

# « DLP » (Data Loss Prevention) - le défi -

20 octobre 2010

Sébastien RAILLARD  
(COEXSI)

## Définition

**Détecter et empêcher  
l'utilisation et la transmission  
non autorisées d'informations  
« confidentielles »**

- **Eviter de faire sortir ce qui ne devrait pas sortir**
- **Vérifier l'usage interne de l'information**

⇒ **C'est le but recherché dans l'intégration d'outils « DLP »**

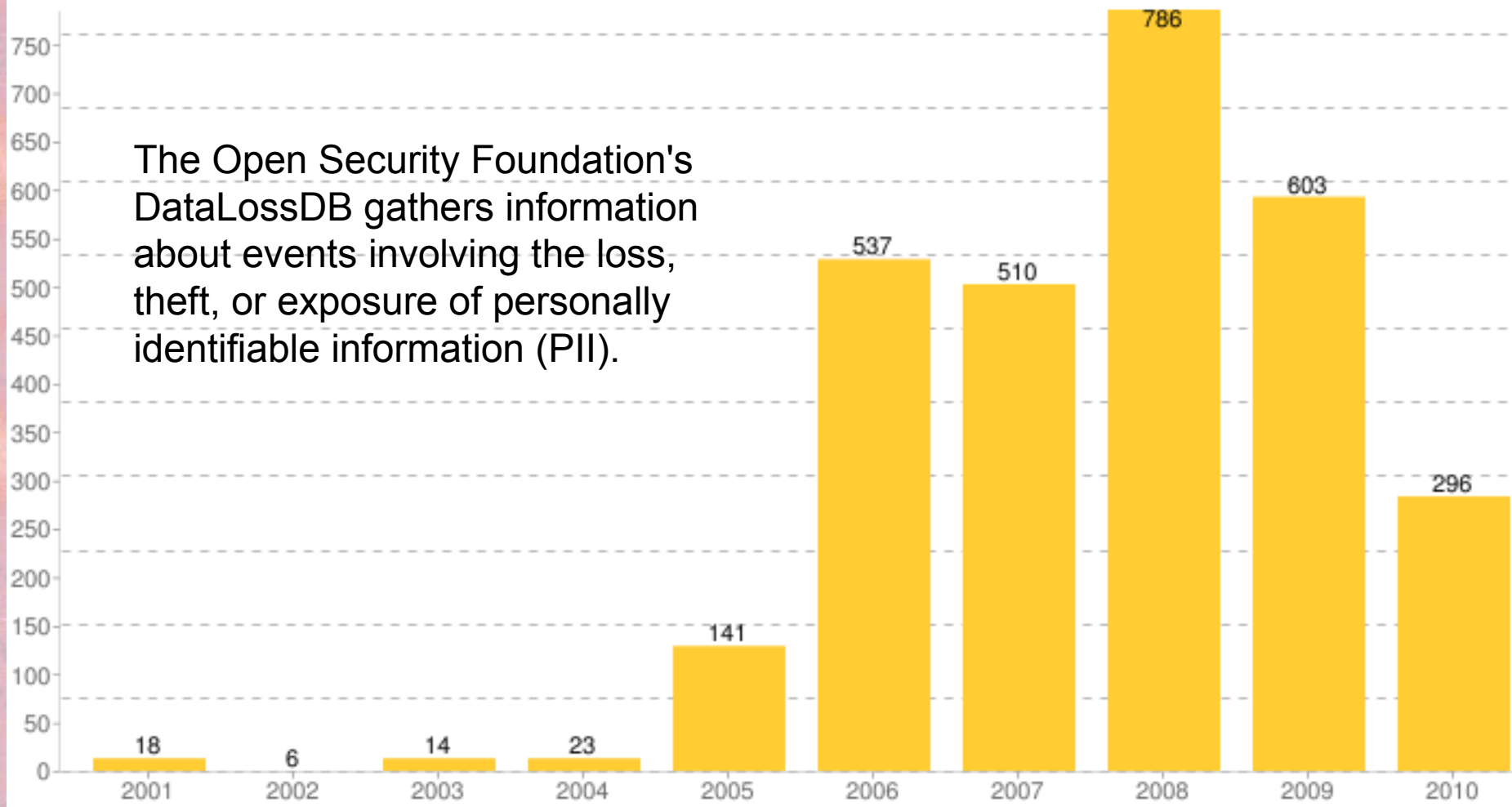


# Aller au-delà de la protection technique des infrastructures

- **Filtrage des flux : Firewall/IDS/IPS**
  - **Filtrage du contenu : Anti-virus, Anti-spyware, Anti-spam**
  - **Gestion des accès : Network Access Control (NAC), VPN**
  - **Politique de configuration et de protection des ordinateurs : GPO Microsoft, chiffrement**
- ⇒ **Permet le contrôle de l'accès aux ressources et leur « propreté »**

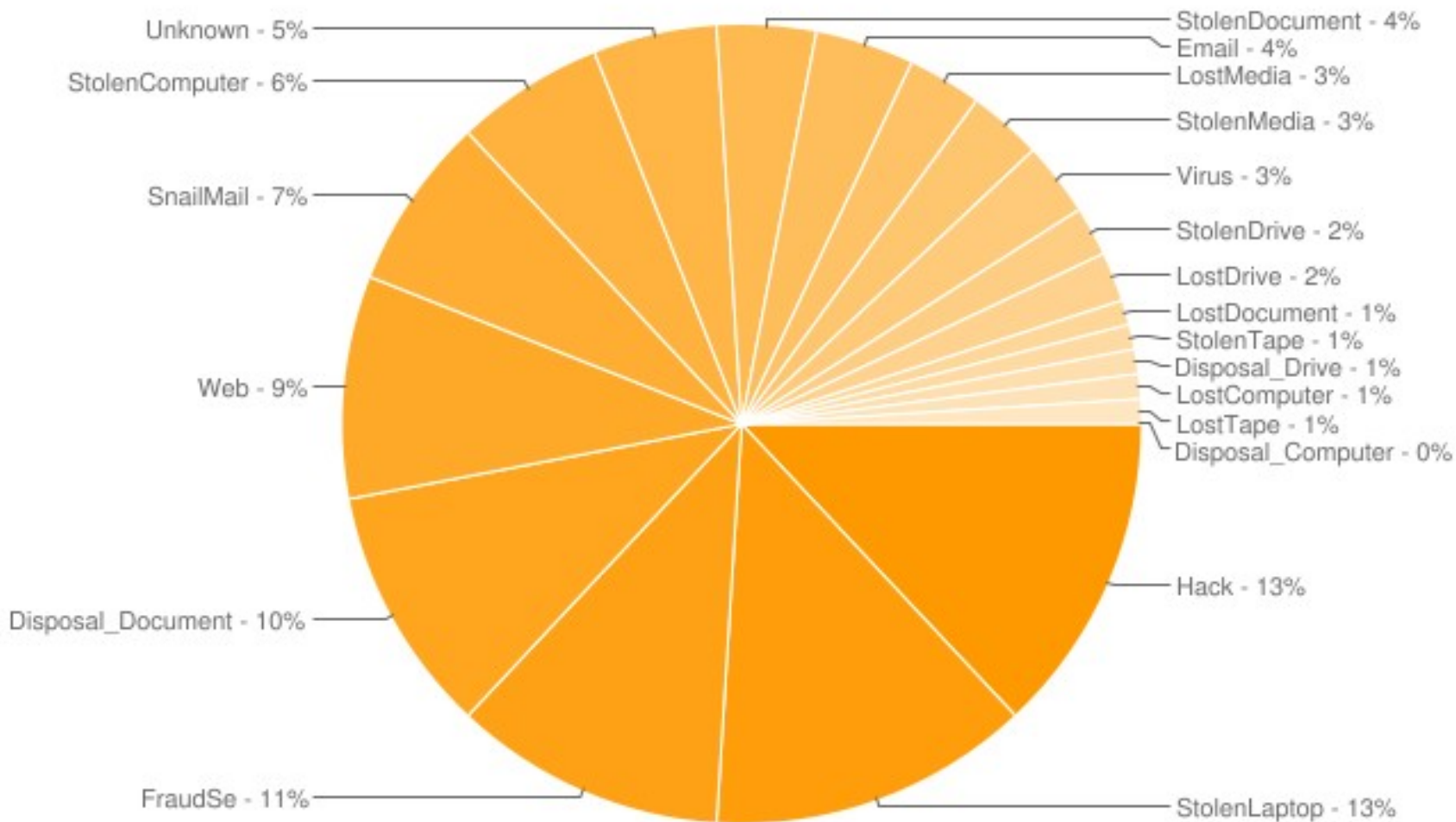
# Graphiques 1/3

DataLossDB.org Incidents Over Time



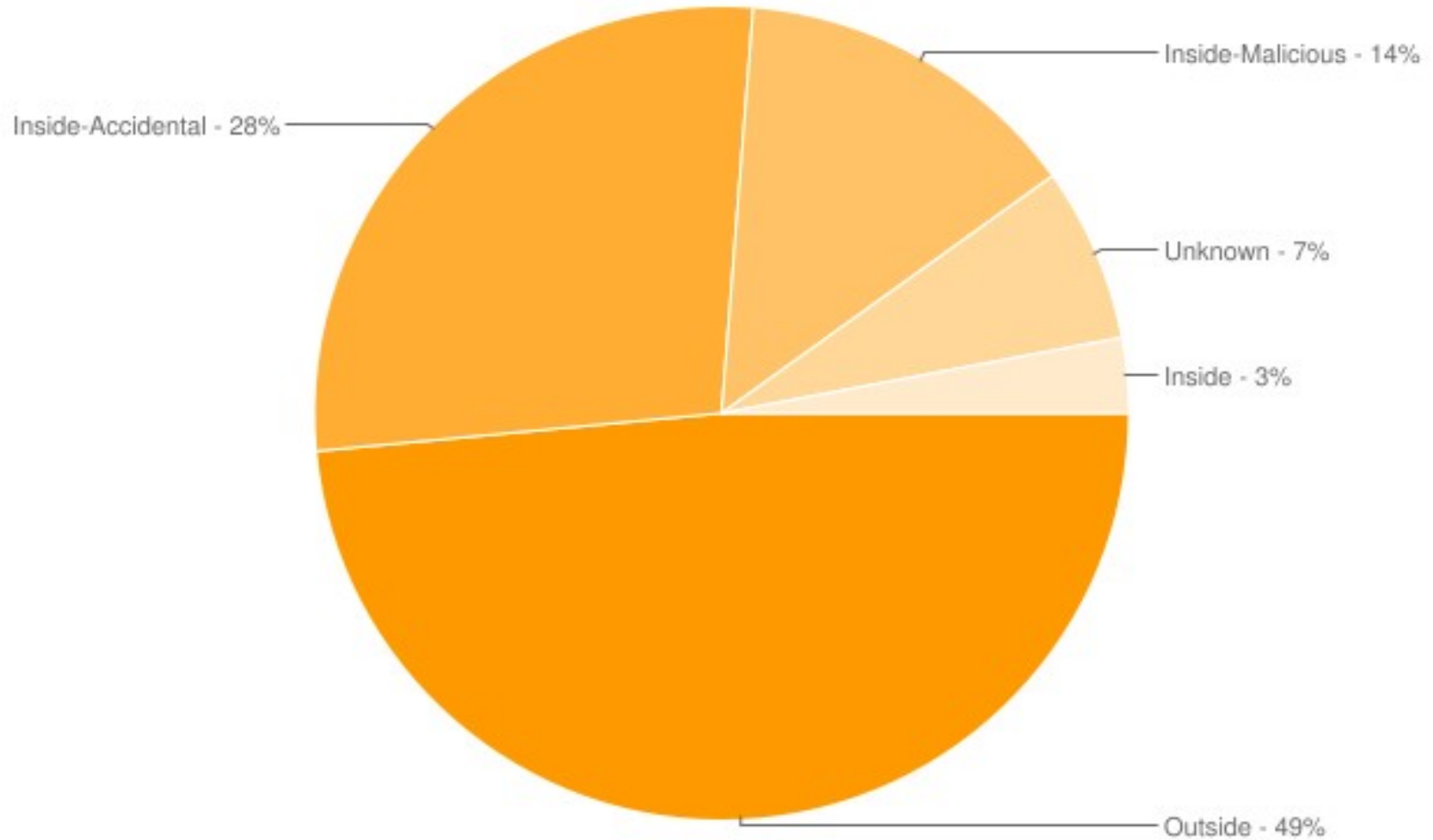
# Graphiques 2/3

Incidents by Breach Type - Current Year



# Graphiques 3/3

Incidents by Vector - Current Year



# Questions sur la gestion de l'information

- Définition des informations « confidentielles » :
  - Aspects légaux
  - Données nominatives
  - Propriété intellectuelle
- Idées de volumétrie :
  - 5% d'informations critiques
  - Loi de Pareto (les fameux 80/20)
  - Tout n'est pas sensible ou critique !
- Définition des actions autorisées (ou interdites)

# Outils DLP - Phase 1

- Exploration
    - Connecteurs et agents pour accéder aux entrepôts de données (centraux / locaux / nomades)
    - Passerelles et sondes pour analyser les flux
  - Identification des données
    - Prise d'empreintes
    - Définition de règles de recherche, de formatage
  - Classification
    - Auteur, destinataire, type de données, horaires
    - Profils préconfigurés pour faciliter la mise en œuvre
    - Outils de classification automatique
- ⇒ **On retrouve les problématiques des moteurs de recherche**

## Outils DLP - Phase 2

- Définition de la sensibilité des informations
  - Catégorie ?
  - Périmètre autorisé ?
- Définition des politiques d'échange :
  - Quelles sont les données pouvant être échangées ?
  - Entre quels interlocuteurs ou media ?
  - Sous quelle forme ?
- Définition des politiques de stockage :
  - Où peuvent être stockées les données ?
  - Qui peut y accéder ?
  - Quand et à partir de quel outil ?

## Outils DLP - Phase 3

- Restitution des analyses
  - Edition de rapports
  - Audits légaux préconfigurés
- Actions
  - Envoi d'alarmes
  - Blocage ou redirection

# Intégration

- Aspect technique de la performance :
  - Besoin de ressources pour l'analyse
  - Besoin de stockage
- Aspect technique de l'accès aux données :
  - Données chiffrées
  - Différents types d'entrepôt
  - Les interceptions locales ou réseau
- Aspect configuration :
  - Responsable des règles
  - Configuration initiale
  - Gestion des faux positifs

# Offres logicielles

- Formats :
  - Agents à installer
  - Serveurs à installer
  - Appliances
- Outil unique complet :
  - Websense / Macafee
- Partenariat entre plusieurs éditeurs :
  - RSA Security avec Cisco / Oracle
- Open Source :
  - OpenDLP