



Menaces Informatiques et Pratiques de Sécurité en France

19 juin 2008
Les Entreprises



Evénement organisé en partenariat avec :

BlackBerry – CA – McAfee – Orange Business Services – Orsy –TelecityGroup



Enquête 2008



Introduction

Analyse du segment Entreprises

M. Laurent BELLEFIN
Directeur de l'Activité Sécurité
Solucom Group

19 juin 2008

Un guide pour tous les acteurs du domaine de la sécurité de l'information

Objectifs de l'enquête 2008

- Établir un **état des lieux** des pratiques de sécurité et de la sinistralité informatique en France
- Déterminer les **tendances générales** en matière de sécurité de l'information

Démarche retenue

- Questionnaire élaboré par le CLUSIF
- Enquête confiée à un cabinet d'étude marketing spécialisé (GMV Conseil + Harris Interactive)
- Résultats analysés par un groupe d'experts membres du CLUSIF

Rapport publié le 19 juin 2008, disponible sur le site du CLUSIF

Une enquête de référence basée sur un échantillon large et représentatif

Enquête téléphonique réalisée de janvier à mars 2008

Réalisée sur 3 cibles différentes

- Les entreprises de plus de 200 employés

354 entreprises

- Les collectivités locales

194 collectivités

- Les internautes

1139 personnes

Sur un échantillon statistiquement représentatif

Entreprises et collectivités : Un questionnaire très complet, basé sur les thèmes de l'ISO 27002

- Thème 5 : Politique de sécurité
- Thème 6 : Organisation de la sécurité et moyens
- Thème 7 : Gestion des actifs et identification des risques
- Thème 8 : 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 et sinistralité
- Thème 14 : Gestion de la continuité
- Thème 15 : conformité (CNIL, audits, tableaux de bord)

Internautes : un questionnaire en 4 volets

- Caractériser la population des internautes
- Connaître les usages d'Internet à la maison
- Evaluer la perception des menaces et des risques par les internautes
- Identifier les pratiques de sécurité des internautes

Les entreprises – présentation de l'échantillon

6% des entreprises françaises de plus de 200 salariés ont été interrogées

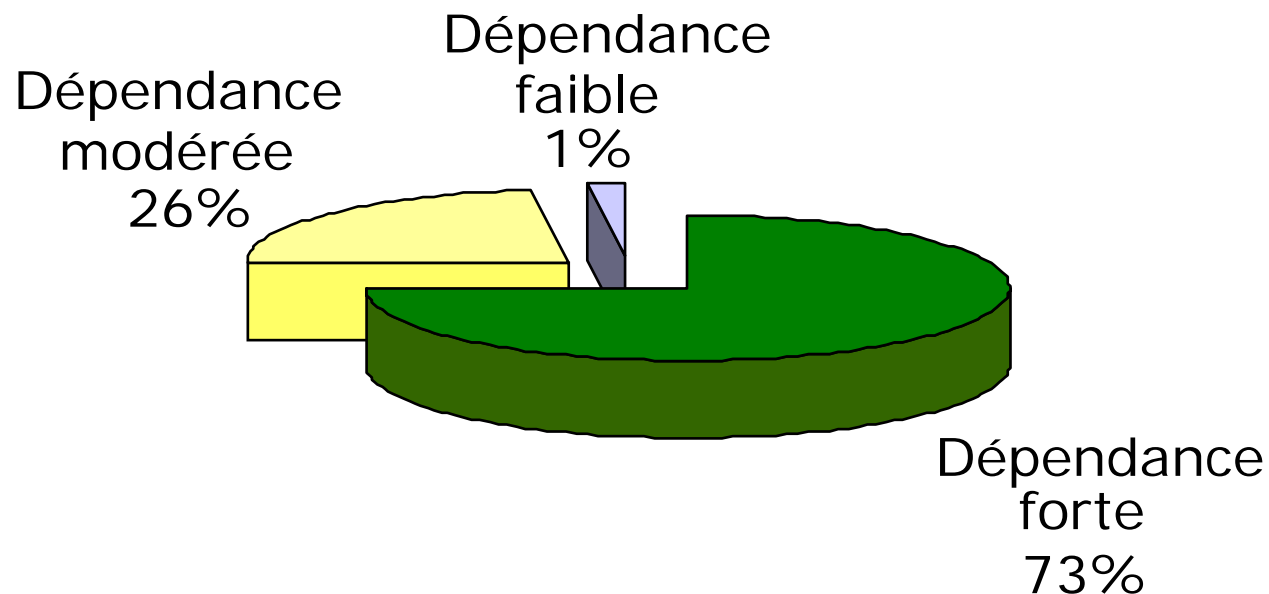
Les personnes interrogées :

- Des RSSI dans 21% des cas (43% pour les grandes entreprises)
- Des responsables informatique dans 44% des cas

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

Le système d'information : l'épine dorsale des entreprises

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

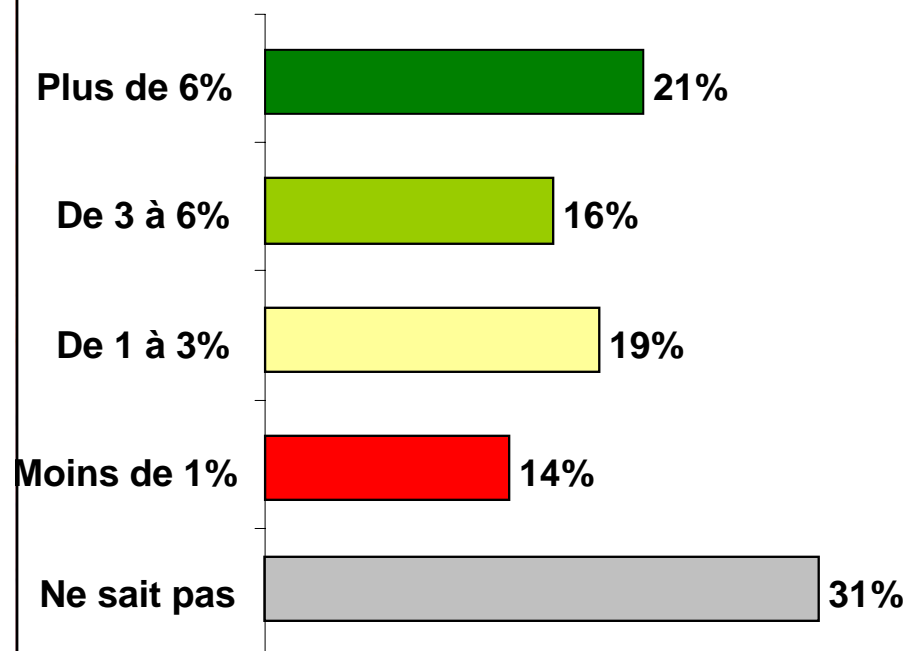


Niveaux de dépendance :

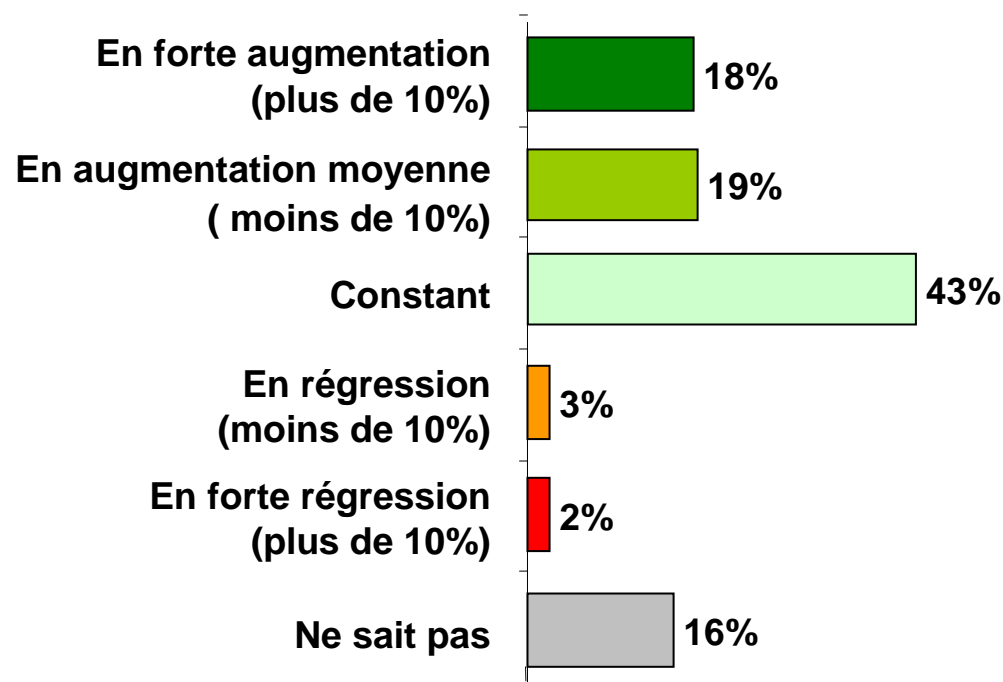
- Forte : une indisponibilité de moins de 24 heures a des conséquences graves
- Modérée : une indisponibilité jusqu'à 48 heures est tolérable
- Faible : une indisponibilité même de longue durée n'a pas de conséquence grave

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 ?



Secteur banque/services/assurance :
28 % des entreprises ont augmenté leur budget de plus de 10%

Des politiques de sécurité voulues par les Directions Générales

- 55% des entreprises sont dotées d'une Politique de Sécurité de l'information :

Un chiffre qui stagne !

- 95% des politiques sont soutenues par la Direction Générale

Mais cela ne suffit pas à leur mise en application !

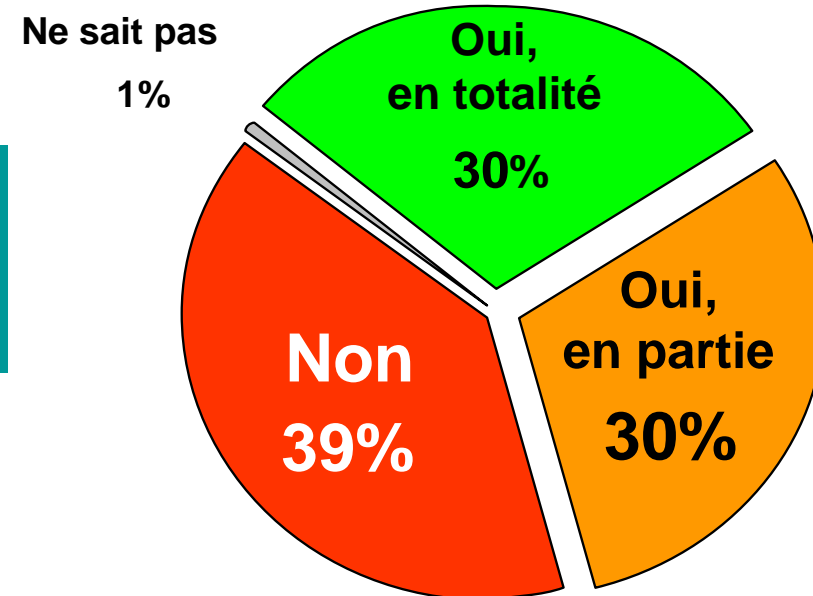
- 47% seulement des politiques de sécurité s'inspirent d'une norme ou d'un standard sectoriel

Organisation : un RSSI plus proche de la Direction Générale, mais disposant de moyens limités

- 37% des entreprises seulement disposent d'une fonction RSSI clairement identifiée (16% à temps plein, 21% à temps partiel)
- Le RSSI est rattaché à la Direction Générale dans 45% des entreprises (contre 39% en 2006)
- Il n'y a pas d'équipe sécurité dans 41% des entreprises et une équipe de 1 ou 2 personnes dans 43% des entreprises

La notion de risque SI mieux prise en compte

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



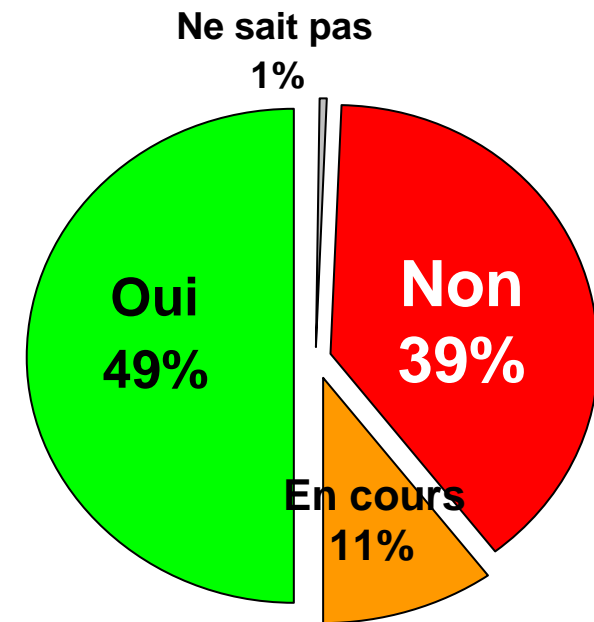
☞ Dans les projets informatiques, les risques et les exigences de sécurité sont-ils identifiés dès la phase de conception ?



Chartes de sécurité : un palier semble atteint

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

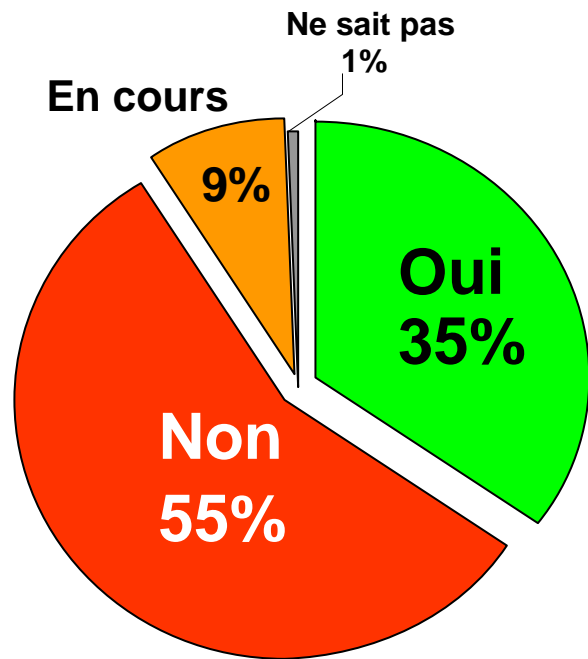
Oui dans 60% des cas pour les entreprises de plus de 1000 salariés



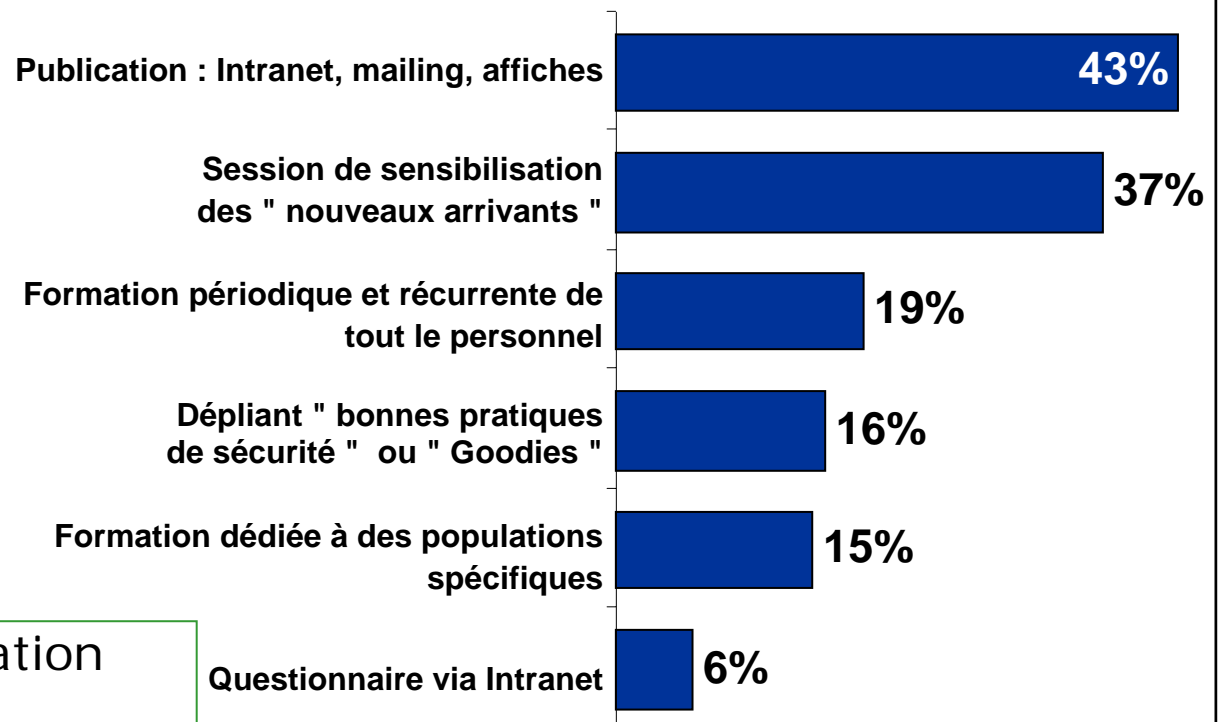
- Une charte présentée aux instances représentant le personnel dans 86 % des cas
- Une charte qui précise des sanctions dans 56% des cas

Des actions de sensibilisation très partielles

☞ Existe-t-il un programme de sensibilisation à la sécurité de l'information ?



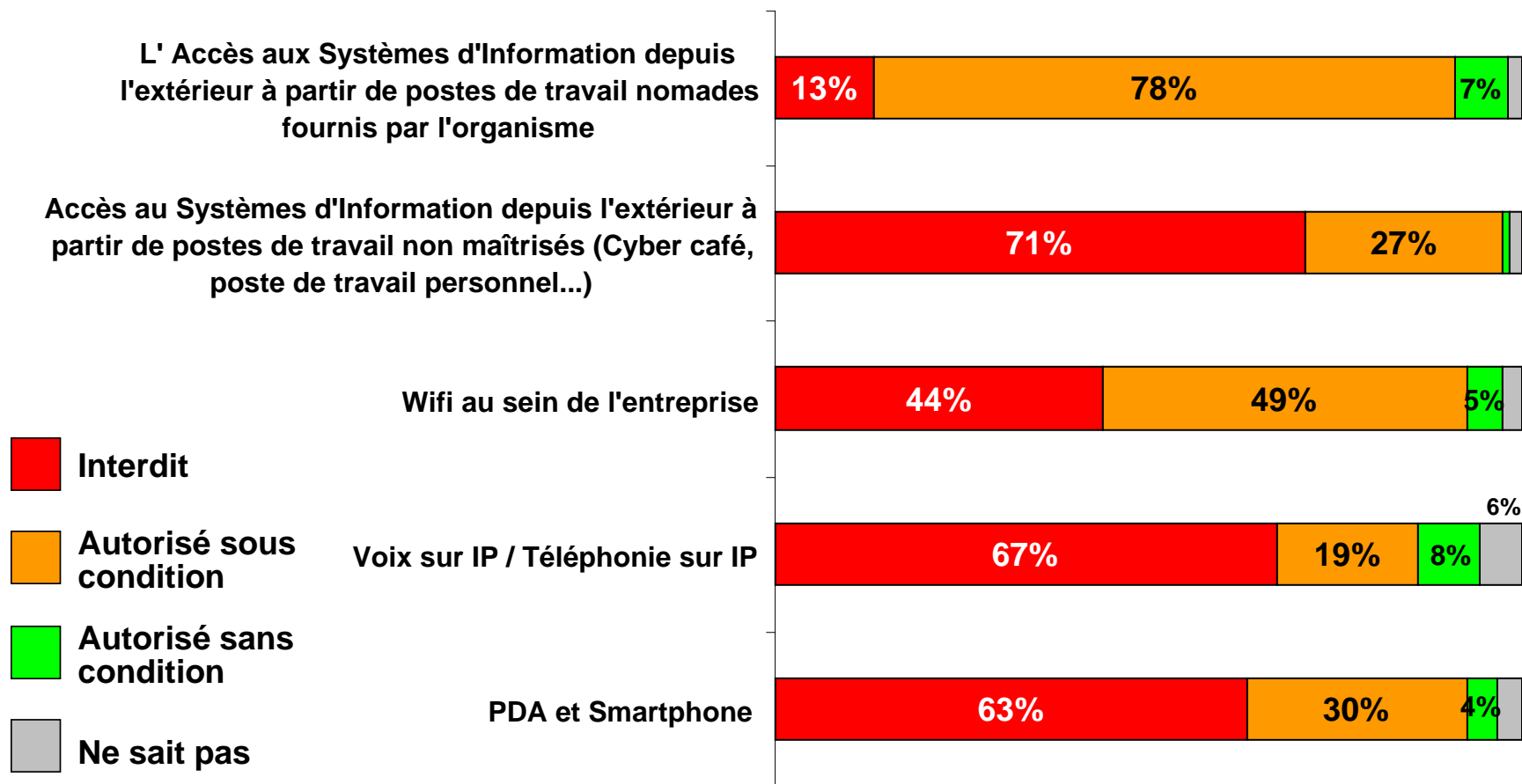
☞ (Si oui) Quels sont les moyens utilisés pour assurer la sensibilisation ? (*multi-réponses*)



L'impact de la sensibilisation est mesuré dans seulement 12% des cas

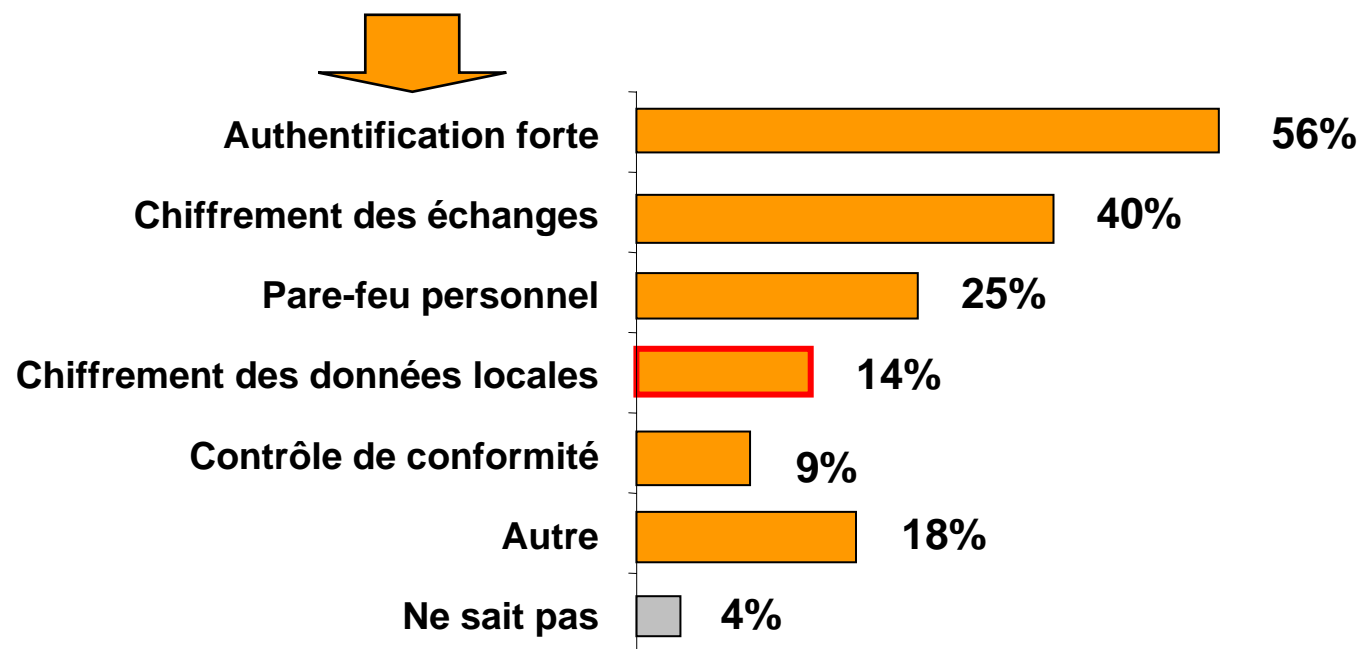
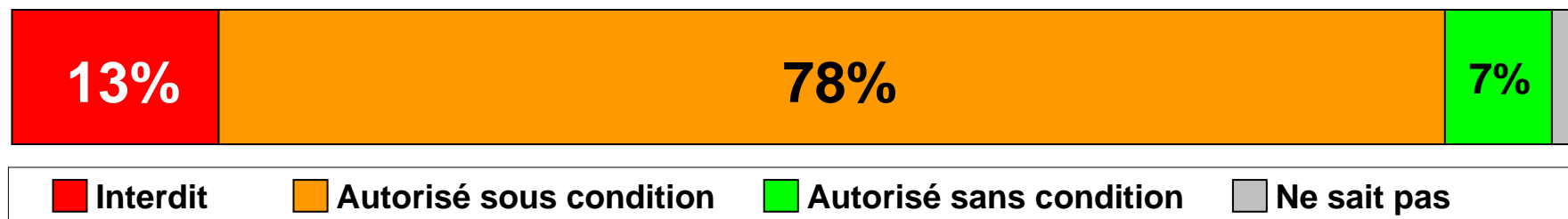
Ouverture du SI et usage des nouvelles technologies : des politiques moins restrictives, sauf pour les Smartphone...

☞ Technologie autorisée ou non autorisée dans votre politique de sécurité ?



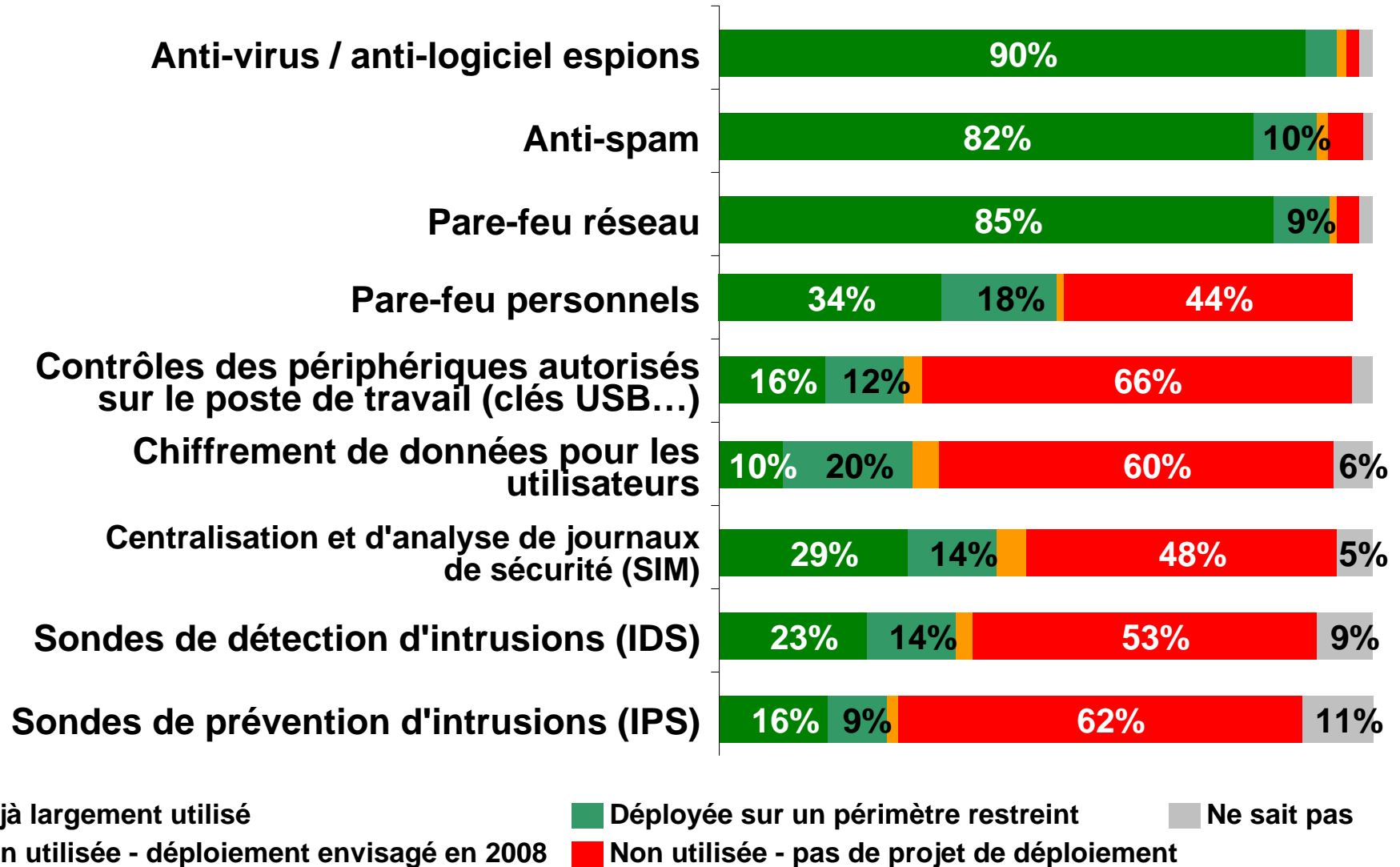
Des PC portables toujours sans outil de chiffrement !

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

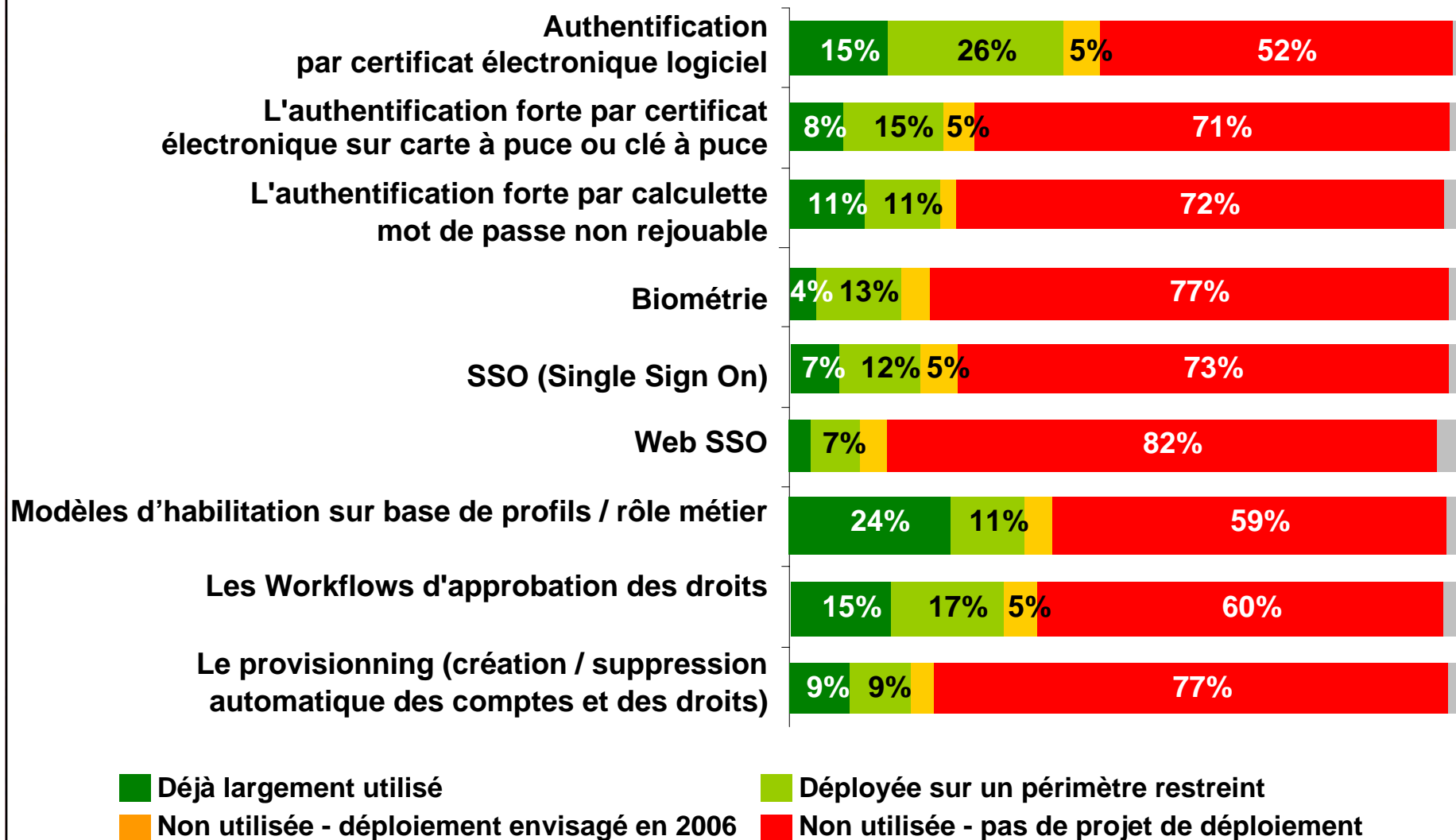




Des nouvelles technologies de sécurité qui se diffusent lentement...

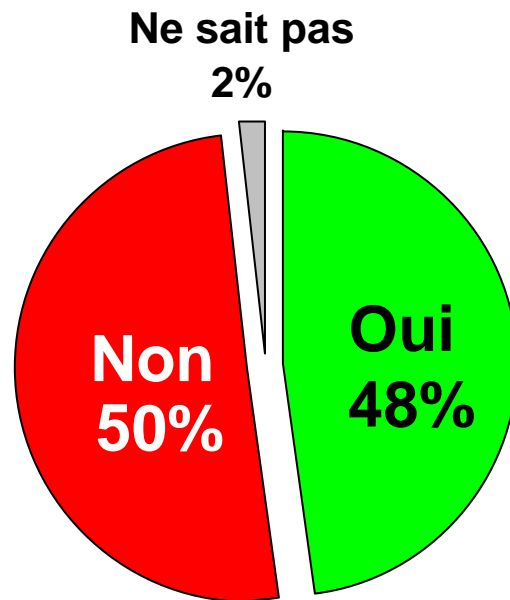
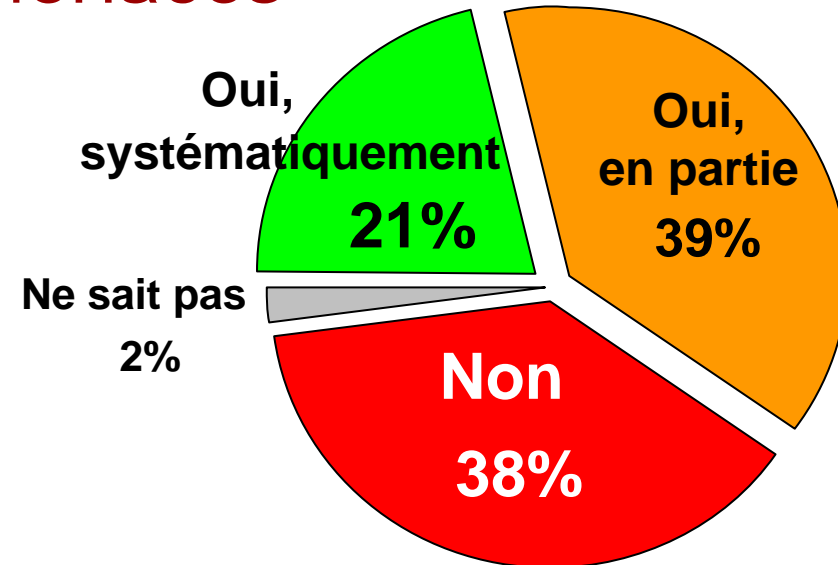


Technologies de contrôle d'accès : des usages qui restent marginaux...



Les entreprises n'ont pas amélioré leur vigilance vis-à-vis des menaces

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

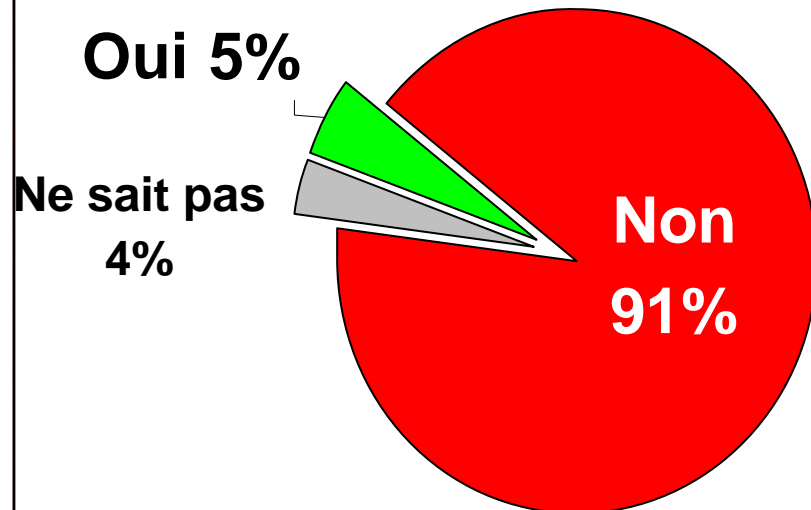


➡ Avez-vous formalisé des procédures de déploiement de correctifs de sécurité (*patch management*) ?

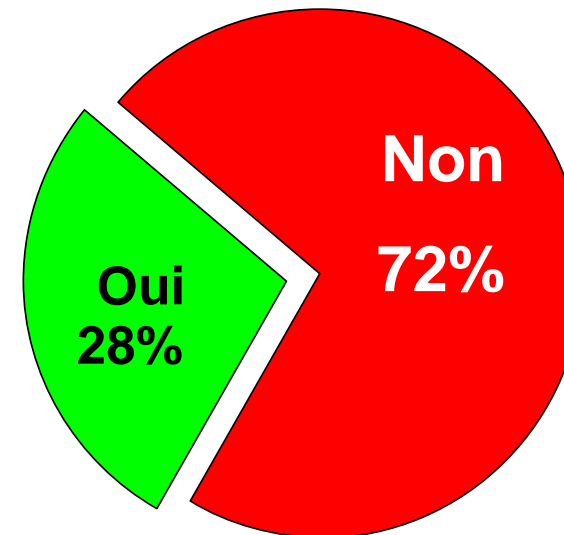
Un suivi et une évaluation de l'impact des incidents encore peu répandus

55 % des entreprises déclarent avoir subi au moins un incident de sécurité sur leur SI

☞ En 2007, votre entreprise a-t-elle déposé des plaintes suite à des incidents liés à la sécurité de l'information ?

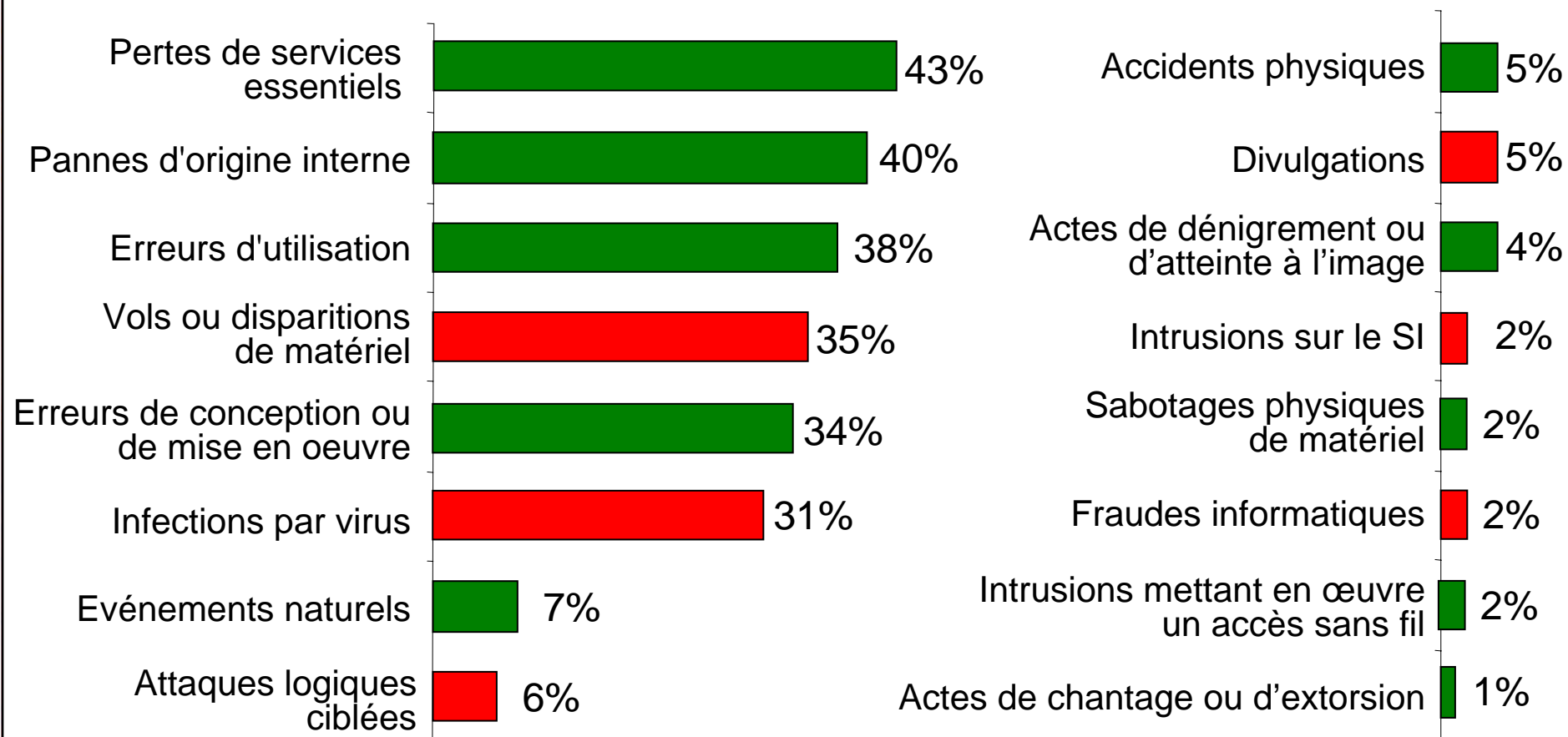


☞ Procédez-vous à une évaluation de l'impact financier des incidents de sécurité SI ?



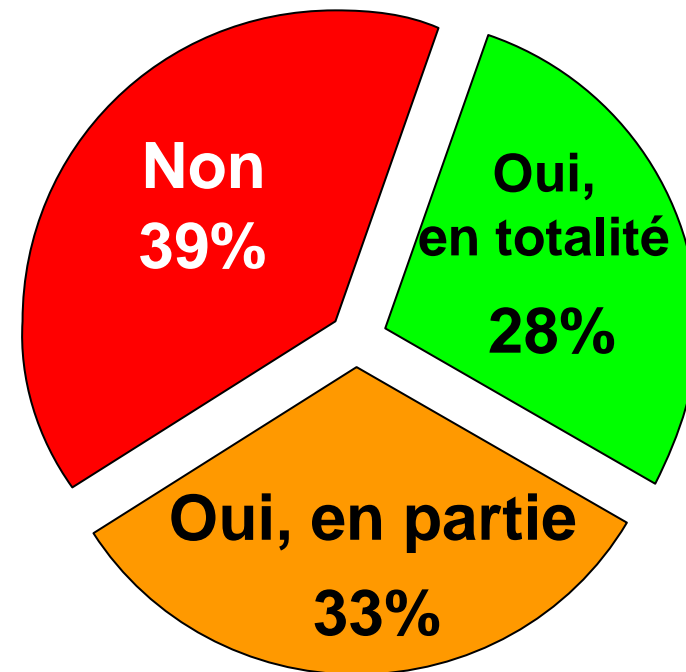
Une malveillance confirmée

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



39 % 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 ?



72 % des entreprises qui disposent d'un Plan de Continuité d'Activité le testent et le mettent à jour au moins une fois par an

Une mise en conformité à la Loi Informatique & Liberté qui ne progresse pas

Conformité des entreprises à la CNIL

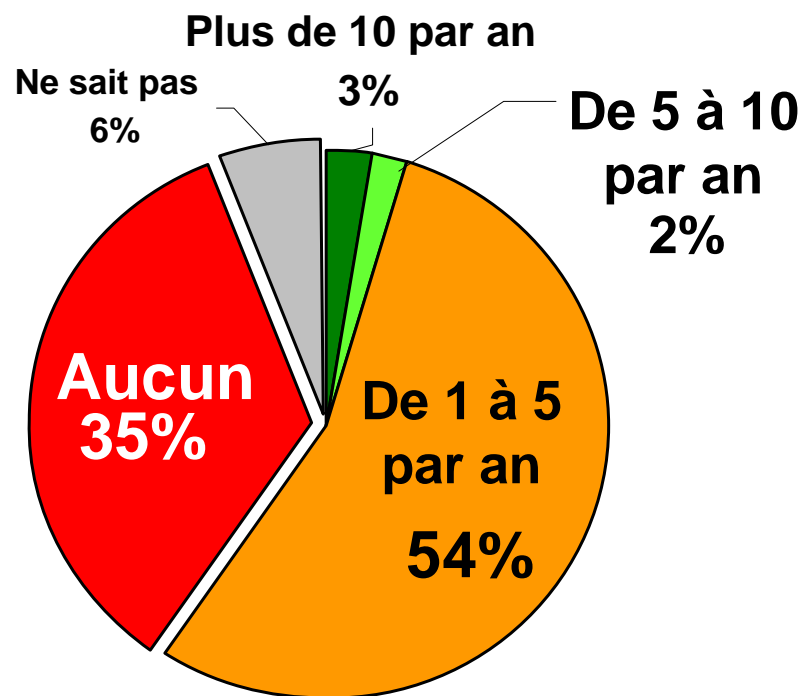
- 64% déclarent être totalement conforme
- 19% déclarent être conforme pour les traitements les plus sensibles

Correspondant Informatique et Liberté (CIL)

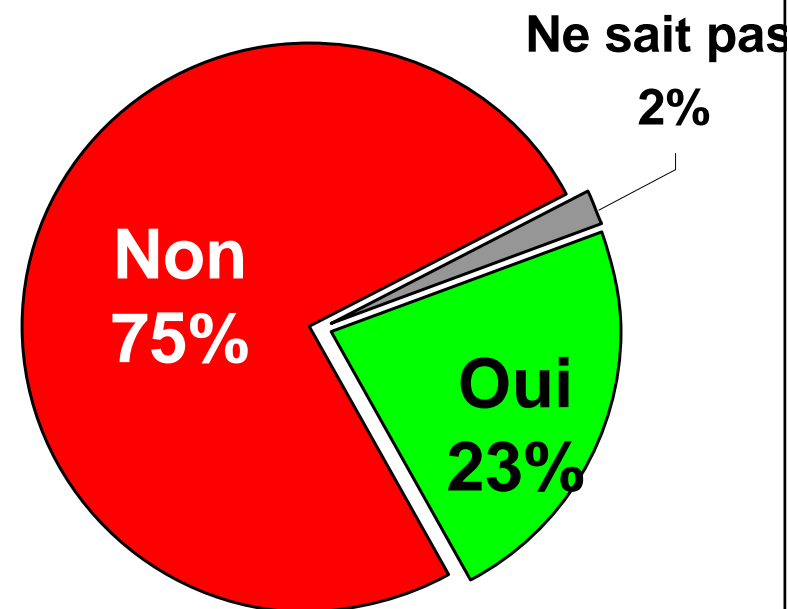
- 25% des entreprises ont un CIL et 5% prévoient d'en nommer un

Un « dispositif de contrôle » 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 ?



Conclusion : un inquiétant sentiment de stagnation...

- 2004 à 2006 : Des progrès sur la formalisation des politiques de sécurité
- 2006 à 2007 : Ces politiques ne se traduisent pas par des actions concrètes d'amélioration de la sécurité

Une recommandation : se concentrer en priorité sur les risques majeurs, mais les traiter jusqu'au bout