POUR DES COMPÉTENCES TOUJOURS À LA POINTE

Télécom Evolution

Mastère Spécialisé

Big Data Gestion et analyse des données massives Programme - MS Big Data :

Période 3 : Sécurité informatique

Session 2 : Data Leak Prevention (fuite de données)

La fuite de données (DLP)

Et si vous perdiez le contrôle de votre capital informationnel ?

Mercredi 22 février 2017

Bruno HAMON
bhamon@mirca.fr

Quelques proverbes et citations

« Face au monde qui change, il vaut mieux penser le changement que changer de pansement »

Pierre DAC

« L'habituel défaut de l'homme est de ne pas prévoir l'orage par beau temps »

Nicolas Machiavel

« C'est au pied du mur qu'on voit le mieux le mur »

Lao-Tseu ou Confucius

« Les tuiles qui protègent de la pluie ont toutes été posées par beau temps »

Proverbe chinois

« Qui n'a rien ne risque rien. Qui ne risque rien n'a rien »

Proverbe Français

Présentation de BHA

Fondateur et DG de MIRCA : Audit, Conseil et Formation

- gestion des risques - cyber risques
- sécurité des systèmes d'informations

Diplômé de l'Institut National des Hautes Etudes de la Sécurité et de la Justice

- Fichiers de police (2014) / Cybercriminalité (2015)

Enseignant sur les enjeux / risques - cyber risques liés à la SSI auprès de grandes écoles et instituts

- ENM / ESIEE Paris / ILDV / ISEP / MINES TELECOM

Membre actif de l'AFNOR, à l'origine de normes/documents normatifs

- PCA (norme) / DLP (guide normatif) / APTs (en cours)

Animateur / Conférencier en gestion des risques

- Afnor / Assises de la Sécurité / Clusif, /Région Centre / Isaca / Medef, ..

Le contexte

Patrimoine Informationnel : les données informatiques font partie du patrimoine d'une organisation.

Rappel : CONTEXTE - ENJEUX ÉCONOMIQUES

2015 : Indicateurs & Coûts Cybercriminalité Monde (tous pays confondus)

Coût = 400 Milliard € (= budget total de la France!) (en 2010, < 40 Milliards €)

- 50 % des escroqueries bancaires sont liées à Internet suite à un achat
- 20 x victimes par seconde soit 1.600.000 par jour

  Source: Allianz Corporate & Specialty

- 950 vols PC Portables dans Thalys pendant le trajet

  Source : DGSI (Dir. Gén. Sécu. Int.)

- Intrusions réseau : 76% des cas se font par vol ou déduction de code d'accès / mdp
- Entreprises : subissent ≈ 16 incidents de sécurité - 2,4 vols de données / mois

  Source : Skyhigh Networks

- 94 % entreprises auraient été victimes incident sécurité provenant attaque externe
- Facture cyberattaques : pourrait atteindre 3 000 Milliards € d'ici à 2020

  Source : lesechos.fr

Rappel : CONTEXTE - ENJEUX ÉCONOMIQUES

Quelques exemples de Fuites en France (Ponemon Institute)

Oct. 2015 : Coût moyen = 3,45 M € / an et par entreprise
Chaque dossier perdu ou volé se négocier ≈ 140 €
60 % = attaques extérieures / 220 jours = durée identification

Sep. 2014 : Vols des DP de 1,3 M clients d'**Orange** suite attaque

Mai 2014 : Perte de 145 M de DP chez **e-Bay** (mdp, adr., coord. banc.)

Nov. 2013 : Un prestataire mandaté par **l'hôpital de St Malo** accède aux DM de 950 patients !

Oct. 2013 : Fuites de données massives (identifiants + mdp) dans **50 x hôpitaux** équipés d'un logiciel de gestion des urgences

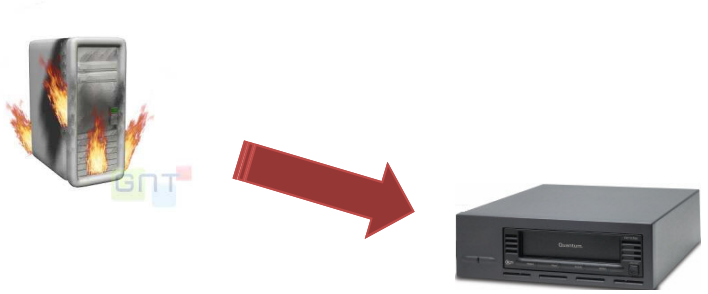
Et on ne dispose pas encore (ou très peu) de chiffres concernant les fuites touchant les Mobiles !

Agenda

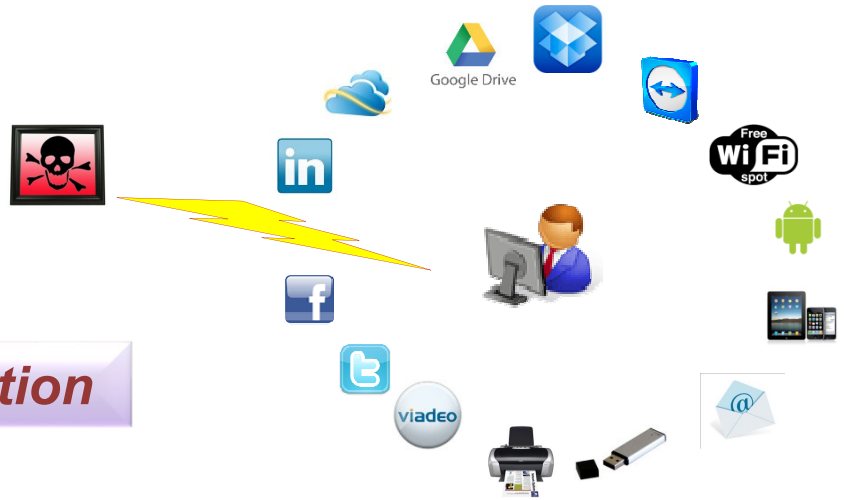
1. **Définition**
2. Pourquoi mettre en place une DLP
3. Classification des Données
4. Les outils DLP
5. Démarche Méthodologique
6. Sensibilisation
7. Aspects juridiques
8. Conclusion

Qu'est-ce que la DLP

- Fuite ou perte ou vol ?
  - Perte => sauvegarde !
  - Vol : difficile à identifier ou à qualifier
  - Fuite : perte de contrôle de l'information



- La prévention de la fuite d'information comme préoccupation de tous les instants au sein d'une organisation
  - Technologies
  - Comportements
  - Sensibilisation et formation des utilisateurs



Data Leak / Loss Prevention

La méconnaissance de la DLP

- **De nombreuses technologies participent déjà à la prévention de la fuite d'information, et elles ne sont jamais toutes complètement maîtrisées !**
  - **Gestion des identités et des droits d'accès (IAM),**
  - **Gestion des droits numériques (DRM)**
  - **Chiffrement**
  - **Authentification forte,**
  - **Détection d'intrusion,**
  - **Firewalls, Antivirus**

Or cela n'arrive jamais !

- **Les fournisseurs de solutions de sécurité prétendent tous avoir un module DLP à leur catalogue.**
- **Les responsables informatiques pensent à 42% qu'ils ont une solution DLP, or seuls 2% en ont réellement une**

Source : Websense

Qu’est-ce que la DLP ?

« Ensemble de mesures organisationnelles et techniques visant à identifier, surveiller, et protéger l’information qu’elle soit stockée, en mouvement ou en cours d’utilisation.

La prévention et la gestion de la fuite de l’information sont basées sur des politiques centralisées et une analyse approfondie du contenu. »

« Informations Sensibles »

- **Informations auxquelles une organisation attache une forte importance, quel que soit le motif de son attachement.**
- **Informations confidentielles :**
  - **Relevant du secret des affaires,**
  - **Secret professionnel,**
  - **offrant un avantage concurrentiel,**
  - **Protégées par un droit de propriété intellectuelle,**
  - **Autres ….**

90 % des données dans le monde ont été produites sur les 2 dernières années !
70 % des données en entreprises ne sont pas utilisées.
6 objets connectés par habitants d'ici 2020 (contenant tous des données privées)

Il appartient à chaque organisation de déterminer elle-même l'importance qu'elle attache à quelles informations.

« Informations Sensibles »

DECEMBER 19, 2015 / BY DAN LOHRMANN

2015: The Year Data Breaches Became Intimate

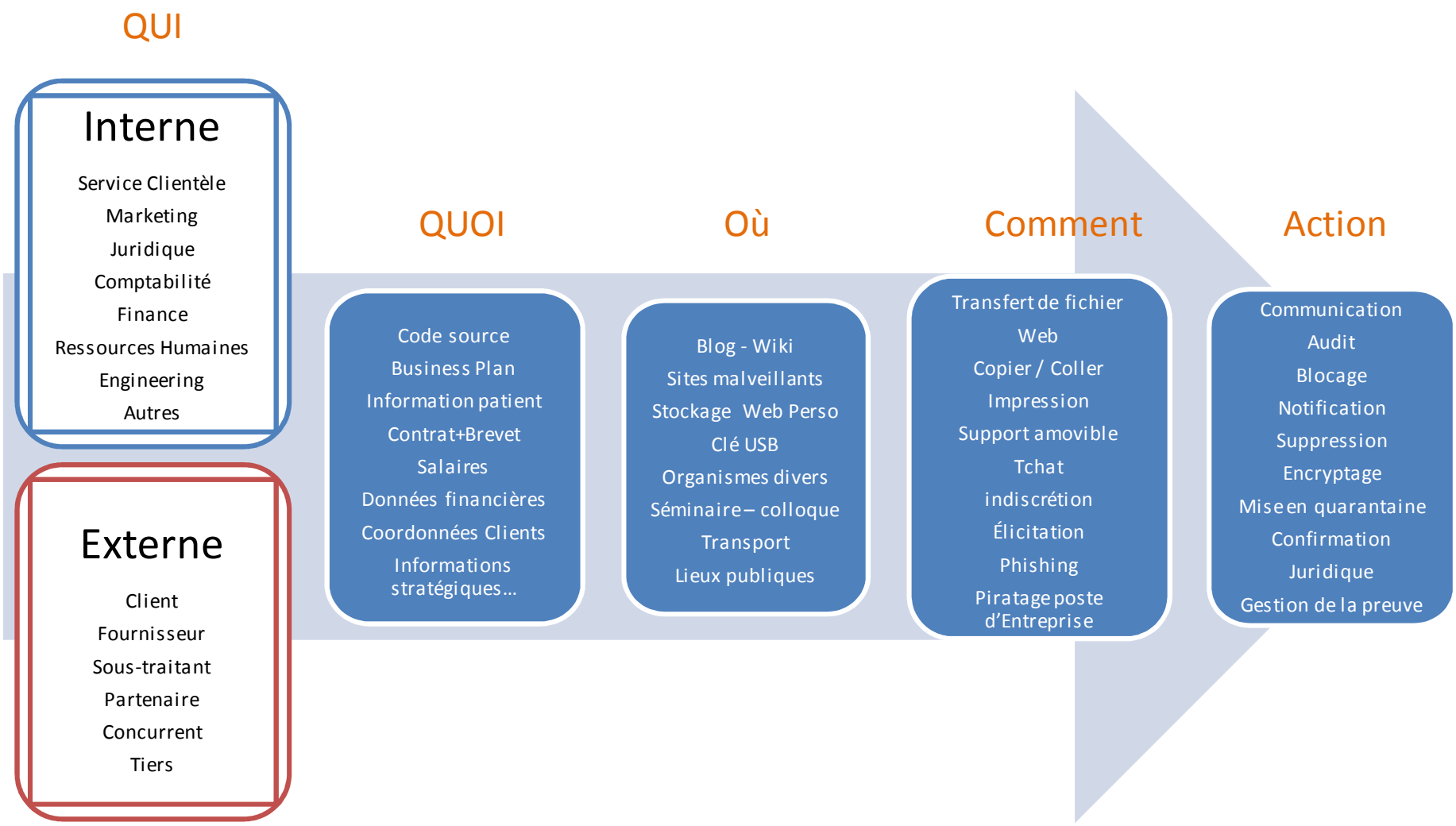
Something new, even unprecedented, happened this year in our cyber world. The most noteworthy data breaches were not focused on financial data.
.... But in 2015, the top data breaches affected something more precious than personally identifiable information (PII). ... most intimate details and actions in life – with the loss of millions of records containing biometrics (like fingerprints), career backgrounds, family relationships, voice recording of children playing with toys, secret liaisons and affairs, hospital records, private habits and much more.

19/07/2016

Des hackers volent 600000 données personnelles de patients américains.

"Les données personnelles sont souvent vendues sur le Dark web... Les informations médicales valent 10 fois plus que des numéros de cartes de crédit sur le marché noir".

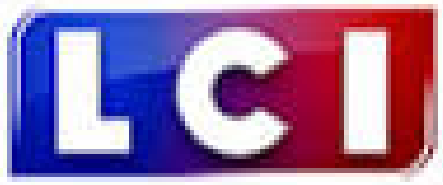
Les Etapes de la Fuite de Données



Agenda

1. Définition
2. **Pourquoi mettre en place une DLP**
3. Classification des Données
4. Les outils DLP
5. Démarche Méthodologique
6. Sensibilisation
7. Aspects juridiques
8. Conclusion

ACTUALITES DE NOS CHERS MEDIAS !



Il y a 17 mois……

Le Parisien, 15 Sept. 2015, 12h11

« Légère » fuite de données

au sein du cabinet de l'avocat Eric Dupond-Moretti
suite à un cambriolage

Une affaire jugée très sensible, prise en charge par la PJ.

Les malfaiteurs auraient dérobé **deux PC portables** dans les bureaux.

Eric Dupond-Moretti, en charge d'affaires jugées très importantes (chantage du roi du Maroc Mohammed VI, dossiers Bernard Tapie / Henri Guaino) indique :

« **les ordinateurs portables volés**

ne contiendraient pas de données sensibles »

Il y a 10 mois……

Tribune de Genève 05.04.2016, 21h28

« Enorme » fuite de données

à Panama : 12 chefs d'Etat touchés, des hauts dignitaires, des hommes d'affaires, mais aussi des criminels

Sur la période de juin à déc. 2015, + de 2,6 To de données sensibles ont été exfiltrées peu à peu du cabinet d'avocats Mossack Fonseca

11,5 M de fichiers, concernant des grandes fortunes et leurs placements financiers opaques, plus ou moins légaux

Il y a 10 mois -1 jour…….

AFP 07.04.2016, 09h23

« Gigantesque » fuite de données personnelles qui expose deux Turcs sur trois

Les DP de 50 millions de Turcs* en danger !

Une base de données mise en ligne par des pirates

Les DP contiennent: N° identification national, sexe, noms des parents, date et lieu de naissance, adresse,...

Zagara (voyante) xxx Paris jj mm 2017

« Titanesque » fuite de données

au sein du groupe multinational DUPONT & DUPOND

« L'intégralité de nos bases de données a été exfiltrée de notre SI »
indique M. Tournesol, actuel DSI de l'organisation,
« et ce, sans que nous ne puissions identifier ni les auteurs, ni la destination ! »

Y’a comme un problème (1/3)

Y’a comme un problème (2/3)

Y’a comme un problème (3/3)

Pourquoi mettre en place une DLP

- 1 message sur 400 contient des données confidentielles

- 1 fichier sur 50 est partagé à tort
- 1 ordinateur portable sur 10 est volé ou perdu
- 1 clé USB sur 2 contient de l'information confidentielle

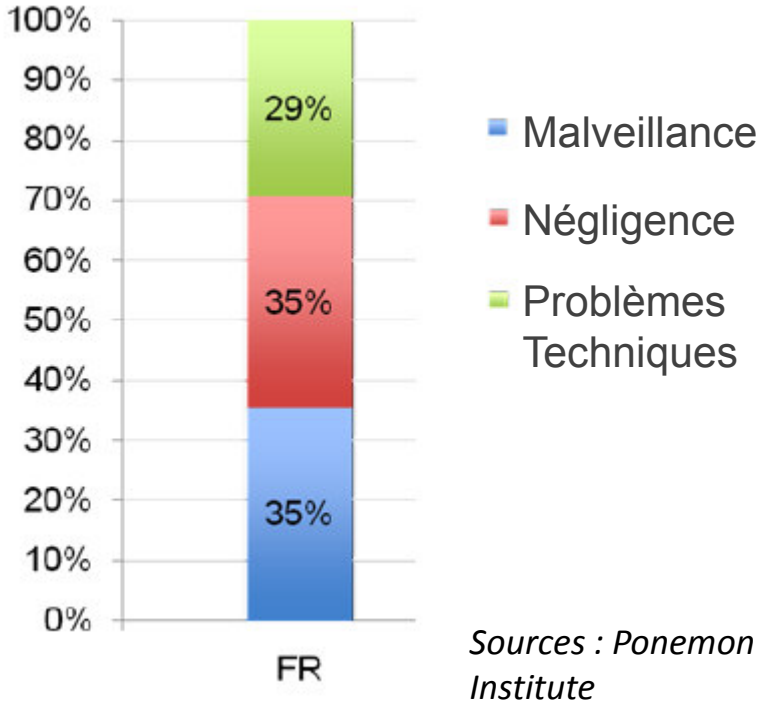
- 1 identité est volée toutes les 4 secondes (USA)

Sources : Ponemon Institute, Verizon,…

Pourquoi mettre en place une DLP

- 67% des entreprises françaises reconnaissent avoir subi un détournement de données
  - 92% de ces détournements ne sont pas révélés
- 59% des employés quittant leur entreprise emportent des données confidentielles

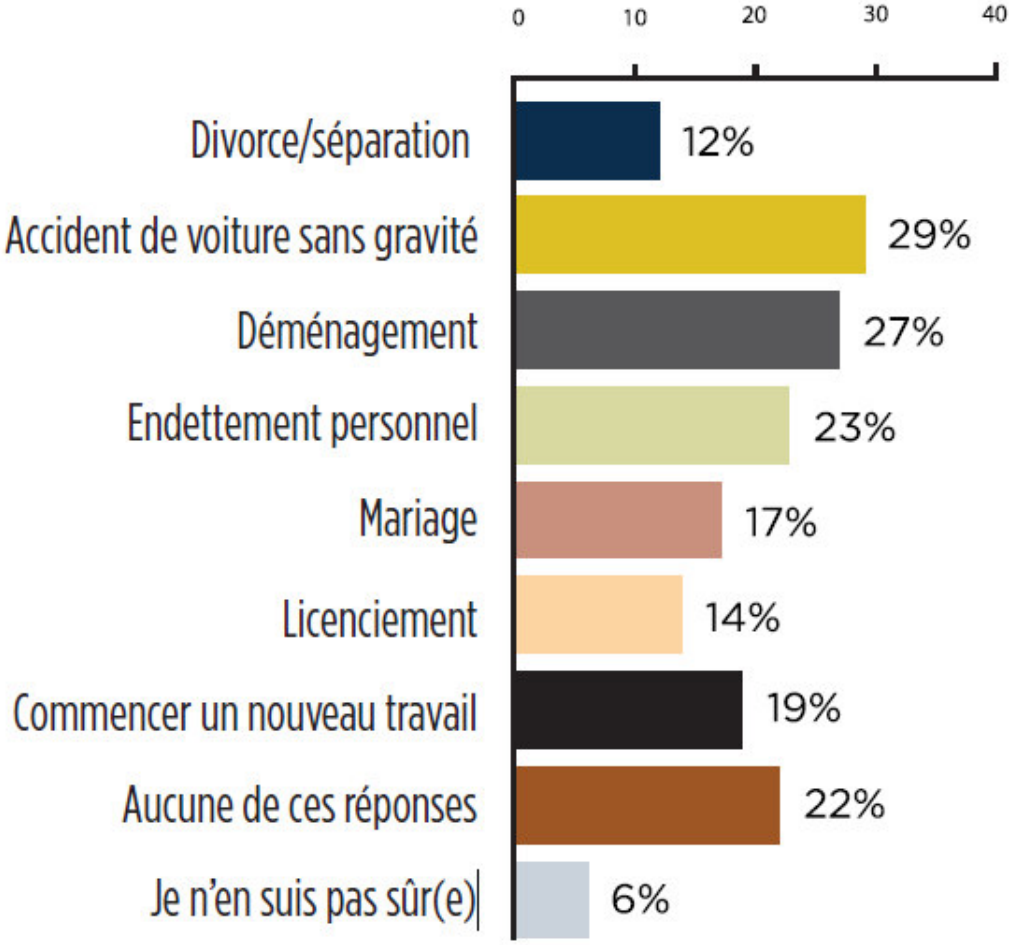
Le coût du détournement d'un enregistrement est évalué à 150 €



Sources : Ponemon Institute

Pourquoi mettre en place une DLP

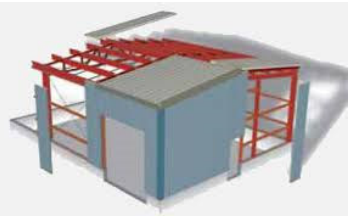
Parmi les propositions suivantes, laquelle trouveriez-vous moins stressante que la responsabilité de protéger les données confidentielles de votre société ?



Sources : Dynamic Markets / Websense

Différents vecteurs de fuites

- **Structures du bâtiment :**
  - **Fenêtres, portes, parois, tuyaux, radiateurs,**



- **Médias : Les câbles, les ondes, les réseaux**
  - **Réseaux électriques, téléphoniques, informatiques, hauts parleurs, sonorisations, vidéo portiers, vidéo surveillance, alarmes, télésurveillance,**

- **Facteur humain : le maillon faible ?**
  - **Principaux moteurs de motivation : argent, pouvoir, sexe, vengeance.**
  - **Distraction, étourderie, maladresse (parfois liés à la fatigue, le stress ou le surmenage).**

Le problème vient de l'intérieur

- Les utilisateurs n'aiment pas la sécurité
  - Ils font n'importe quoi
  - Ils sont de bonne volonté si on leur explique
  - Et ils restent les principaux actifs de l'entreprise !
- Différentes catégories d'utilisateurs dangereux
  - Les analphabètes de la sécurité
  - Les nerds / geeks
  - Les contrevenants patentés
  - Les employés mécontents et malveillants

Près de 80% des violations de données viennent de membres autorisés du personnel de l'entreprise
Le personnel trouve toujours de bonnes raisons pour « détourner » de l'information.

Risques de la fuite d'information

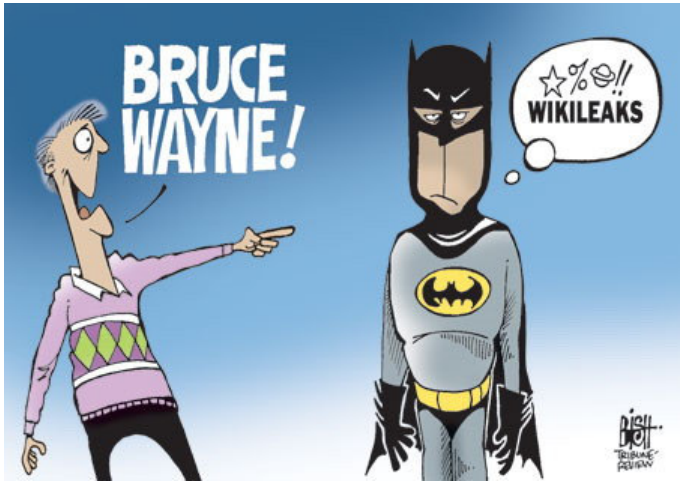
- Sensibilité des informations manipulées par les collaborateurs
  - Données personnelles identifiables (DPI)
  - Coordonnées bancaires
  - Liste de clients / de prix
  - Informations stratégiques (réorganisation, acquisitions, ventes, plans marketing)
  - Savoir faire / brevets
  - Dossiers médicaux
  - Programmes de cours, documents d'évaluation
- Vulnérabilité des systèmes
  - Surtout quand on ne s'imagine pas être une cible pour les pirates / voleurs !
  - Passage par des réseaux non sécurisés
  - Traitement de données par tierces parties
- Facteur humain

Hilton Hotels Hit by Cyber Attack *November 25, 2015*

US hotel chain Hilton revealed Tuesday that hackers stole credit card information from some of its point-of-sale computer systems.

Impacts de la fuite d'information

- **Impacts d'une fuite d'information**
  - Perte de confiance des salariés, des clients, des partenaires, des fournisseurs, des actionnaires,
  - Pertes financières
  - Déni d'image
  - Sécurité des personnes
  - Poursuites pénales



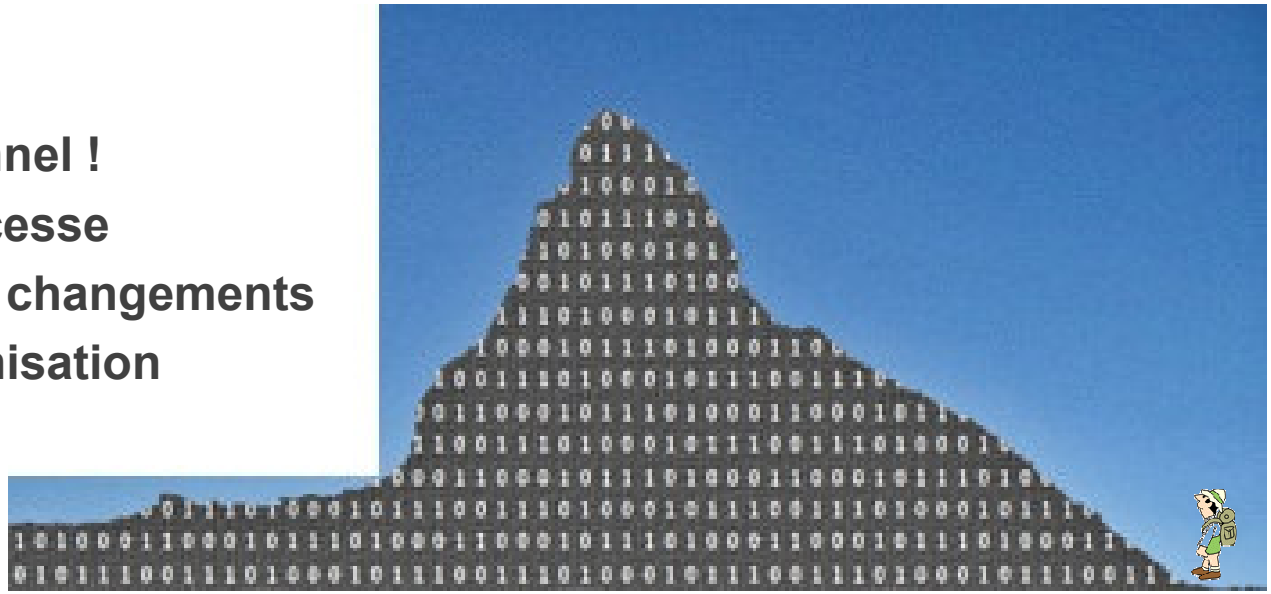
- **Prise de conscience**
  - « Avec toutes les protections existantes, le risque de fuite d'information est minime ! »
  - « Ca n'arrive qu'aux autres !»
  - « Chez nous, le personnel est loyal !»
  - « Nous ne sommes pas une cible intéressante pour les pirates !»

Agenda

1. Définition
2. Pourquoi mettre en place une DLP
3. **Classification des Données**
4. Les outils DLP
5. Démarche Méthodologique
6. Sensibilisation
7. Aspects juridiques
8. Conclusion

L'ampleur de tout projet DLP

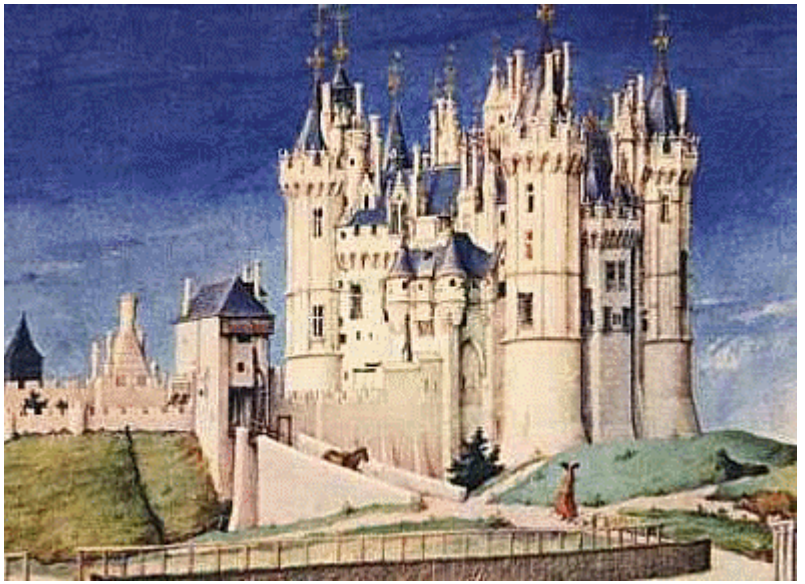
- **Périmètre : difficulté à identifier les contours du projet DLP**
  - **Où commence et où s'arrête la Prévention de la Fuite d'Information ?**
  - **Culture d'entreprise, politique de sensibilisation du personnel, projet organisationnel ?**
  - **Projet métier ou projet technologique ?**
- **Appréhender l'ensemble des données ainsi que leurs flux au sein de l'entreprise**
  - **Vaste chantier !**
  - **Peur de l'effet tunnel !**
  - **Processus sans cesse renouvelé par les changements au sein de l'organisation**



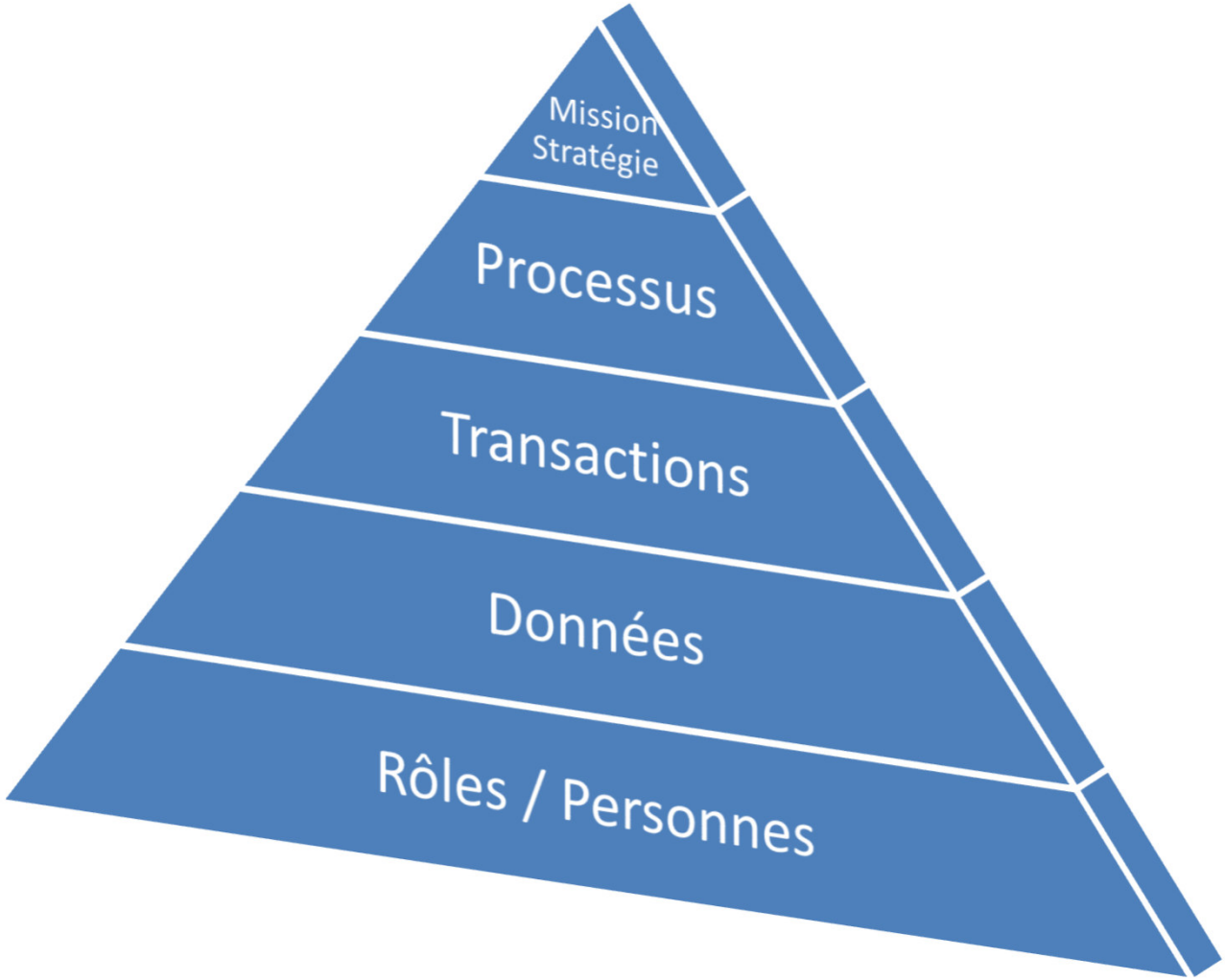
L'ampleur de tout projet DLP

- **Recherche d'un Quick Win**
  - Procéder par étapes itératives
  - Département pilote, et famille réduite de données
  - Processus simple et non bloquant ayant un sens réel pour l'organisation
  - Continuer à bâtir son projet DLP à partir de ce premier succès

Notre expérience montre que seules 5 à 10 % des informations sont réellement critiques.



Démarche « Top / Down »



Démarche « Top / Down »

- Mission / Stratégie de l'Organisation
  - On n'aborde pas de la même manière un centre hospitalier, un ministère, une banque ou une société industrielle.,…
  - Identification des grands enjeux de l'organisation, ce qui en fait sa valeur présente et à venir
- Identification des processus stratégiques
- Transactions utilisées lors de ces processus
- Données traitées lors de ces transactions
- Rôles / Personnes impliquées lors de ces transactions

Initiative	Processus	Famille de données	Utilisateurs	Classification	Impact Fuite

Gestion du Risque

- **L'objectif est d'identifier les données les plus sensibles, celles dont la fuite, le vol, la perte de contrôle, auraient un *impact* majeur sur l'organisation. Il s'agira par la suite d'identifier les *vulnérabilités* de ces données, et la *probabilité* d'une fuite (volontaire ou non).**

Description						
Données	**Propriétaire**	**Processus**	**Classification**	**Contraintes**	**Valeur (B,M,H)**	**Impact DLP**

Technique				*Utilisation / Mouvement*		
Lieu de Stockage	**Volume**	**Format**	**Resp. Tech.**	**Fréq changement**	**Auteur**	**Transactions Autorisées**

Exemple – Processus Récurrent : Commandes sur Internet

- **Mission / Stratégie:** ***Site de vente en ligne***
  - **Vente de produits sur Internet**
- **Processus stratégique:** ***Commande d'un produit en ligne sur le portail***
  - **A l'occasion d'une commande, un client enregistre ses coordonnées**
- **Transaction:** ***Saisie des coordonnées***
  - **Le client enregistre ses coordonnées sur le site de vente**
- **Données traitées:** ***Coordonnées personnelles***
  - **Nom, prénom, adresse, n° téléphone, n° carte bancaire, date validité, n° de contrôle, adresse email, identifiant, mot de passe**
- **Rôles / Personnes:**
  - **Client**
  - **Service facturation**
  - **Service livraison + tierces parties (transporteurs,…)**
  - **Administrateur base de données**
  - **Service marketing**
- **Conservation sécurisée des données jusqu'à suppression.**

Projet « Métier » !

- **Projet « métier » sponsorisé par la Direction Générale**
  - **Sensibiliser, convaincre et encourager les utilisateurs.**
  - **Déployé, la DLP devient un processus récurrent impliquant des utilisateurs *non-IT*,**
  - **La DLP doit sans cesse se renouveler : introduction de nouvelles applications et de nouvelles données, ou retrait des anciennes.**
  - **A l'image d'un ERP ou d'un CRM, la DLP doit être considérée comme une application métier,**
- **Seules les directions métier peuvent**
  - **Identifier les informations qui ne doivent pas sortir de leur contrôle,**
  - **Gérer la crise en cas de fuite d'informations.**

La solution et le processus retenus ne peuvent pas être uniquement techniques ni gérés par des techniciens

Agenda

1. Définition
2. Pourquoi mettre en place une DLP
3. Classification des Données
4. **Les outils DLP**
5. Démarche Méthodologique
6. Sensibilisation
7. Aspects juridiques
8. Conclusion

Outils DLP : Principe

Où sont stockées les données sensibles ?

DECOUVERTE

Comment sont-elles utilisées ?

SURVEILLANCE

Comment prévenir leur fuite ?

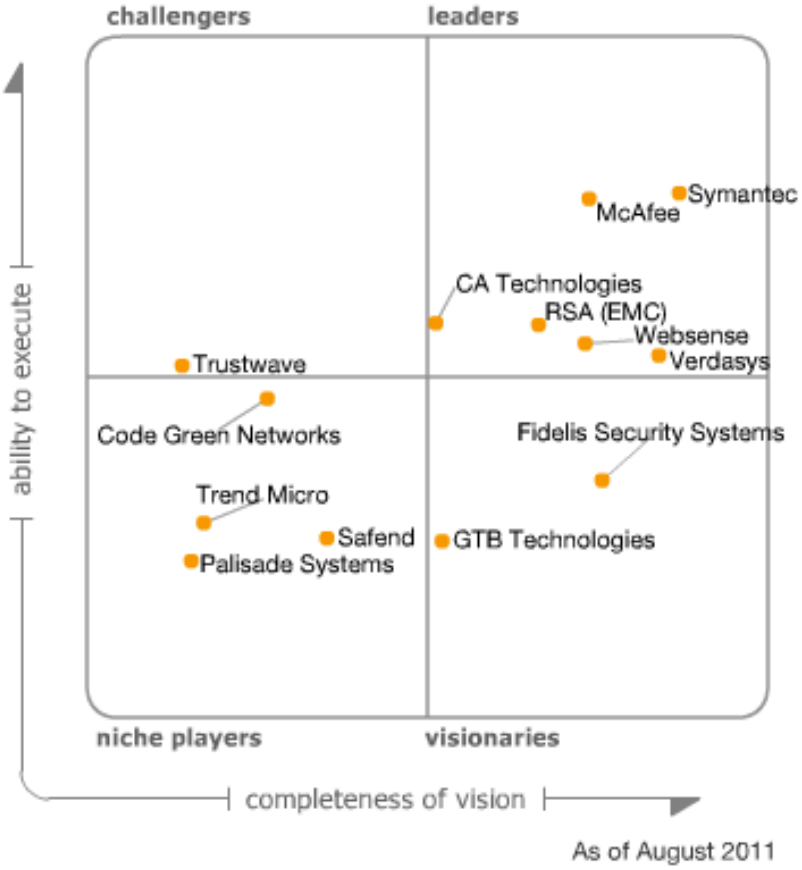
PROTECTION

Outils DLP

- **Principales Fonctions :**
  - **Analyse des contenus stockés en profondeur**
  - **Restriction des transferts en fonction des politiques définies**
  - **Analyse et filtrage du trafic réseau**
  - **Surveillance des postes de travail (endpoints)**
  - **Alarmes sur tentatives de violation des politiques prédéfinies**
- **Mécanismes :**
  - **Réseau : analyse des flux email, IM, http, https, FTP**
  - **Poste de travail et serveur : données stockées et manipulation utilisateurs (impression, clef USB,…)**
  - **Identification des données**
    - **Mots clefs et expressions**
    - **Empreintes des documents (FingerPrinting)**
    - **Meta Data (extension, taille de fichiers)**
    - **Politique systématique (PCI, CNIL,…)**

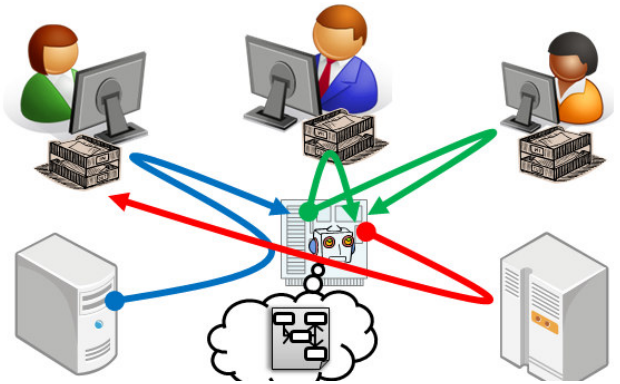
Les Outils DLP

- On retrouve les grands noms de la Sécurité, suite à des acquisitions
  - Orchestria
  - Tablus Content S.
  - Reconnex
  - Vontu
  - Websense
  - Verdasys
- D'autres présentent des modules DLP ciblés

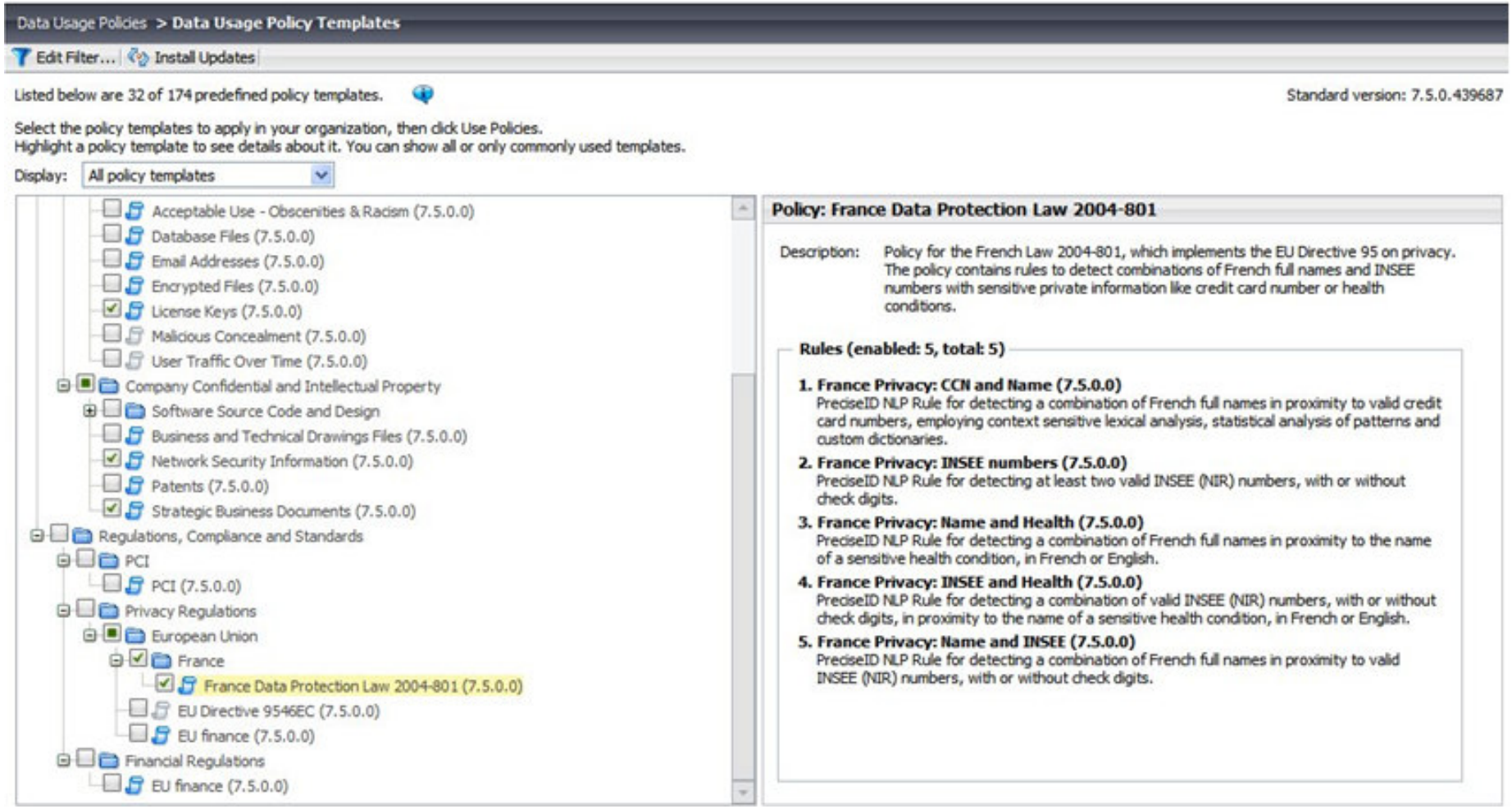


Choix de l'Outil

- L'outil doit répondre aux besoins définis lors de la classification des données et des règles DLP
- Intégration dans l'environnement existant,
- Prise en charge de la volumétrie réseau,
- Existence de règles prédéfinies,
- Workflow performant,
- Simplicité de déploiement,
- Maquette / Proof Of Concept,
- Différenciation
  - Surveillance du réseau (Data in Motion), des postes de travail (End Points / Data in Use) et des espaces de stockage (Data at Rest).

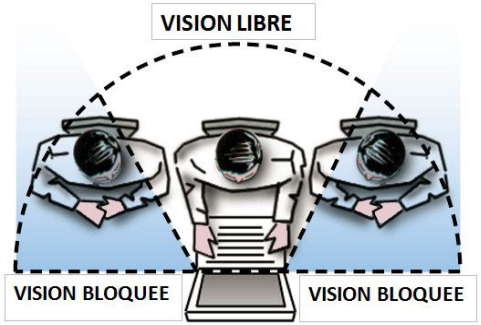


Exemple


Data Usage Policies > Data Usage Policy Templates
Edit Filter...
Install Updates
Listed below are 32 of 174 predefined policy templates.
Standard version: 7.5.0.439687
Select the policy templates to apply in your organization, then click Use Policies.
Highlight a policy template to see details about it. You can show all or only commonly used templates.
Display: All policy templates
Acceptable Use - Obscenities & Racism (7.5.0.0)
Database Files (7.5.0.0)
Email Addresses (7.5.0.0)
Encrypted Files (7.5.0.0)
License Keys (7.5.0.0)
Malicious Concealment (7.5.0.0)
User Traffic Over Time (7.5.0.0)
Company Confidential and Intellectual Property
Software Source Code and Design
Business and Technical Drawings Files (7.5.0.0)
Network Security Information (7.5.0.0)
Patents (7.5.0.0)
Strategic Business Documents (7.5.0.0)
Regulations, Compliance and Standards
PCI
PCI (7.5.0.0)
Privacy Regulations
European Union
France
France Data Protection Law 2004-801 (7.5.0.0)
EU Directive 9546EC (7.5.0.0)
EU finance (7.5.0.0)
Financial Regulations
EU finance (7.5.0.0)
Policy: France Data Protection Law 2004-801
Description: Policy for the French Law 2004-801, which implements the EU Directive 95 on privacy. The policy contains rules to detect combinations of French full names and INSEE numbers with sensitive private information like credit card number or health conditions.
Rules (enabled: 5, total: 5)
1. France Privacy: CCN and Name (7.5.0.0)
PreciseID NLP Rule for detecting a combination of French full names in proximity to valid credit card numbers, employing context sensitive lexical analysis, statistical analysis of patterns and custom dictionaries.
2. France Privacy: INSEE numbers (7.5.0.0)
PreciseID NLP Rule for detecting at least two valid INSEE (NIR) numbers, with or without check digits.
3. France Privacy: Name and Health (7.5.0.0)
PreciseID NLP Rule for detecting a combination of French full names in proximity to the name of a sensitive health condition, in French or English.
4. France Privacy: INSEE and Health (7.5.0.0)
PreciseID NLP Rule for detecting a combination of valid INSEE (NIR) numbers, with or without check digits, in proximity to the name of a sensitive health condition, in French or English.
5. France Privacy: Name and INSEE (7.5.0.0)
PreciseID NLP Rule for detecting a combination of French full names in proximity to valid INSEE (NIR) numbers, with or without check digits.

Visual Hacking

- **La Mobilité induit des effets « pervers » :**
  - **le travail dans des environnements à risque (salles d'attentes, trains, avions, aéroports, gares, restaurants, halls d'hôtels),**



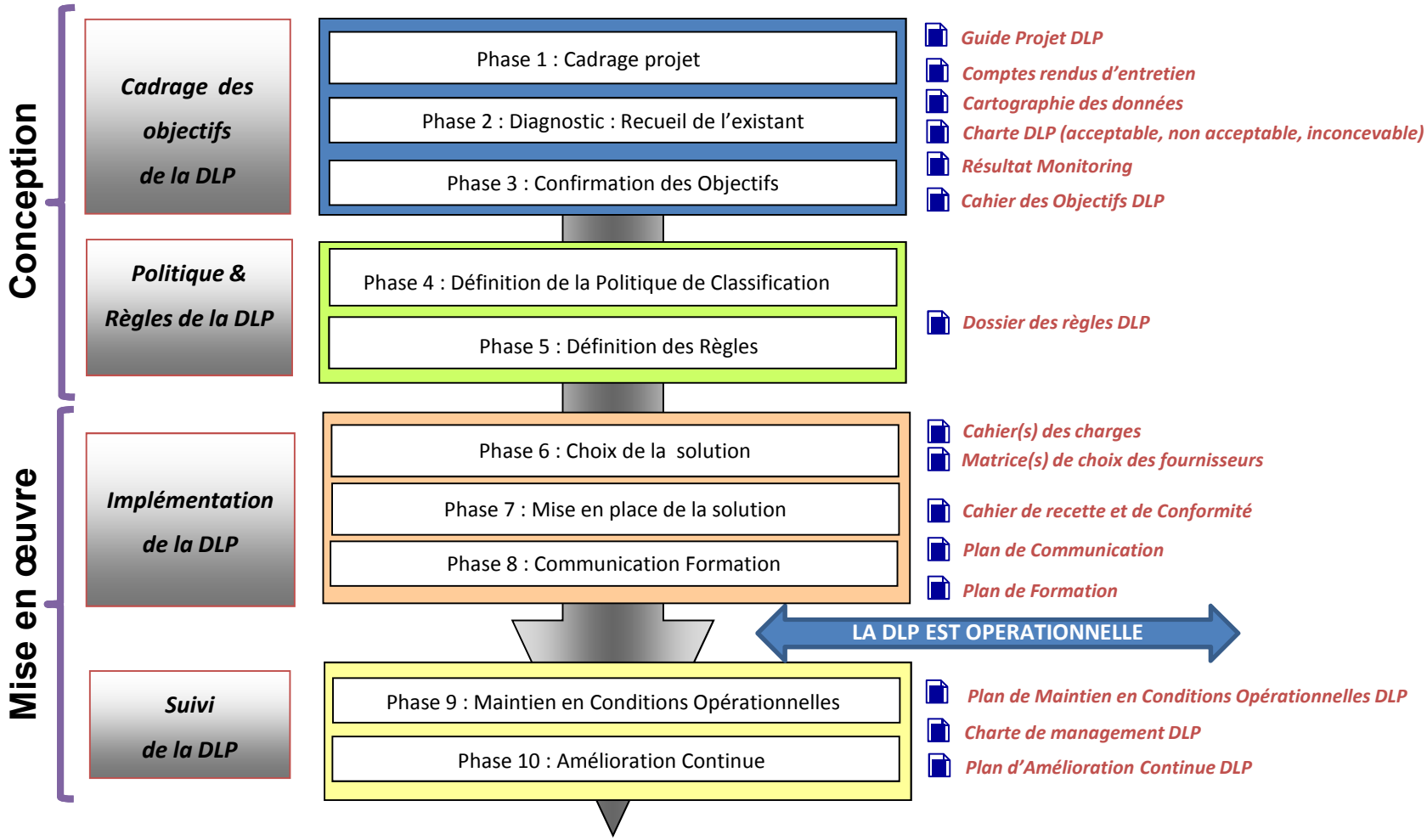
- **Le filtre de confidentialité :**
  - **Indispensable pour tous types d'appareils mobiles (ordinateurs portables, tablettes et téléphones,…) mais aussi pour les écrans fixes,**

- **Principe de fonctionnement :**
  - **Limite l'angle de vision latérale et éventuellement vertical).**

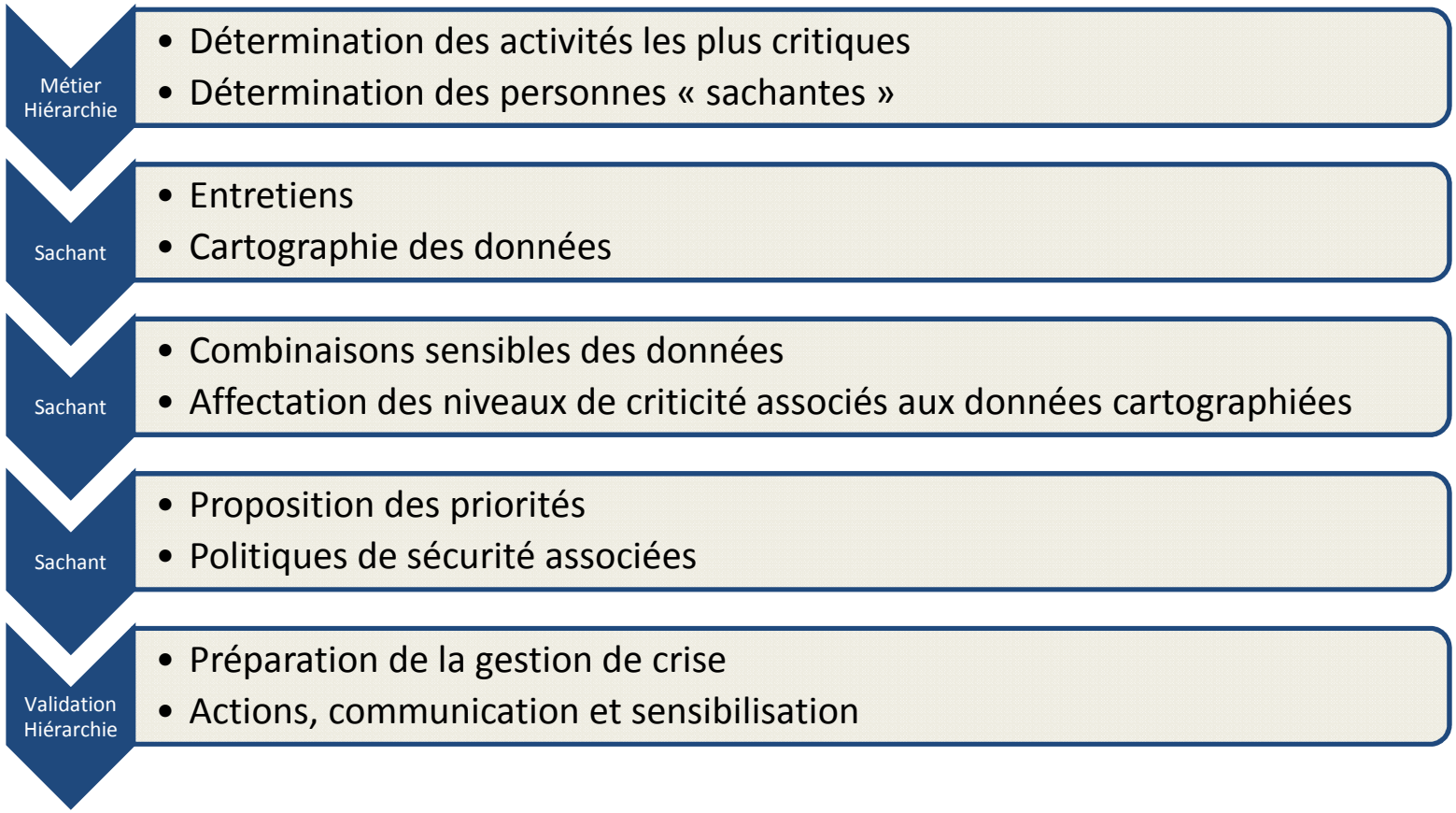
Agenda

1. Définition
2. Pourquoi mettre en place une DLP
3. Classification des Données
4. Les outils DLP
5. **Démarche Méthodologique**
6. Sensibilisation
7. Aspects juridiques
8. Conclusion

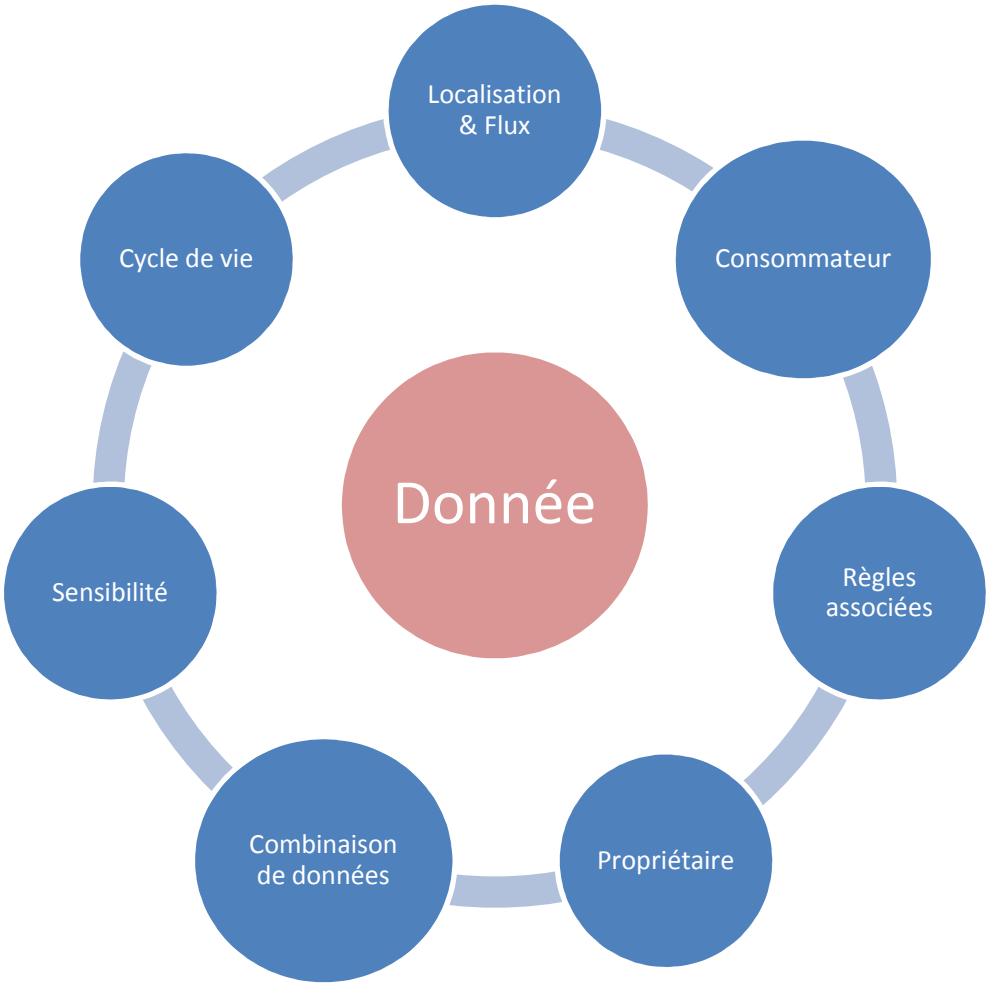
Méthodologie pour la DLP



Méthodologie pour la DLP (Variante)



Cartographie des Données



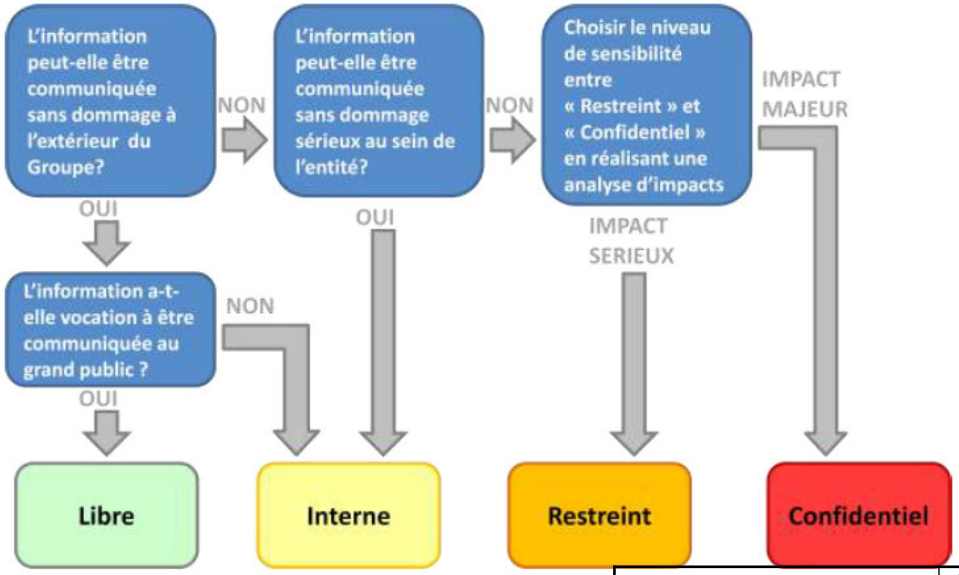
Cartographie des Données

Description						
Données	**Propriétaire**	**Processus**	**Classification**	**Contraintes**	**Valeur (B,M,H)**	**Impact DLP**

Technique				*Utilisation / Mouvement*		
Lieu de Stockage	**Volume**	**Format**	**Resp. Tech.**	**Fréq changement**	**Auteur**	**Transactions Autorisées**

Utilisation / Mouvement			*Règles DLP*		
Fréq changement	**Auteur**	**Transactions Autorisées**	**Actions**	**Notifier à**	**Escalader vers**

Politique de Classification



Impacts	Sérieux / Niveau Restreint	Majeur / Niveau Confidentiel
Perturbation de l'organisation / l'équilibre social	Risque de perturbations sociales limitées ne pouvant pénaliser que très temporairement la productivité de l'entité et /ou la qualité du dialogue social, sans impact sur d'autres entités du Groupe.	Risque de mouvement social, de blocage de l'entité ou de l'entreprise, d'une perte de compétence, etc. ; rupture du dialogue social ou risque de séquelles importantes et pénalisantes pour le futur.
Altération de l'image de l'entité	Risque d'altération de l'image de l'entité ou de l'entreprise, auprès de ses clients, du grand public, avec risque de médiatisation locale, voire régionale.	Risque d'altération de façon significative de l'image de l'entité avec des conséquences commerciales, juridiques et/ou politiques pour l'entité ; risque de médiatisation nationale, voire internationale.
Perte ou mise en danger de projets, conséquences financières	Impacts sur l'activité opérationnelle ou concurrentielle de l'entité, sans toutefois présenter une perte commerciale significative.	Impacts forts sur l'activité opérationnelle ou concurrentielle de l'entité, avec risque de perte financière importante de nature à affecter gravement l'exercice en cours.

Agenda

1. Définition
2. Pourquoi mettre en place une DLP
3. Classification des Données
4. Les outils DLP
5. Démarche Méthodologique
6. **Sensibilisation**
7. Aspects juridiques
8. Conclusion

Sensibilisation

- **Réticence et résistance des utilisateurs**
  - **Comme pour tout changement,**
  - **Perception d'espionnage, de flicage,**
  - **Sentiment de mise en place de nouveaux processus supposés anti-productifs, de contraintes supplémentaires sur les processus existants,**
  - **Méfiance face à ce genre de message venant de l'interne (passage par consultants extérieurs),**

- **Forte implication du management**
  - **Parfois contre son gré (un manager est bien plus conscient de la valeur des informations !!).**

Sensibilisation Primordiale

- C’est un sujet sensible !
  - Association / sensibilisation des utilisateurs dès le début du projet,
  - La mise en application ne fonctionnera qu’après adhésion de tous,
  - Approche progressive par la prise de conscience de la valeur des données manipulées
    - Politique de classification,
    - Campagne de communication,
  - Compréhension des risques pour l’entreprise et pour eux-mêmes,
  - L’outil de contrôle n’est là que pour mettre en application la politique centralisée,
  - Formation des utilisateurs et des équipes support.

Il n’y a plus d’impunité, la technologie préviendra les actes malveillants, mais protègera aussi contre les actes involontaires !

Gestion de Crise

- Que faire en cas de fuite de données :
  - Identifier avec exactitudes les données perdues,
  - Déterminer le canal de fuite et corriger la faille (suppression des accès, correctif,…),
  - Porter plainte auprès des autorités,
- Communication de crise
  - Réunir la cellule de crise (DG, métier, juriste, IT, communication, RH),
  - Préparer les communiqués (courrier, web, email, téléphone)
    - Presse,
    - Clients,
    - Fournisseurs,
    - Personnes / organismes impactés,
    - Personnel.

Gestion de Crise

LEMONDE INFORMATIQUE

Rechercher

Le 07 Mai 2014

Le vol de données clients d'Orange révèle une menace plus large

Contraint à la transparence sur le vol de ses données clients, Orange figure parmi les entreprises qui communiquent sur le sujet en France. Il pourrait bientôt y en avoir davantage, conséquence de réglementations plus contraignantes et de la surveillance renforcée des systèmes IT imposée par la montée des cyberattaques.

Agenda

1. Définition
2. Pourquoi mettre en place une DLP
3. Classification des Données
4. Les outils DLP
5. Démarche Méthodologique
6. Sensibilisation
7. **Aspects juridiques**
8. Conclusion

Aspects juridiques

Un pirate informatique qui « dérobe » des données risque 2 ans de prison et 30.000 € d'amende.

Une société qui n'a pas déclaré un traitement de données personnelles à la CNIL risque 5 ans de prison et 300.000 € d'amende.

Aspects juridiques : le GDPR

- **Mise en application : mai 2018**
- **Objet : Règlement Européen de Protection des Données**
  - **27 pays concernés,**
  - **Amendes substantielles : jusqu'à 4% du CA global d'un groupe ou 1 M€ pour les organismes publics** (exigible par chaque pays membre),
  - **DPO (Data Protection Officer) obligatoire dans les établissements publics et les entreprises > 250 personnes,**
  - **Obligation de notification à l'autorité nationale de contrôle des violations de données personnelles < 24h,**
  - **Notification aux personnes concernées**
  - **Adoption du règlement en 2018.**

Un « chief data officer » pour la France

Un « chief data officer » (CDO) pour la France va prochainement être nommé par Marylise Lebranchu, selon une communication de la ministre de la reforme de l'Etat en Conseil des ministres mercredi 21 mai.

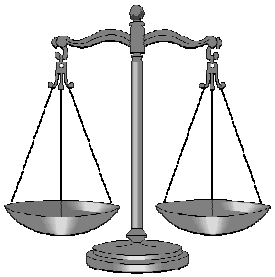
Lemonde.fr 21/05/2014

Aspects juridiques

- **Protection des données individuelles**
  - Loi Informatique et Liberté 1978 – CNIL,
  - Loi Détraigne Escoffier 2010 : obligation de protéger les DPI, et de déclarer tout détournement de ces données (US : *Data Breach Notification*),
  - Droit à la vie privée,
  - Directive Européenne 95/46/CE,
- **Protection des données médicales**
  - HIPAA : Health Insurance Portability and Accountability Act,
  - Loi Informatique et Liberté 1978 – CNIL,
  - Directive Européenne 95/46/CE,
  - Secret médical,
- **Protection des données financières**
  - Loi de Sécurité Financière,
  - Bâle II, SOX,
  - Contrôle interne : mise en place de mesures de sécurité adéquates pour ne pas mettre en péril l'entreprise,
  - PCI DSS: Payment Card Industry Data Security Standard.

Aspects juridiques

- **Normes et Standards de sécurité**
  - **ISO 27002 : Norme de Sécurité des SI,**
  - **IT Sec : Standard de la Sécurité des SI,**
  - **ITIL v3 : Service Design – Information Security Management,**
- **Mise en place d'outils DLP**
  - **Surveillances des activités des collaborateurs,**
  - **Déclaration à la CNIL, et autorisation le cas échéant,**
  - **Avis du Comité d'Entreprise,**
- **Difficultés**
  - **Aucune norme actuellement,**
  - **Très difficile de porter plainte pour « vol de données », et pourtant c'est indispensable !**
  - **Difficile d'identifier les auteurs,**
  - **Collaborateur risque au pire un licenciement,**
  - **Préjudice très difficile à évaluer.**



Agenda

1. Définition
2. Pourquoi mettre en place une DLP
3. Classification des Données
4. Les outils DLP
5. Démarche Méthodologique
6. Sensibilisation
7. Aspects juridiques
8. **Conclusion**

Mythes et légendes de la DLP

- C'est réservé aux grands groupes,
- Cela coûte cher et ne présente aucun ROI,
- Cela m'évite les autres outils de sécurité,
- Cela s'adresse comme n'importe quel projet technologique,
- Une fois installée, le travail est terminé,
- Cela va me générer des problèmes juridiques à n'en plus finir.

Recommandations 1/2

- La politique DLP doit tenir compte des caractéristiques intrinsèques de l'organisation pour laquelle elle est destinée,
- La mise en œuvre d'une politique DLP est un réel projet d'entreprise (impliquer les métiers dont la DSI),
- Les Clefs du succès :
  - Méthode itérative constituée d'étapes successives, sur un périmètre préalablement identifié,
  - Disposer d'une organisation de gestion de crise (le risque zéro n'existe pas),
  - travailler sur la gestion d'une fuite, c'est déjà s'y préparer,
- L'arsenal législatif et réglementaire s'étoffe, ce qui induit des contraintes que l'organisation ne peut plus ignorer. La DLP concourt à répondre en partie à toutes les obligations existantes comme celles à venir,
- La mise en place d'une politique DLP est un argument concurrentiel non négligeable.

Recommandations 2/2

Réalisation audits juridiques /techniques pour localiser les risques (int. et ext.)

- quels types de données ? quelles personnes / activités sont concernées ? quelles règles applicables ?

Mise en conformité : loi ; formalités auprès de la CNIL; …

Mise en place : règles internes pour la protection et sécurisation des données

- information et/ou consultation des instances représentatives du personnel
- adaptation du règlement intérieur / mise à jour de la charte informatique
- renforcement des obligations de confidentialité et de non-concurrence des employés
- sécurisation : postes de travail, terminaux mobiles, comptes utilisateurs, réseau local
- mise en place : processus accès fichiers / politique d'archivage électronique

Mise en place : mesures pour assurer la confidentialité des données par les prestataires et sous traitants

Mise en place : politiques de sensibilisation employés (BOYD), **utilisateurs, sensibilisation** (prestataires et sous-traitants)

Conclusion 1/2

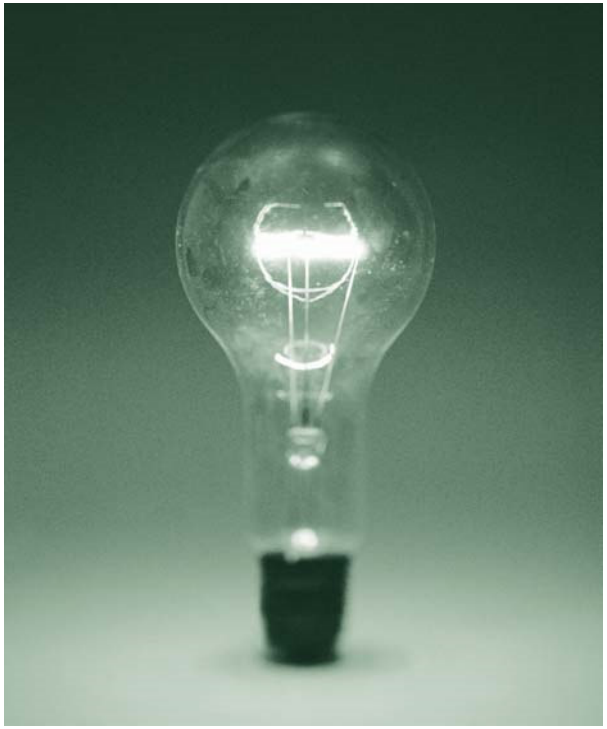
- **Face à une inévitable et constante augmentation des tentatives de captation d'informations, il est indispensable de mettre en place une politique DLP au sein de toute organisation,**
- **Une fuite de données entraîne des répercussions individuelles, institutionnelles ou économiques parfois graves, voire traumatisantes,**
- **DLP avec un L pour « Leak » : Fuite de données = « perte de contrôle » de l'information,**
- **Trouver le juste équilibre entre la protection des informations et leur accès légitime,**
- **Facteur humain = menace principale (volontaire ou non) pour intégrité et sécurité du patrimoine informationnel ?**

Conclusion 2/2

- Les limites de la DLP
  - Ne concerne que les données électroniques, ne peut remplacer une forte sensibilisation du personnel,
  - Prise de conscience du risque et de l'impact,
  - Les freins : forte implication du management et sensibilisation des utilisateurs,
  - La DLP dans le Cloud, la DLP sur le mobiles.
- Les forces de la DLP
  - Résident dans ses limites : la DLP doit être délimitée !
  - Permet de constituer une culture d'entreprise et une prise de conscience collective autour du patrimoine informationnel,
- La garantie à 100% n'existe pas.

Comme toute solution technique associée à un processus, elle répond à la problématique qu'on aura bien voulu correctement poser !

Questions ?



MANAGEMENT DE L'INFORMATION, DU RISQUE ET DE LA CONTINUITÉ D'ACTIVITÉ