



Menaces Informatiques et Pratiques de Sécurité en France

19 juin 2008

Les Collectivités locales



Evénement organisé en partenariat avec :

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



Enquête 2008



Les collectivités locales

M. Lionel MOURER

Responsable du Pôle Conseil & Audit

BULL Services & Solutions

Direction Réseau & Sécurité

19 juin 2008

Les collectivités – présentation de l'échantillon

194 collectivités interrogées

- 79 mairies de plus 30 000 habitants
- 27 communautés de communes
- 42 communautés d'agglomération
- 41 conseils généraux
- 5 conseils régionaux

Échantillon redressé sur la base de données nationales

Les collectivités – présentation de l'échantillon

Interlocuteur

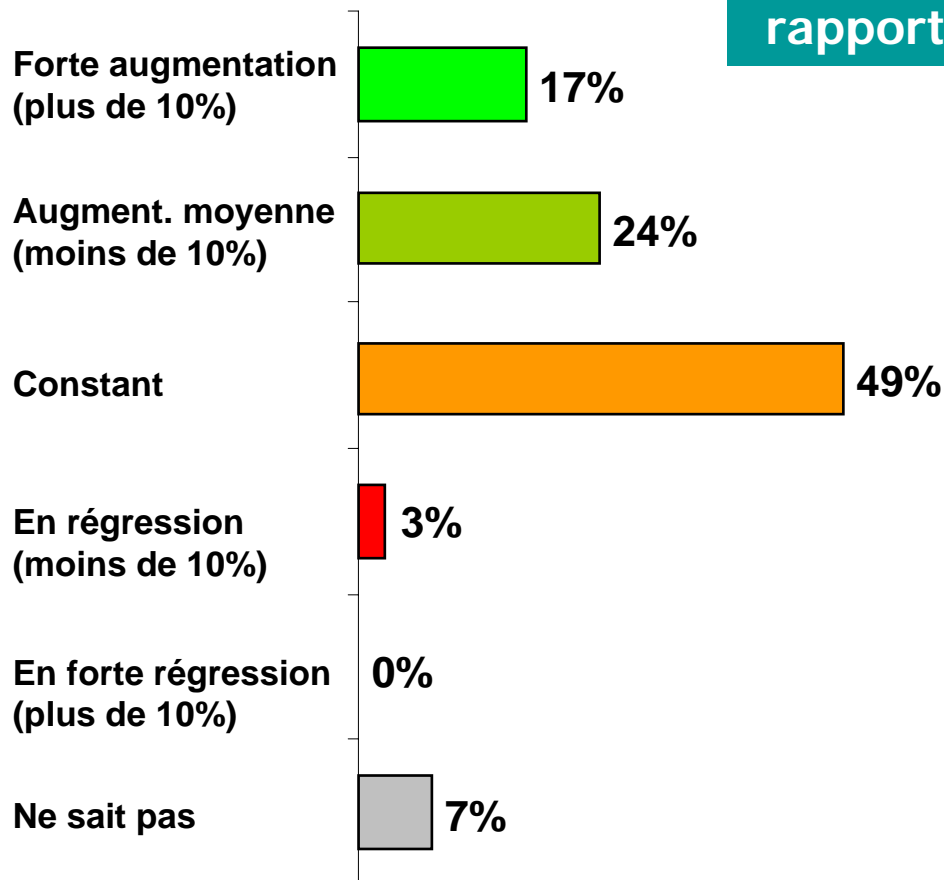
- Le RSSI dans 3% des cas
- Le FSSI dans 1% des cas
- Le Resp. Informatique, DSI, Resp. Réseau, Technicien ou Resp. Infrastructure dans 85% des cas !

Dépendance ressentie à l'informatique

- Forte : 68% des cas
- Modérée : 31% des cas
- Faible : 1% des cas

Des budgets sécurité qui augmentent « plus vite » que dans les entreprises...

Évolution du budget sécurité par rapport à l'année précédente ?



Freins principaux

- 62% : manque de moyens (budget ou personnel qualifié)
- 38% : réticence de la hiérarchie

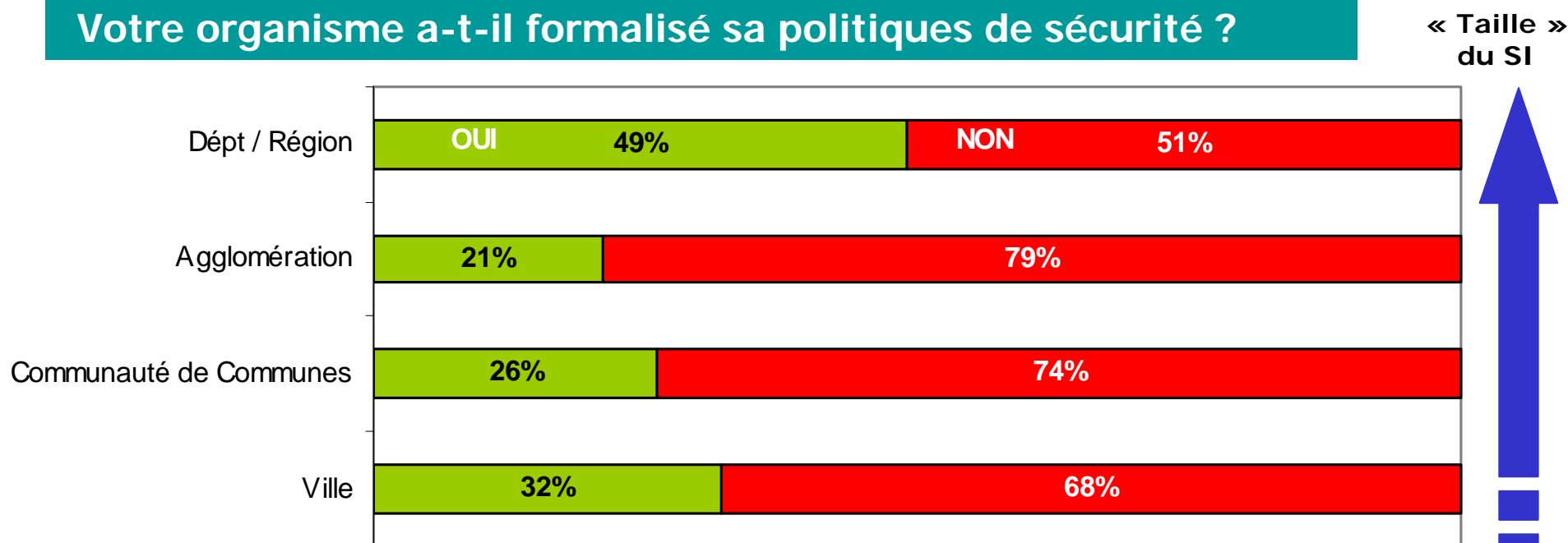
PSI portée par la DG (92%)

- 70% en totalité
- 22% : en partie



Formalisation des politiques de sécurité : encore du chemin à parcourir...

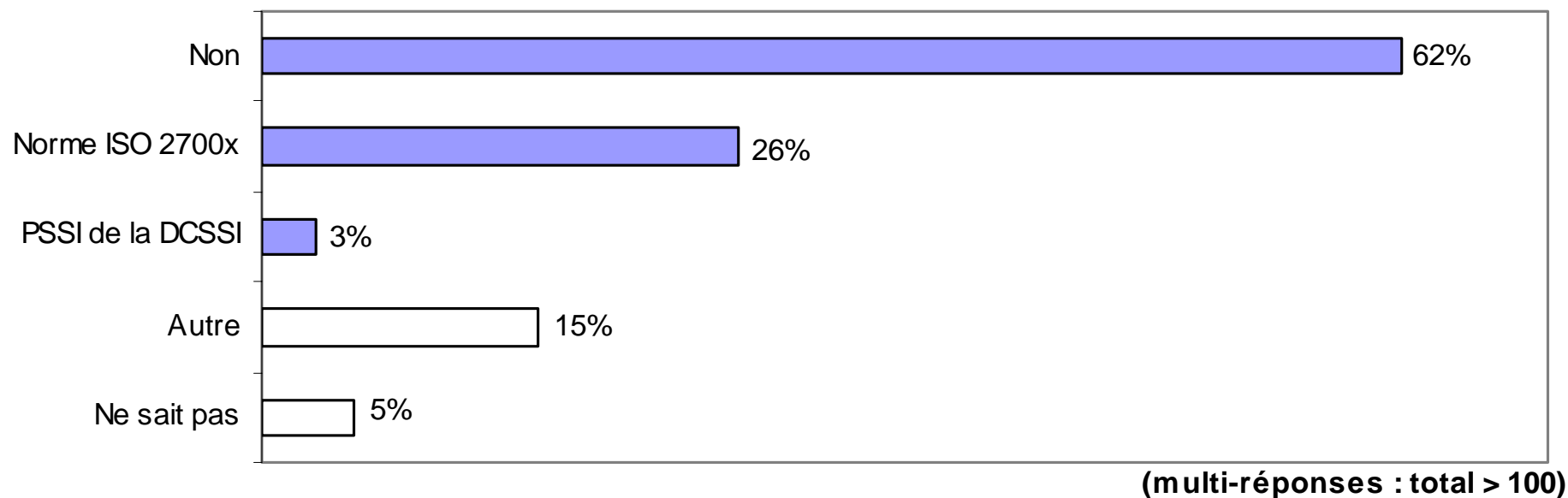
Votre organisme a-t-il formalisé sa politiques de sécurité ?



Issues très majoritairement du travail des
informaticiens (95%)

Utilisation des « normes de sécurité » : l'ISO 2700x majoritaire

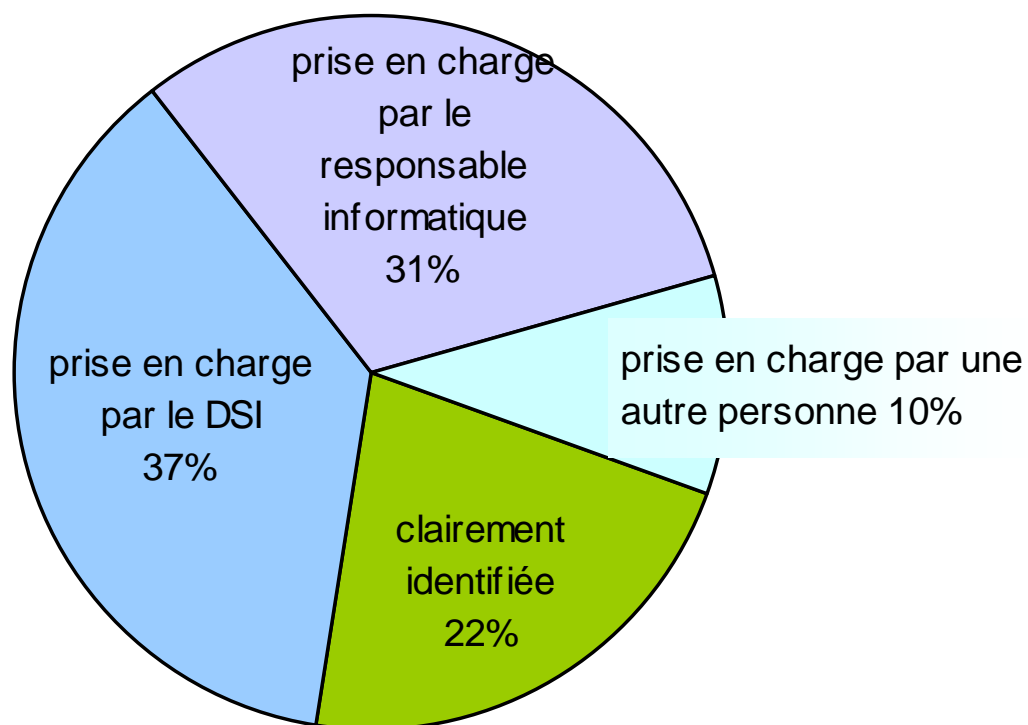
La PSI de votre organisme s'appuie-t-elle sur une « norme de sécurité » ?



Quels sont les « autres » cadres méthodologiques de PSI ?

RSSI (ou FSSI) : encore peu identifié et souvent rattaché à la DSI

La fonction RSSI est...

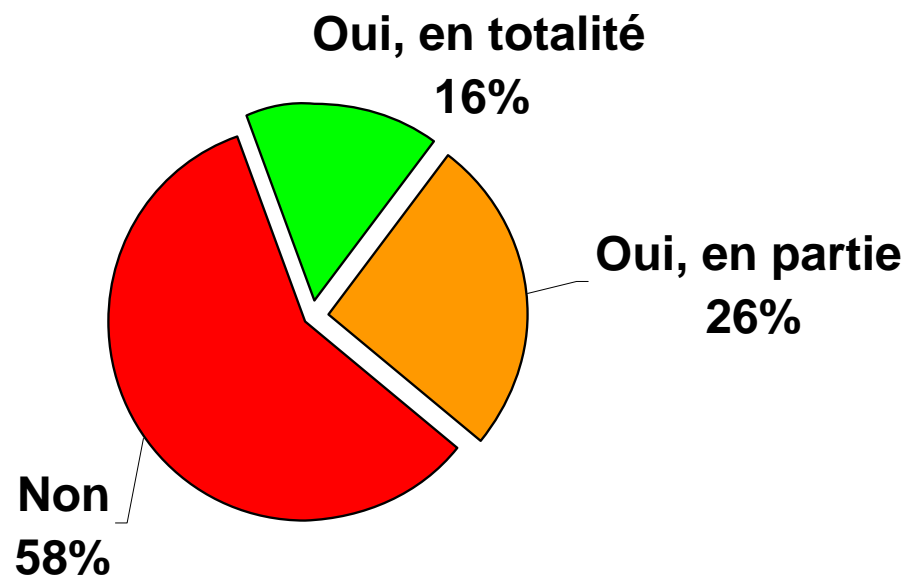


RSSI rattaché dans

- 61% des cas à la DSI
- 15% des cas à la Direction Générale des Services
- 8% des cas à l'élu de plus haut niveau (ou son cabinet)

Gestion des risques : peu d'analyses formelles

Avez-vous réalisé une analyse globale des risques liés à la SSI ?

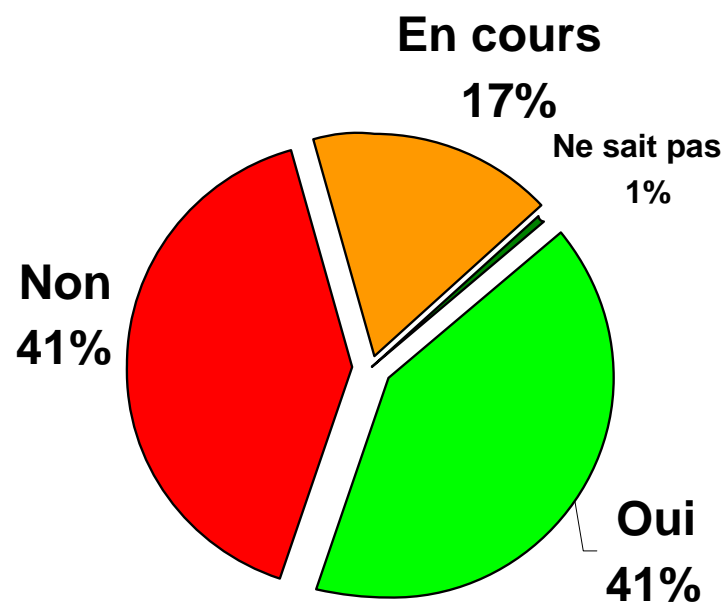


Prise en compte des « risques » dans les projets structurants

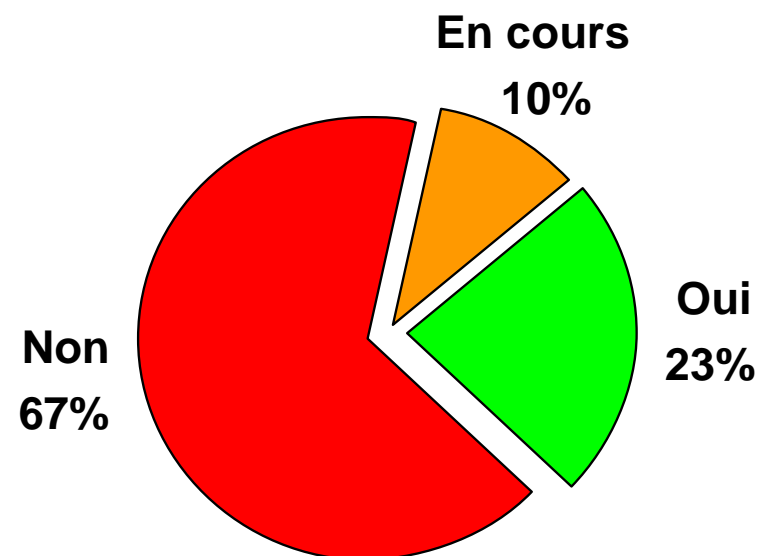
- 36% : oui, systématiquement
- 39% : oui, parfois
- 24% : non

Charte et sensibilisation

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



Existe-t-il un programme de sensibilisation ?



Mobilité et innovation : l'interdit reste la règle !...

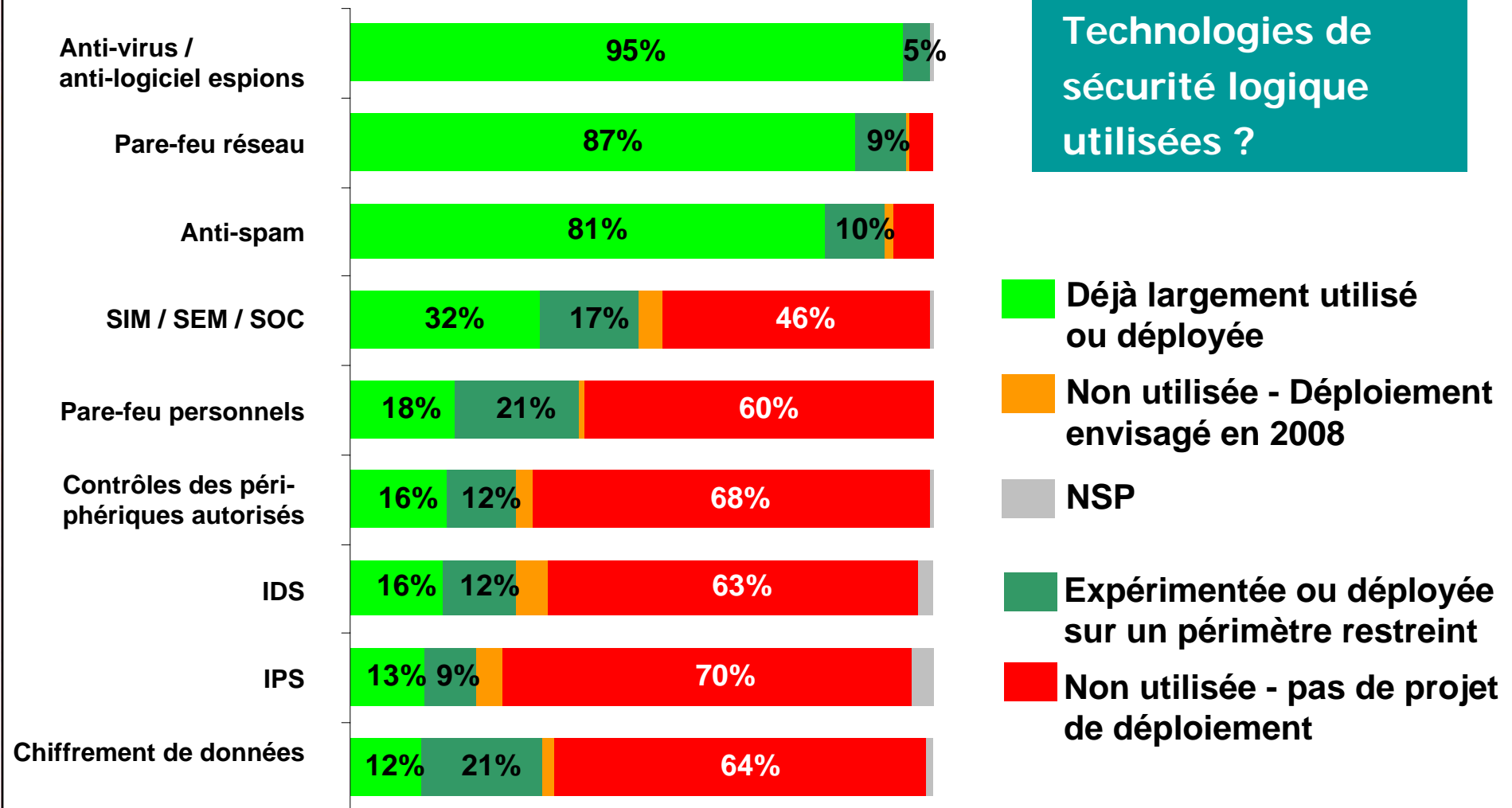
Interdiction de l'accès en Mobilité

- depuis les PC portables contrôlés : 42%
(13% en entreprises)
- depuis les PC portables non contrôlés : 76%

Interdiction des technologies innovantes

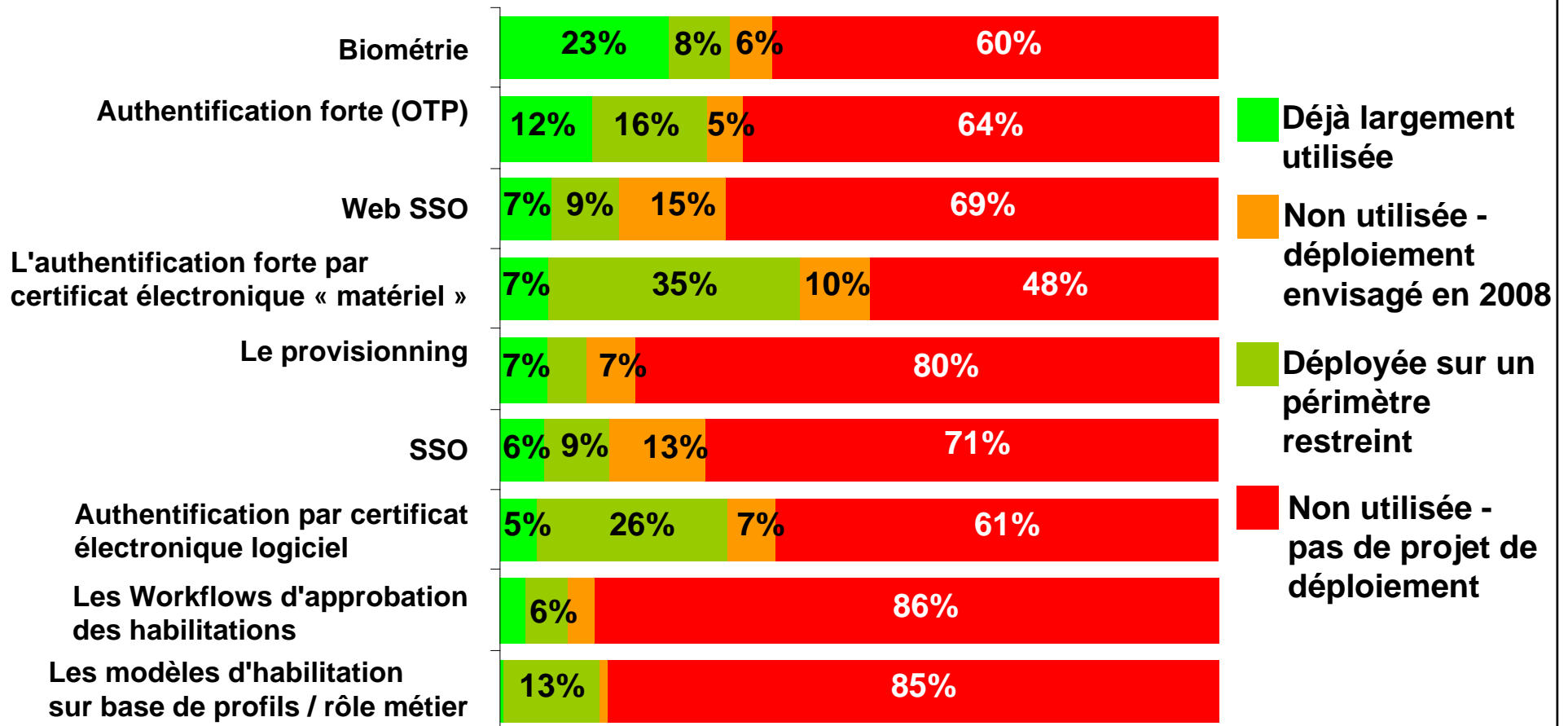
- PDA & smartphone : 61%
- Wifi (interne) : 51%
- ToIP / VoIP : 55% (67% en entreprises)

Sécurité logique : montée de l'anti-spam...



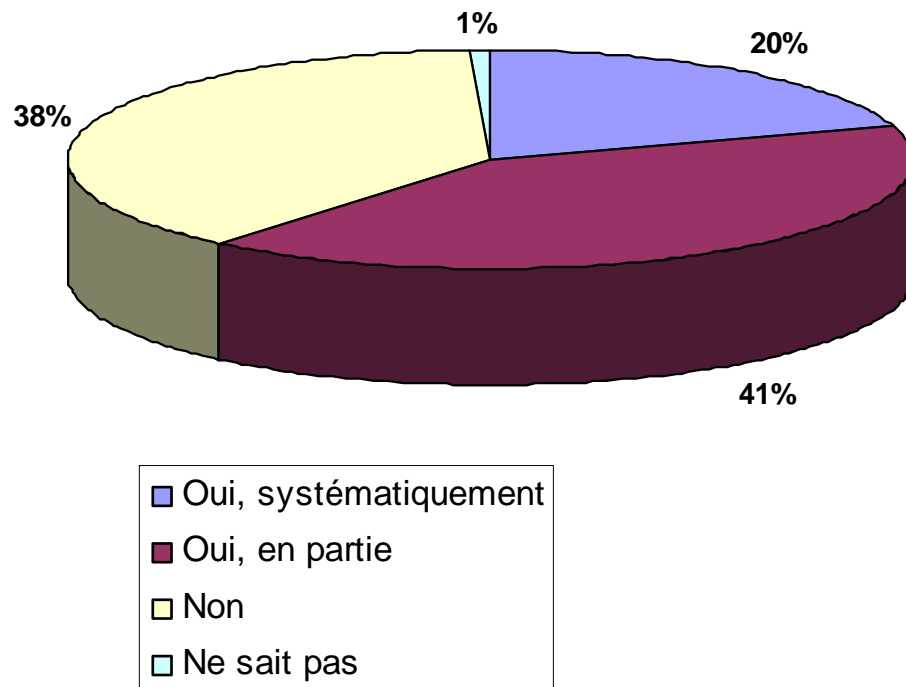
Contrôle des accès : satisfecit (très mesuré...) à la biométrie et à l'OTP

Technologies de contrôle d'accès utilisées ?



Veille et correctifs de sécurité

Veille permanente en vulnérabilités ?

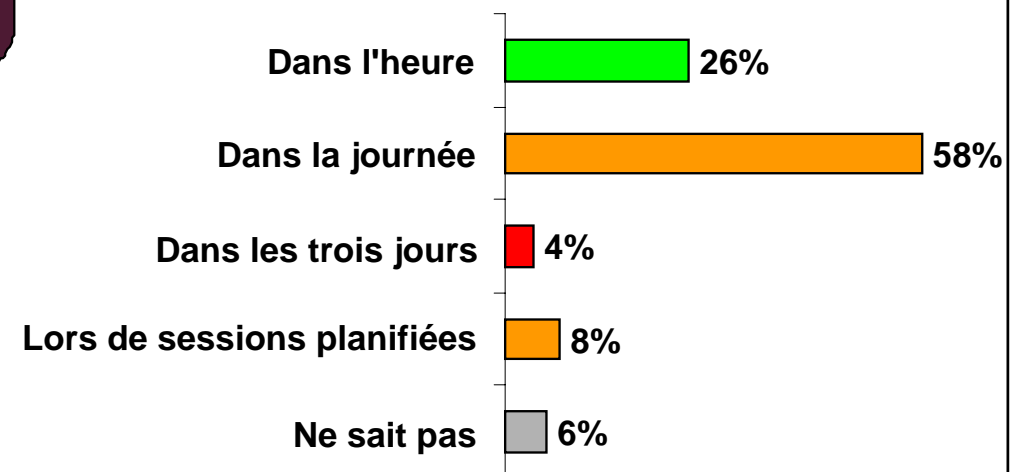


Procédures de déploiement des correctifs existantes

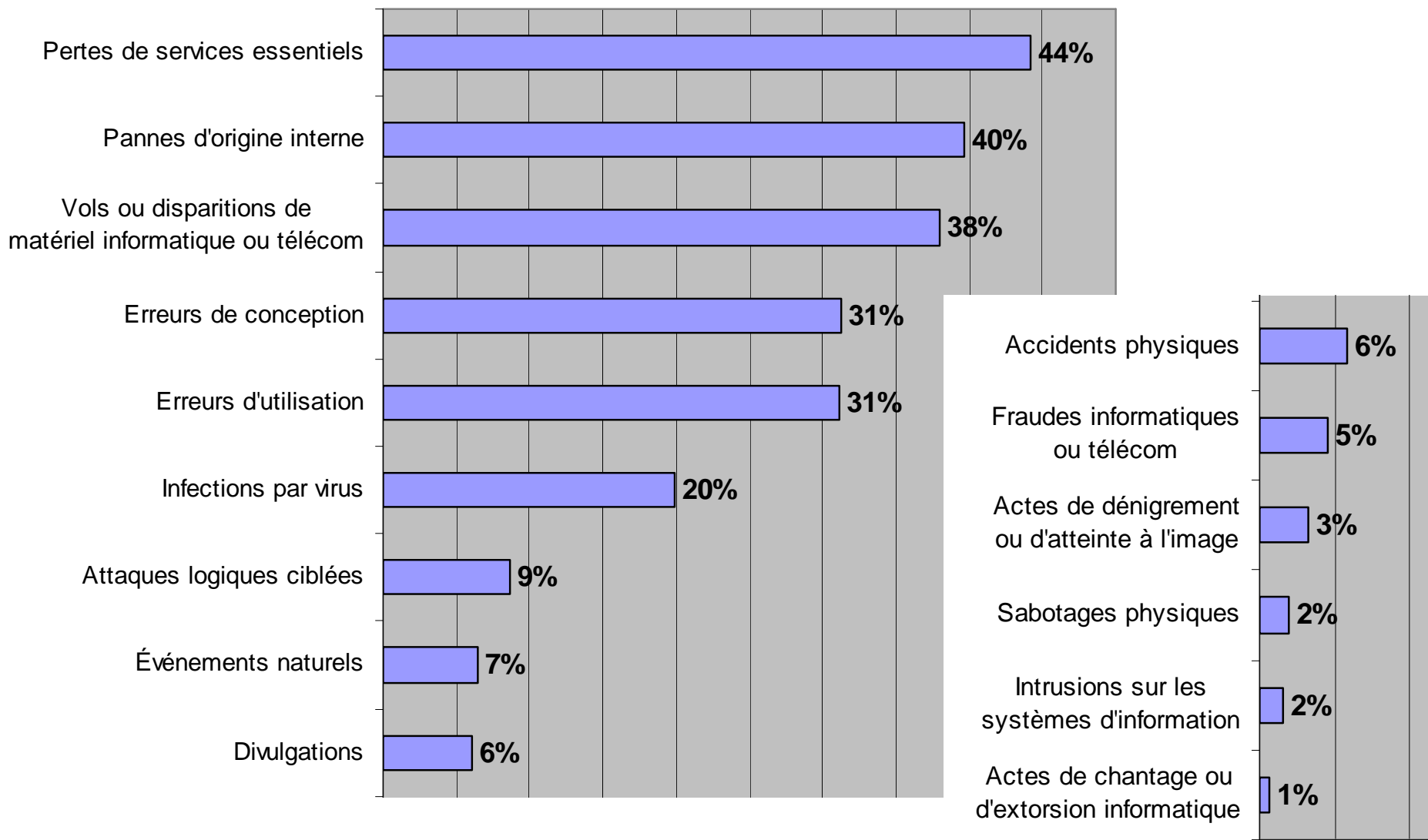
- Oui : 52%
- Non : 48%

Délai est nécessaire pour déployer les correctifs ?

(base : « si oui »)

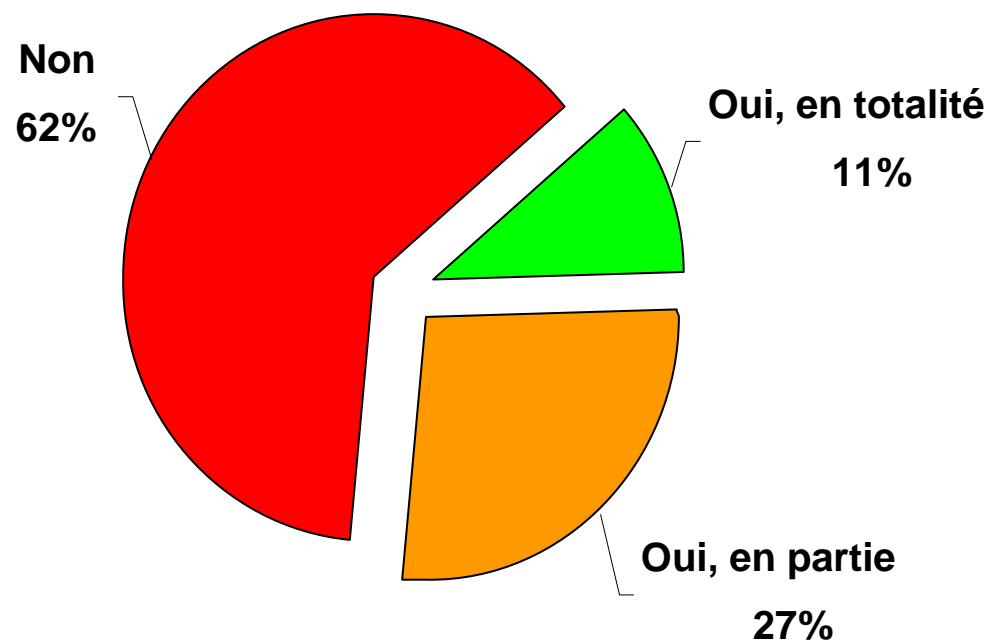


Incidents de sécurité



Continuité d'activité : encore des efforts à faire...

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



Testé

- 11% : plus d'une fois par an
- 34% : une fois par an

Conformité (CNIL, audit et tableaux de bord) : des axes de progression importants...

Conformité avec les obligations de la CNIL ?



Combien d'audits de sécurité ?

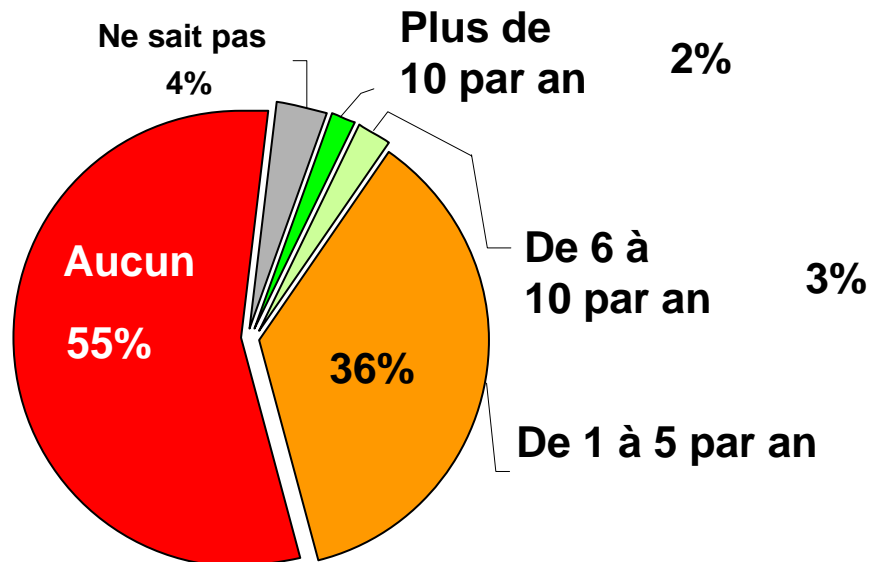
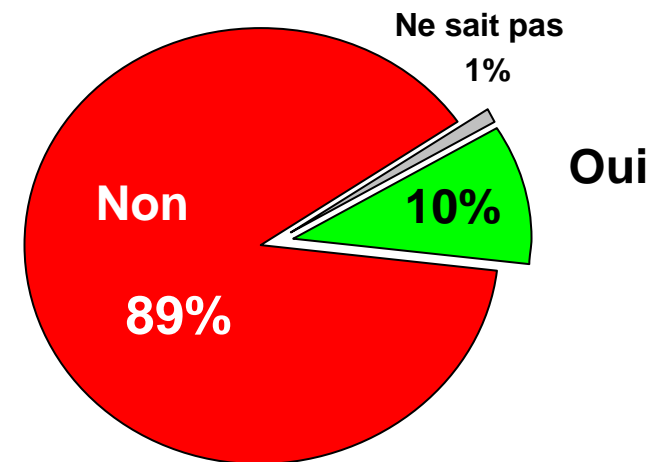


Tableau de bord de la sécurité informatique ?



Conclusion

Pas de grandes distorsions par rapport aux entreprises

- avec globalement une sécurité inférieure...

Les grands « chantiers » restants à travailler

- la sensibilisation
- l'organisation (PSI, RSSI, etc.)
- la continuité
- la conformité