MEDEF Ile de France

Lundi de l'IE – 18 février 2013

ACCULTURATION AUX RISQUES NUMERIQUES

Pierre-Luc REFALO (DG adjoint)

INTERVENANT

Pierre-Luc Réfalo

DGa « business development »

Directeur associé : Activité « sensibilisation / formation »

Directeur du programme « Sécurité de l'information » *(1997 – 2002)*

Membre du Comité de Pilotage

Auteur des Livres bleus des Assises

Animateur du Groupe de travail « Fonction SSI » et « Economie SSI »

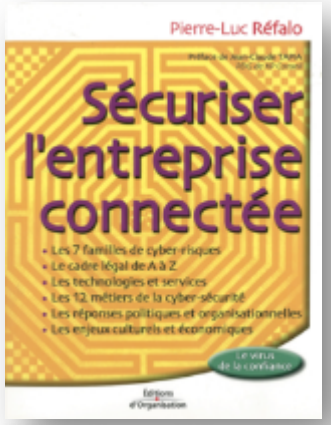
Pilote des enquêtes annuelles sur la « Fonction SSI »
et « Economie de la SSI »

INTERVENANT

Pierre-Luc Réfalo

hapsis

Auteur



2002

2012

FIC 2013

Prix du Livre Cyber 2013

Enseignement

utt université de technologie Troyes

ESIEE PARIS

TELECOM & Management SudParis

Conférences

lesassises de la sécurité et des systèmes d'information

FIC 2013

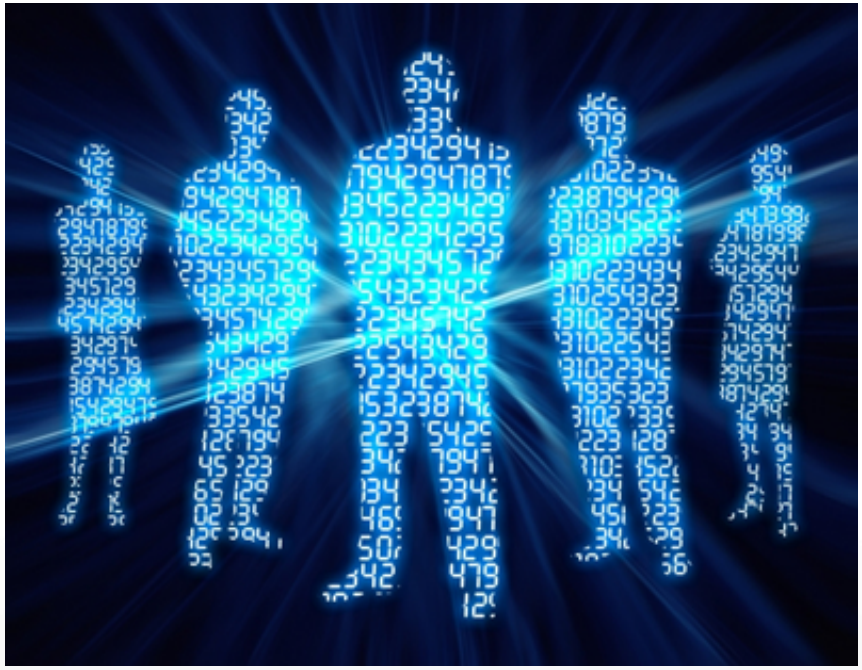
MET FOCUS

ISACA Trust in, and value from, information systems

Gartner

CSI COMPUTER SECURITY INSTITUTE

Pour plus d'informations, http://www.securitenumerique-entreprise.fr

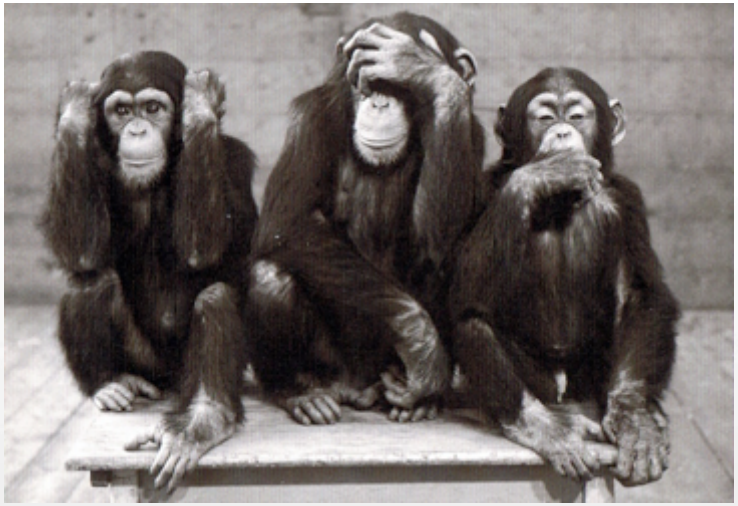


APPRÉHENDER LA COMPLEXITÉ

Comprendre d'où l'on vient, où on est …

Combien cette voiture a-t-elle de roues ?
Que représentent les équipements de sécurité routière ?
Quel est le « poids » du numérique dans sa conception / fabrication ?
Dans son utilisation ?

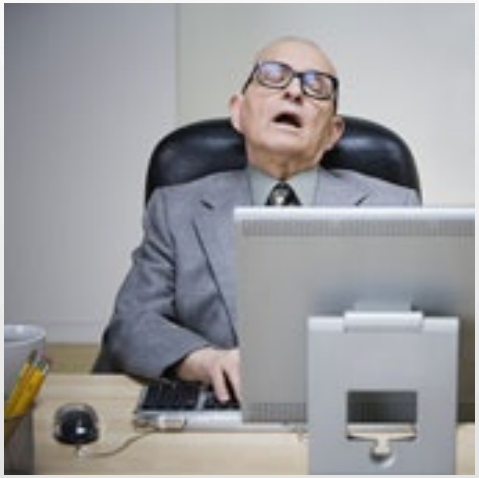
SÉCURITÉ : QUELQUES ATTITUDES



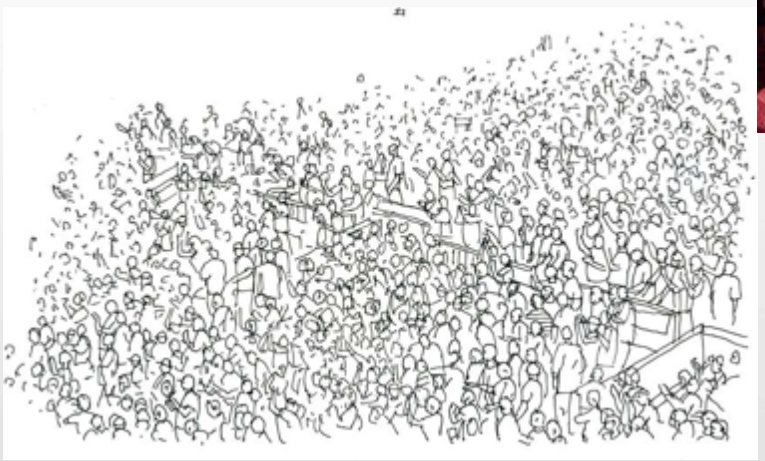
SÉCURITÉ SI : QUELQUES ATTITUDES

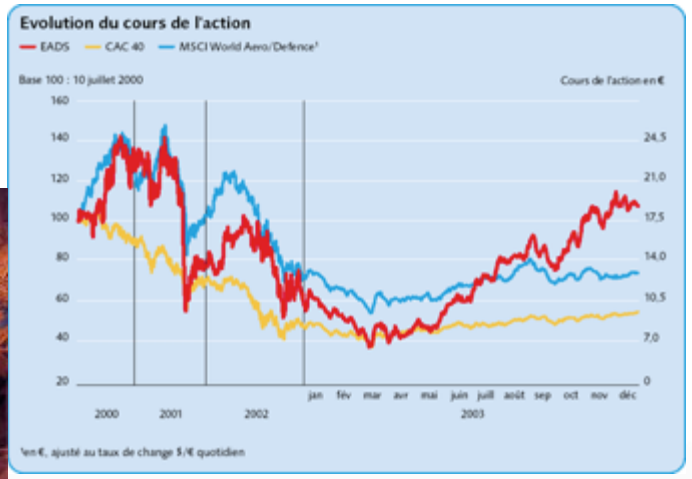
SÉCURITÉ SI : QUELQUES ATTITUDES

ET LES DIRIGEANTS ?



POSTURE MANAGÉRIALE (1/2)





« Après moi le déluge ! »

POSTURE MANAGÉRIALE (2/2)

« J'voudrais bien, mais … »

LE MONDE REEL (1/3)

LE MONDE REEL (2/3)

Les données « personnelles » et bancaires : une cible privilégiée

RSA SECURITY™

ALLOCATIONS FAMILIALES

Quick

HEARTLAND BANK

LinkedIn

twitter

La faiblesse chronique de la gestion des mots de passe

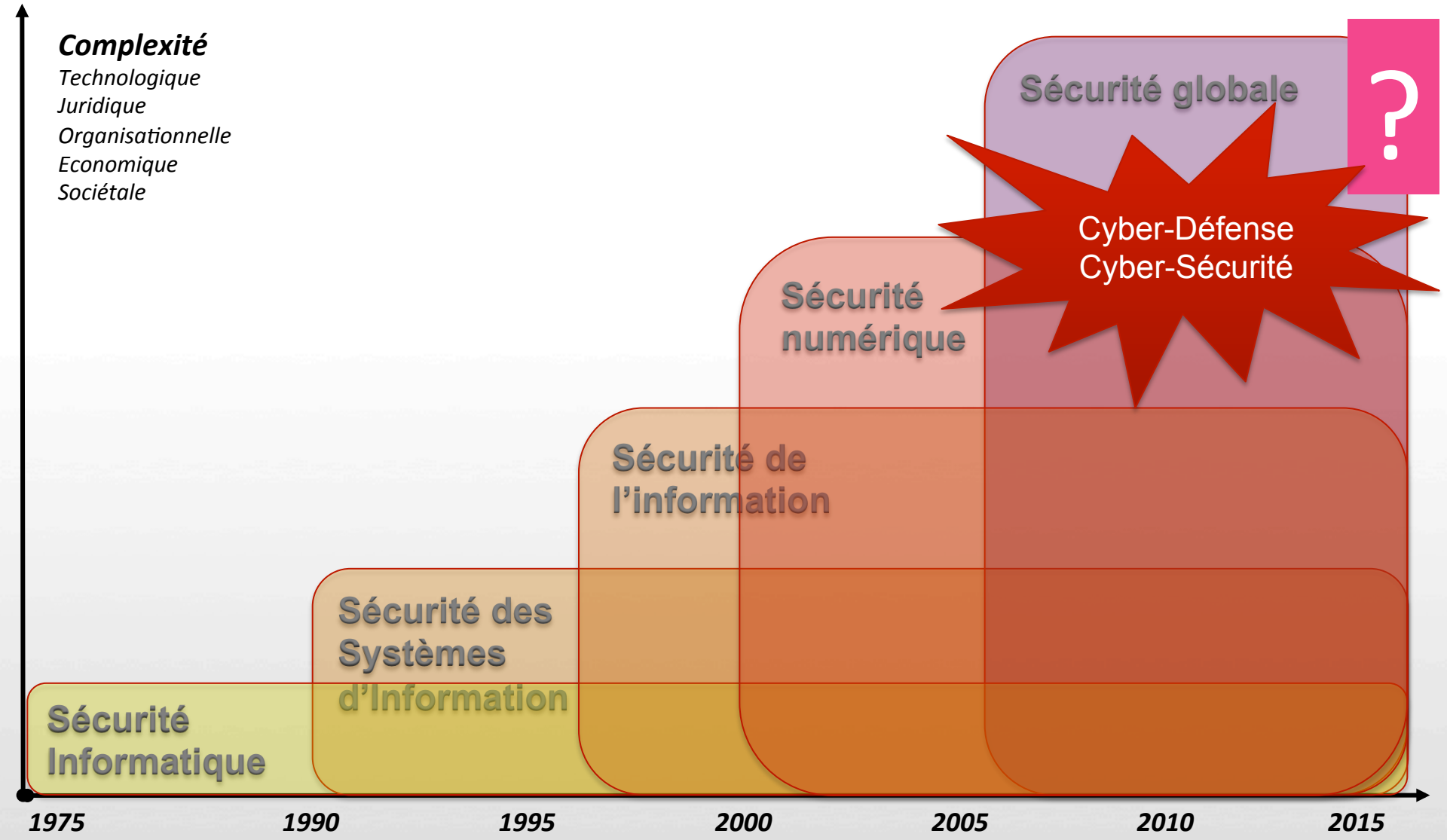
LE MONDE REEL (3/3)

Les atteintes au secret :
un sport international

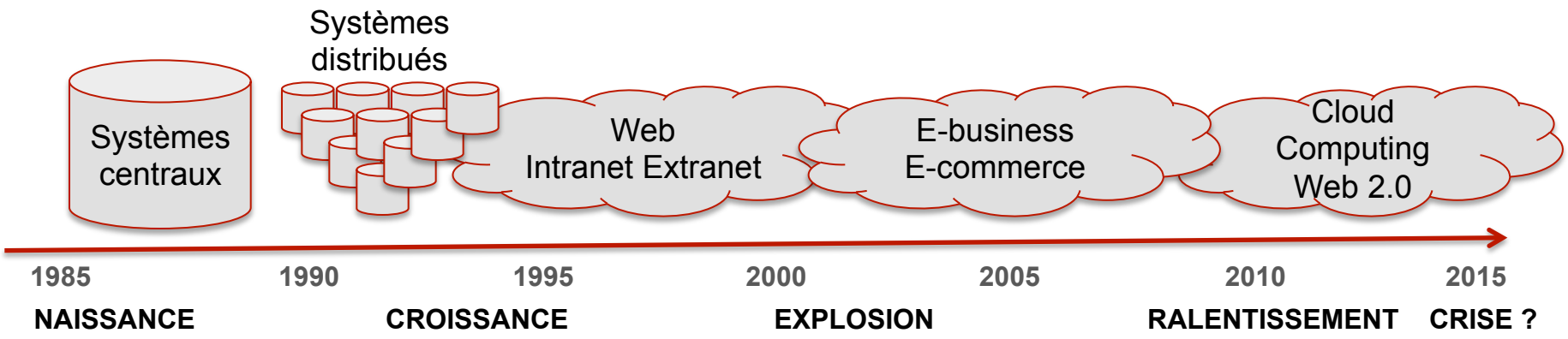
AREVA

clearstream

VASTE, COMPLEXE, IMMATURE



UN MARCHE ATOMISE



1- Gestion des accès et continuité (méthodes et scénarios de risque)

2- Marketing de la peur « Internet » (attaques logiques)

3- Protection du patrimoine (sécurité économique)

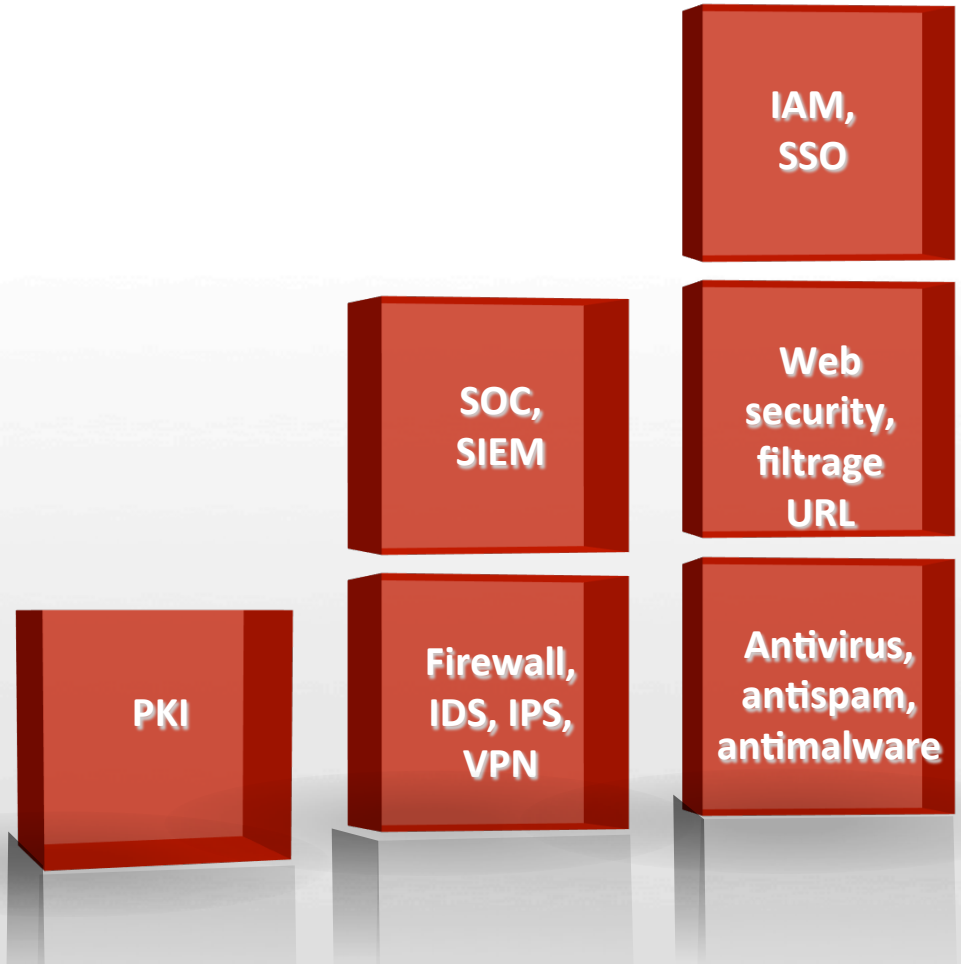
4- Dématérialisation (confiance numérique)

5- Sécurité globale

?

LES OUTILS SE SONT EMPILES

La sécurité progresse-t-elle ?
Les risques sont-ils correctement couverts ?



LA “FOLIE” REGLEMENTAIRE

QUELQUES ENJEUX MAJEURS

Les Echos CONFÉRENCES

1ère conférence annuelle
SÉCURITÉ DE L'INFORMATION NUMÉRIQUE 2012
Protéger le patrimoine informationnel pour gagner en compétitivité

Juin 2012

« On est en train de prendre conscience qu'on quitte les rives du patrimoine matériel pour se rendre vers la protection **du patrimoine immatériel**. »

« Le problème de fond, dont on ne parle pas assez, c'est **l'identité numérique. »**

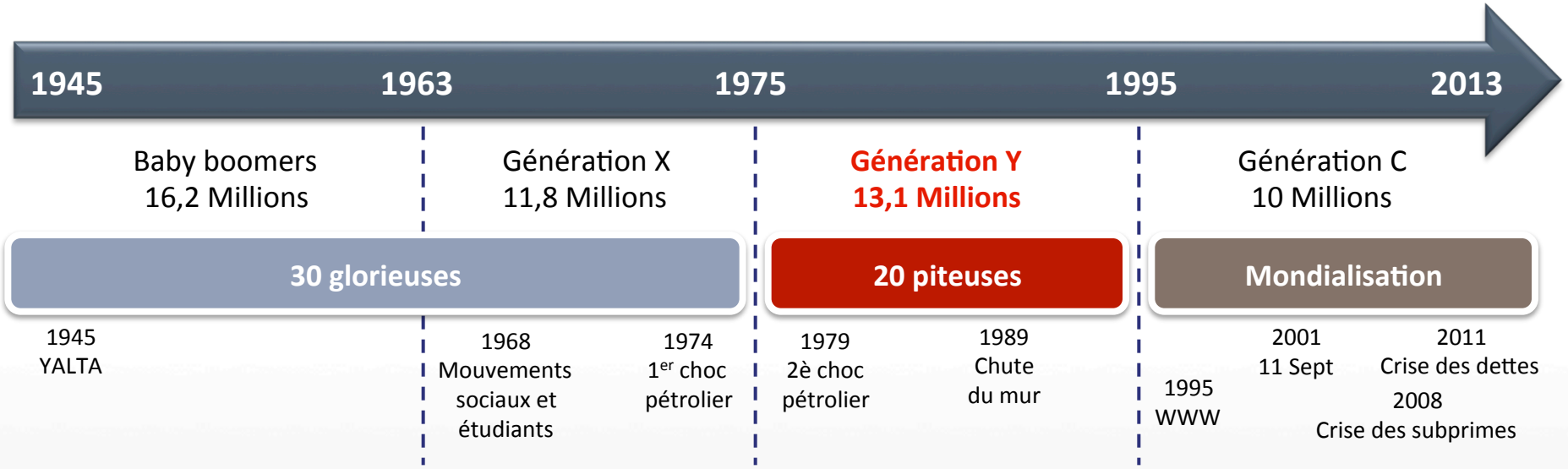
« Le cybercrime n'est pas très méchant, il ne fait qu'exploiter la stupidité et la gentillesse des gens. **Les organisations cybercriminelles ont des revenus supérieurs à ceux de n'importe quelle grande entreprise mondiale et fonctionnent selon les règles de l'économie de marché.** »

Rapport parlementaire « Cyber Défense » - sept 2012 (Rec n°18)

*« Faire de la protection des systèmes d'information une véritable priorité en matière de management des entreprises en **sensibilisant les dirigeants et en rehaussant le niveau hiérarchique et le rôle des responsables de la sécurité informatique**. »*

SÉNAT

3 GENERATIONS AU TRAVAIL



Découvrent Internet

A la retraite **Dans l'entreprise** **A la maison** **A l'école** **Au berceau**

Rois du paradoxe !

Transparence vs secret dans la sphère publique / privée

Défiance vs négociation dans l'entreprise (cyber-surveillance)

Pratiques plus sécuritaires parfois (smartphones)

DES MENACES STRATEGIQUES

Lucratif : 400 Mds de dollars (OCDE)

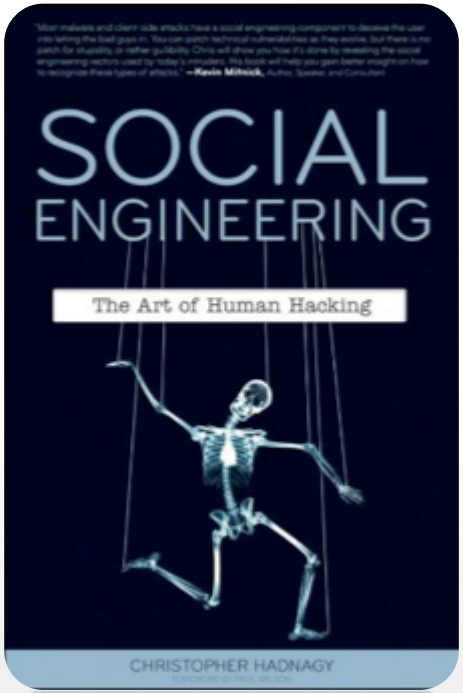
Impunité : Dimension internationale, à distance

Idéalistes : Défense des libertés individuelles et de la vie privée, lutte contre les dictatures, pédophiles et scientologie

Ambigus : liens avec LulzSec (pirates), violation de données personnelles, actions en occident mais en Chine ?

ANONYMOUS : AMBITION 2013

VIEILLE COMME LE MONDE



Le piratage informatique est un jeu d'enfant ?
Hacker le cerveau humain : encore plus !

RÉSEAUX SOCIAUX : LA MINE D'OR

- Vidéo belge

INCERTITUDE …
CE QU'ON NE SAIT PAS (BIEN) …

- Si on a été, est ou sera victime … ni de qui, et de quoi, ni quand
- Classifier et gérer la confidentialité / le secret (matériel, immatériel) dans le numérique
- Valoriser les actifs immatériels (réputation, …)
- Si des textes / législations conduiront à une meilleure professionnalisation (ex : le DPO, CPO)
- Avenir d'Internet (neutralité, surveillance, monopoles, noms de domaines, …)

LE TROUSSEAU A 5 CLES

Entre fondamentaux et innovations …

LES 3 PILIERS DE TOUTE “CONSTRUCTION”

L’art du compromis

Le bon usage des technologies

L’acculturation des acteurs

RÈGLES

RESSOURCES HUMAINES

OUTILS

L'HUMAIN : MAILLON FAIBLE …

… OU DERNIER REMPART ?

La Lettre du Plan Séisme – Juillet - Août 2008

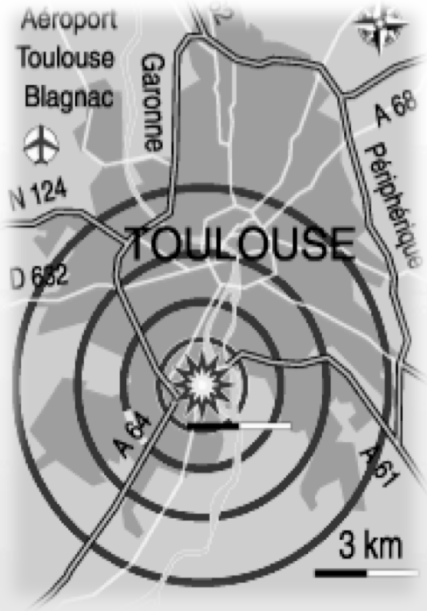
Lors du tsunami qui a accompagné le violent séisme de Sumatra en décembre 2004,

une jeune fille ayant appris à reconnaître les premiers signes d'un tsunami au cours d'une leçon de géographie a réussi à sauver sa famille ainsi que d'autres personnes dans une station balnéaire de Thaïlande.

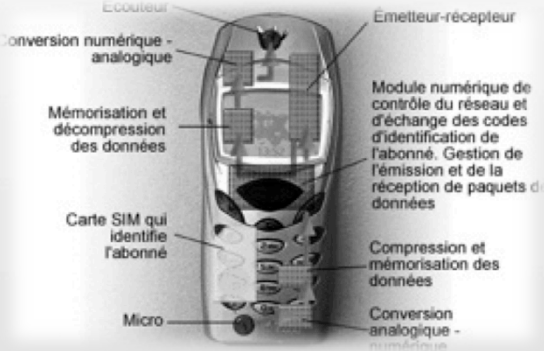
CLÉ N°1 : CULTURE DU RISQUE (1/4)

CLE N°1 : CULTURE DU RISQUE (2/4)

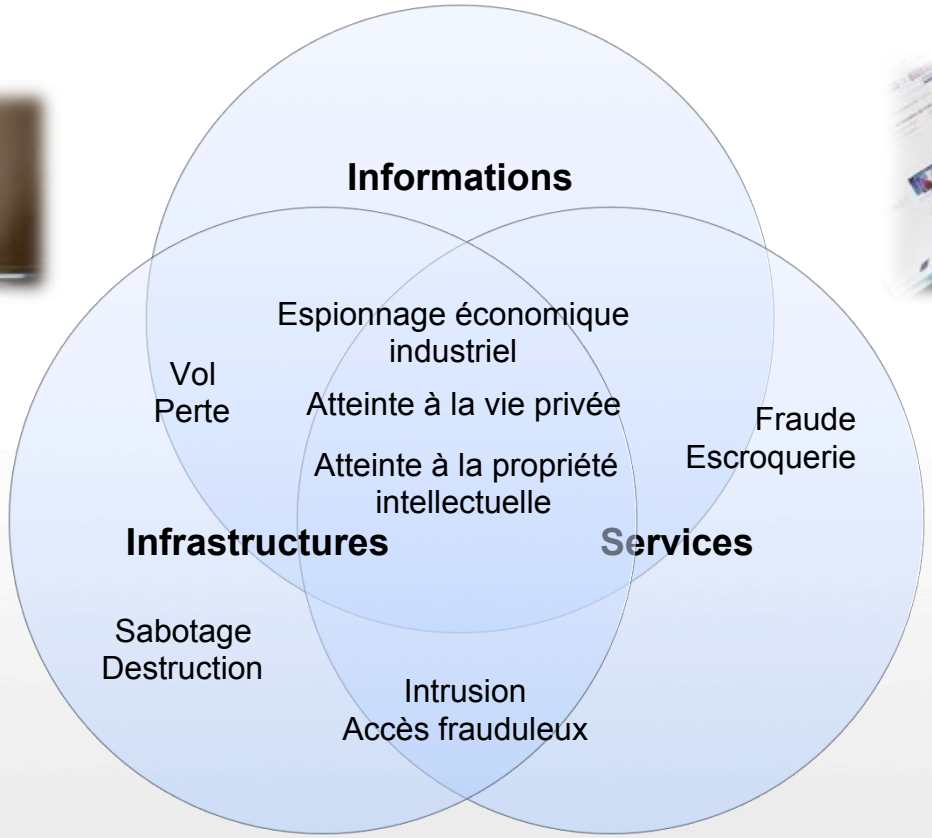
CLE N°1 : CULTURE DU RISQUE (3/4)



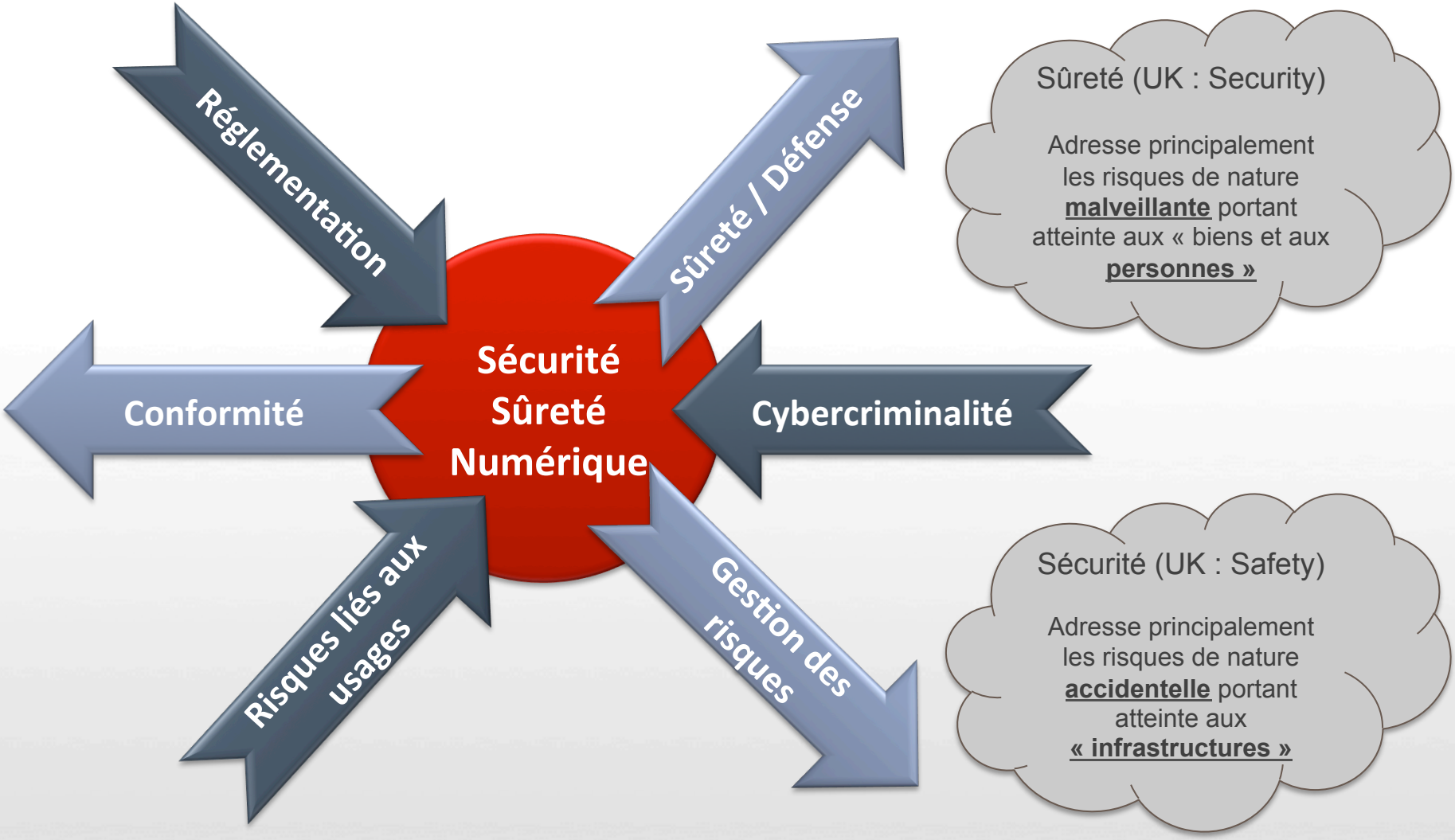
CLE N°1 : CULTURE DU RISQUE (4/4)



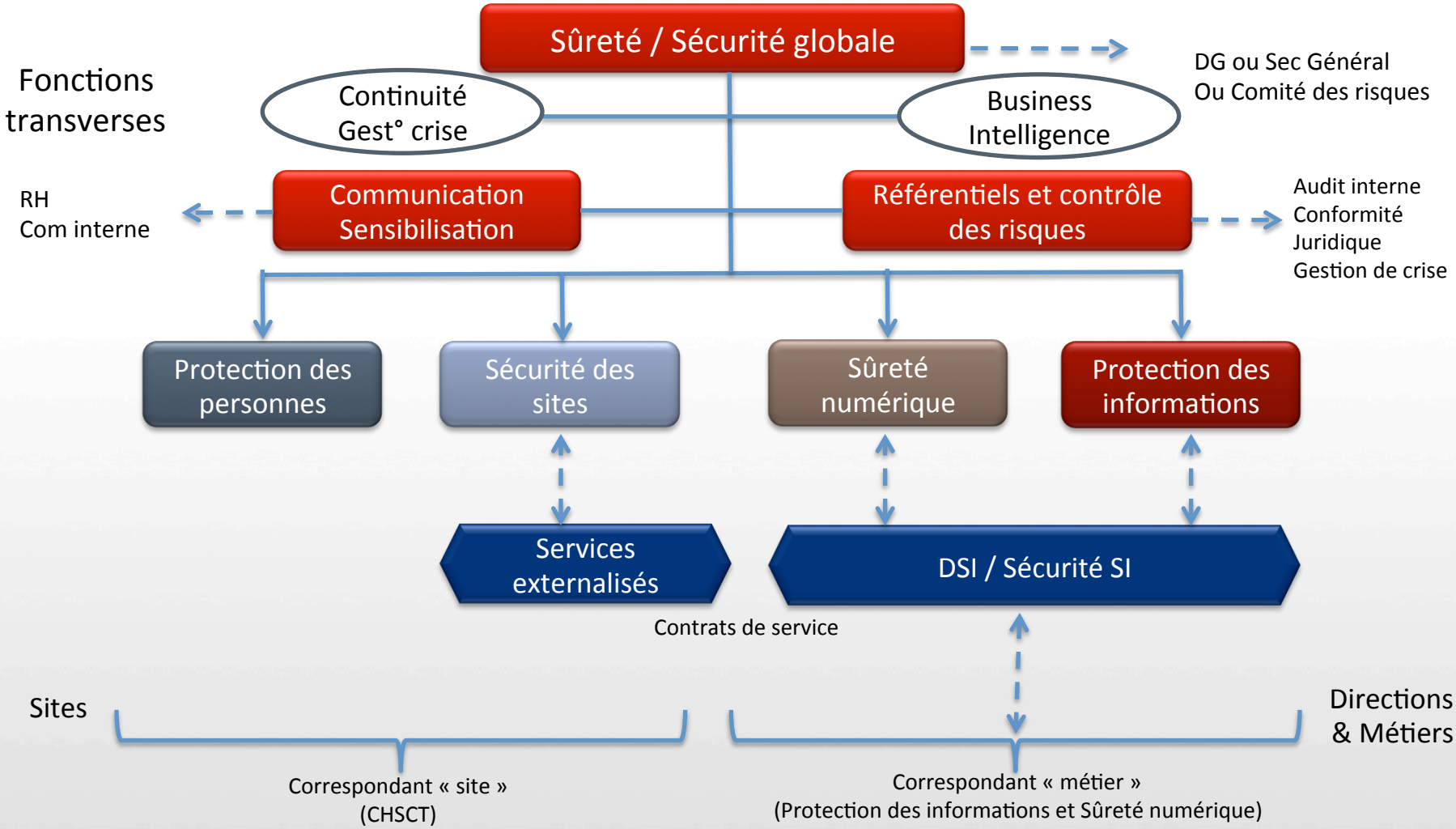
MODELE DES CYBER-RISQUES



DES TENSIONS ORGANISATIONNELLES



GOUVERNANCE CIBLE

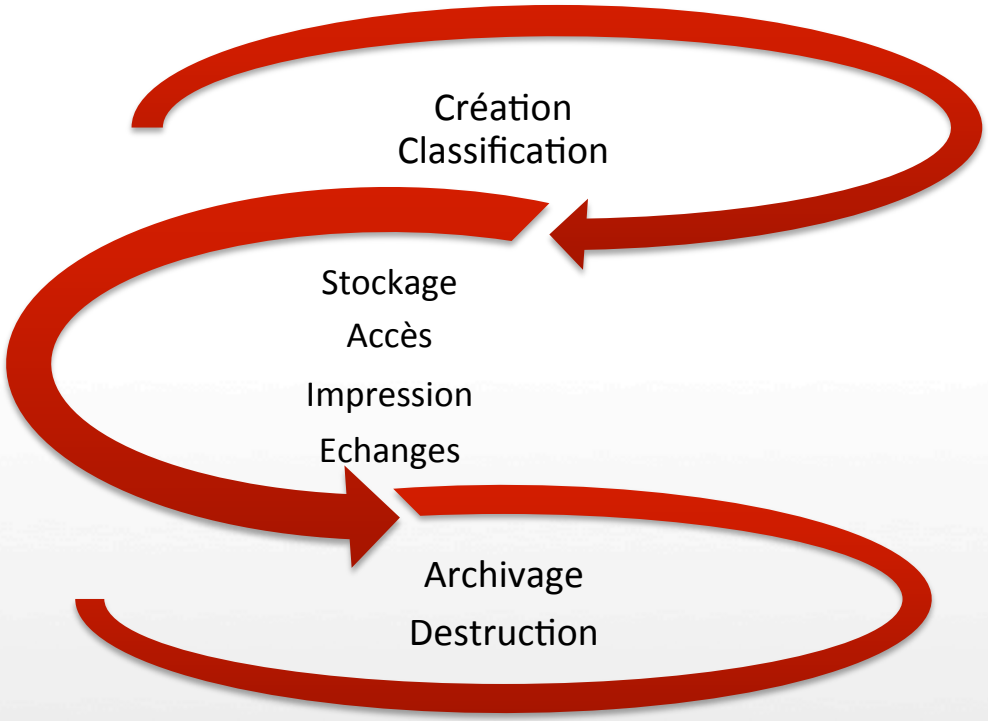


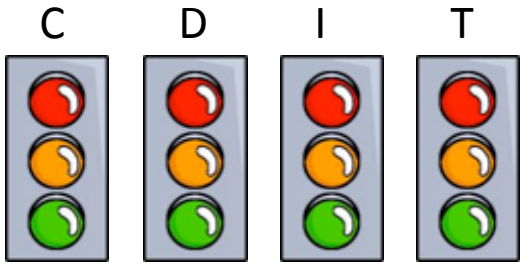
« Imaginez le pire,
vous ne serez pas déçu ! »

Winston Churchill

L'INFORMATION : QUELLE VALEUR ?

LA CLASSIFICATION EN PRATIQUE





Quelles sont les mesures de prévention / protection associées à chaque niveau de classification selon la nature, le support et le cycle de vie de l'information ?

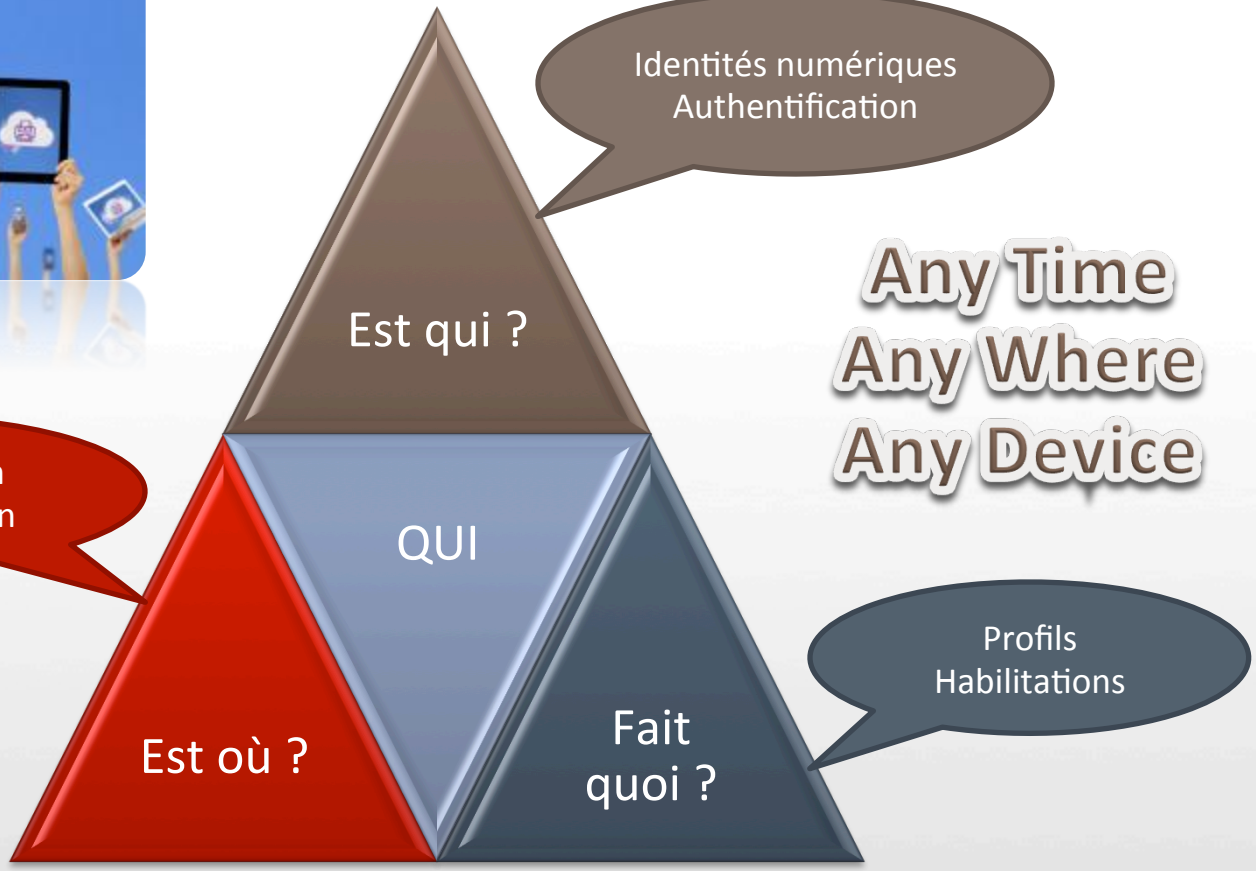
CLÉ N°2 : LA CULTURE DU SECRET

La tension : Secret vs Transparence

PROPRIETE VS PARTAGE

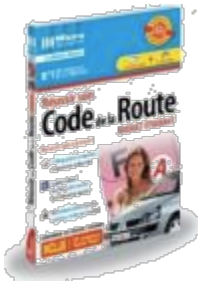
Locationlonguedurée

CLE N°3 – LA CULTURE DE L'ACCES



Any Time
Any Where
Any Device

ANALOGIE ROUTIERE

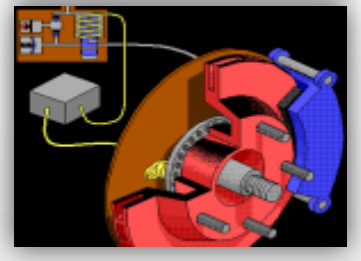


Prévention

Education

Protection

Dissuasion



Détection

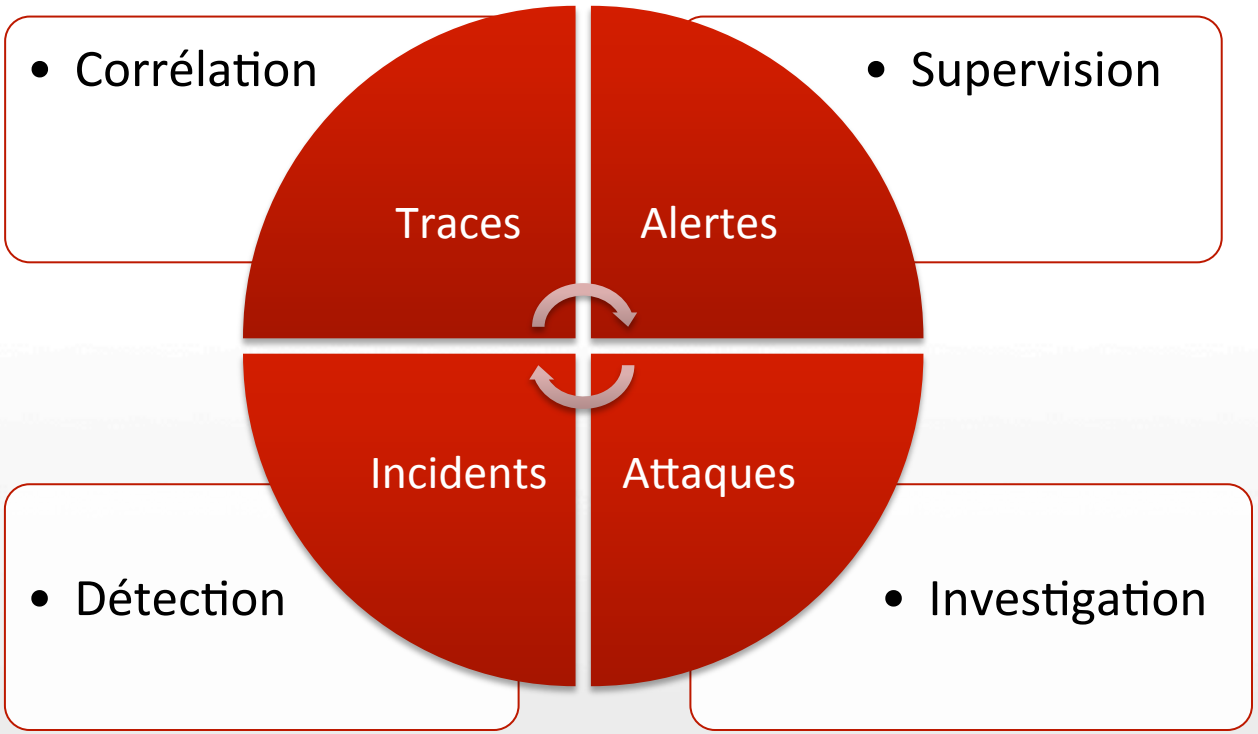
Répression

Réaction

Motivation

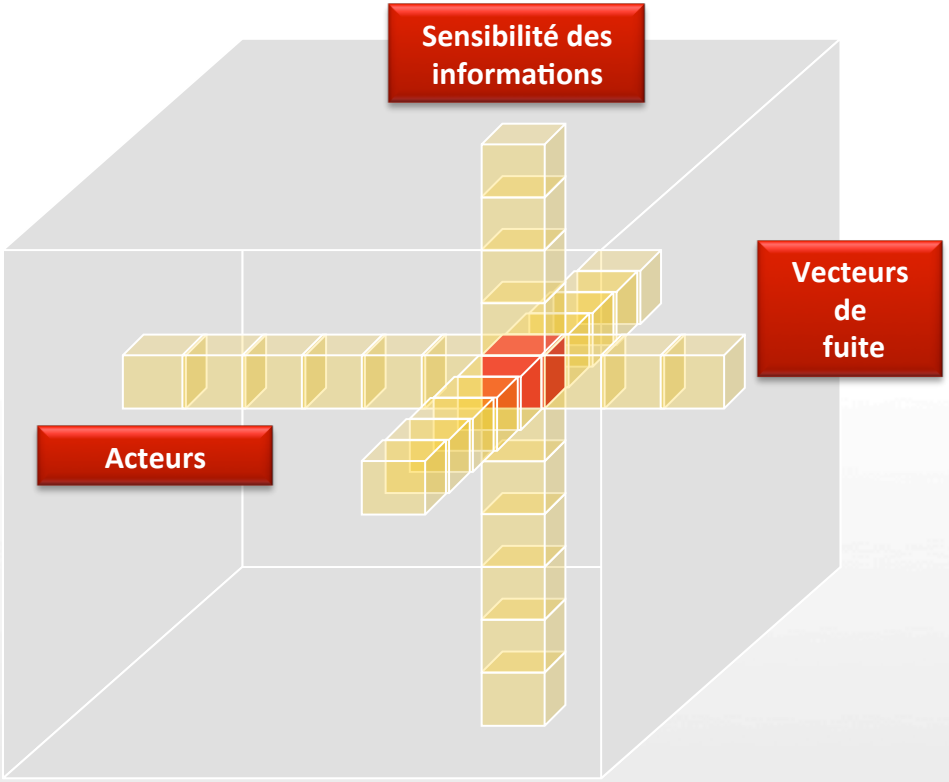
CLÉ N°4 - LA CULTURE DU CONTRÔLE
SIEM ET CYBER DÉFENSE

Menaces et attaques externes



Comment détecter, identifier, corréler, analyser, investiguer
des évènements anormaux et menaçant ?

CLÉ N°4 - LA CULTURE DU CONTRÔLE
FUITES ET DIVULGATIONS D'INFORMATION



Inconsciences et négligences internes

Comment accompagner efficacement la mise en œuvre d'un processus de détection des fuites d'information ?

DES SYSTEMES AUX USAGES

Normal
Approprié
Toléré

Anormal
Inadapté
Inapproprié

Abusif
Interdit
Illégal

UNE AFFAIRE DE COMPORTEMENTS

MALVEILLANCE

Des collaborateurs portent atteinte aux intérêts d'autrui

EXCÈS DE CONFIANCE

Les collaborateurs considèrent que les mesures de sécurité les protègent bien

CONTOURNEMENT ET DÉROGATION

Les collaborateurs trouvent des voies de contournements aux règles autorisées ou non

RÉSISTANCE AUX PROCESSUS

Les collaborateurs résistent aux règles "perturbantes" ou "dévoreuse de temps"

IGNORANCE DES RÈGLES

Les collaborateurs ne peuvent pas appliquer des règles qu'ils ne connaissent pas

INCONSCIENCE DES MENACES

Les collaborateurs ne perçoivent pas la menace ou les dangers

Des solutions toujours utiles

Des arbitrages essentiels DG / Métiers / SI / SSI

Une charte fondamentale

L'exigence du contrôle et de l'audit

Les apports de la sensibilisation

LE CAS DE LA CHARTE

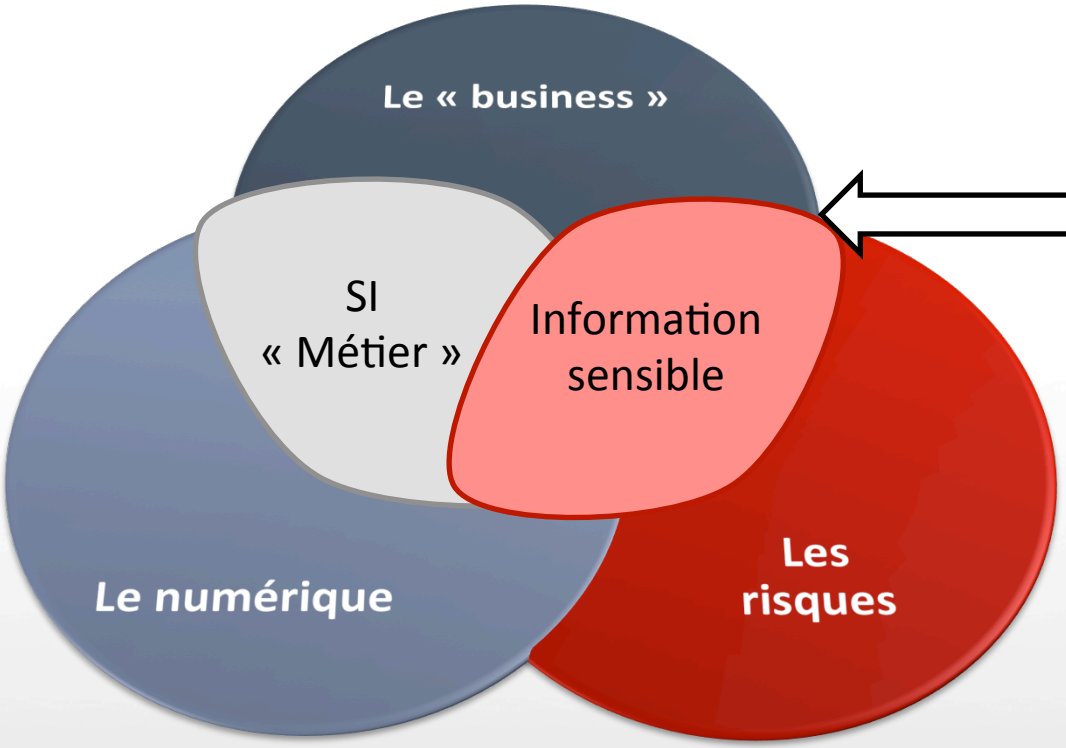
La charte des obligations et des devoirs

L'engagement individuel selon les usages

Nous avons tous été victimes d'ingénierie sociale !

IL FAUT QUE VOUS M'AIDIEZ …

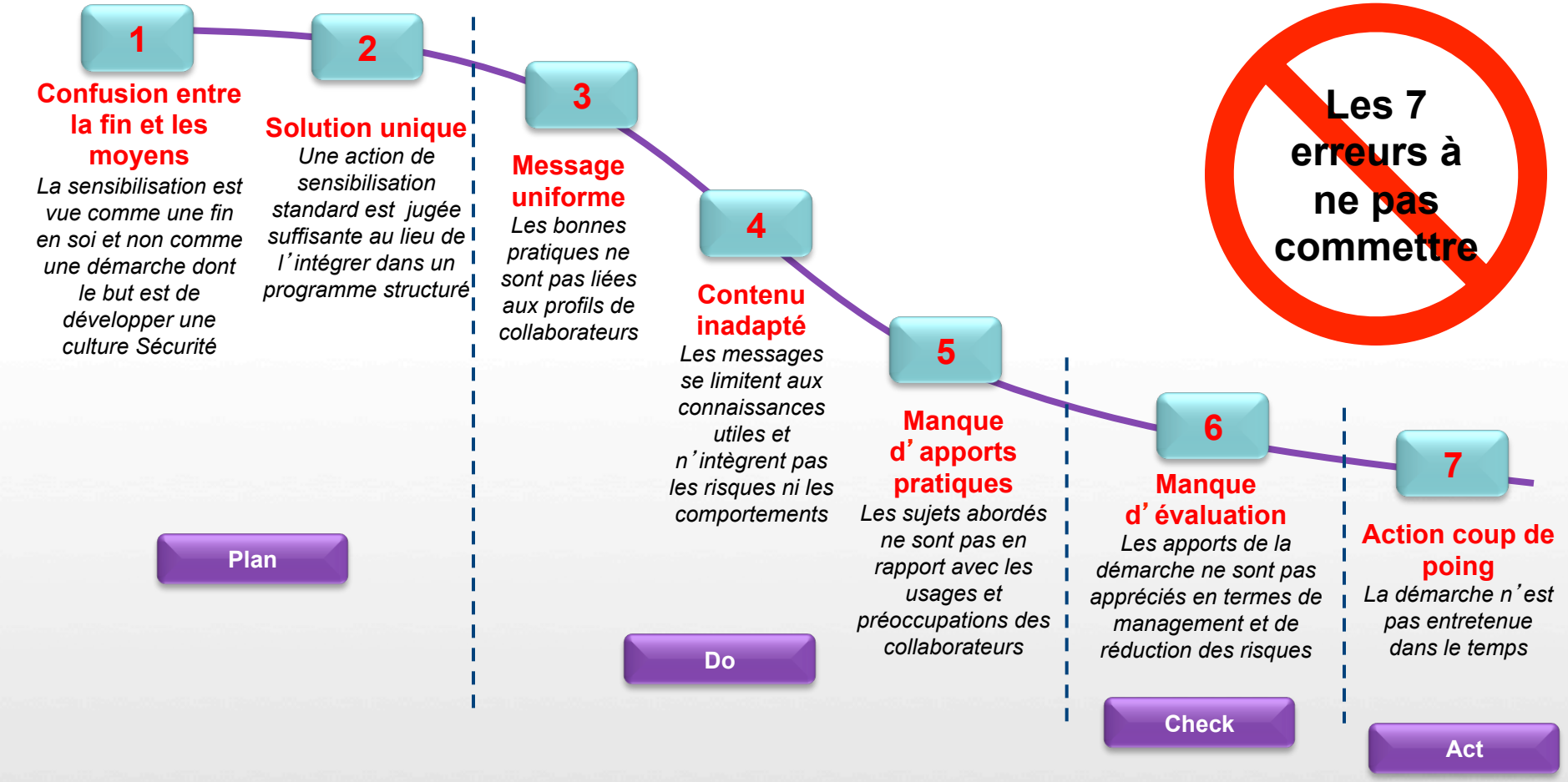
CLE N°5 - ACCULTURATION "RISQUES NUMERIQUES"



Développer une culture de protection des informations et de sécurité / sûreté numérique

« Acculturation : processus selon lequel un individu ou un groupe d'individus acquiert une culture qui lui est étrangère »

CLE N°5 - DE L'ACTION AU PROCESSUS



*Selon **Information Risk Executive Council**, 2006*

CLE N°5 : DANS LA PRATIQUE

Stratégie

Pourquoi ?
Pour qui ?
Quoi ?
Comment ?
Quand ?
Avec qui ?
Combien ?

Boite à outils

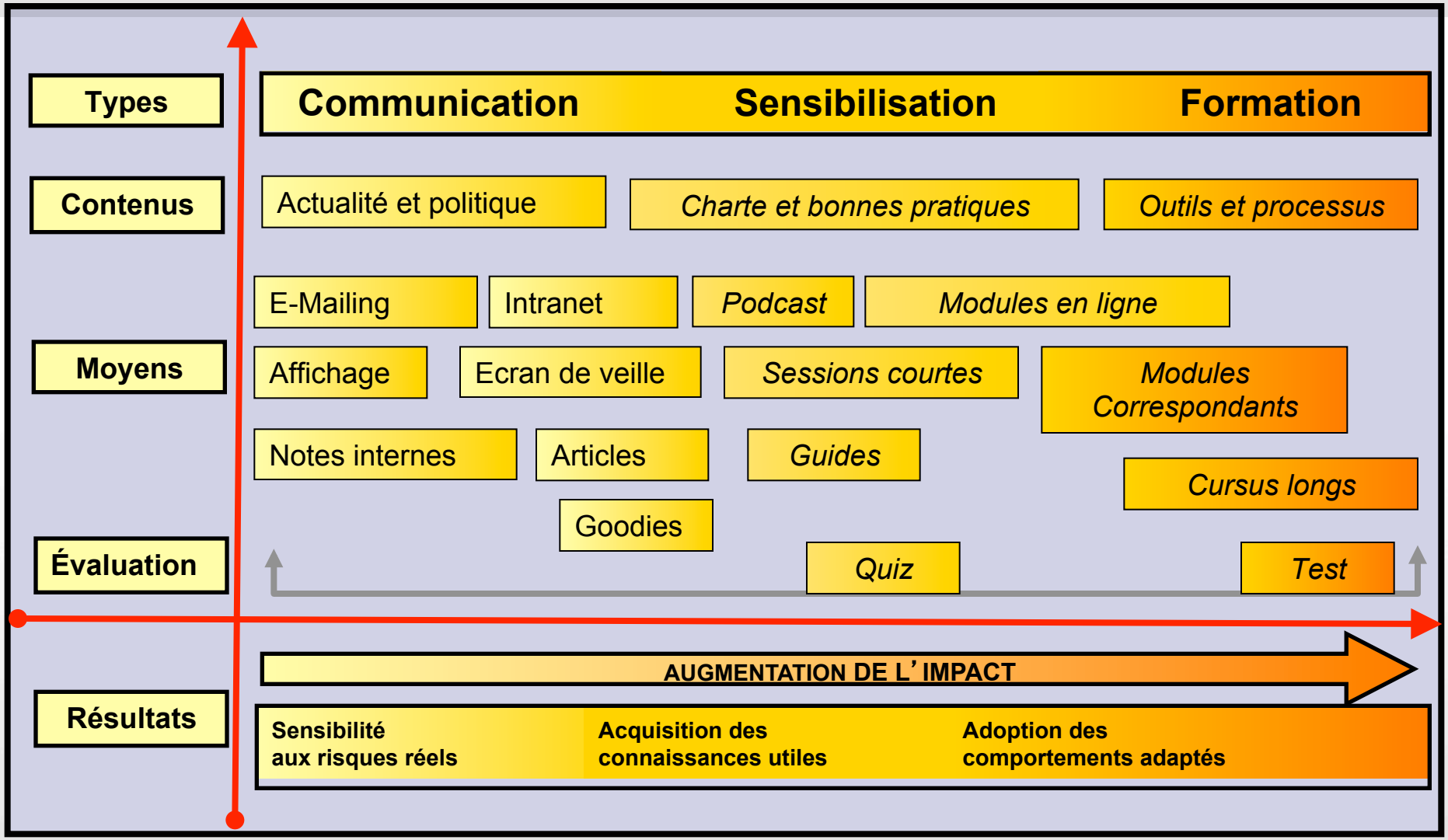
Communication
Sensibilisation
Formation

Indicateurs

Maturité
Sensibilité
Connaissances
Comportements

Un processus d'acculturation n'a de sens que s'il s'appuie sur une stratégie et sur la production d'indicateurs.

CLE N°5 : LA BOITE À OUTILS



« Si vous pensez que l'éducation coûte cher, essayez l'ignorance. »

Abraham Lincoln

PERSPECTIVES

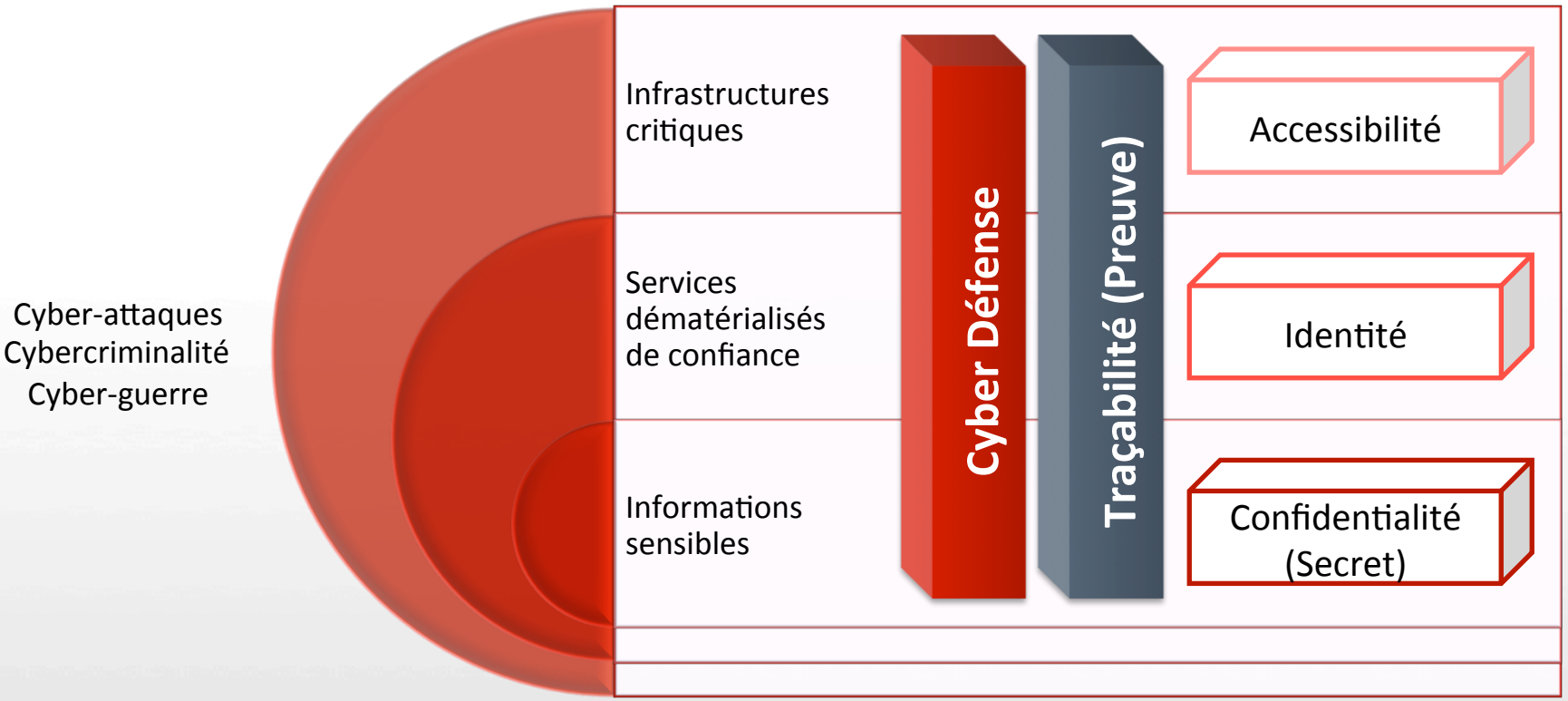
De nouveaux modèles …

MESSAGE CLÉ

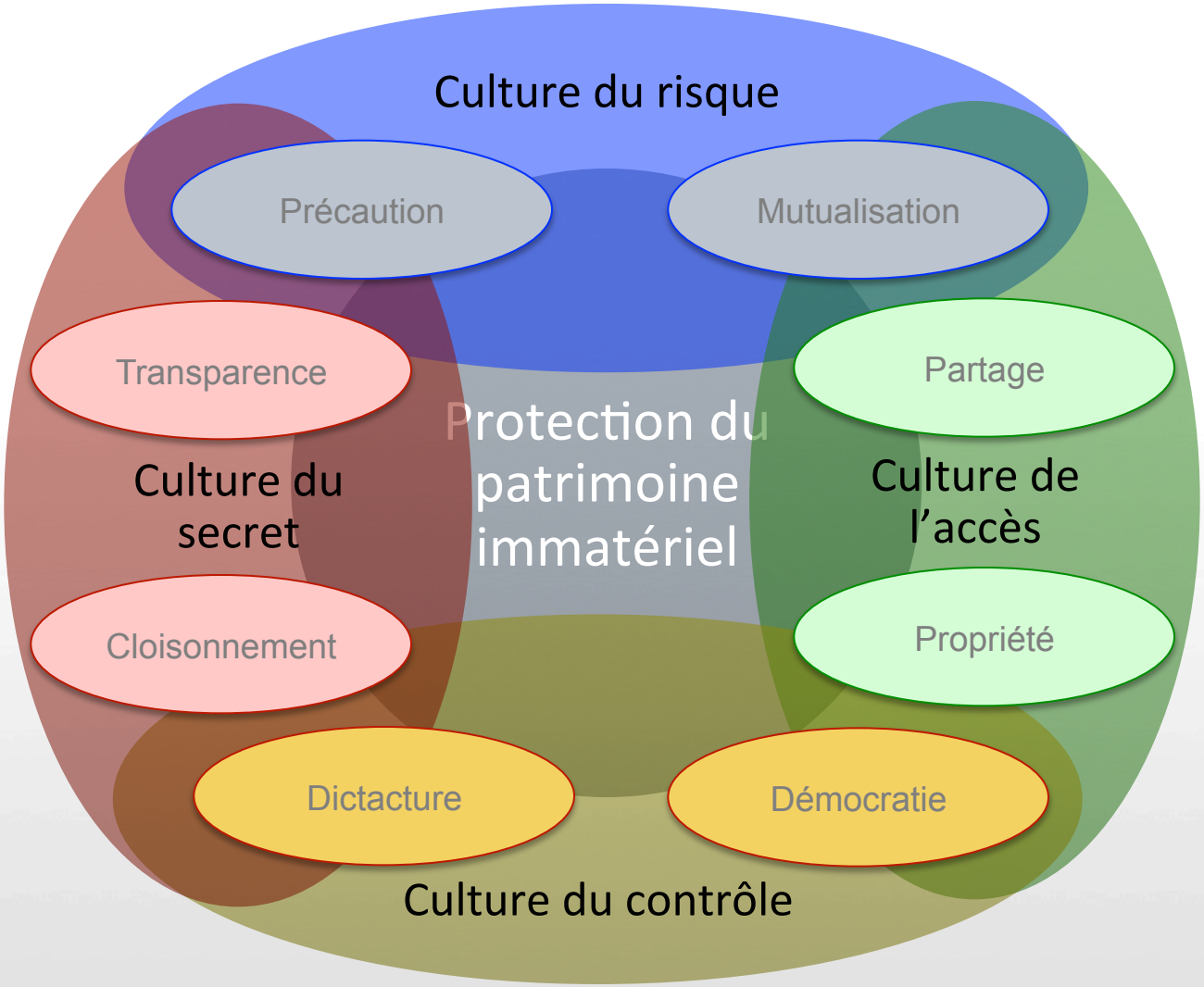
« La perfection est atteinte, non lorsqu'il n'y a plus rien à ajouter, mais lorsqu'il n'y a plus rien à retirer. »

Antoine de Saint Exupéry

MODELE DE GOUVERNANCE
SIMPLIFIER LE CHAMP DE LA SECURITE NUMERIQUE



MODELE DE L'ACCULTURATION
ORIENTER LES CHOIX « POLITIQUES »



A RETENIR

« Réglementer et outiller sans acculturer n'est que ruine de la sécurité ! »

MERCI

POUR ALLER PLUS LOIN

Retrouvez- moi sur le web :
www.securitenumerique-entreprise.fr

Suivez-moi sur Twitter : www.twitter.com/plrefalo

Ecrivez-moi : plrefalo@hapsis.fr