Petite introduction à la protection du patrimoine informationnel

Bruno KEROUANTON, CISSP

Responsable Sécurité & Nouvelles Technologies

CLEAR CHANNEL France

17 septembre 2004 - Paris

De l’ère industrielle…

Dans le monde industriel du XIX^{ème} siècle :

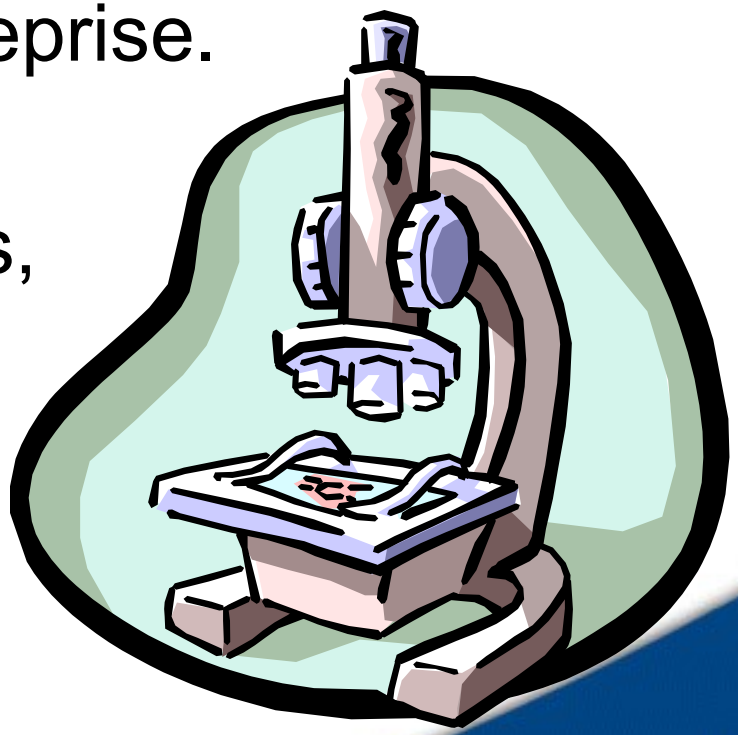
Ce sont les machines
et les outils qui créent
la richesse.

… à l'ère de l'information

- Au XXI^{ème} siècle, l'information est essentielle pour l'entreprise.

Idées, concepts, brevets, savoir faire, etc.

➔ Contribuent à la richesse de l'entreprise.



Le patrimoine informationnel

Concerne tous les domaines :

- Brevets, savoir-faire, procédés de fabrication
  - ➔ *Risque de contrefaçon ou clonage*
- Recherche et développement, prospective
  - ➔ *Risque de vol de concepts innovants*
- *Historique, bases clients et prospects*
  - ➔ *Risque de détournement de clients*
- *Données financières et stratégiques*
  - ➔ *Risque de déstabilisation, OPA, etc.*
- *Données personnelles*
  - ➔ *Atteinte à la vie privée, risque légal (CNIL)*
- *Etc.*
  - ➔ ***et là, le DG ne dort plus du tout !***

Comment protéger tout cela ?

Tout le contraire d'un bien matériel…

- Virtuel, impalpable.
- Duplication aisée, invisible, à faible coût.
- Contrôle de la diffusion difficile.
- Ils n'assurent pas, les assureurs !

Un premier bilan pessimiste

Postulat :

L'ère numérique a considérablement amélioré la communication de l'information en temps réel (média, réseaux, etc.)

ET

Les informations sont infiniment plus nombreuses (bases de données, etc.)

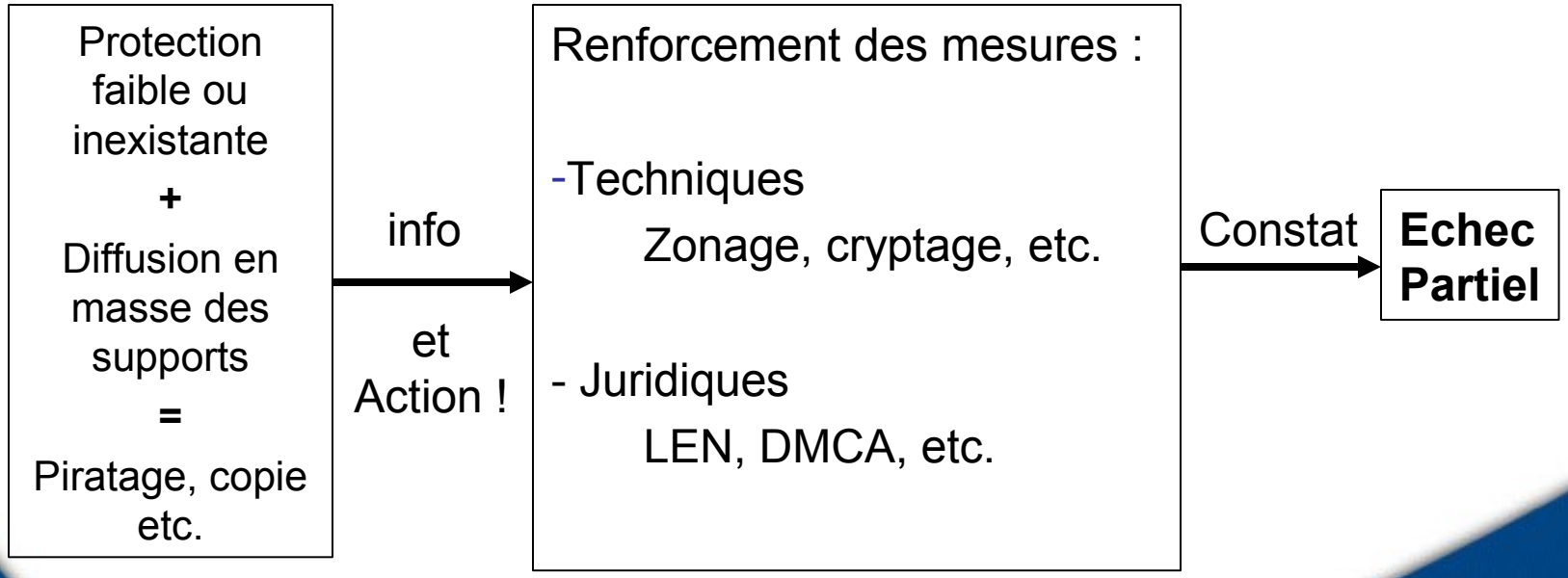
DONC

Les fuites et vols d'informations sont beaucoup plus fréquents…
(et le seront de plus en plus ?)

Petit exemple pris au hasard

Les atteintes à la propriété intellectuelle

(communément appelées DivX, Mp3 et autres bestioles)



Ce n'est pas simple… il manque sûrement quelque chose !

Les mesures « techniques »

- Sécurité des systèmes d'information

  Firewalls, chiffrement, authentification, etc.

- Sécurité physique

  Badges, caméras, gardiens, broyeurs, etc.

- Législation

  Contrats de travail, règlement intérieur, lois et décrets, etc.

Le facteur humain…

… c’est le souci numéro 1 !

- Diffusion par erreur

  erreur de manipulation d’un logiciel, documents imprudemment laissés sur un bureau ou dans une imprimante, bavardages, forums internet etc.

- Manipulation par autrui

  ingénierie sociale, sondages, téléphone ou messagerie, flatterie, pressions etc.

- Mauvais jugement

  erreur d’appréciation de la criticité de l’information manipulée, une fois hors contexte (annuaire interne).

- *Etc.*

Sensibiliser et impliquer

Nécessité de sensibiliser à tous les échelons

- Par une culture d'entreprise adaptée,
- En illustrant par des exemples courants,
- En présentant l'ingénierie sociale (démonstration ?),
- Par des règles appropriées.

Sensibiliser et responsabiliser

- Ne pas se reposer aveuglement sur les outils de sécurité, car le maillon faible de la chaîne sécurité, c'est souvent l'utilisateur.

- Inciter à adopter un « réflexe » sécurité en permanence, pas seulement face à son poste de travail : documents papier, conversations, déplacements, etc.

- Ne pas hésiter à utiliser : règlement intérieur, charte informatique, clauses de confidentialité, etc. pour responsabiliser.

- Dans certains secteurs sensibles, une formation complémentaire peut être justifiée.

Le projet « cercles de diffusion »

Acteurs :

Directions de l'entreprise : ressources humaines, informatique, communication, direction générale.

Objectif :

- établir une liste des informations « sensibles »,
- identifier les flux et canaux de diffusion,
- recenser les émetteurs, intermédiaires et destinataires,
- optimiser les canaux de diffusion si nécessaire,
- sensibiliser et responsabiliser.

Classification des informations

Civil	Militaire	
Public	Non classifié	Sites web, communiqués de presse, plaquettes commerciales, etc.
Interne	Restreint	Données du personnel (salaires etc.), reporting, procédures, etc.
Critique / Sensible	Confidentiel	Plans de développement, achats stratégiques, R&D, etc.
Stratégique	Secret / Top secret	Données financières sensibles, rachats potentiels, etc.

« Un classique… oublié » !

Fuite involontaire d'informations

- Mauvaise compréhension des mécanismes de diffusion et de stockage de l'information sur Internet.
- Nomadisme et télétravail, portables volés, clefs USB perdues, etc.
- Logiciels et outils mal conçus, provoquant des fuites dans les documents.
- Etc.

➔ **Former et sensibiliser.**

Fuite volontaire d'informations

Risque faible, mais conséquences importantes.

Motivations de la personne indélicate

Argent, ego, amour, pouvoir, pressions

➔Permet parfois de retrouver l'individu par déduction.

Détection et suivi difficiles, mais possibles

Nécessite vigilance, temps, rigueur et souplesse.

Ex : insertion de « traceurs » dans l'information pour suivre son cheminement.

Dénouement

A l'amiable (discret) ou procès (retentissant).

Faits divers

Affaire DuPont (1989)

5 personnes impliquées pour vol de procédés de fabrication de l'élasthane (Lycra), exigeant 10M$ en échange des documents. Se finit en course poursuite autour du monde puis arrestation des malfaiteurs par le FBI et la police helvète.

Affaire Lopez (1993)

Un cadre de Volkswagen fournit des documents confidentiels à General Motors. Arrangement amiable entre les deux constructeurs automobiles : Volkswagen contraint d'acheter 1,1 Mds $ de pièces détachées auprès de GM en compensation.

Perspectives

- Failles logicielles
- Intelligence économique
- Désinformation - déstabilisation
- Cryptographie quantique ???

Ce n’est pas de la fiction, mais ne devenons pas pour autant paranoïaques !

Questions ?

CLEARCHANNEL

Vous pouvez me joindre en allant sur ***http://bruno.kerouanton.net/cv.php***