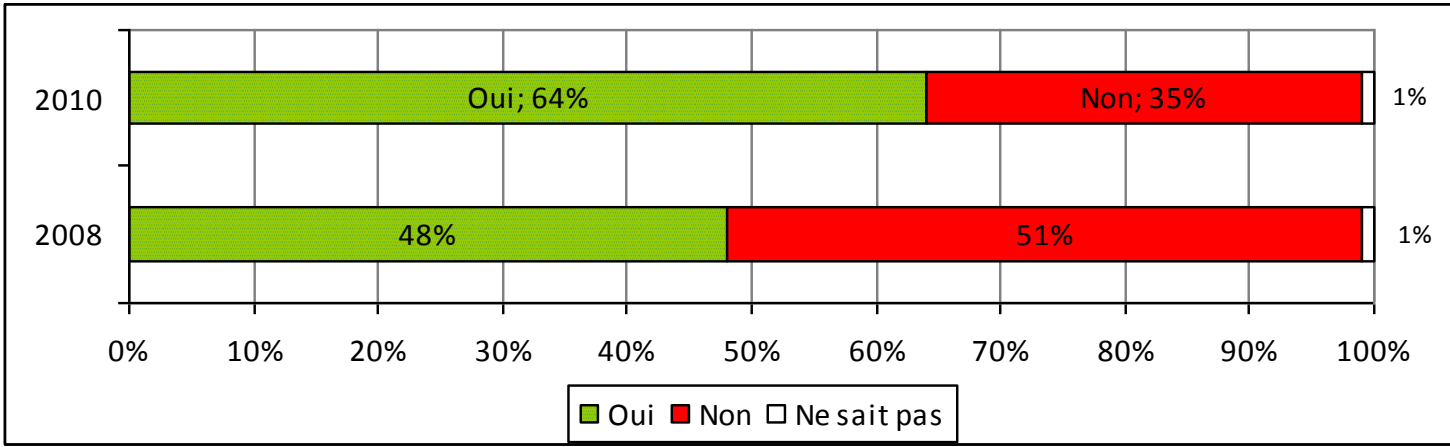


# Les entreprises ont amélioré leur vigilance vis-à-vis des menaces

Réalisez-vous une veille permanente sur les nouvelles vulnérabilités et sur les nouvelles attaques ?



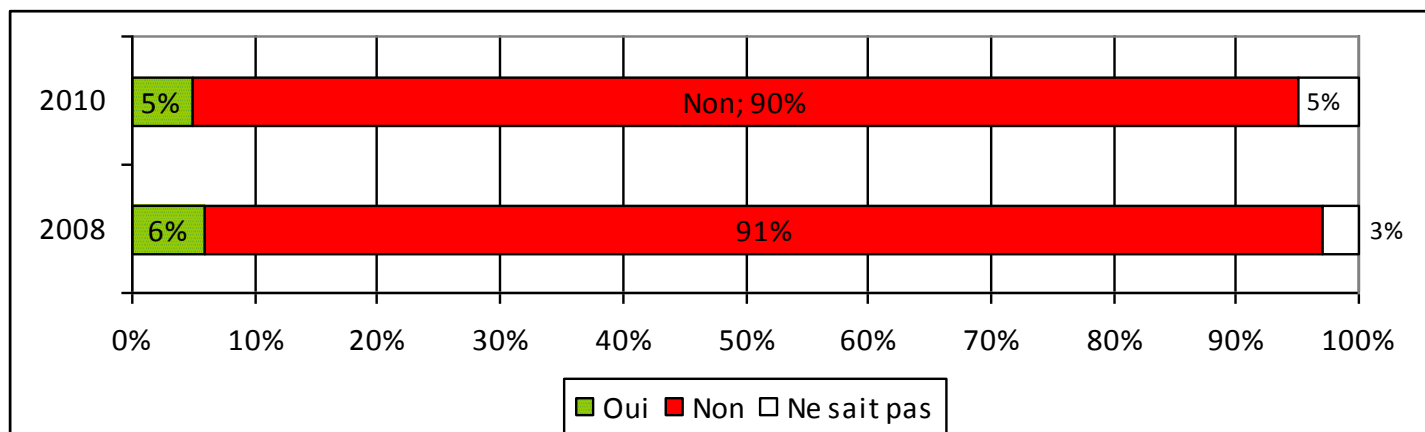
Avez-vous formalisé des procédures de déploiement de correctifs de sécurité (*patch management*) ?



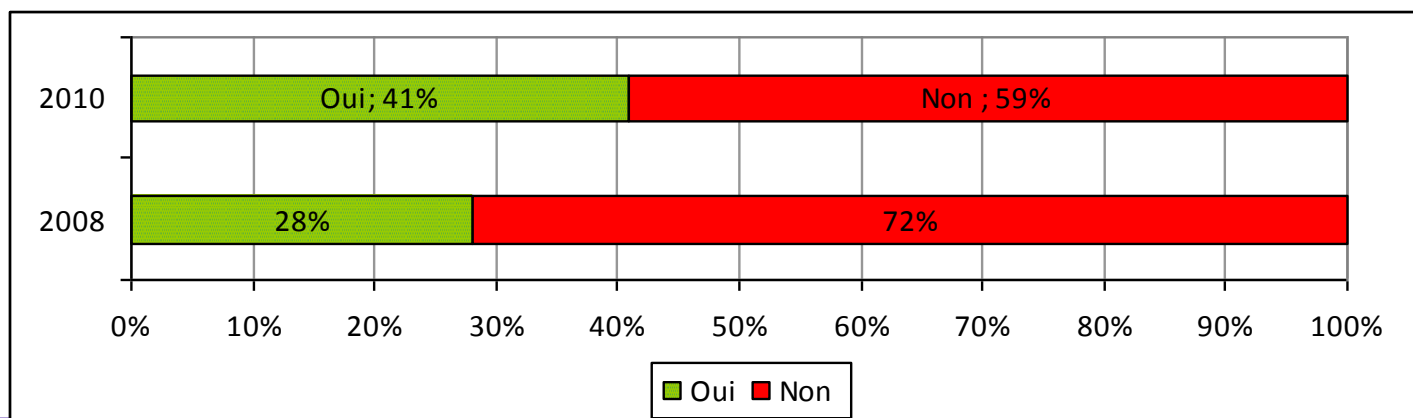
# Un suivi et une évaluation de l'impact des incidents en amélioration...

74% des entreprises déclarent avoir subi au moins un incident de sécurité (+19%)

Au cours de l'année passée, votre entreprise a-t-elle déposé des plaintes suite à des incidents liés à la sécurité de l'information ?

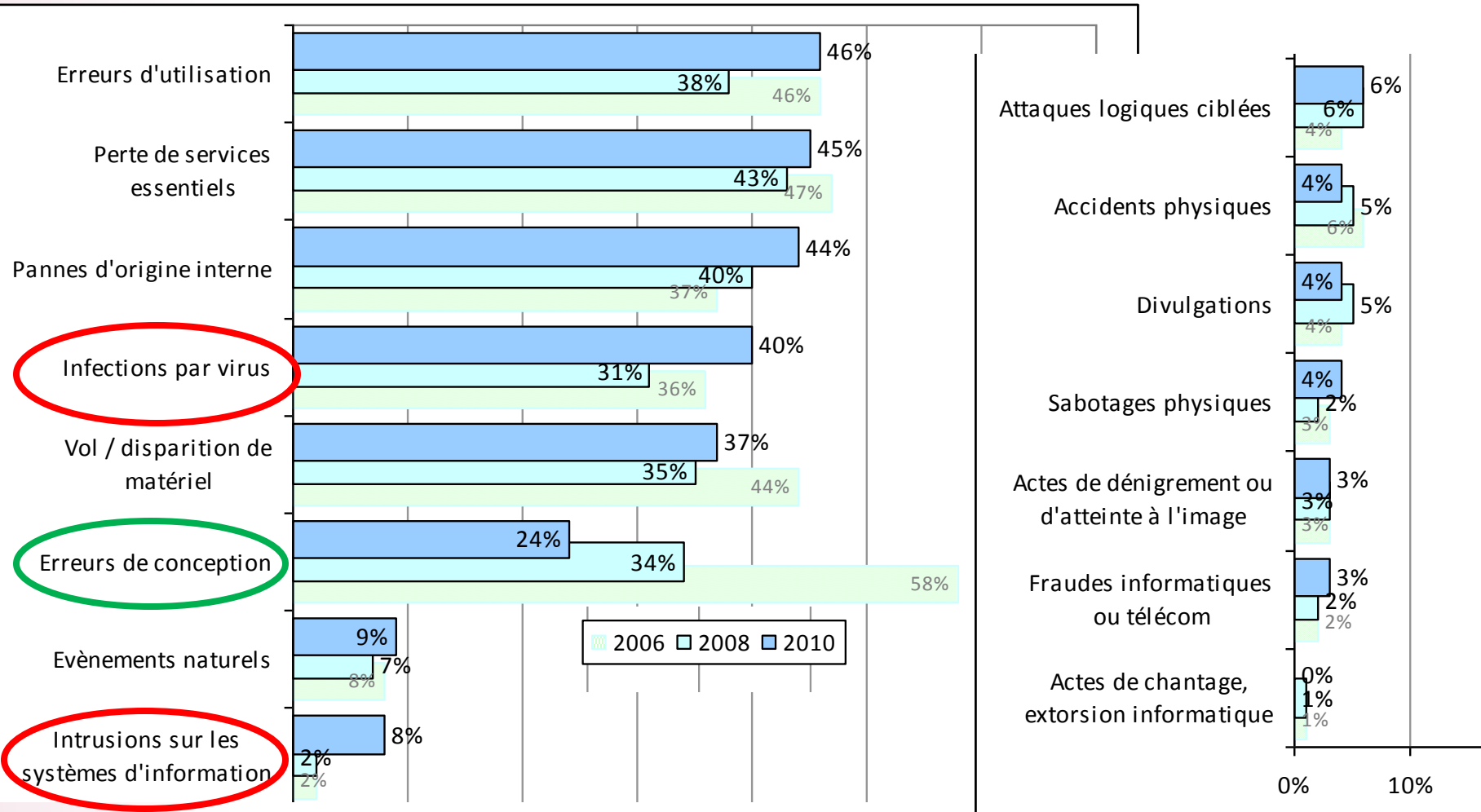


Procédez-vous à une évaluation de l'impact financier des incidents de sécurité SI ?



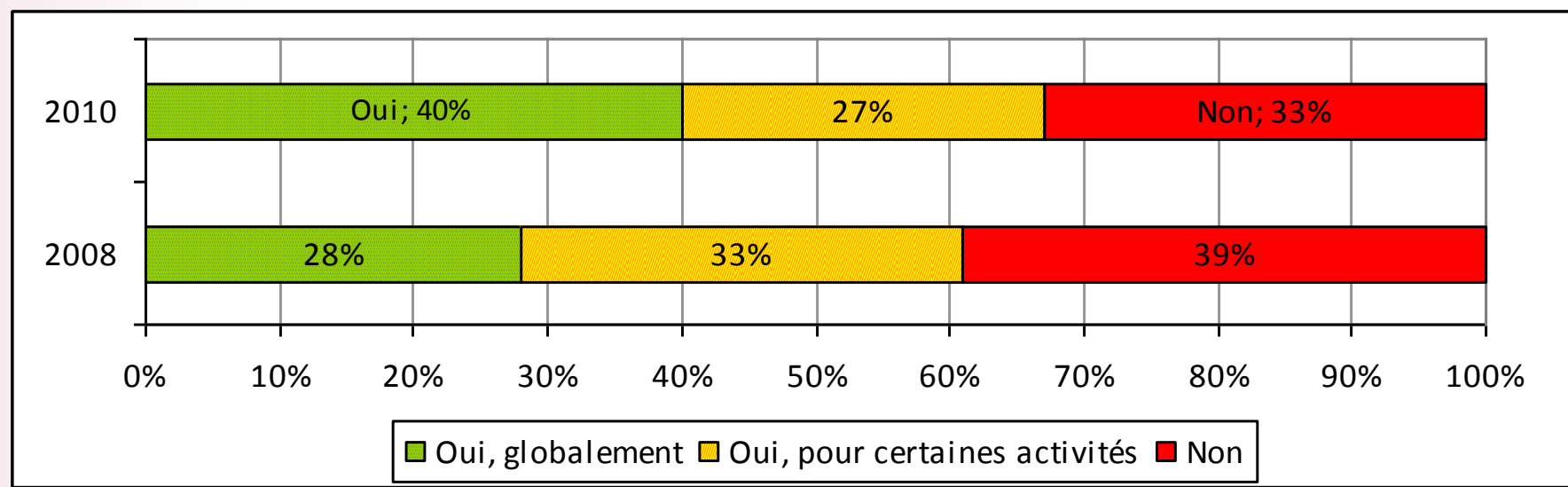
# Une malveillance toujours présente...

Quels types d'incidents votre entreprise a-t-elle recensés dans l'année ?



# 33 % des entreprises n'ont toujours pas de Plan de Continuité d'Activité !

Existe-t-il un processus formalisé et maintenu de gestion de la continuité d'activité du SI de votre entreprise ?



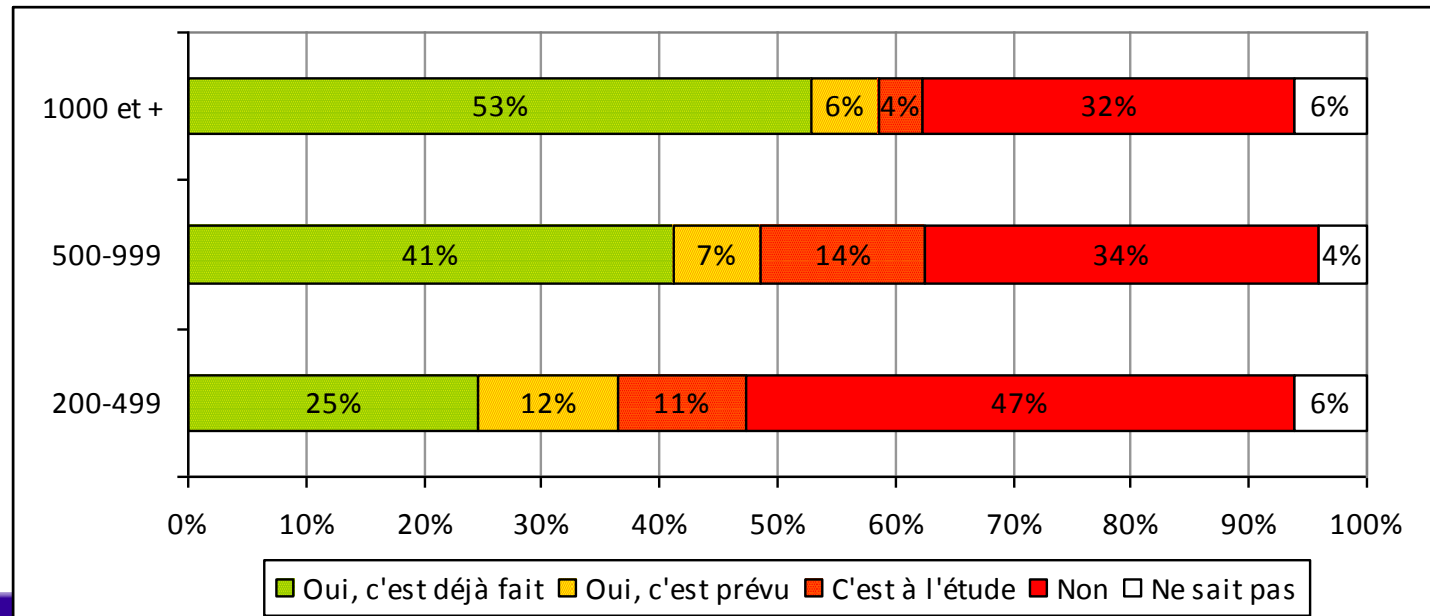
77 % des entreprises qui disposent d'un Plan de Continuité d'Activité le testent et le mettent à jour au moins une fois par an (+5% vs 2008)

# Une mise en conformité à la Loi Informatique & Liberté qui progresse lentement...

## Conformité des entreprises à la CNIL

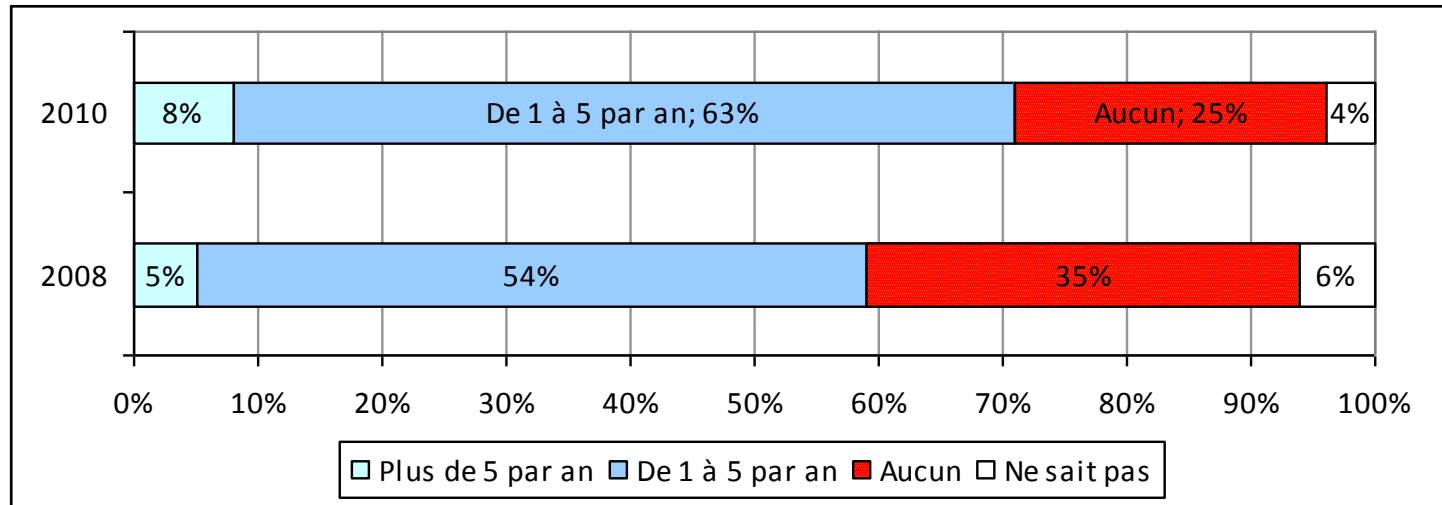
- 68% (+4%) déclarent être totalement conforme
- 20% (+1%) déclarent être conforme pour les traitements les plus sensibles

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

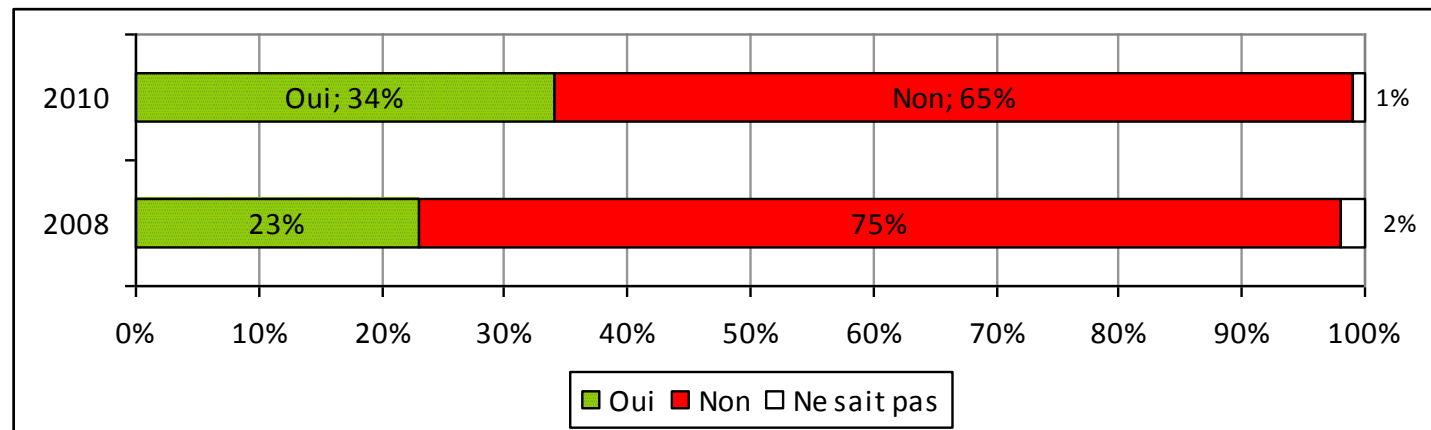


# Un « dispositif de contrôle » toujours déficient

Combien d'audits de sécurité sont menés en moyenne au sein de votre entreprise sur 1 an ?



Votre entreprise a-t-elle mis en place un tableau de bord de la sécurité informatique ?



CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

## Au final : un étonnant sentiment de stagnation !...

- 2004 à 2006 : des progrès sur la formalisation des politiques de sécurité
- 2006 à 2008 : ces politiques ne se traduisent pas par des actions concrètes d'amélioration de la sécurité
- 2008 à 2010 : une très légère amélioration, bien insuffisante au regard des enjeux !

Une recommandation :  
Identifiez les risques majeurs et  
traitez-les jusqu'au bout !