ADHÉRENT
CLUSIF
2015

Mobilité et Sécurité, peut-on encore espérer faire coexister ces deux concepts ?

Jean-Marc GREMY
jmgremy@cabestan-consultants.com
@gremyjm

Vice –président du Clusif

GS Days
LES JOURNÉES FRANCOPHONES DE LA SÉCURITÉ

ADHÉRENT CLUSIF 2015

Cabestan Consultants

- **Jean-Marc GREMY**, fondateur et consultant
  - Militaire de formation (Marine Nationale)
  - Expériences réussies comme client final : Alcatel (ABS) et Groupe Synthélabo (Sanofi)
  - Développement puis création d'entreprises
  - Vice-Président du CLUSIF
- Cabinet de conseil et d'audit indépendant
  - Conseil en entreprise : Gestion des risques, politique de sécurité, continuité, audit…
  - Formation et sensibilisation SSI, dont le CISSP® en Europe

Cabestan)(Consultants

Quel contexte en 2015 pour la mobilité ?

Mobilité de l'information, dès 1947

Cabestan)(Consultants

Le contexte de la mobilité

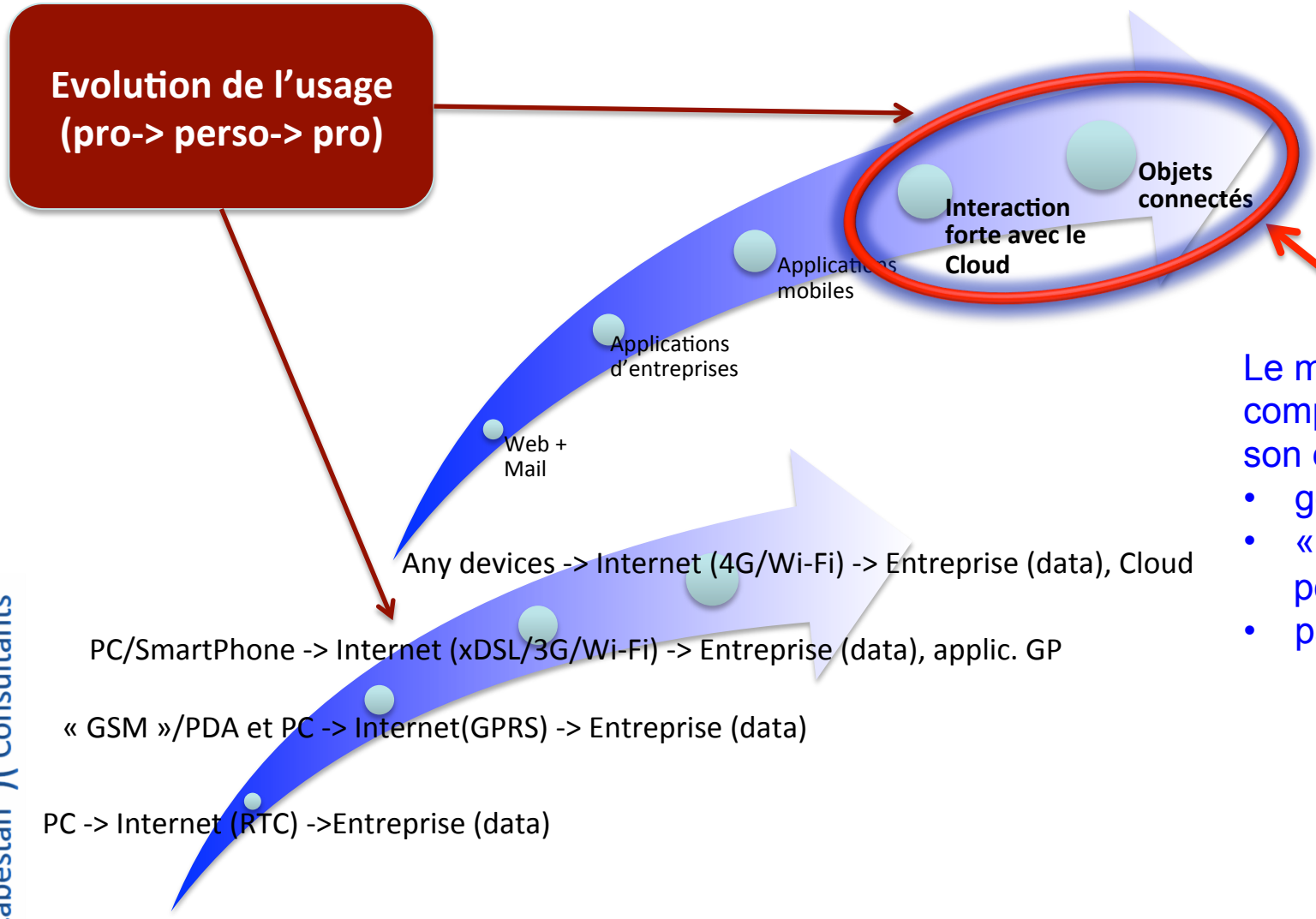
- L'homme est **naturellement** mobile , il s'est toujours déplacé, il est nomade
  - découverte du monde, commerce…
  - colonisation, migration…
- Le terminal est **devenu** mobile
  - ordinateur fixe, portable, PDA puis tablette
  - téléphone, cellulaire, puis
  - utilisation de moyens partagés (i.e. « cybercafé »)

smartphone et ***phablet***

- Les données sont **potentiellement** mobiles
  - dans le périmètre de l'entreprise
  - à l'extérieur de son périmètre

Cabestan)(Consultants

Les évolutions de la mobilité



Le mobile « tient compte » de son environnement

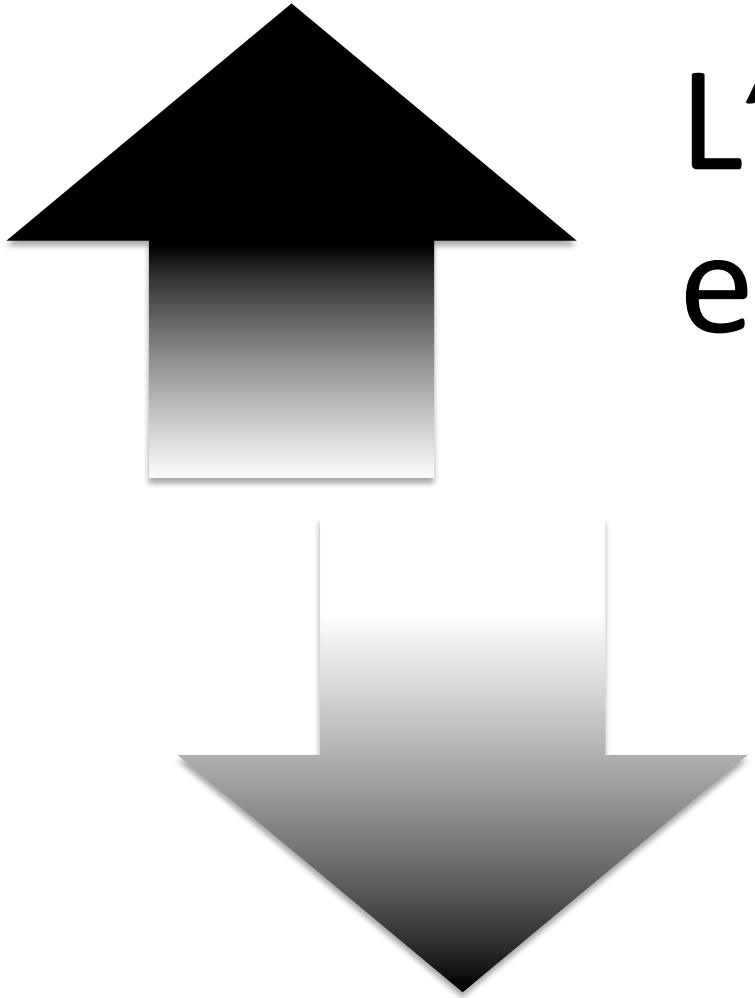
- géolocalisation
- « état du porteur »
- paiement…

Cabestan)(Consultants

Le téléphone n'est plus un téléphone

- Utilisation du téléphone pour les réseaux sociaux et applications connectées (Internet)
  - Exemple : pour les messages groupés
    - pas la même application entre les mobiles (i.e. iMessage™)
    - donc Facebook™ !
- Plus facile que la voix (téléphone), asynchrone
- Fonction téléphone vers les parents ;-)

Vont-ils se rencontrer ?



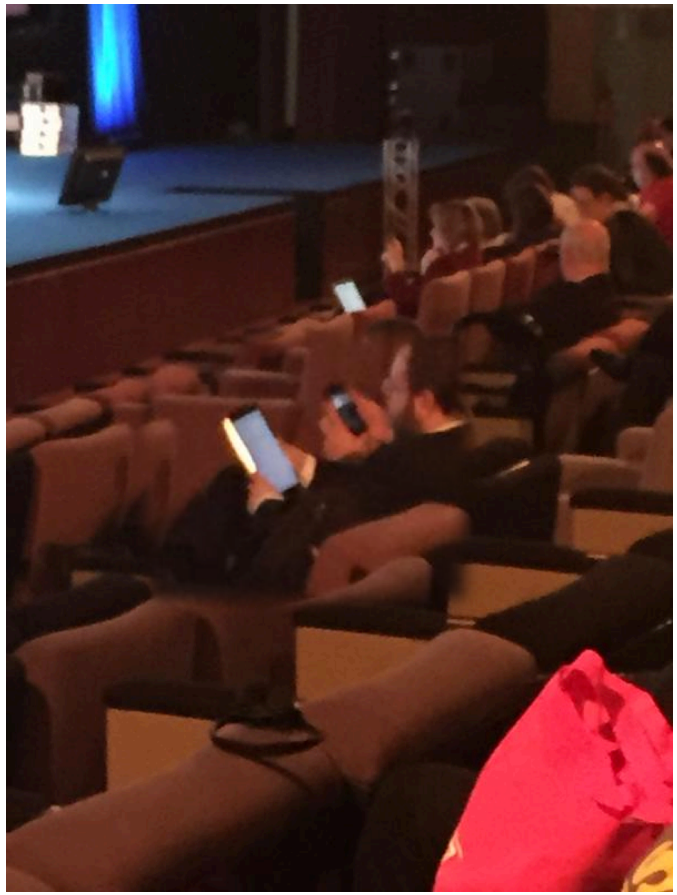
L'homme
est nomade

Les données
sont mobiles

Cabestan)(Consultants

Peut-on objectivement échapper aujourd'hui à la mobilité dans l'entreprise, dans nos vies privées ?

Personne n'y échappe !



crédit photo : @drambaldini

Cabestan)(Consultants

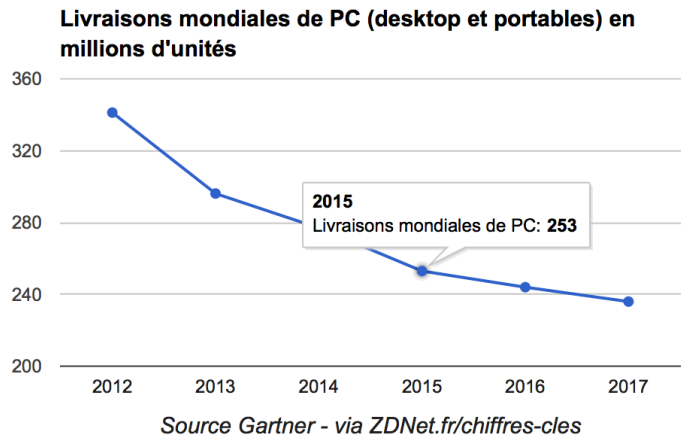
l'Homme

- Vu du SI, l'homme redevient nomade !
- Il « doit » être en capacité d'utiliser un SI en toutes circonstances
- Conditions qui le nécessitent
  - situation de terrain (sourcing de produits, maintenance, relevé d'information…),
  - travail à distance, aménagement de l'organisation de son travail et de l'espace associé,
  - capacité d'assurer la continuité des opérations, même dans des situations de crise (c.à.d. sinistre, pandémie, grève…),
  - …

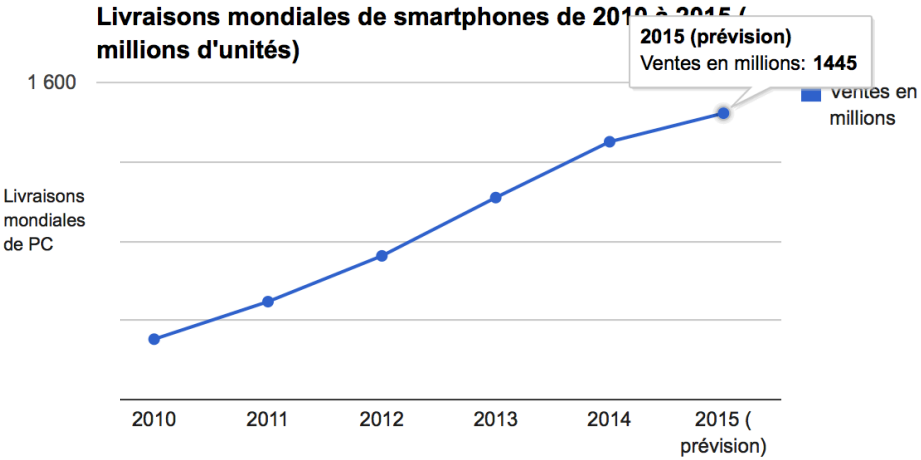
Cabestan)(Consultants

Le terminal

- En 2010, à l'horizon 2015 >1Md d'internautes mobiles
- En 2015 :
  - Le **nombre* atteint 2,1 milliards**
  - > 35% de la population mondiale en sera équipée fin 2015



Source Gartner - via ZDNet.fr/chiffres-cles



Source IDC - via ZDNet.fr/chiffres-cles

(*) cabinet Strategy Analytics

Cabestan)(Consultants

La mobilité la seule sur le banc des accusés ?

Que se cache t'il derrière cet « unique » port *USB-C* ?

Mobilité

« Applications tueuses »

Cloud Computing

Cabestan)(Consultants

Les données

- Dispersion des données : elles sont mobiles !
  - offre des constructeurs : stockage + applications (Apple™, Microsoft™, Google™…)
  - stockage « gratuit » (DropBox™, Hubic™…)
- Elles ne sont plus uniquement stockées (protégées ?) par le SI interne
  - données sensibles sur les moyens mobiles
  - données partagées entre partenaires économiques
  - données à caractère perso/professionnelle (c.à.d. réseaux sociaux, ex. LinkedIn™)

Cabestan)(Consultants

Le réseau ??

- On ne dit pas « *Avez-vous un accès Internet par un réseau sans-fil ?* » on dit « *Avez-vous du Wi-Fi ?* »
- IP est le protocole de fédération des communications
  - arrivée d'IPv6 (?) Notamment pour les objets connectés ???
- Le terme « *seamless* » prend tout son sens
  - possibilité de connexion de poste à poste : VoIP, partage de document (i.e. Skype™), prise de contôle à distance (TeamViewer™)
  - abandon de la frontière entre le réseau privé et public

- Rappel d'une des 5 caractéristiques essentielles du Cloud
  - **Accès universel** : Les ressources sont accessibles en tout point du réseau mondial et au travers de mécanisme standards favorisant ainsi l'utilisation de plateformes hétérogènes

Cabestan)(Consultants

Le réseau ??

- On ne dit pas « *Avez-vous un accès Internet par un réseau sans-fil ?* » on dit « *Avez-vous du Wi-Fi ?* »
- IP est le protocole de fédération des comm… s
  - arrivée d'IPv6 (?) Notamment …
- Le terme « se…
  - p… do… …ance (TeamViewer™)
  - ab… …e réseau privé et public

Ne serait-il pas le coupable ? Par exemple, pas de Wi-Fi « ouvert » dans l'entreprise => pas de BYOD ?

- Rappel d'une des 5 caractéristiques essentielles du Cloud
  - **Accès universel** : Les ressources sont accessibles en tout point du réseau mondial et au travers de mécanisme standards favorisant ainsi l'utilisation de plateformes hétérogènes

Cabestan)(Consultants

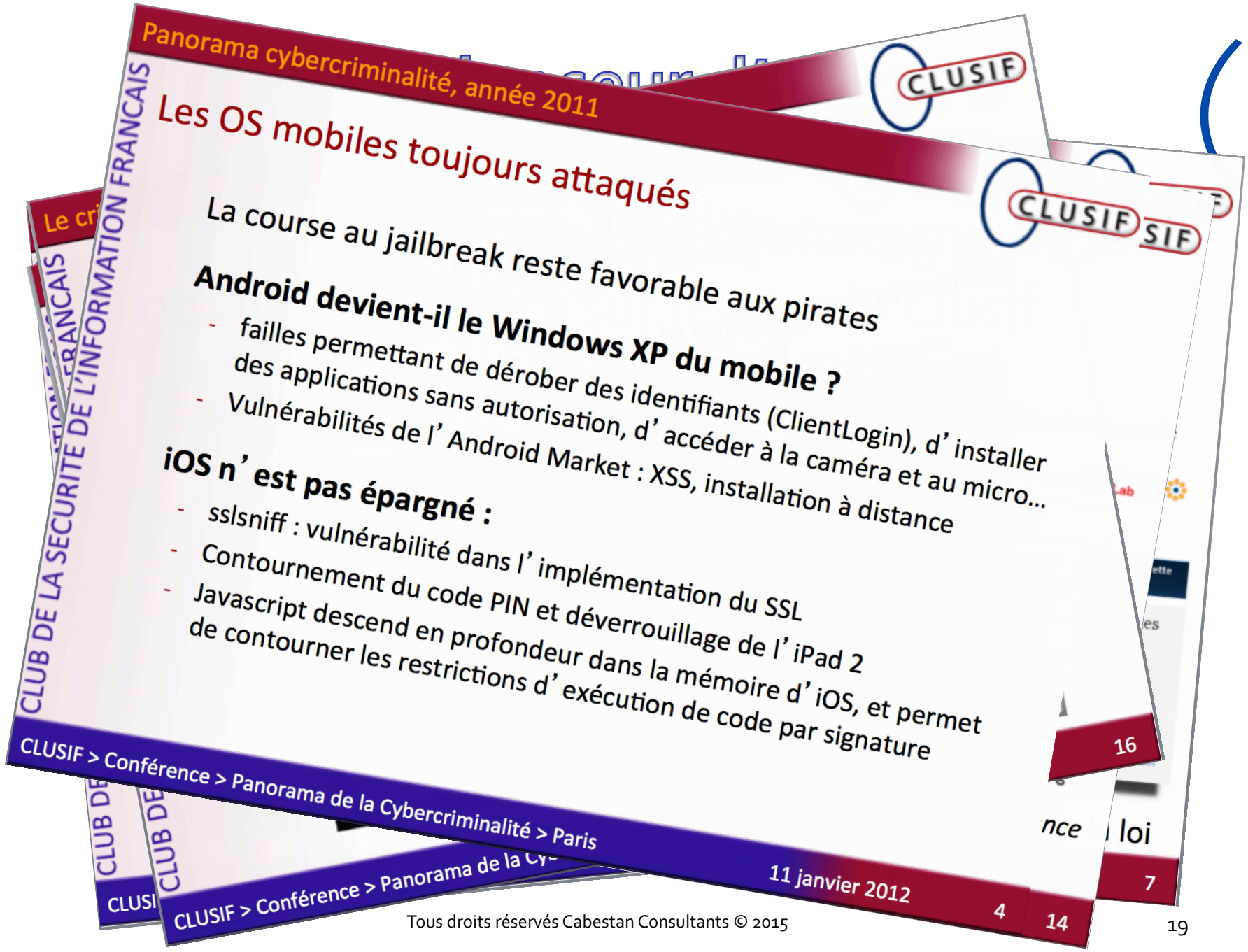
Quels enjeux en termes de sécurité ?

Sont-ils bien perçus et compris ?

Sécurité de l'information : Quelle information ?

- Pourquoi la mobilité devient un enjeu **majeur** de sécurité pour **l'entreprise et le citoyen** ?
  - interception des communications
  - géolocalisation des personnes, des données
  - stockage et échange d'information sensible
  - interaction du mobile
    - avec l'homme
    - avec ses objets connectés
  - outil de paiement, circulation d'effet financier

Cabestan)(Consultants



Cabestan)(Consultants

Vision de la *Cloud Security Alliance*

- *The Evil 8** : Principales menaces pour les mobiles
  1. Perte de données, fuite, vol ou équipement décommissioné
  2. Vol d'information par des malwares
  3. Perte et fuite de données dues à des faiblesses dans les développements d'applications tierces
  4. Vulnérabilités dans les équipements, les Os, la conception et les applications tierces
  5. Réseau Wi-Fi sans sécurité, contrôle d'accès faible, faux point d'accès Wi-Fi
  6. Fausse ou manque de sécurité pour les places de marché applicative
  7. Outils de gestion insuffisant, faible capacité, pas de ségrégation des rôles
  8. Attaque sur les communications de proximité (NFC, BlueTooth, Wi-Fi…)

Source : Security Guidance for Critical Areas of Mobile Computing, 2012

cloud security alliance℠

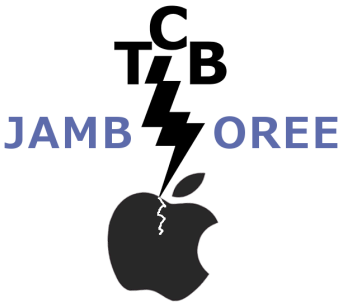
Cabestan)(Consultants

Info ou intox ?

- D'après son avocat* : « *Il n'utilise jamais un iPhone®, mais un téléphone simple. Il craint l'activation d'un logiciel espion qui pourrait atteindre à sa vie privée* »

(*) *Source : www.techtimes.com*

- Article de l'EFF* : « *Devine qui n'a pas été invité au Jamboree des « hackers » de la CIA ? …. Apple et Microsoft* :-)



(*) Electronic Frontier Foundation

Cabestan)(Consultants

Info ou intox ?

- D'après son avocat* : « *Il n'utilise jamais un iPhone®, mais un téléphone simple. Il craint l'activation d'un logiciel espion qui pourrait atteindre à sa vie privée* »

- Article de l'EFF* : « *Devine qui n'a pas été invité au Jamboree des « hackers » de la CIA ? …. Apple et Microsoft* :-)

(*) Source

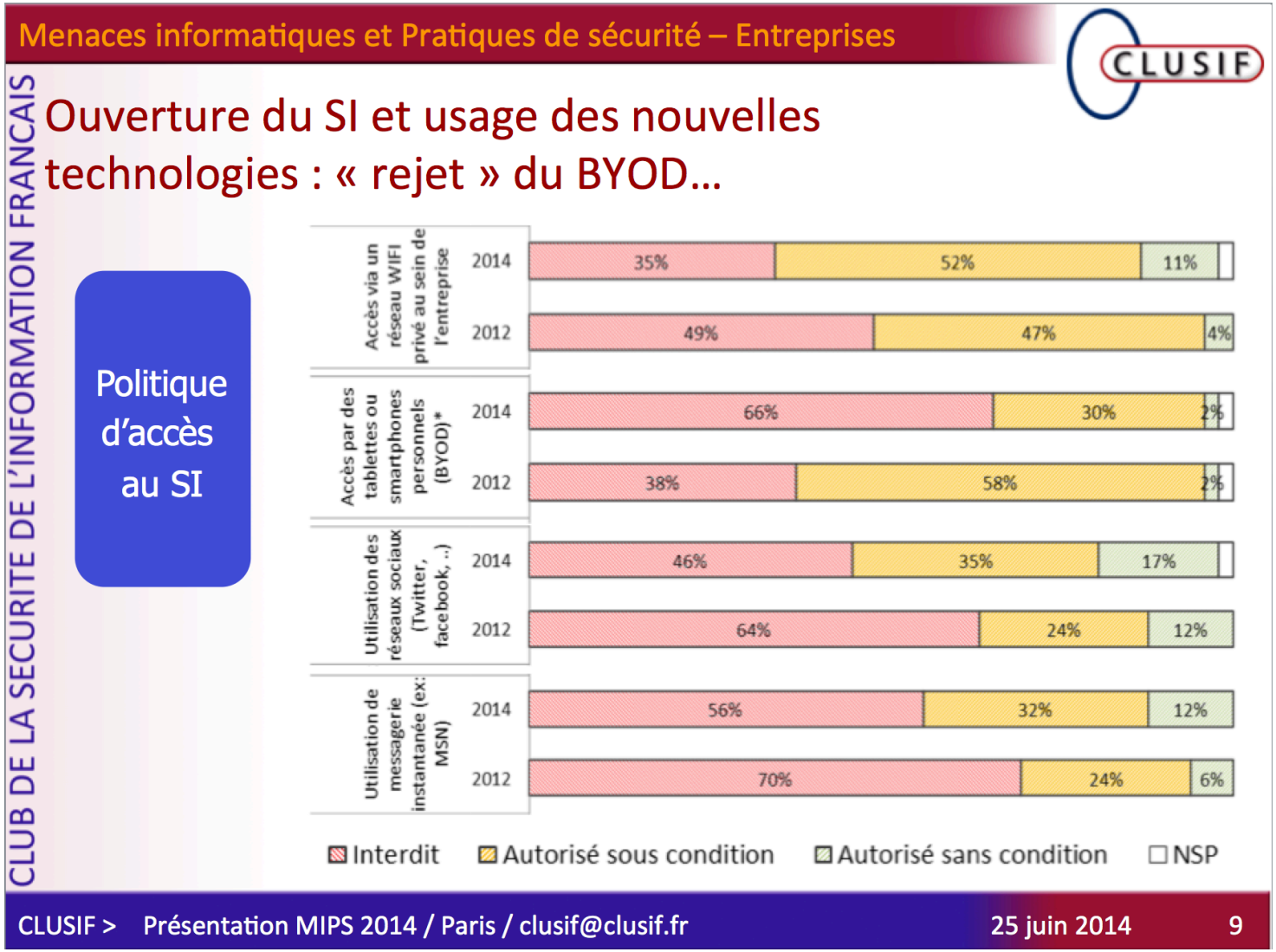
Cabestan)(Consultants

Quels contextes de sécurité ?

- L'entreprise doit reprendre la main !
- Identifier les « architectures hors de contrôle »
- Mais une vision de l'information ne suffit pas : trop conceptuel ! Parler des données, dimension technique, et de leur sécurité
  - classification des données, nouveau critère de mobilité ?
  - droits des personnes, nouveau critère de nomadisme ?
  - étendre la notion de donnée en dehors de la sphère professionnelle ?

Cabestan)(Consultants

Certains fronts tiennent !



Source : Etude MIPS 2014 du Clusif, partie Entreprise

Cabestan)(Consultants

Quels enjeux de sécurité pour le Cloud ?

- Établir les bases de la confiance et du contrôle
  - contrat(s) avec l'hébergeur ou l'offreur service de Cloud
  - contrôle d'accès : identités, comptes d'admin., appli...
  - cryptographie : authentification, données, échanges...
  - offuscation des données, des codes...
  - traçabilité : des connexions, des actions, des opérations...

Sécurité de l'infrastructure → *MyCloud*™
- tout en gardant le contrôle (?)

Sécurité de l'infostructure → *MyCompany*™
- car une méfiance à l'égard de *MyCloud*™

Cabestan)(Consultants

La sécurité par défaut de sécurité ?

- Chiffrement des disques durs d'un portable ?
- Conteneur de sécurité sur un mobile ?
  - PIM / Applications métiers
  - vs. Applications et données personnelles
- La bataille est-elle perdue ?

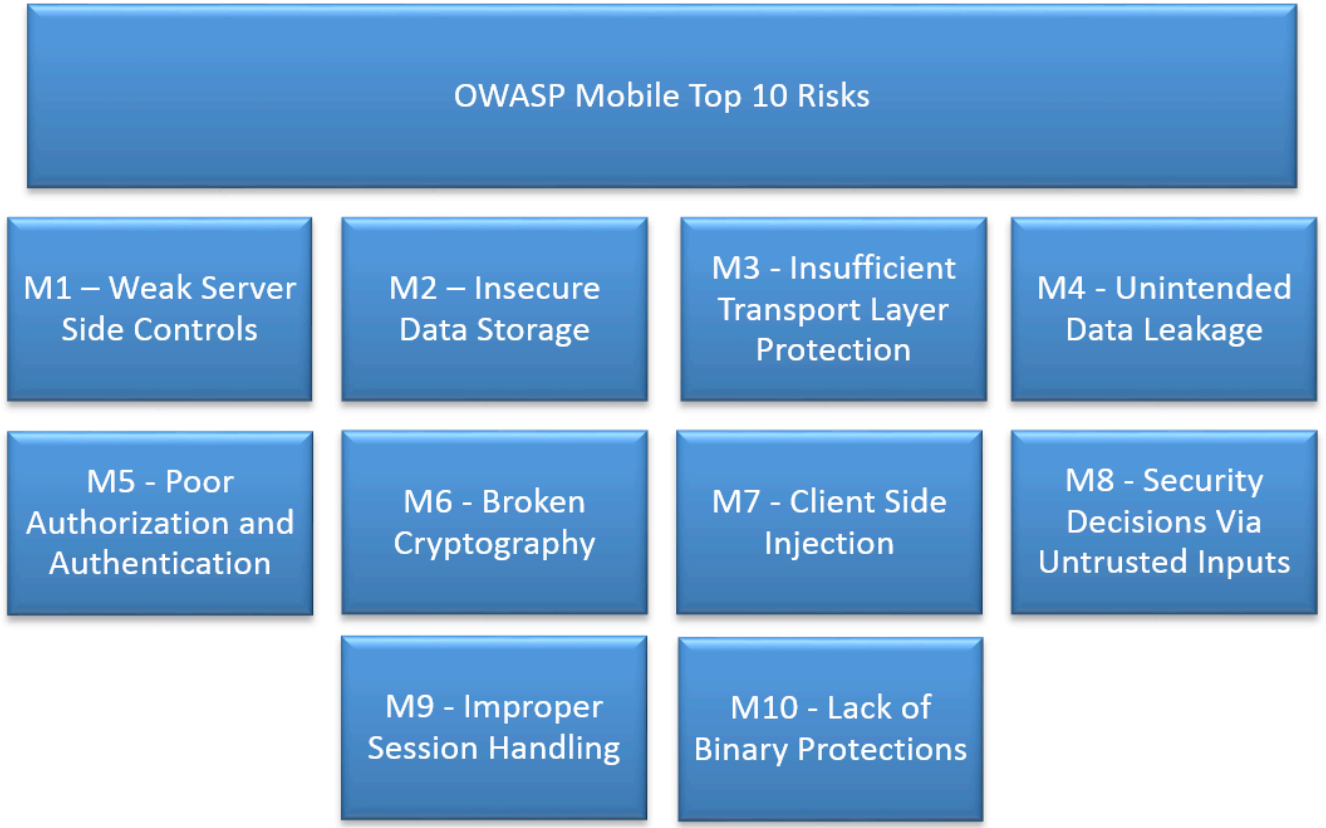
→ Documents à lire :

- ✓ ***Recommandations de sécurité relatives aux ordiphones***, NT de l'ANSSI en 2013
- ✓ l'ANSSI et le CDSE* proposent un « ***Passeport de conseils aux voyageurs*** »

* *Club des Directeurs de Sécurité des Entreprises*

Cabestan)(Consultants

Le développement des applications mis à contribution



Source : OWASP Mobile Security Project

OWASP
The Open Web Application Security Project

Cabestan)(Consultants

La sensibilisation intègre la mobilité

- Une preuve que la mobilité fait aujourd'hui partie du SI dans l'entreprise, **son existence est acceptée !**

Source : Exemple d'une entreprise de la grande distribution

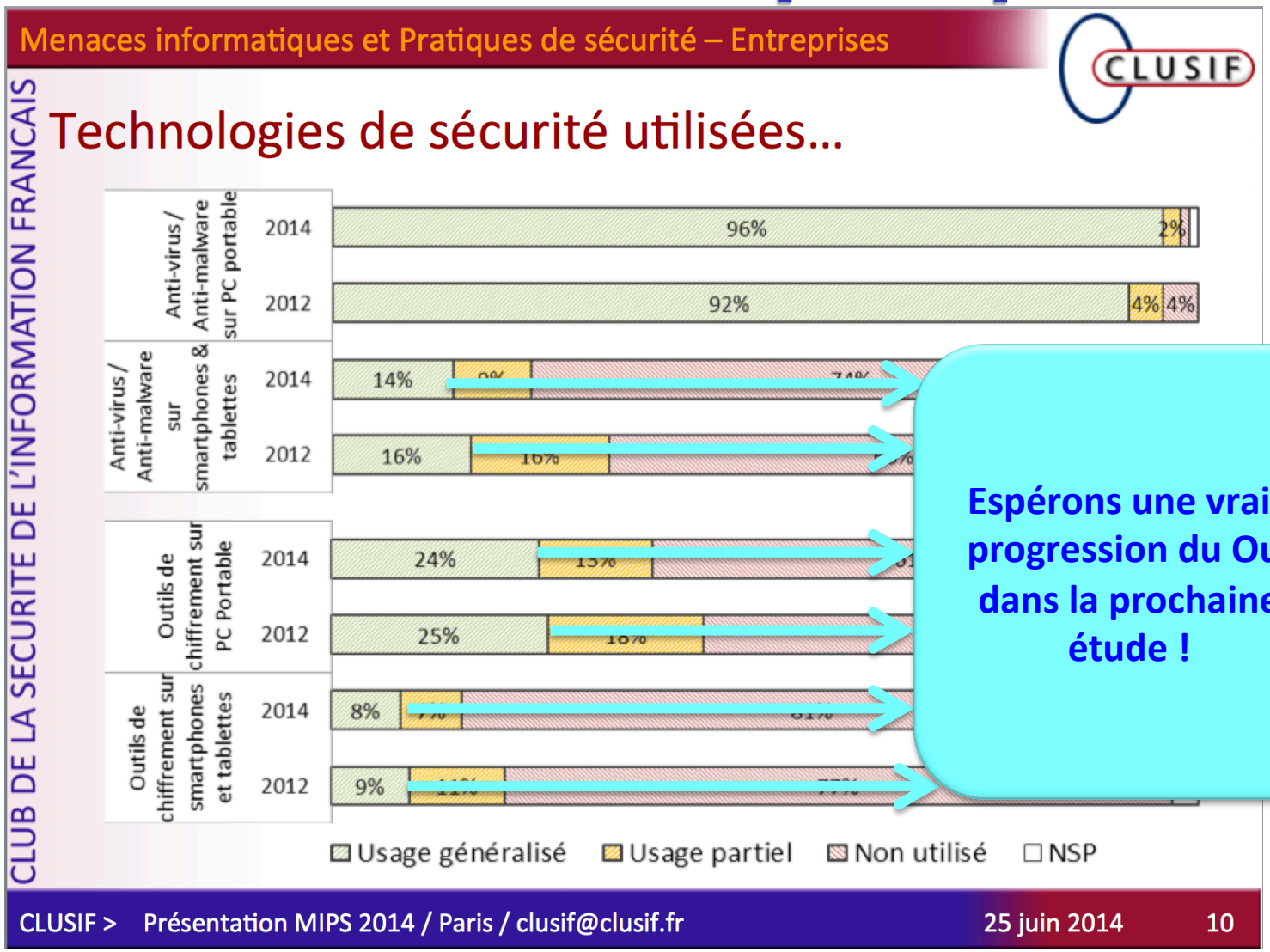
Prospective, rester les bras croisés ?

Pour la sécurité ?

- **Tout reste à faire, à (re)inventer…**
- Les solutions techniques de sécurité doivent intégrer
  - les nouvelles applications et leurs fonctions
  - les données associées, leur mouvement
  - l'écosystème de la mobilité (objets connectés, domotiques…)
- Peut être est-ce enfin le moment de remettre l'homme à sa place !
  - sensibilisation et formation pratique
  - créer, a minima, une charte de catégorisation des données
  - associer les sphères privées, publiques et professionnelles
- Sans oublier le volet Juridique ☺

Cabestan)(Consultants

Faire évoluer les pratiques !



Ne pas abandonner ses lignes !

- Dé-périmétrisation du SI
  - ce n'est pas l'abandon des responsabilités
  - juste l'élargissement du périmètre
  - sémantique : sécurité informatique → sécurité du patrimoine informationnel

- Défense en profondeur
  - plusieurs lignes de défense autonomes
  - la perte d'une ligne ne remet pas en cause la sécurité globale
  - identification préalable des menaces et des scénarii de risques
  - améliorer ses capacités de réaction

Cabestan)(Consultants

Merci de votre participation !

Cabestan Consultants

8, rue Maurice Ravel

91380 Chilly-Mazarin –France

Cell. +33 (0) 6 60 64 59 45

jmgremy@cabestan-consultants.com

@gremyjm

ADHÉRENT CLUSIF 2015

Si NOUS pensons que la technologie peut résoudre NOS problèmes de sécurité, alors NOUS ne comprenons pas les problèmes et NOUS ne comprenons pas la technologie

- Bruce Schneier, Secrets and Lies

Cabestan)(Consultants