CNIS-Mag Event

Nouveaux besoins

+ Nouveaux usages

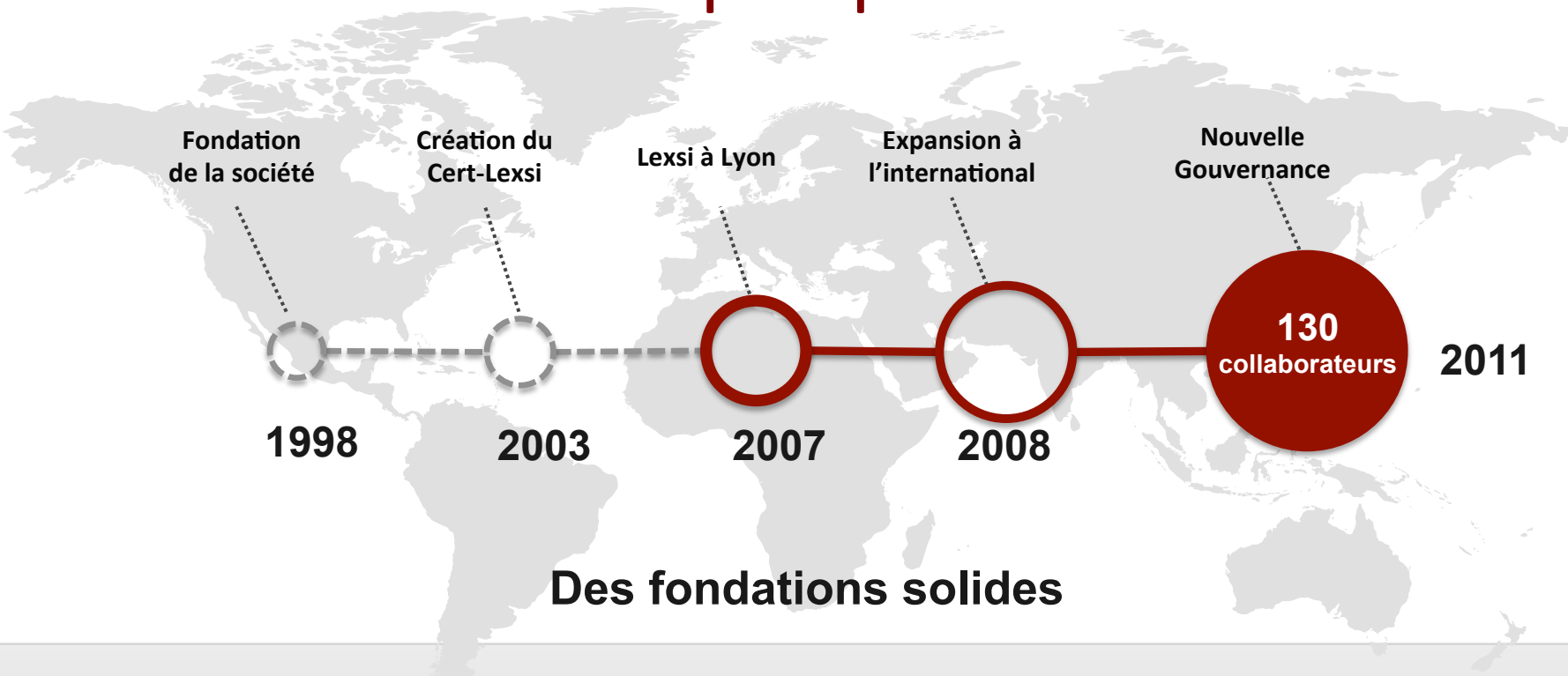
= Nouveaux risques

Référence : CNIS-MOBILE

Date : 28 juin 2011

Version : V 1.0

LEXSI en quelques dates



Des fondations solides

1ère équipe Cybercrime
Notre CERT est le premier en Europe de par sa taille et le nombre d'interventions

1ère équipe d'Audit et Conseil Technique en France
Elle mobilise ses bases de connaissances et son savoir-faire unique pour évaluer le niveau de sécurité et la résistance des sytèmes d'information de ses clients

Conseil
L'équipe Conseil apporte une force d'innovation tournée vers le management des risques et la protection des SI

Formation
L'université Lexsi apporte aux professionnels de la sécurité des connaissances et des outils au service de leur performance

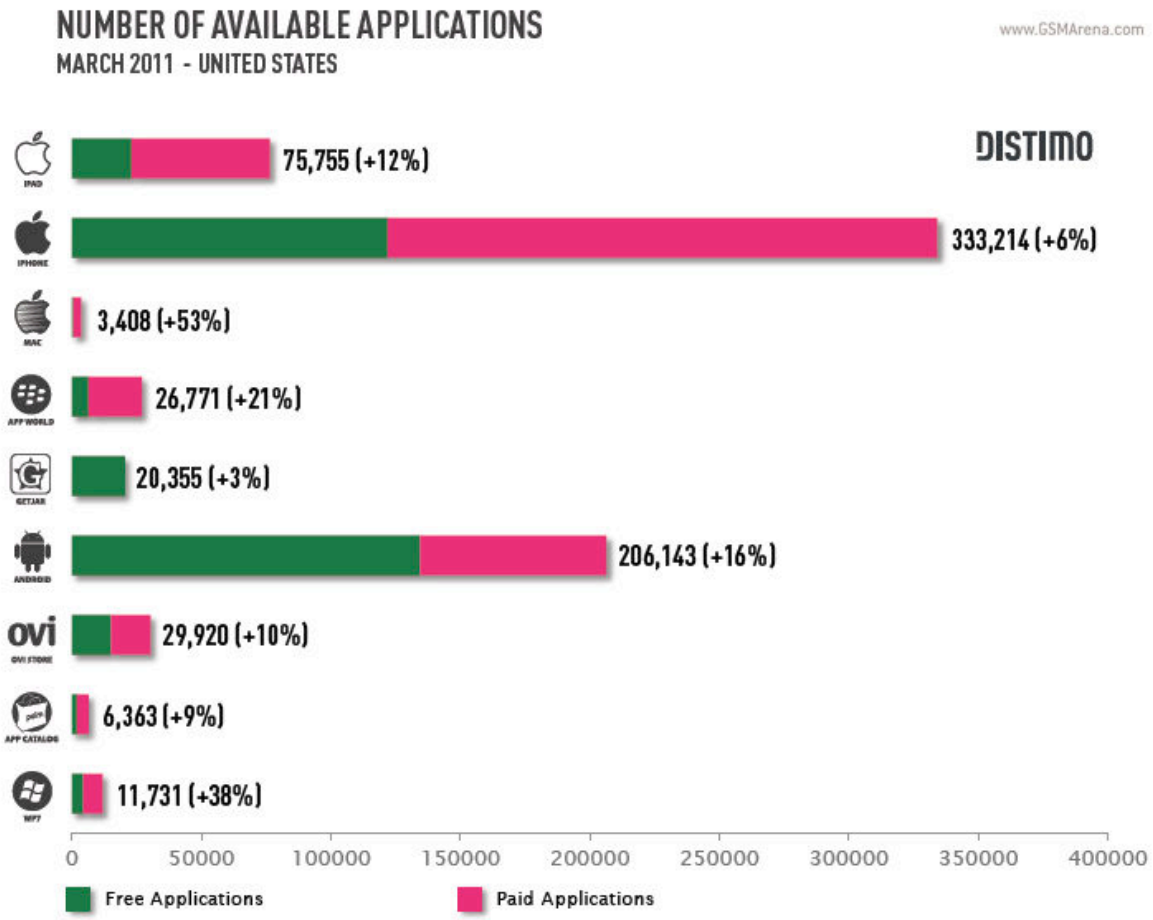
Nouveaux besoins : professionnels ET personnels

- Mobilité : nomadisme (et télétravail)
- Réactivité : accès permanent,
- Fidélisation : contenus dynamiques,
- Profits : services, réduction des coûts,
- Interaction : lien social,
- Communication : image de marque,

Nouveaux usages : nouvel outillage

- Mobilité (tablettes, smartphones)
- Réactivité (WiFi, OWA)
- Fidélisation (flux RSS, API)
- Profits (Cloud, WebServices)
- Interaction (réseaux sociaux, wiki)
- Communication (Twitter, blogs)

Nouveaux usages : les applications mobiles



Applications téléchargées

AppStore : +10 Mds
AndroidMarket : 5Mds

Nouveaux usages : un peu de sociologie

Particuliers

- Du rejet à l'addiction
- Frontière vie privée/ publique caduque
- Dépréciation valeurs des informations diffusées
- Perte de rationalité
- Sensibilisation insuffisante

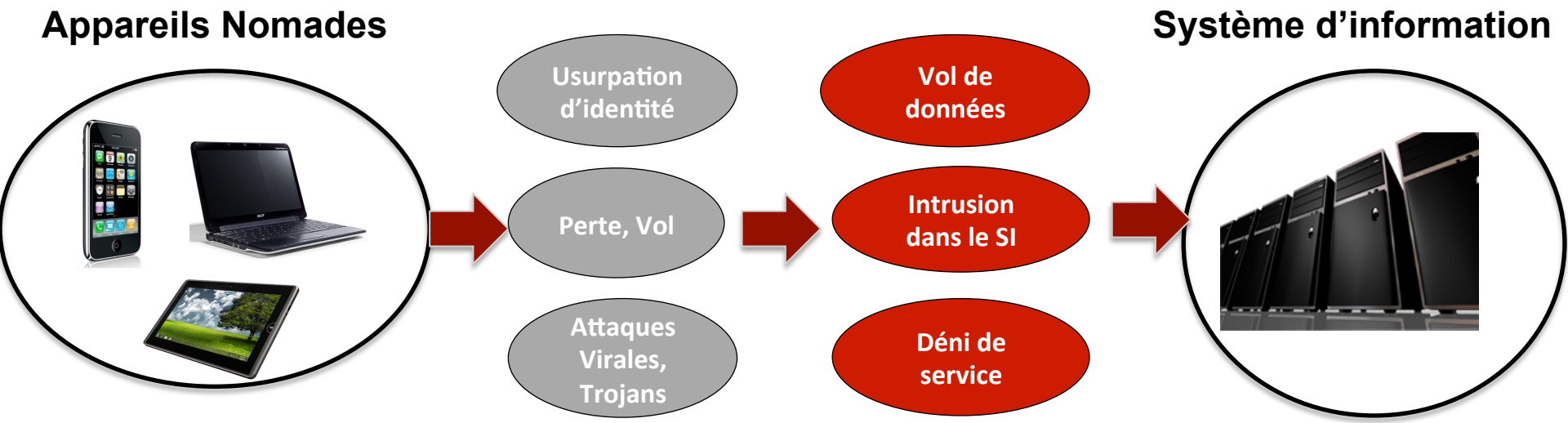
Entreprises

- Effet de mode
- pression MKTG ou métier
- Prérogatives diffuses
- Différences de traitement (DG, DSI, fournisseurs/ sous-traitants
- Sensibilisation insuffisante

Nouveaux risques

- **Intégrité :**
  - **Exemple intrusion SI**
- **Confidentialité :**
  - **Exemple fuites d'informations**
- **Disponibilité :**
  - **Exemple SMS bombing**
- **Traçabilité :**
  - **Exemple gestion de flotte**

Nouveaux risques : extension du périmètre du SI



Nouveaux risques : vecteurs d'attaques

1) SMS
2) Plateformes de Téléchargement
3) Mails & Site Web Malicieux
4) Hotspots Wifi
5) Accès Physique

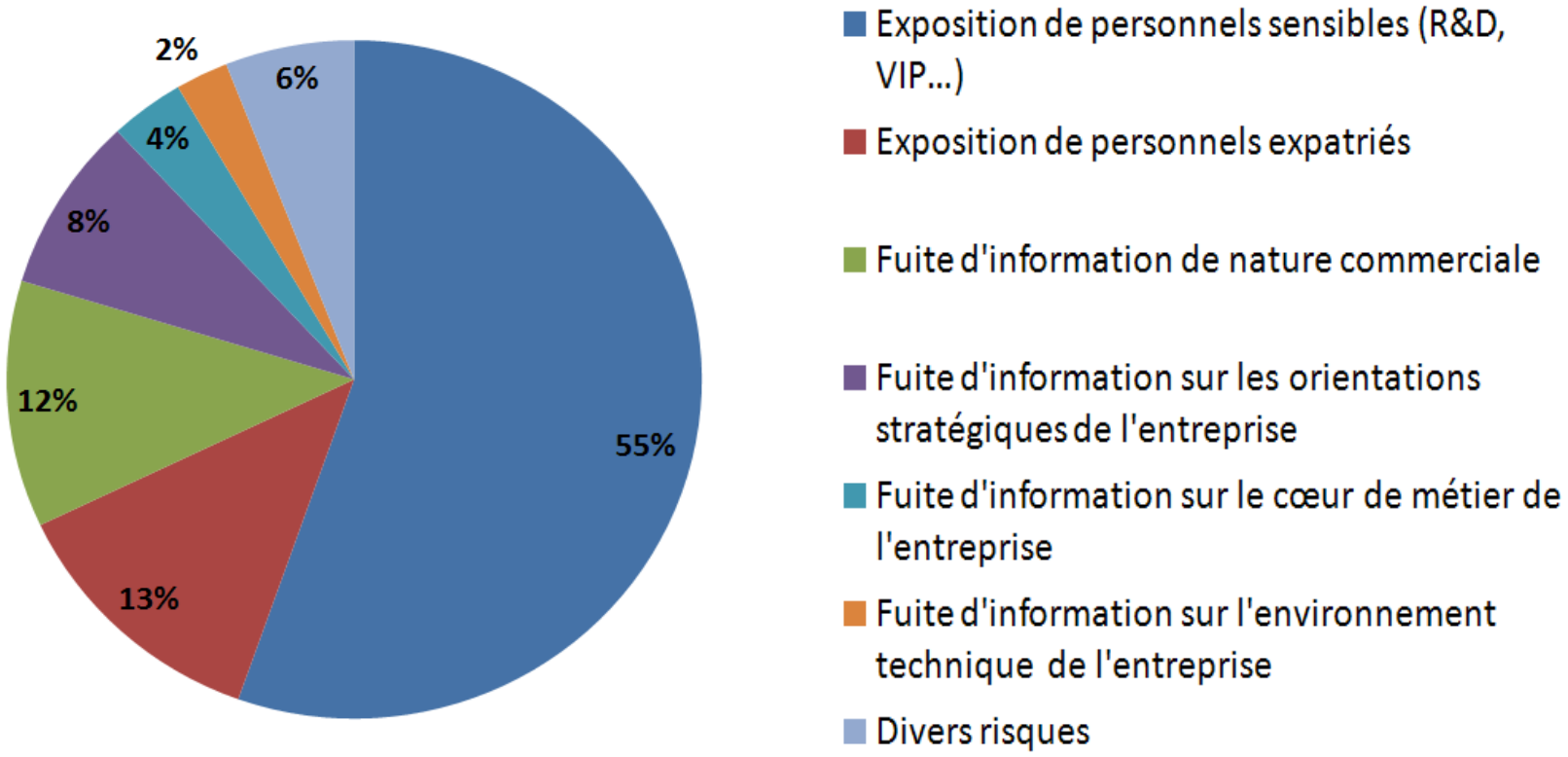
Nouveaux risques : réseaux sociaux

- Confiance aveugle dans les RS
  - Fuites d'informations régulières (1 profil sur 7)
  - Risques physiques (géolocalisation, emploi du temps)
  - Environnement non maîtrisé (paramètres par défaut)

- Or modèle de sécurité :
  - Opacité technique et administrative,
  - Priorité faible des contraintes de sécurité

Nouveaux risques : fuites d'information

- **Périmètre : Enquête réalisée entre juillet 2010 et octobre 2010 sur un échantillon de 4244 internautes sur les réseaux Facebook, Viadeo, LinkedIn, Xing, et Orkut**



Nouveaux risques : fuites d'information

Administrateur système et réseau, [redacted]

2005-2008

Administration systèmes et réseaux
- Gestion des parcs informatiques de plusieurs sociétés sur des plateformes: Windows 2000 serveur, Windows2003 avec ou sans AD, SBS2003 (Win2003+AD+Exchange)
- Prestataire informatique: [redacted]

Administration systèmes, réseaux et gestion du parc informatique.
Structure réseau complexe, 5 zones, 30 VLAN, Backbone HP, classe IP Public, Firewall Sonicwall/Cisco, Fibres optiques informatiques et vidéo, VPN Hardware Cisco/Soniwall.
Liaison VPN site to site avec d'autres filiales
Structure informatique hétérogène, Windows, Macintosh, linux Debian pour les serveurs et Windows, Macintosh pour les postes clients
Etude et mise en œuvre de plusieurs projets :
- Migration application métier « [redacted] », mise en œuvre d'un cluster Oracle 10gR2 Actif-Actif
- Migration des applications comptables et des serveurs sur Windows 2003 et migration serveur Oracle 8 en Oracle 9
- Migration du domaine NT4 vers Windows 2003
- Etude et mise en œuvre d'outils de monitoring sous apache2 SSL « Nagios, Ntop, phpsyslog Mysql et PHP... »
- Migrations des firewalls « Sonicwall » et de leurs stratégies de sécurité.
- Etude nouvelle stratégie de sécurité des réseaux LAN-DMZ-WAN-VISTEUR-VPN de permissif à restrictif
- Etude et mise en œuvre serveur de mail avec groupware Kerio sous Macintosh
- Etude et mise en œuvre d'un système de sauvegarde « Netvault » et élaboration de sa stratégie d'archivage sur disques répartie sur 2 sites dont un distant et archivage sur bandes.

Nouveaux risques : smartphones

- Paradoxe :
  - Smartphones potentiellement plus sécurisés que PC :
    - Boot sécurisé (Trusted platform module),
    - Signature de code
    - Chiffrement
    - Sandbox d'application,
    - Kill switch ?
  - Vraiment ?
    - Disponibilité selon matériel
    - Jailbreak / Market permissif
    - Gestion de flotte (applications des correctifs)
    - Et PEBKAC !

Synthèse

	iOS	Android	BlackBerry	Windows Phone 7
Robustesse du modèle de sécurité	★★★	★★	★★★	★★
Disponibilité d'outils d'attaque	★	★★	★★	★★
Innocuité du « Market »	★★★	★	★	★★★
Difficulté d'installation d'applications hors Jailbreak	★★★	★	★★	★★★
Gestion des mises à jour de sécurité	★★	★	★★	★
Facilité de gestion de flotte	★★	★★	★★★	★★

Nouveaux risques : importance des Mobile Device Management System

- **Application d'une politique de sécurité sur une flotte**

- **Nombreuses fonctionnalités d'amélioration de la sécurité :**
  - Firmware Over The Air
  - Monitoring
  - Prise de contrôle à distance
  - Gestion d'inventaire
  - Backup/Restore
  - Blocage et effacement à distance
  - Software Installation
  - Gestion du Roaming

INNOVATIVE SECURITY

Pour vous aider à maîtriser vos risques

vhinderer@lexsi.com

Tél. (+33) 01 55 86 88 88

cert.lexsi.com

LEXSI LYON
Bois des Côtes 1 - Bâtiment A
300 route Nationale 6
69760 LIMONEST
Tél. (+33) 08 20 02 55 20

LEXSI CANADA
1010, rue de la Gauchetière Ouest
Bureau M110
Montréal QC H3B 2N2
Tél. +1 514 903 6560

LEXSI SINGAPORE
60 Bayshore Road / Bayshore Park
#10-07 - Jade Tower
469982 - Singapore
Tél. +65 65191705