

# Les défis de la Sécurité IT en temps de crise

CSO Interchange  
9 Juin 2009, Paris

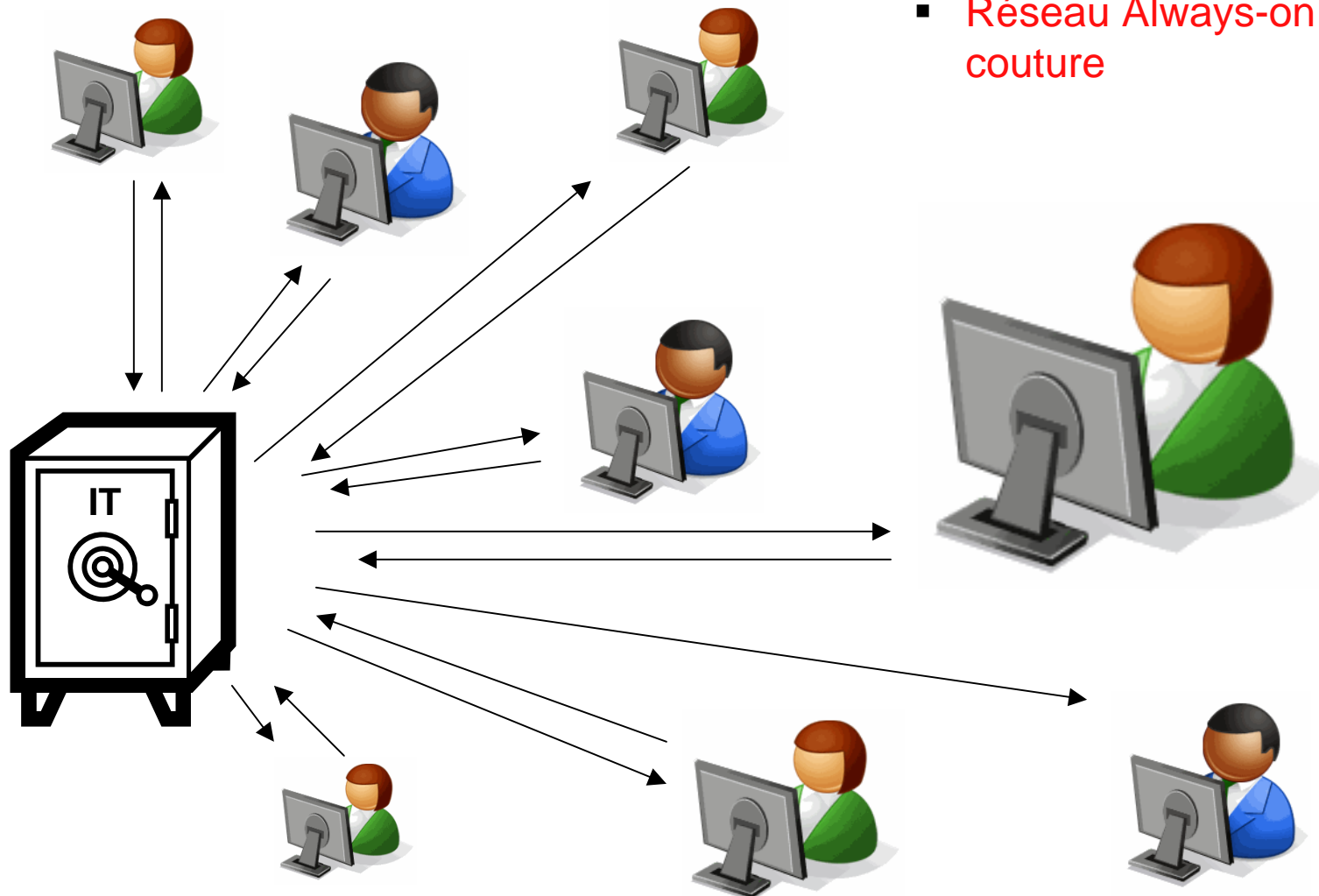
Eric DOMAGE



# Notre problème à tous en 2009 ...

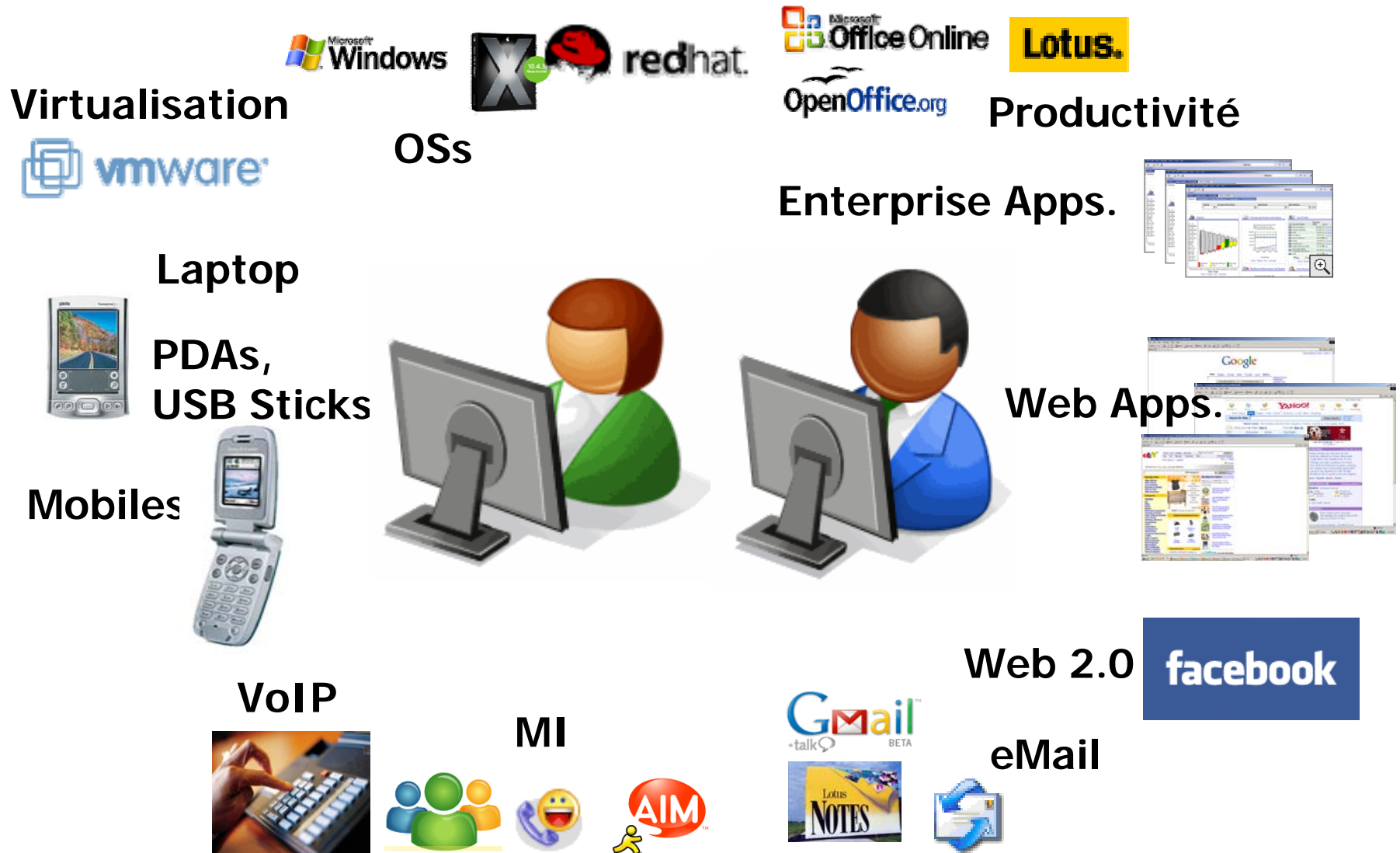


# L'utilisateur est agile...mais dangereux !



- Ubiquité pour tous
- Réseau Always-on / Sans couture

# Le paysage de la menace : vue incomplète !



# L'utilisateur est un vrai cauchemar !

L'utilisateur :



**...est un indispensable !**

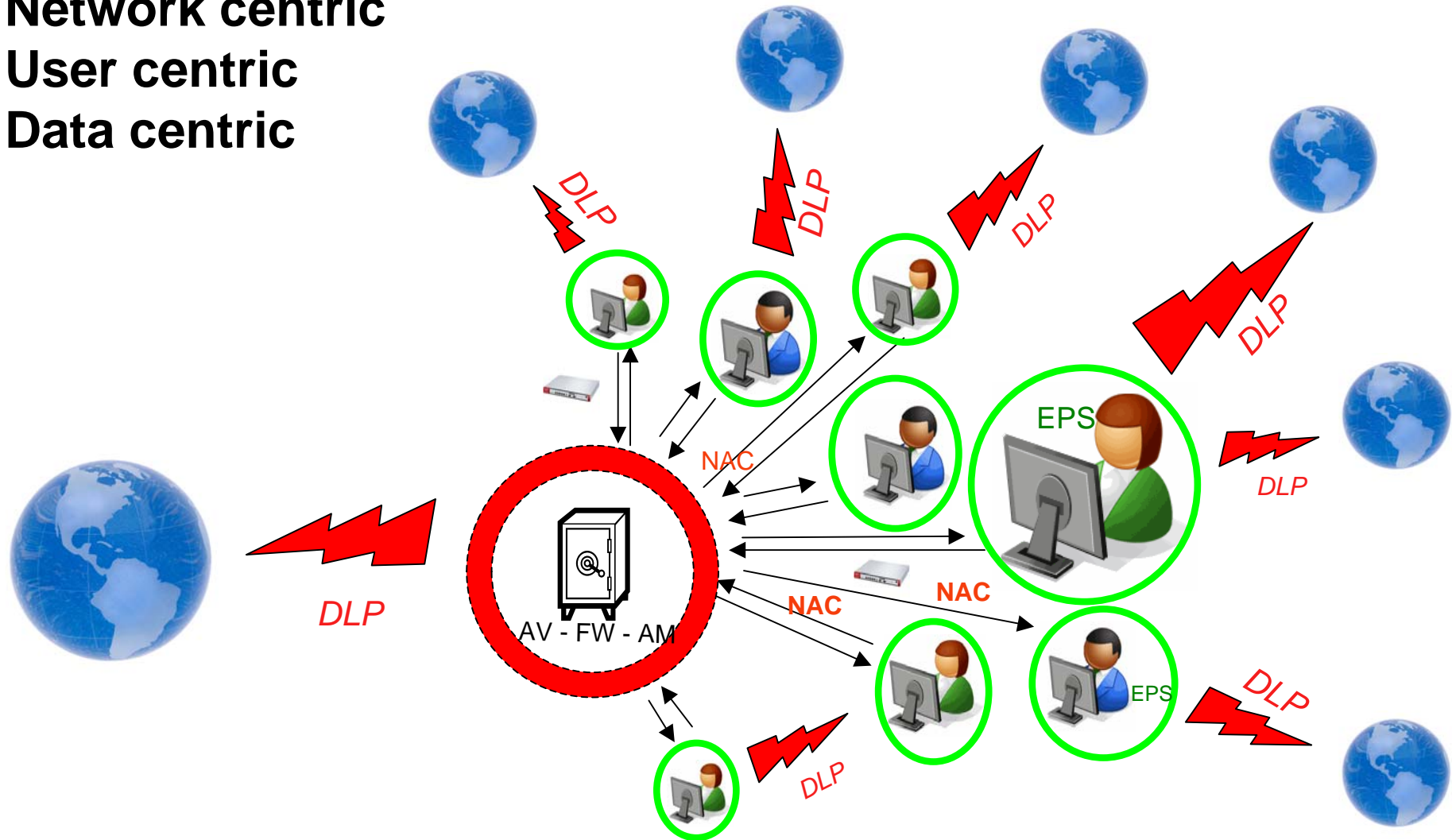
- Don d'ubiquité, fournisseur de productivité (travailler plus...)
- Accès permanent, réactivité, inventivité

**...et génère les crises !**

- Ignore, le risque, les alertes et la douleur IT ...
- Confond Vie pro et vie perso
- Préfère le confort à la sécurité
- Raconte sa vie sur FB, TW et autres

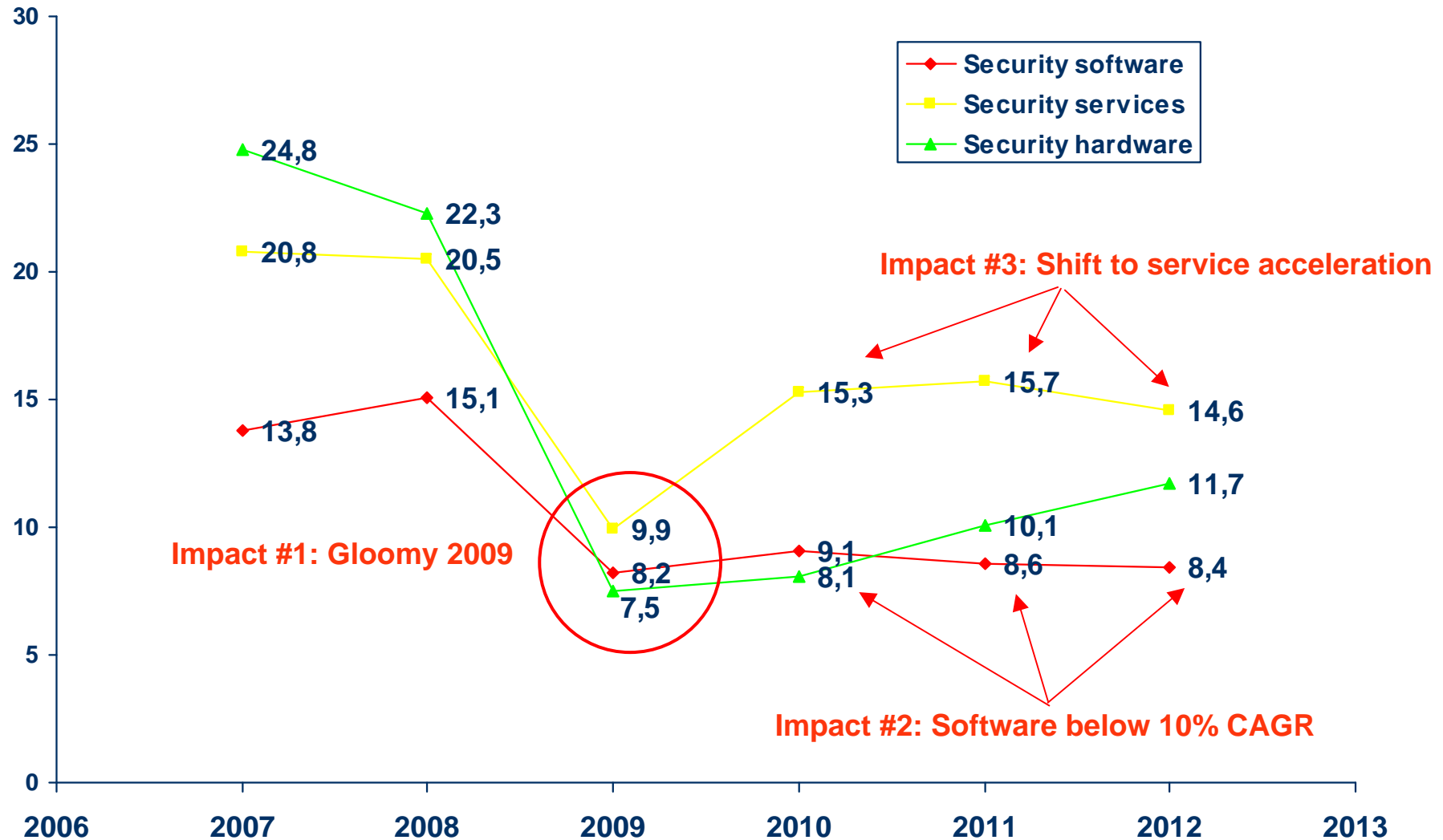
...

**Network centric**  
**User centric**  
**Data centric**



# **Evolutions de marché 2009**

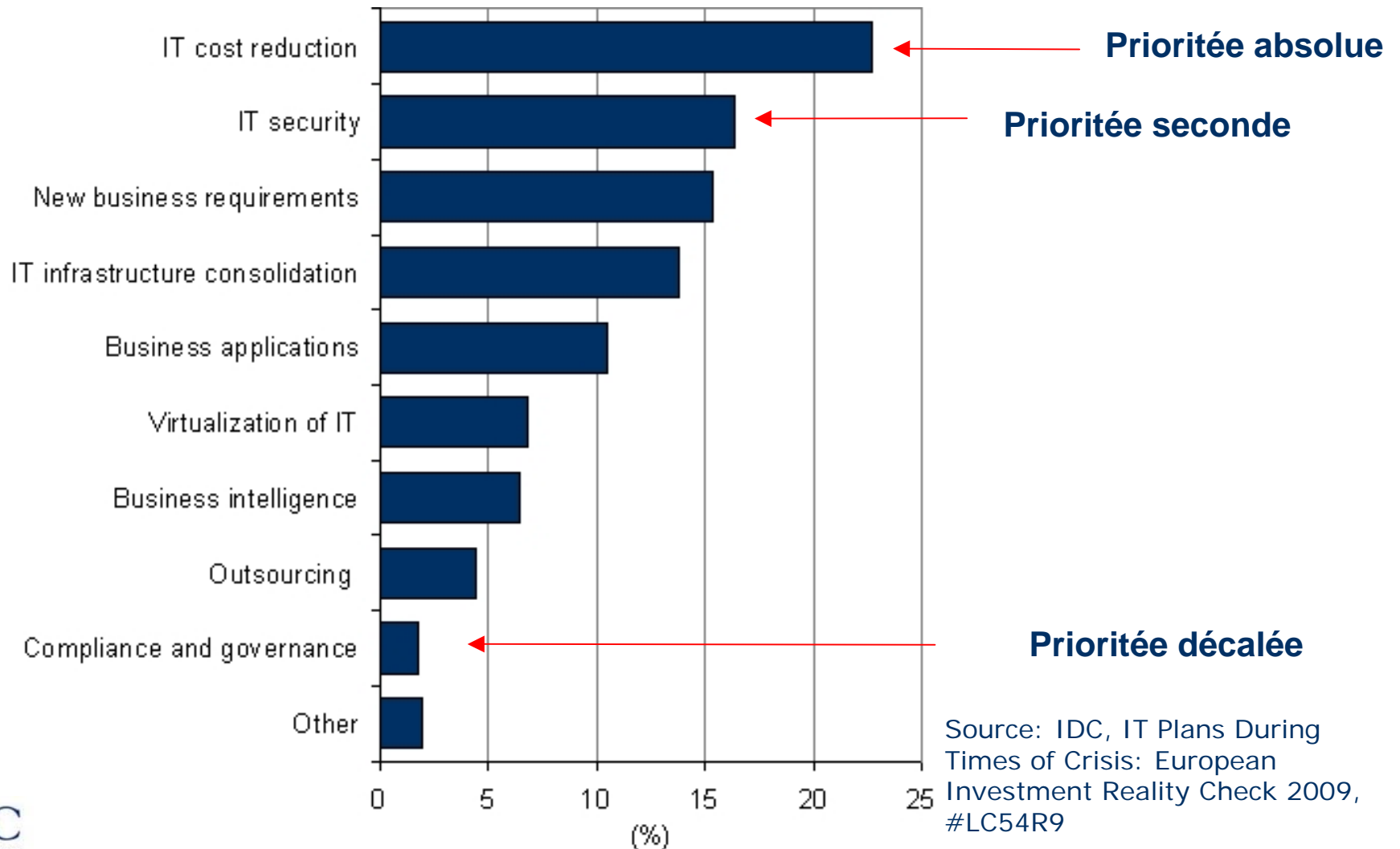
# WE Security Markets Updated – Forecast 2008–2012 (%)



# WE Reality check, IDC Survey Feb.2009 n: 515 – IT Decision Makers



Q: Please select, from the following list, your top IT priority for the next 12 months



Source: IDC, IT Plans During Times of Crisis: European Investment Reality Check 2009, #LC54R9



## - Recherche de l'efficacité financière

- Calculs de ROI (Externalisation)
- Expression de besoin réaliste
- Liens entre projets (DLP/IAM/SIEM)

## - La réduction de budget est-elle possible ?

- Consolidation des fournisseurs ? Migration vers le service ?

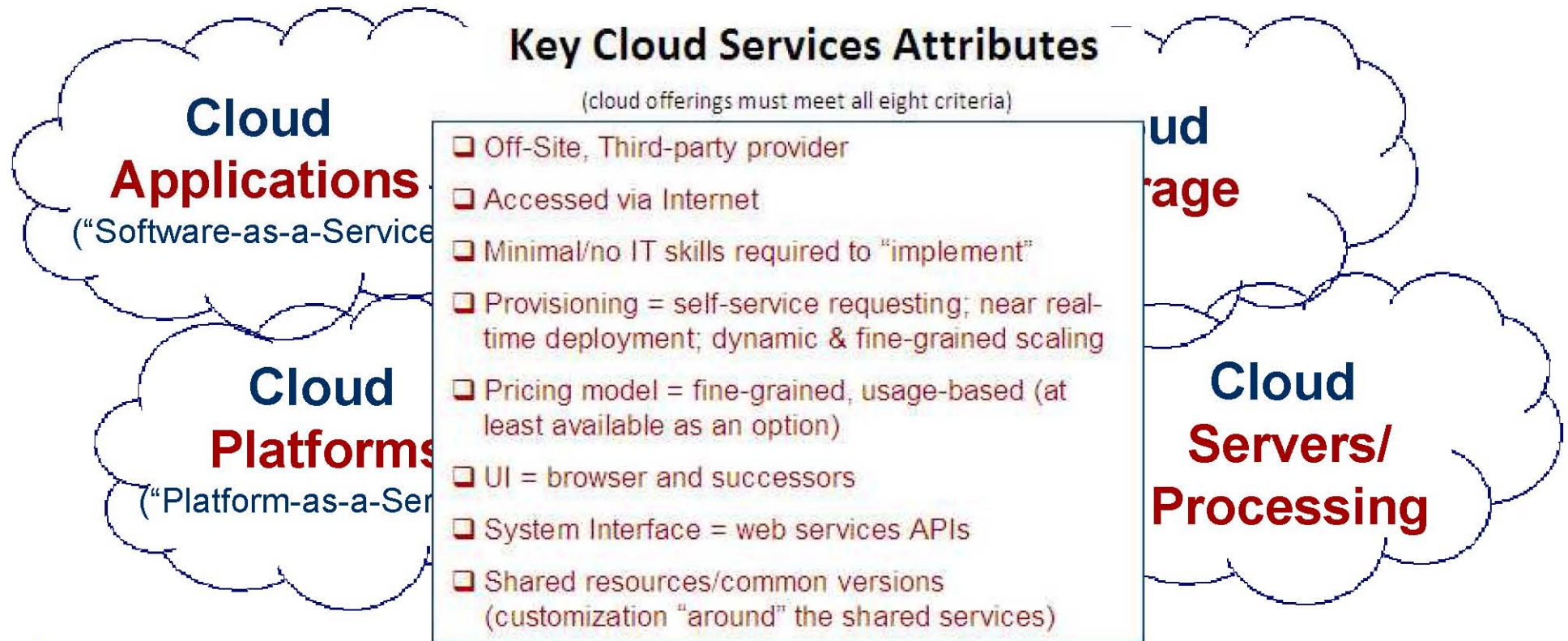
**Défi 1** : limiter la réduction des budgets, le gel des projets dans un univers toujours autant réglementé, pressuré par des périls évolutifs et des décisions d'entreprise " aveugles "

# Sécurité et Cloud Computing

# What Is **Cloud Computing**?

## **Cloud Computing**\* =

IT Capabilities Requested/Provisioned/Delivered/Consumed  
 in (near) Real-Time Over the Internet



\* a.k.a. IT Cloud Services

1. Les types de Cloud sont très variés (Private, Public, Managed, Hybrid), appelant des **niveaux de contrôle, de qualité et de sécurité très variables ! Traçabilité ?**
2. Le nombre de fournisseurs sur 1 projet de Cloud est....incertain. Portabilité des contrats, dilution des responsabilités, conformité des accès tiers...**Qui sont les acteurs de mon cloud ? Quelles responsabilités ? Quelles réglementations ?**
3. **Localisation : où sont les données ?**

Trois solutions semble s'imposer :

**DLP**, **SIEM** et la **fédération d'identité** pour traverser tous les nuages....et garder le contrôle des accès, des identités, des rôles, des conformités et de l'information.

**Defi 2**: garder le contrôle des Identités dans un univers dicté par des lois économiques. Agir plutôt que subir

# Sécurité et Virtualisation

Solution technique contrôlée en Interne  
d'optimisation/consolidation des ressources techniques pour  
un usage plus complet (Disponibilité, ROI, reprise...) sur un  
domaine localisé.

- Virtualisation du Stockage et de la Continuité
- Virtualisation du poste de travail
- Virtualisation des serveurs, CPU et puissance de production
- Virtualisation des accès et des réseaux sécurisés
- Virtualisation de l'OS, des applications, du test

Phénomène d'*Information Sprawl* (Extension anarchique de l'information)

*Plus d'information, plus distribuée, plus de points d'accès, plus d'accédants, plus de profils, plus de d'autorisations, plus de versions du même fichier....*

## **Besoin :**

- Gestion + fine des usages, des usagers et des faits (I/O)
- Gestion + fine du versionnage (Originaux, répliques, versions)

Quelques solutions émergent :



DLP : avec les solutions de discovery, data classification, Watermarking-finger printing, Network sniffing, Forensic and alert : le voyage des données et de leur usage devient visible en univers virtualisé et “ Cloud”

**Défi 3** : anticiper les conséquences de la virtualisation, envisager un discovery-tracking élaboré

L'IT est au coeur d'alternances technologiques majeures :

- **Dépéremétrisation** . Moins de frontières, moins de barrières = moins de points de contrôles physiques
- **Externalisation**. Plus de nuages, plus de tiers = plus de contrôle du nuage, dans le nuage.
- **Virtualisation** . Plus avec autant...

L'alternance technologique appelle plus de management centralisé (SIEM), plus de politiques globales, plus de contrôles aux bordures physiques, logiques et légales

De plus, une crise économique oblige à mieux dépenser...

Une seule règle : **anticiper** !

Merci de votre attention



**Eric Damage**

Program Manager,  
European Security Products  
and Strategies

IDC EMEA Software Group



13 rue Paul Valery

+33156262669

**+33607030776**

edamage@idc.com

[www.idc.com](http://www.idc.com)

