Introduction à la sécurité des échanges

Dr. Y. Challal

« Ce ne sont pas les murs qui protègent la citadelle, mais l'esprit de ses habitants »

Thucydite

Confiance et Internet

Dans la vie courante la plupart des transactions reposent sur une « confiance » acquise par une relation en face à face ou un contact physique

Dans le cybermonde cette relation de proximité est rompue

Comment établir une relation de confiance indispensable à la réalisation de transactions à distance entre personnes qui ne se connaissent pas ?

Environnement de l'entreprise

- **Avant:**
  - Centralisé
  - Échange papiers
  - Pas d'accès distant.
- **Aujourd'hui**
  - Distribué sur plusieurs sites: siège, filiales, télé-travailleurs, commerciaux, …
  - Accès distants,
  - Mondialisation des échanges.
  - Haut débit sur GSM, UMTS, …
- **Demain**
  - 3.000.000.000 de personnes Internautes

Risques liés aux réseaux

- **Interception de messages**
  - Prise de connaissance des mots de passe
  - Vol d'information
  - Perte d'intégrité du système et du réseau
- **Intrusion des systèmes**
  - Vol ou compromission des informations
  - Destruction des informations
  - Virus
  - Détournement de biens
- **Perte d'accessibilité au système ou au réseau**
- **Faux clients, marchands escrocs**

Motivations d'un attaquant

- **Le gain financier**
  - Récupération de num de cartes bancaires, …
- **Vengeance**
  - Site www.aljazeera.net lors de la couverture de la guerre d'irak
- **Besoin de reconnaissance**
  - Attaque contre le site du cerist avec un message sur les restrictions d'accès à Internet à Cuba.
- **Curiosité**
  - Attaques d'étudiants du MIT sur le premier ordinateur IBM 704 au MIT en 1959.
- **Recherche d'émotions fortes**
- **Ignorance**
  - Envoie de mots de passes par email, …

Pertes phénoménales !!!

- **74% des pertes financières sont dûent aux :**
  - attaques de virus (plus de 15 millions de dollars de perte)
  - accès non autorisés aux systèmes d'information (plus de 10 millions de dollars de perte)
  - vols d'équipement mobile (plus de 6 millions de dollars)
  - vols de la propriété intellectuelle (plus de 6 millions de dollars)

- **52% des organisations sondées ont déclaré avoir été attaqué les 12 derniers mois (2006) :**
  - 24% d'entre elles ont reporté plus de 6 attaques
  - 48% ont reporté 1 à 5 attaques

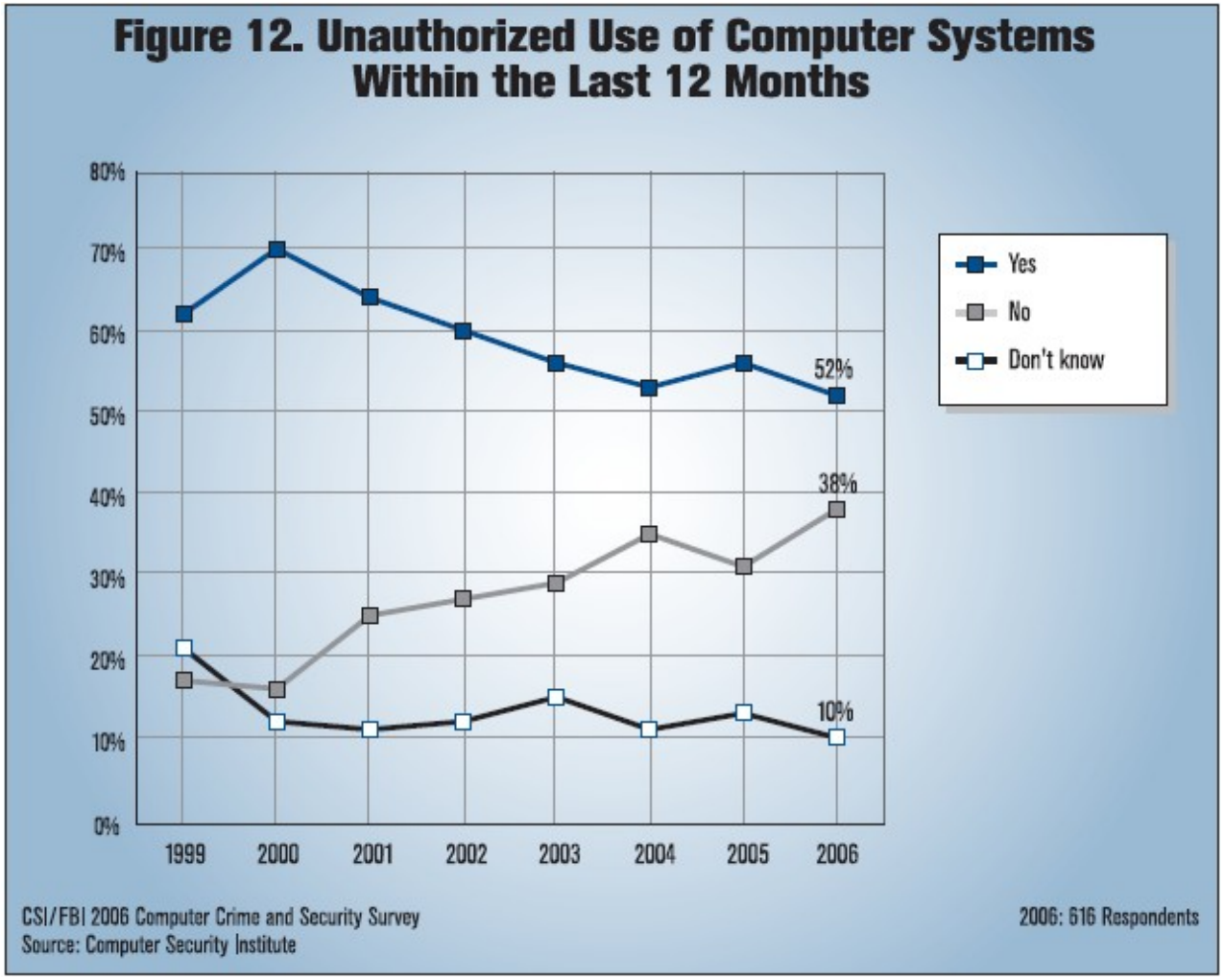
Conséquences !

- **34% des organisations allouent pas moins de 5% du budget informatique à la sécurité informatique**
  - En 2006, les compagnies de revenues inférieurs à 10 millions de dollars ont dépensé en moyenne 1349 dollars par employé pour la sécurité informatique-
  - un rehaussement de 210% par rapport à l'année 2005

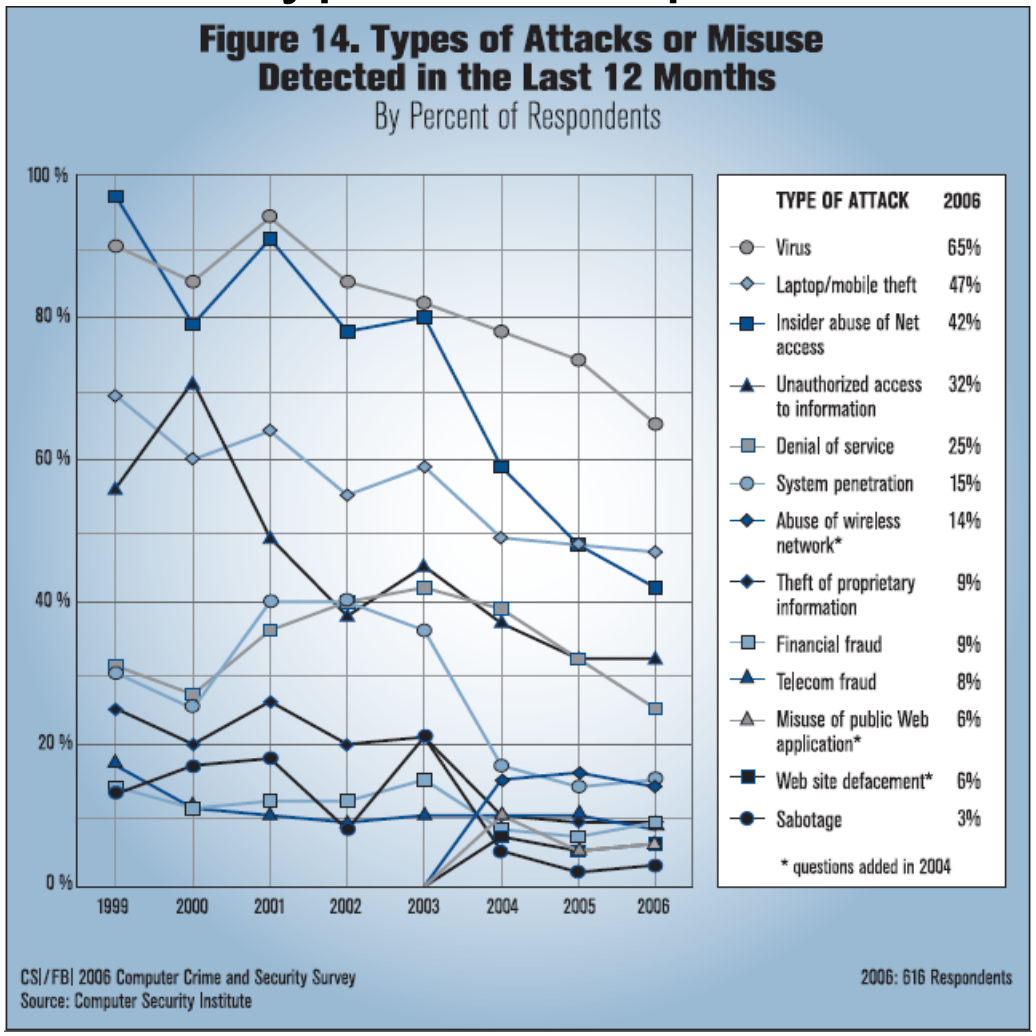
- **plus de 80% des institutions conduisent un audit de sécurité informatique**

- **la majorité des institutions jugent la formation en sécurité informatique comme importante et stratégique**
  - 61% de ces organisations refusent de sous-traiter leurs fonctions de sécurité informatique

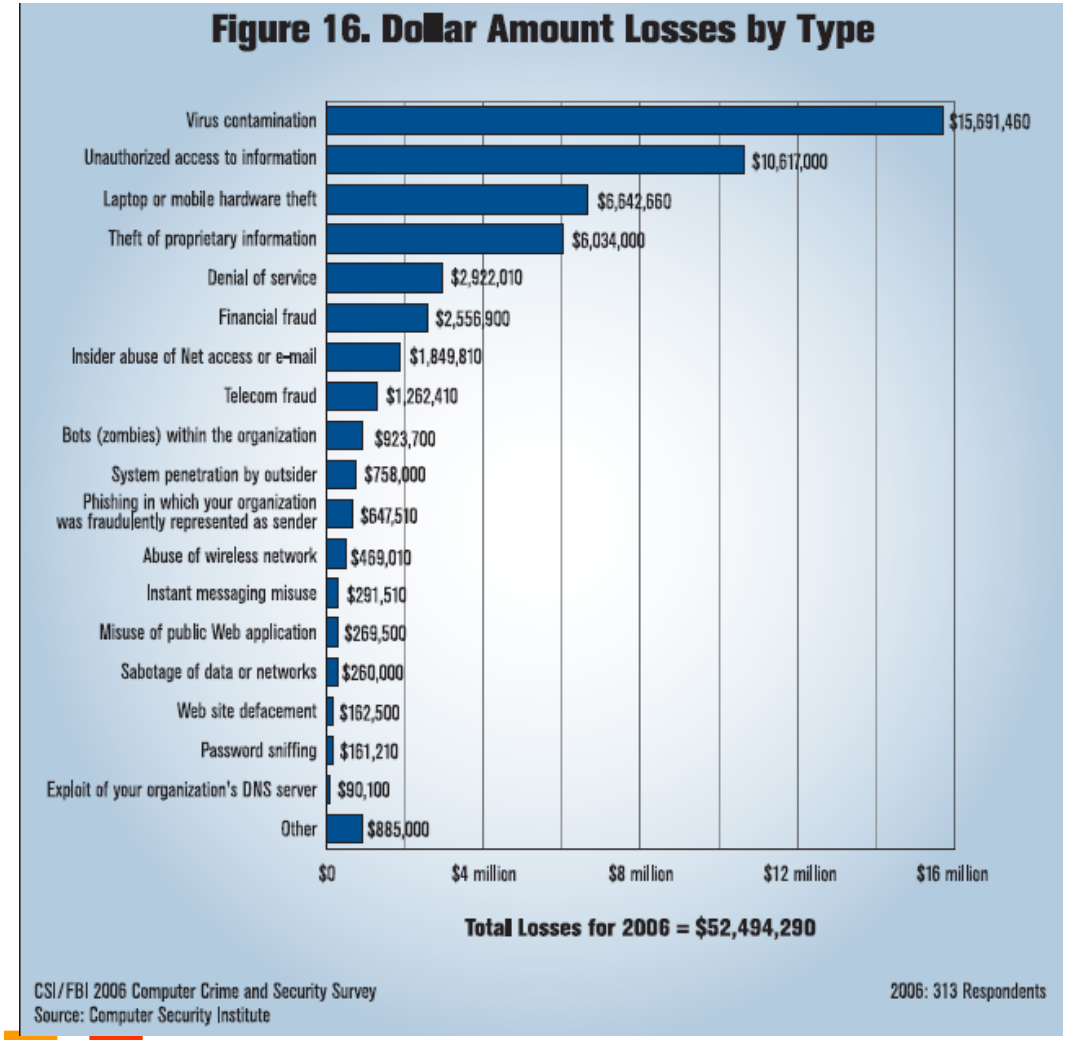
Accès frauduleux aux SI



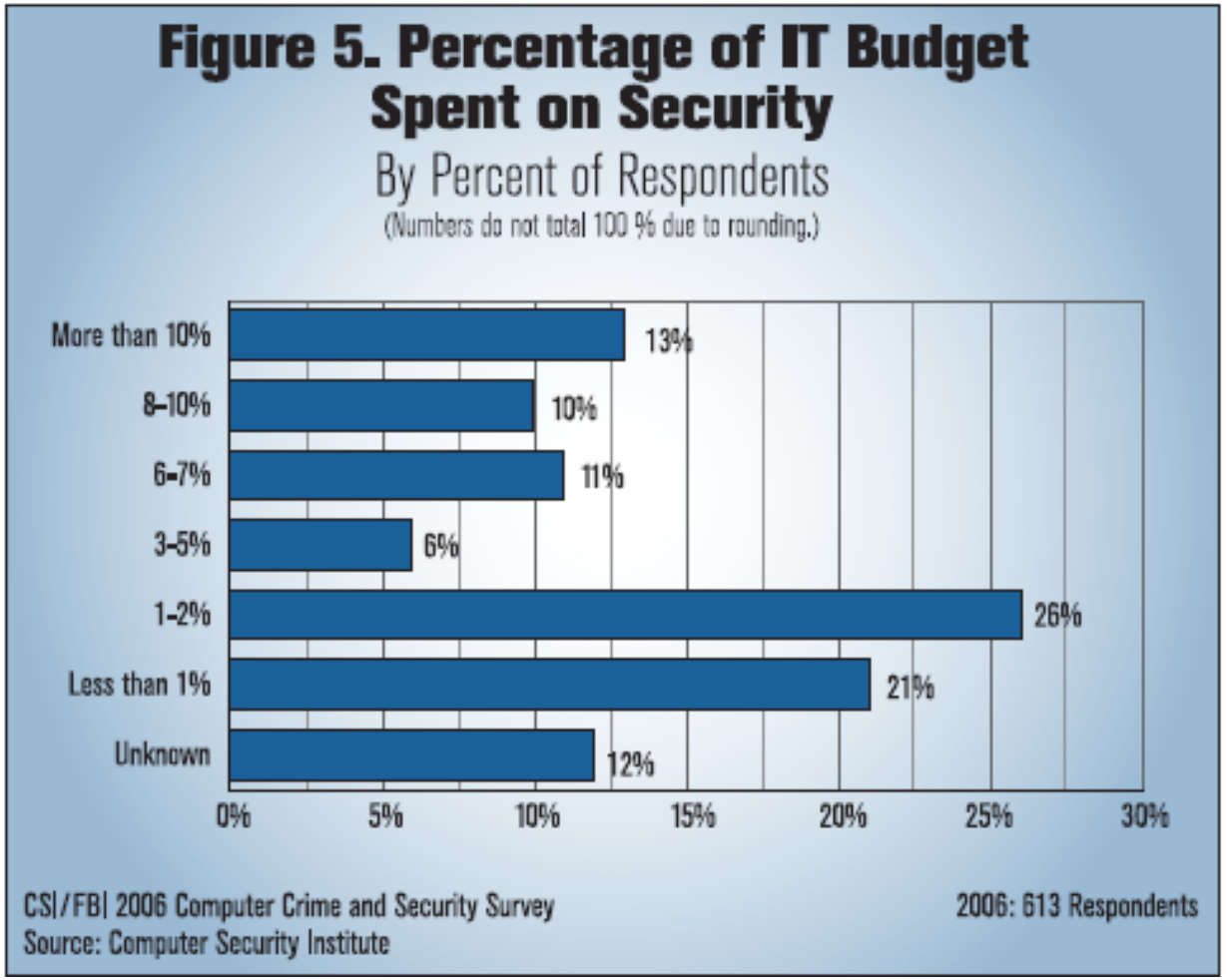
Types d'attaques



Enjeux: pertes financières



Pourcentage de dépenses sur la sécurité

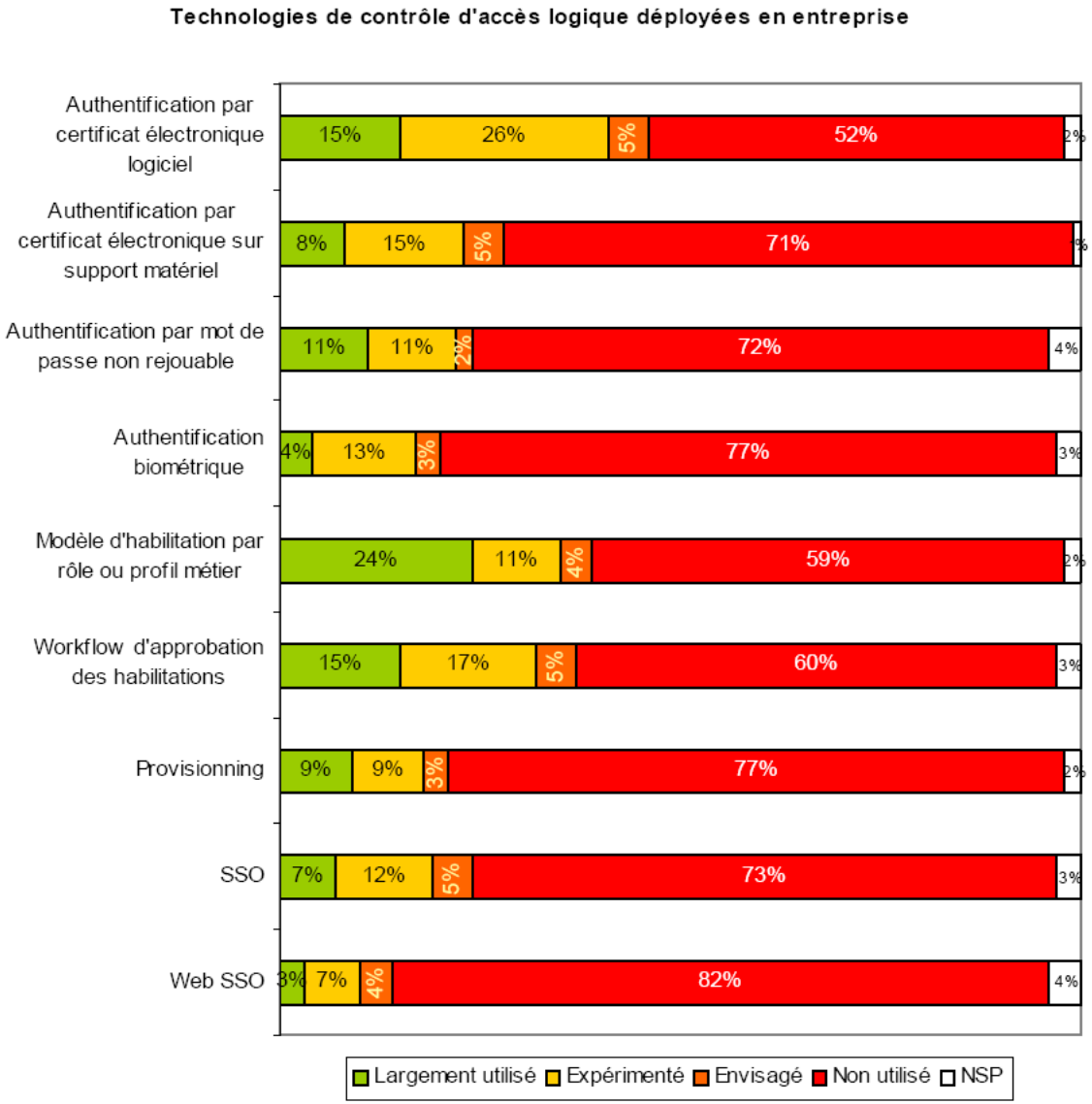


Menaces Informatiques et Pratiques de Sécurité en France

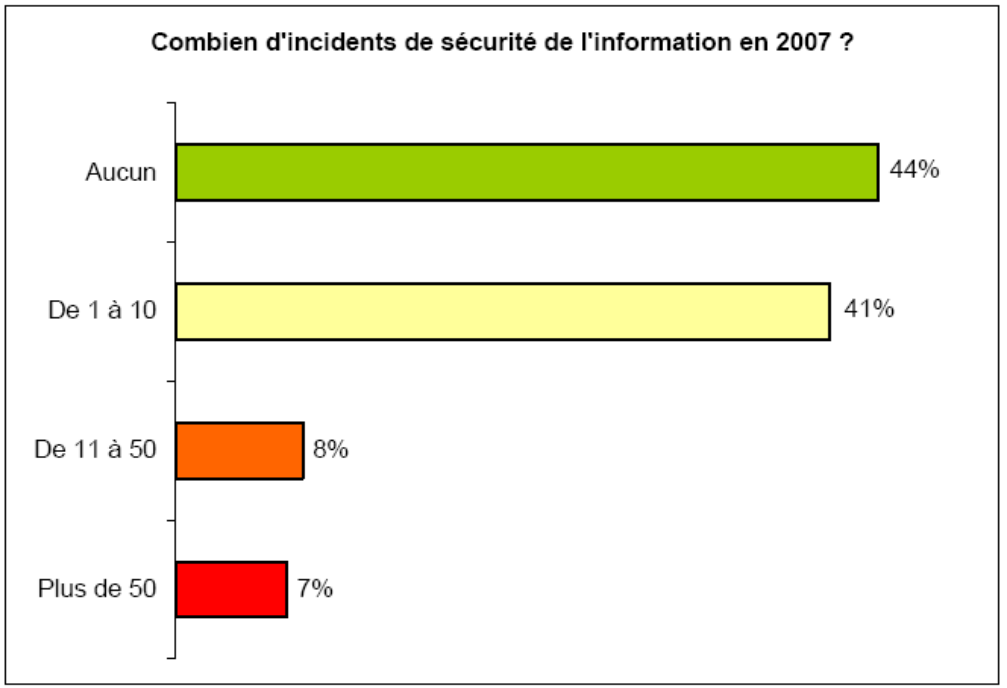
Rapport 2008 du CLUSIF (Club de la Sécurité de l'Information Français)

- Plus de 70% des entreprises françaises ont une forte dépendance à l'informatique
- Le budget moyen alloué pour la sécurité du SI dépasse 114K€ dans 21% des cas.
- 28% des entreprises du secteur des services, banques et assurances ont augmenté leur budget sécurité du SI de plus de 10% en 2008
- 53% des Responsables de Sécurité du SI (RSSI) dénoncent le manque de personnel qualifié comme frein majeur à la conduite de leur mission.
- Plus de 30% des entreprises n'ont pas une Politique de Sécurité de l'Information (PSI), et 45% de celles qui en ont ne respectent pas une norme de sécurité.
- Le rattachement de la RSSI à la DG passe de 39% en 2006 à 45% des cas en 2008.

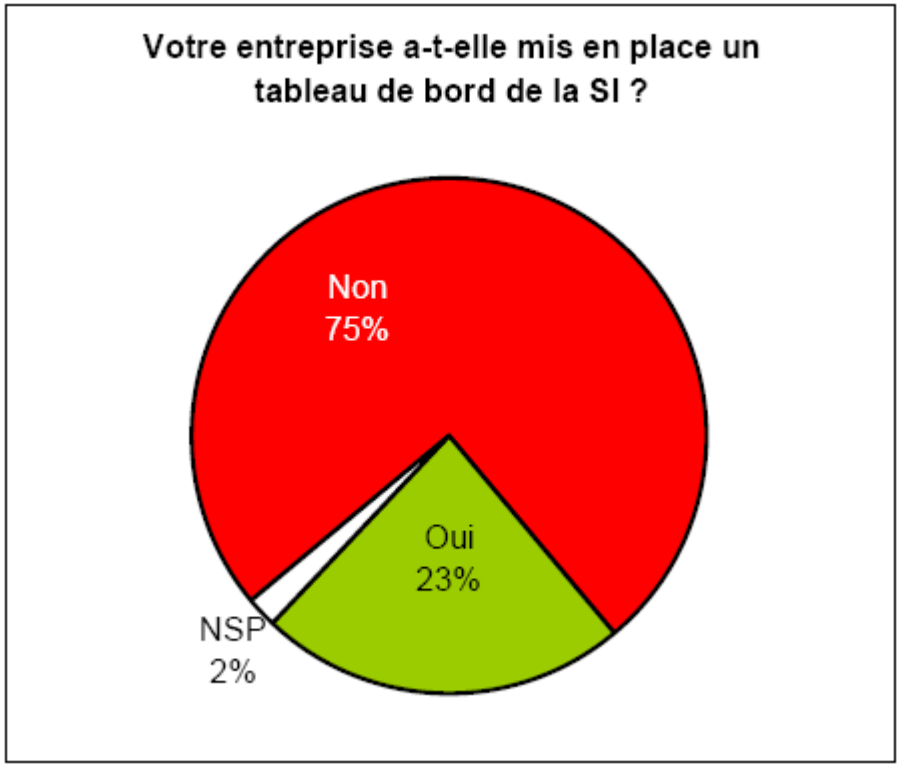
Suite Rapport CLUSIF 2008: Technologies de contrôle d'accès méconnues et/ou non utilisées en entreprises françaises



Suite Rapport CLUSIF 2008:
56% des RSSI constatent au moins
Un incident de sécurité



Suite Rapport CLUSIF 2008:
Plus de 75% des entreprises
Ne mesurent pas leur niveau
De sécurité régulièrement



– Conclusion de l'enquête :

- Le manque de personnel qualifié freine la mission des RSSI dans les entreprises
- Mise à niveau nécessaire des SI des entreprises du point de vue de la sécurité
- Constante évolution du rôle, de l'importance et des budget alloués à la RSSI dans l'entreprise
- **Un marché national très demandeur de formation en sécurité informatique**

Services de sécurité

- **Authentification**
  - Permet de vérifier l'identité revendiquée par une entité, ou l'origine d'un message, ou d'une donnée
  - Le terme authentification recouvre plusieurs interprétations
- **Confidentialité**
  - Permet de se protéger contre la consultation abusive des données par des entités tierces indésirables
- **Contrôle d'intégrité**
  - Permet de vérifier qu'une données n'a pas été modifiée par une entité tierce (accidentellement ou intentionnellement)
- **Contrôle d'accès**
  - Permet de vérifier que toute entité n'accède qu'aux services et informations pour lesquelles elle est autorisée

Services de sécurité

- **Non répudiation**
  - Permet de se protéger contre la contestation d'envoi et de réception de données lors d'une communication