CIGREF

Sécurisation de la mobilité

Octobre 2010

Synthèse

L'évolution des technologies (innovation) et l'évolution des usages en entreprises (intensification, généralisation et mixité des usages personnels et professionnels) a accru et banalisé les besoins de mobilité en entreprises.

Ainsi, il est devenu normal de pouvoir accéder à sa messagerie professionnelle ainsi qu'à toutes les applications essentielles, où que l'on se trouve, en utilisant des outils tels que les ordinateurs portables et les Smartphones. En créant de nouveaux risques et de nouvelles menaces informationnelles, **ces outils mobiles sont devenus un point critique de la gestion du parc informatique.**

Si les risques sont parfaitement maitrisés pour les ordinateurs portables, il n'en va pas de même pour les smartphones, plus compacts, moins matures en matière de sécurité et moins intégrés au SI de l'entreprise.

Pourquoi le CIGREF s'est intéressé à ce sujet?

Le CIGREF s'est déjà intéressé en 2002 aux usages en matière de mobilité et en 2009 aux usages en matière de communication unifiée. **La nouveauté en 2010, c'est l'accent mis sur la gestion des risques informationnels,** de la protection de l'information et de la souveraineté numérique des entreprises autour des smartphones.

En effet, les entreprises françaises, ou européennes, en concurrence avec leurs homologues anglo-saxons, sont confrontées à un problème de sécurisation des smartphones, dont l'offre est principalement américaine. Ces entreprises recherchent une offre française ou européenne qui leur permettra de protéger leurs systèmes d'information de la concurrence étrangère et plus précisément de la concurrence anglo-saxonne.

Quelles sont les principales conclusions ?

1. **Créer un écosystème de fournisseurs français ou européens**
    - **Une liste d'acteurs français de la sécurité a été établie** afin de dresser un panorama de l'offre nationale actuelle en matière de sécurisation de la mobilité.
    - **Les grandes entreprises françaises souhaitent que les fournisseurs français ou européens « têtes de file » bâtissent une offre de sécurité de bout en bout**, alternative aux solutions essentiellement américaines.

2. **Continuer à sensibiliser les utilisateurs** – Au-delà des solutions techniques, une approche par des solutions comportementales et organisationnelles est indispensable. **Le passeport pour les voyageurs** élaboré par l'ANSSI avec le CIGREF est une première avancée sur ce sujet.
3. **Contribuer à l'émergence de véritables normes et standards spécifiques à la sécurisation de la mobilité** - La sécurisation de la mobilité doit également reposer sur l'utilisation des normes et des standards.
4. **Renforcer les partenariats avec l'Etat**
    - **Relayer les évaluations de l'Etat auprès des entreprises et faire part à l'Etat des contraintes des entreprises**. L'état enfin doit contribuer à stimuler et consolider l'offre française actuelle. Cela peut se traduire par une meilleure communication sur le processus d'évaluation de la performance des solutions de sécurité existantes ou nouvelles, ou encore la participation d'acteurs privés ou associatifs au processus d'évaluation public, afin d'aider les entreprises à choisir les meilleures solutions.
    - **Piloter l'innovation.** Afin de renforcer cette offre, l'état français doit soutenir les PME innovantes en matière de sécurité, intégrer de manière systématique le thème de la sécurité dans son dispositif de soutien aux PME innovantes. **Le thème de la sécurité de la mobilité doit être un des axes majeurs de la politique de soutien à l'innovation de l'Etat.**
5. **Le CIGREF peut servir de plateforme d'échange** et aider à renforcer les échanges entre l'industrie, les clients et l'état français, par exemple en contribuant via ses membres au processus d'évaluation de la performance des solutions de sécurité mis en place par les pouvoirs publics, **mais également de centre d'expertise** pour tout ceux qui veulent " ... mieux comprendre les enjeux de la sécurité des usages numériques" à l'image de la formation mise en place récemment en partenariat avec l'INHESJ.
6. **Les grandes entreprises doivent prendre conscience de leur rôle et animer leur écosystème.**
    - Les grandes entreprises ont-elles aussi **un rôle moteur à jouer dans l'animation de bout en bout de la sécurité au sein de leur écosystème**. Les grandes entreprises seules ont la capacité à créer et orienter un marché, de part leur volume d'achats et leur cahier des charges.
    - Les grands groupes et les PME pourraient **participer aux exercices nationaux de sécurité ou de gestion de crise** organisés par l'ANSSI ou l'élaboration de « Livres blancs » ou aux guides de bonnes pratiques en matière de sécurité.
    - Enfin les entreprises peuvent **se regrouper au sein de structures associatives** ad hoc, à l'instar de ce qui s'est fait en matière de ebusiness ou d'archivage, afin de bâtir des cahiers des charges communs, en vue de mieux structurer le marché et d'orienter l'offre.

Remerciements

Ce groupe de travail a été piloté par Jean SASS, DSI Dassault Aviation. Cette synthèse a été rédigée par Fatine LAAMIRI et Alexis MILLOT, étudiants en Mastère Spécialisé HEC / Mines ParisTech « Management des Systèmes d'Information et des Technologies », stagiaires au CIGREF de janvier à avril 2010, et Stéphane ROUHIER, Chargé de mission au CIGREF.

Publications CIGREF 2009-2010

- L'architecture d'entreprise dans les Grandes Entreprises
- Cahier de recherche n° 6 : Pratiques et discours des grandes entreprises sur la valeur et la performance des SI - *Etude Exploratoire*
- Communication et influence de la DSI
  Quelle démarche pour une communication au service d'un leadership durable ?
- Les dossiers du Club Achats 2010 : *le point sur … le cloud computing, les audits de licences, l'offshore, les achats IT éco-responsables et l'infogérance*
- Du Green IT aux SI éco-responsables
  2ème édition, augmentée des conclusions du groupe de travail CIGREF 2010
- Impact du Cloud computing sur la fonction SI et son écosystème
  Rapport d'étape et témoignages d'entreprises
- Maturité et gouvernance de l'Open source : la vision des Grandes Entreprises
- Nomenclature 2010 : premier pas vers l'Europe des compétences IT
  Les emplois-métiers du SI dans les grandes entreprises,complété par le référentiel européen des compétences IT
- Le rôle de la fonction SI dans la gestion des grands risques
  Un exemple avec la Grippe A(H1N1)
- Position du CIGREF sur le Cloud Computing
- Relations avec Orange Business Services *(réservé aux membres du CIGREF)*
- Sécurisation de la mobilité

Publications en partenariat

- Audit de la gouvernance des SI (avec l'AFAI et l'IFACI) – A paraître fin 2010
- Les fonctions SI et Organisation au service des métiers (*avec l'AFOPE*) *Optimiser la création de valeur pour l'entreprise*
- L'information : prochain défi pour les entreprises - Pratiques de création de valeur par les SI et leur usage (*avec Capgemini Consulting*)
- Information: the next big challenge for business - Harnessing best practice in IS-driven value creation: 2009 map (*with Capgemini Consulting*)
- SAP Bonnes pratiques commerciales (*avec l'USF*) – A paraître fin 2010

Sommaire

Figures

1. Introduction

Objectif et périmètre

L'objectif de l'étude est de mettre en évidence les problèmes de sécurisation des systèmes de mobilité rencontrés par les grandes sociétés françaises ou européennes, dont les principaux concurrents sont américains. L'étude s'intéresse plus généralement à la problématique de la confidentialité des données transitant sur les terminaux mobiles des entreprises. Dans cette étude la mobilité concerne uniquement les *Smartphones* et ne prend pas en considération le travail collaboratif.

Déroulement de l'étude

Un travail de documentation sur le thème « Sécurisation de la mobilité » a précédé l'élaboration d'un guide d'entretien, et la réalisation d'une série d'entretiens auprès d'un panel d'entreprises membres du CIGREF.

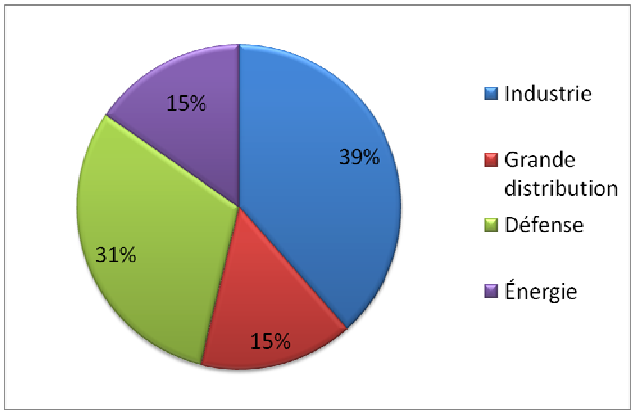

Figure 1 : Secteurs d'activité des entreprises interviewées

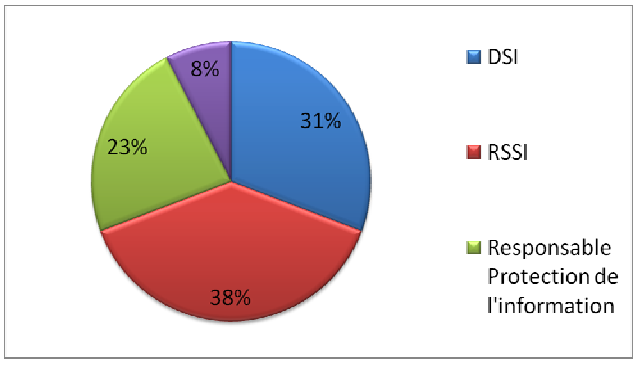

Figure 2 : Fonction des personnes interviewées

2. La mobilité et ses enjeux

Définition de la mobilité

La mobilité permet d'accéder aux systèmes d'information de l'entreprise indépendamment du lieu où se trouvent les collaborateurs en utilisant des outils comme les *Smartphones* ou les PC portables.

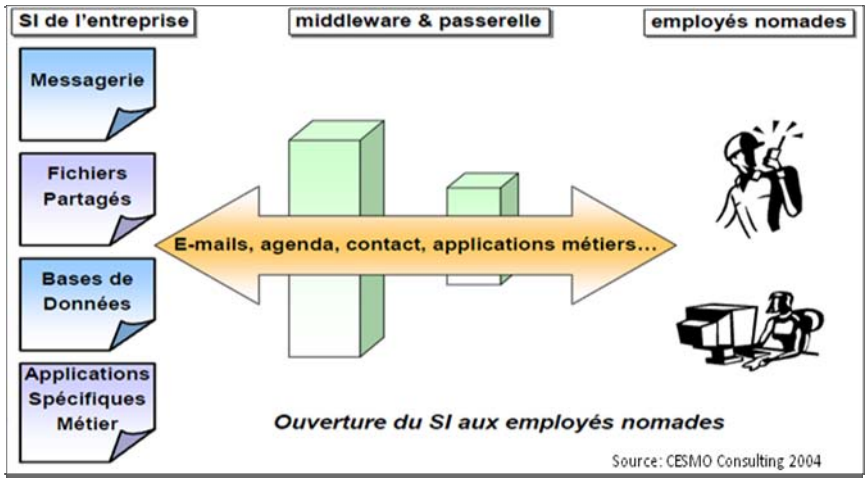

Figure 3 : La mobilité

Source : Cesmo Consulting

La mobilité n'est plus aujourd'hui une affaire de mode, car elle joue un rôle fondamental dans l'agilité et la performance des entreprises. Il s'agit de faire circuler les informations, rapidement et en toute sécurité, via le système d'information, aux collaborateurs, indépendamment du lieu où ils se trouvent et des outils de communication qu'ils utilisent. Cette demande de mobilité est synonyme de nouveaux challenges pour les DSI : l'enjeu est de protéger les informations sensibles, tout en équipant les utilisateurs de solutions ergonomiques, conviviales, peu contraignantes et favorisant la fluidité des usages et l'accès à l'information en tout lieu et à tout moment.

Menaces et risques de la mobilité

Développer la mobilité au sein d'une entreprise n'est pas aisée. Cette démarche doit être réfléchie car elle amène de grands bouleversements au sein de l'organisation informatique et par conséquences elle devient la source de nouveaux risques. Les entreprises doivent en amont définir ce qu'il faut sécuriser, pour combien de temps, quelles sont les données sensibles, quels sont les types de risques, les niveaux de risques acceptables / inacceptables (occurrence, gravité, stratégie de gestion des risques).

Le schéma ci-dessous résume les principaux risques liés à la mobilité.

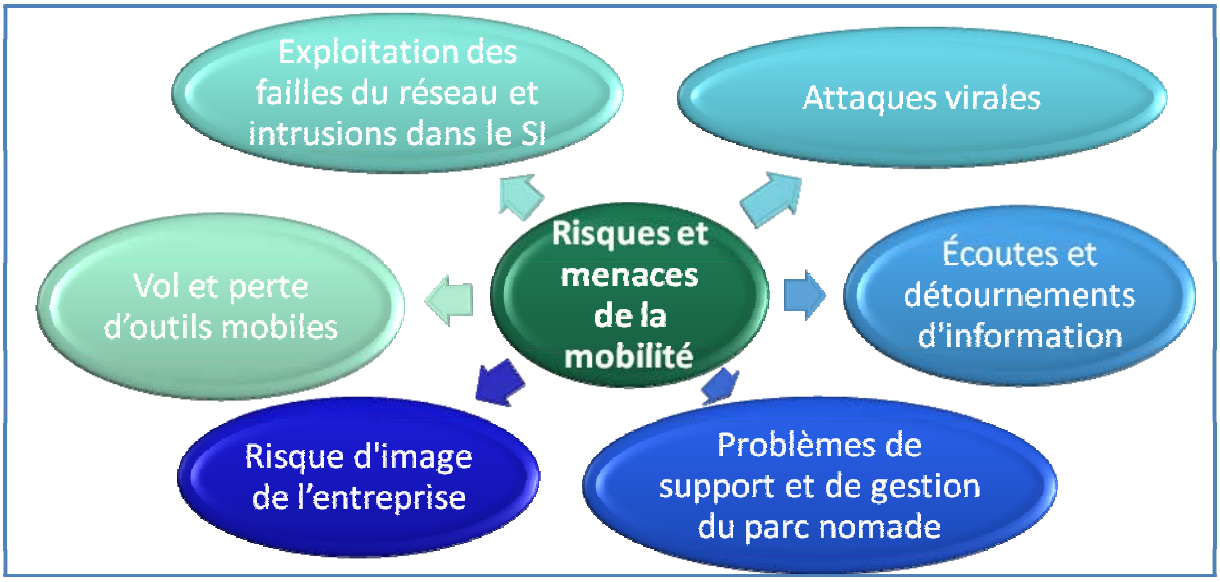

Figure 4 : Les principaux risques

Source : CIGREF

Le principal risque est le vol ou la perte des outils de mobilité. Que ce soit le *Smartphone* ou l'ordinateur portable, ces terminaux mobiles contiennent des informations sensibles, appartenant à l'entreprise, qui sortent du périmètre de sécurité traditionnel. La perte du matériel en tant que tel ne représente quasiment rien en terme financier pour les entreprises, comparativement à la valeur potentielle des informations stockées sur l'équipement.

Ces équipements de mobilité ne peuvent pas être surveillés en temps réel par les administrateurs réseaux ou RSSI car ils ne sont pas en permanence connectés au réseau de l'entreprise. Ces mobiles sont connectés dans des lieux publiques dont les politiques et les besoins de sécurité sont faibles ou hétérogènes ce qui peut augmenter la vulnérabilité de ces outils aux attaques ou écoutes externes.

Enjeux de la mobilité

Les besoins ne sont pas les mêmes selon les entreprises, et selon les utilisateurs au sein d'une même entreprise. En tout état de cause, face aux attentes fortes de leurs utilisateurs finaux, les DSI doivent tenir compte de la culture, et de la sensibilité de l'entreprise à la protection de l'information.

Cette sensibilité dépend de plusieurs facteurs :

- Degré de confidentialité de l'information / Nature de l'information
- Départements et secteurs d'activité de l'entreprise
- Type de projet et pays
- Niveau hiérarchique de l'utilisateur

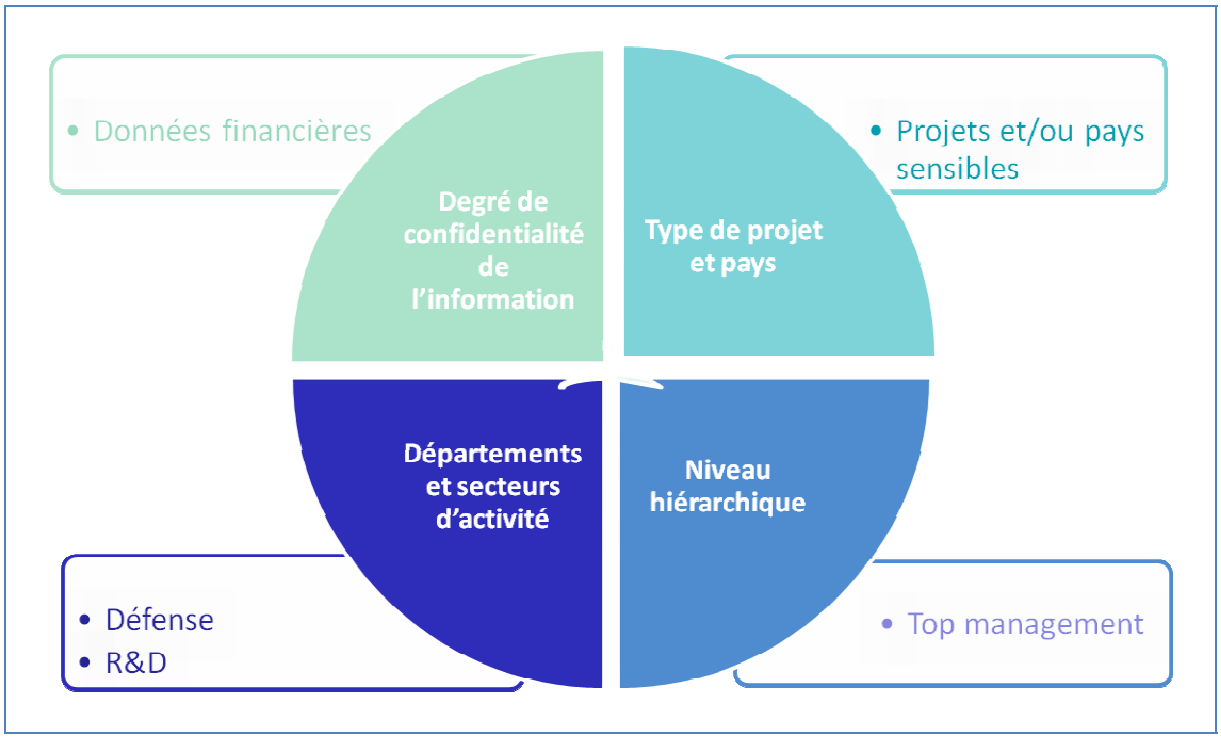

Figure 5 : Enjeux de la mobilité

Source : CIGREF

Le dilemme mobilité - sécurité

Un projet de mobilité est bien souvent mis en place dans le but d'augmenter la productivité. Pouvoir récupérer des documents internes, des messages ou accéder à des applications critiques depuis l'extérieur de l'entreprise est devenu un besoin important. Cependant, afin protéger le SI de l'entreprise il est nécessaire d'appliquer une politique de sécurité assez stricte pour garantir un niveau de sécurité homogène et cohérent dans le temps et dans l'espace.

L'importance économique de la mobilité doit être mise en balance avec le risque moins appréhendable lié aux menaces, qui est plus diffus, plus rare, et dont les conséquences n'entrent pas encore dans le bilan des entreprises.

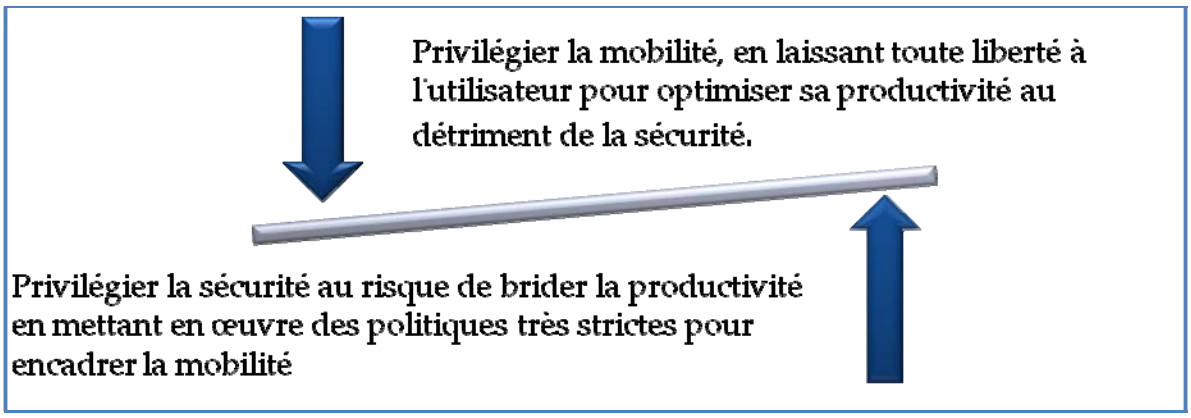

Figure 6 : L'arbitrage mobilité – sécurité

Le principal enjeu est de proposer des solutions simples et ergonomiques aux utilisateurs tout en respectant la politique de sécurité de l'entreprise. Les buts recherchés sont la transparence, la fluidité et la sécurité de cette solution.

Les entreprises doivent déterminer un compromis – propre à chacune d'elle - entre le niveau de services désirés et le niveau de sécurité requis.

3. Solutions techniques

Pour les ordinateurs portables

La sécurisation des ordinateurs portables est un sujet mature dans ses quatre composantes :

- La connexion à distance : Les clients VPN *(Virtual Private Network)* permettent au collaborateur nomade d'accéder de manière sécurisée au SI de l'entreprise lorsqu'il est en déplacement
- L'authentification : une majorité d'entreprises utilise une authentification forte qui consiste en la combinaison de deux éléments d'authentification, par exemple un badge et un mot de passe. La finalité est l'utilisation d'un « *Single sign on* » (SSO) ou authentification unique qui permet à l'utilisateur d'accéder à plusieurs applications avec une seule authentification.
- La sécurité des flux : anti-virus et pare-feu filtrent les flux de l'entreprise et la protège des attaques extérieures.
- Le chiffrement : le chiffrement concerne les données stockées sur le disque dur, ainsi que les données échangées (e-mails et pièces jointes).

Les solutions techniques ont acquis un niveau de maturité suffisant et la sécurisation des portables ne pose plus de difficulté désormais dans les grandes entreprises.

Pour les *Smartphones*

« *Pour les PC, on a fait 90% de ce qu'on pouvait, sur les Smartphones, 10%* »

Le marché récent en pleine évolution, combiné à de nombreux types de terminaux, explique l'immaturité de l'offre. Les principaux Smartphones utilisés en France sont les BlackBerry, les iPhone et les appareils équipés en Windows Mobile.

BlackBerry (RIM) possède une solution native de sécurité et un bon outil de gestion de flotte, *l'iPhone* (Apple) est simple et ergonomique, les terminaux équipés avec le système *Windows Mobile* peuvent bénéficier d'une surcouche de sécurité proposée par des sociétés françaises.

Il existe également des terminaux *Nokia* équipés du système d'exploitation *Symbian* ainsi que des terminaux équipés du système d'exploitation *Android* (Google), ces derniers sont trop récents et peu utilisés en entreprises pour avoir un certain recul sur leur niveau de sécurité.

Le cas *BlackBerry*

Parmi les premières solutions arrivées sur le marché, la solution *BlackBerry* a fait l'objet de nombreuses critiques et rumeurs autour de sa sécurité il y a quelques années. Au cœur du problème se trouvait le NOC (*Network Operating Center*), serveur mutualisé de routage par lequel transitaient les mails entre l'entreprise et le terminal. Ces serveurs mutualisés sont hébergés au Canada, en Angleterre et en Asie. Ses détracteurs ont souligné le côté « boite noire » de la solution, et le risque d'accès aux informations transitant sur ces serveurs par les services étatiques canadiens ou américains.

A l'inverse, RIM a affirmé que la sécurité de son système reposait précisément sur son architecture maitrisée de bout en bout. Et pour répondre à la crainte exprimée sur la localisation des serveurs mutualisés, RIM a également proposé une seconde offre de serveurs, dédiés par entreprise, le BES (*BlackBerry Enterprise Server*) hébergé au sein de chacune des entreprises utilisatrices, permettant de définir les politiques de sécurité de l'entreprise et permettant d'assurer le chiffrement des échanges.

Cette solution intégrée qui rassure certains clients, en inquiète d'autres. Les derniers évènements survenus entre RIM et certains pays (Inde, Arabie Saoudite) montrent que le risque d'interruption de service ou d'écoute existe bien.

Liste noire et liste blanche de Smartphones en entreprise

Utilisés à des fins professionnelles, les *Smartphones* contiennent des données confidentielles de l'entreprise et ils sont une porte d'entrée dans le système d'information de celle-ci.

Pour ces raisons, les entreprises refusent parfois certains terminaux *(blacklist)* ou rédigent des listes de terminaux autorisés (whitelist).

Les raisons de l'interdiction au sein des entreprises sont parfois contradictoires : il y a autant d'entreprises qui refusent le *BlackBerry* que d'entreprises qui le mettent comme seul terminal autorisé

Par ailleurs, il est de plus en plus difficile d'interdire les Smartphones en entreprise : de plus en plus de collaborateurs en sont équipés à titre personnel.

Terminal / Plateforme	Raison de l'interdiction
BlackBerry	Les données transitent sur des serveurs en dehors des entreprises et de l'Union Européenne
iPhone	Peu de solutions de sécurité propres à *l'iPhone* Pas encore de solution conçu pour les entreprises (administration de flotte, sécurité…)
Windows Mobile	Solution de sécurité non native, devant être rajoutée

Figure 7 : Liste de terminaux interdits et raisons invoquées

Risques à utiliser des solutions anglo-saxonnes

Le risque perçu à utiliser des solutions anglo-saxonnes varie d'un secteur d'activité à un autre. Les secteurs d'activité dont les concurrents sont essentiellement américains, y sont très sensibles, ainsi que le secteur de la défense.

La menace principale actuelle qui peut être perçue comme émanant des pays anglo-saxons va provenir également à terme des pays émergeants (inde, chine…).

Recherches de solutions alternatives

Pour les entreprises sensibles à la sécurité de l'information vis-à-vis du monde anglo-saxon, une recherche de solutions alternatives, s'impose. Ces solutions sont dites alternatives soit en raison de leur origine géographique (France), soit en raison de leur origine technologique (open source).

Nous constatons un certain fatalisme dans certaines entreprises françaises au motif que toutes les entreprises possédant au moins une brique américaine dans leur SI (le microprocesseur par exemple).

La concentration se poursuivant (cf le rachat de Mc Affee par Intel), la relation de dépendance avec de « mégafournisseurs » anglo-saxons risque de devenir critique pour les entreprises françaises, dans les années à venir, d'où la nécessité de recourir à des solutions alternatives.

Or les solutions proposées ne sont pas à la hauteur cotée fournisseurs français et on constate un manque de volontarisme côté clients.

Par ailleurs, il n'est pas toujours possible d'imposer des solutions françaises, lorsque les entreprises sont mondiales avec des filiales sur plusieurs continents et des clients à travers le globe.

Utilisation de laboratoire de tests

Certaines entreprises, dans les secteurs les plus exposés aux risques, évaluent souvent les nouveaux produits dans un laboratoire interne.

Utilisation de solutions d'origine françaises

Nos entretiens nous ont permis de constater :

La France présente une multitude de PME dans le secteur de la sécurisation de la mobilité. La société Arkoon a par exemple été citée par une majorité des entreprises[1].

Les entreprises déplorent ce trop grand nombre d'acteurs de petite taille pas toujours adaptés aux entreprises du CAC40. Les performances de leurs solutions ne sont pas adaptées à un grand groupe, le support à l'international est limité, les entreprises peuvent être fragiles financièrement.

Les produits français ont pu être décrits comme très efficaces d'un point de vue sécurité, mais peu ergonomiques et nécessitant des efforts d'intégrations importants. Des solutions intégrées de bout en bout seraient les bienvenues.

Par ailleurs, plus que la nationalité de l'entreprise, c'est la pérennité des produits et la pérennité de l'entreprise qui intéresse les entreprises.

Utilisation de solutions Open Source

On peut citer OpenTrust qui est la seule solution largement utilisée. Elle n'est pas forcément utilisée pour des raisons de coûts, argument en faveur des logiciels libres, mais plutôt pour sa reconnaissance sur le marché.

[1] Arkoon est une entité qui a repris les activités sécurité de Bull, ce qui explique sans doute sa bonne notoriété auprès des grandes entreprises françaises

A part OpenTrust, les solutions Open source ont été très peu citées lors des entretiens. Elles semblent pour le moment très peu utilisées. Cela est sans doute dû d'une part à une offre moindre, et d'autre part à une exigence de niveau de service de la part des clients.

Le tableau ci-dessous reprend les entreprises françaises proposant des solutions de sécurité et leurs principaux concurrents étrangers. Nous avons classé les entreprises selon leur métier principal : opérateur, constructeur, éditeur, intégrateur/SSII, audit/conseil.

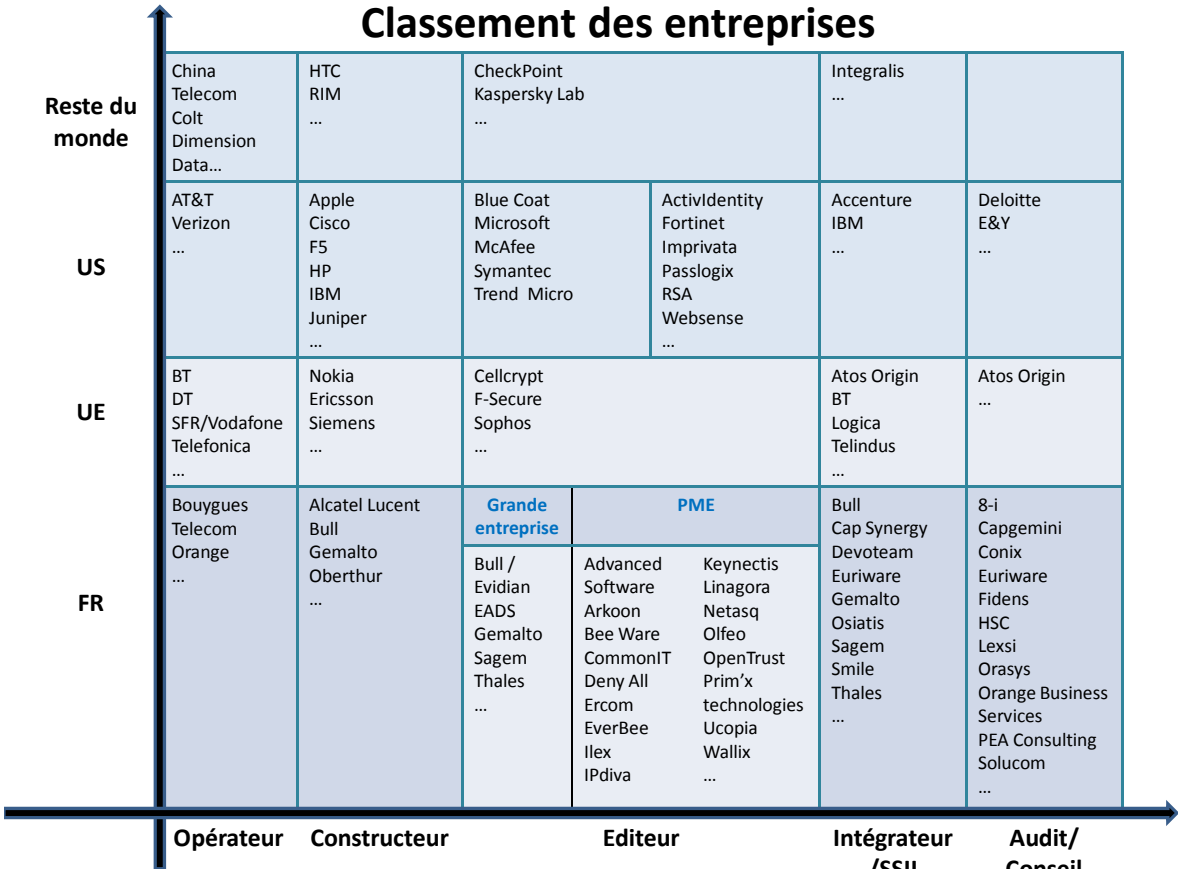

Figure 8 : Classement des entreprises

Source : CIGREF

Puis, pour les entreprises françaises, nous avons classé les produits proposés selon deux axes, le type de terminal pour lequel ils étaient conçus (PC portable, *Smartphone* ou clé USB / média amovible) et la fonction de sécurité qu'ils satisfaisaient (Authentification et gestion des identités, sécurité des données, sécurité des flux, connexion à distance).

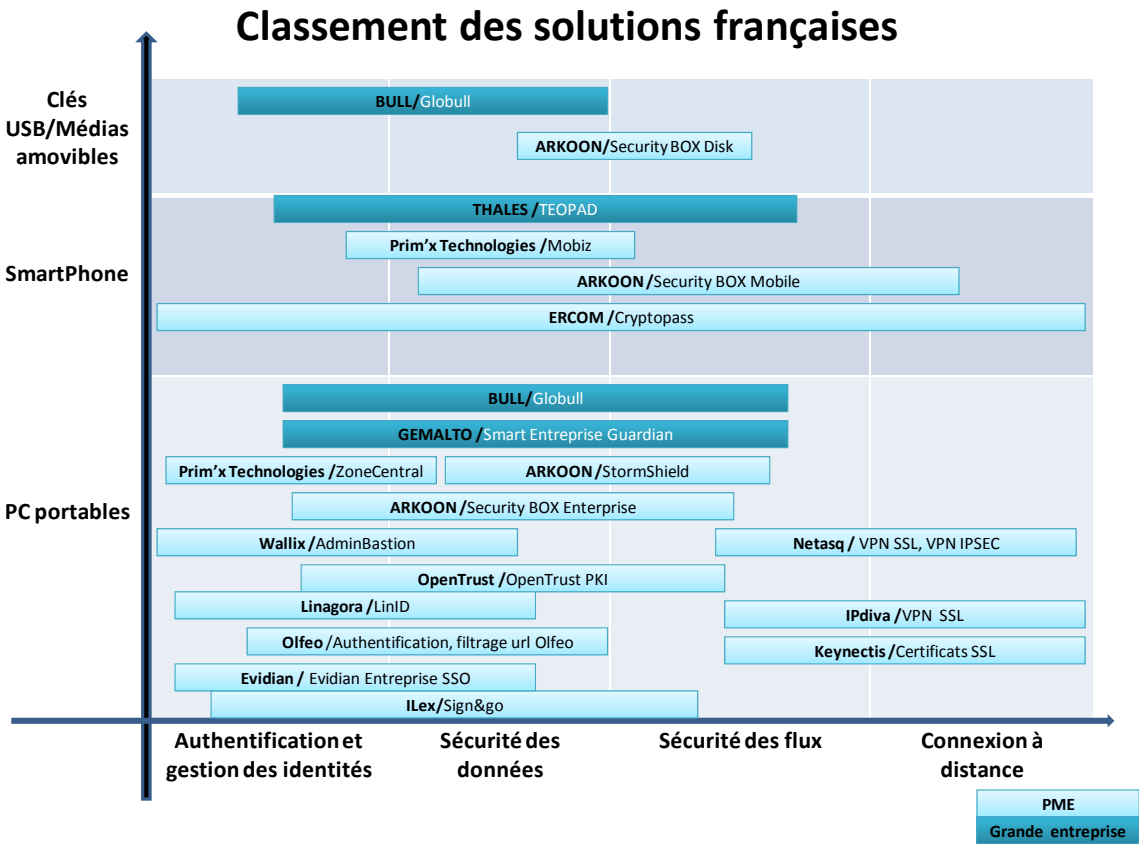

Figure 9 : Classement des solutions françaises

Source : CIGREF

4. Solutions comportementales et organisationnelles

La mise en œuvre d'une solution de mobilité ne s'improvise pas.

Si des technologies sont aujourd'hui disponibles, il est crucial de ne pas négliger la dimension humaine et organisationnelle car les solutions techniques seules ne suffisent pas pour garantir le meilleur niveau de sécurité.

Le risque humain occupe une place centrale dans la politique de sécurité, y compris dans son volet mobilité. Il est donc vital de sensibiliser les collaborateurs en situation de mobilité, par la formation par exemple

Les solutions mises en place montrent qu'à 1/3 ce sont des solutions techniques et les 2/3 restants sont des solutions non techniques.

Solutions organisationnelles

Les entreprises ont toutes intégré une composante humaine dans leur politique de sécurité. Celle-ci se traduit par :

- L'organisation des sessions de sensibilisation par des organismes externes (services de l'Etat)
- L'organisation de sessions de formation en interne : à l'arrivée dans l'entreprise, ou au fil de l'année.

Solutions comportementales

Ces sessions de formation ou de sensibilisation sont axées sur des bonnes pratiques : ce sont un ensemble de comportements qui font consensus et qui sont considérés comme indispensables pour garantir le meilleur niveau de sécurité.

Les bonnes pratiques les plus pertinentes en cas de mobilité (professionnelle ou personnelles) sont :

- Ne jamais vous séparer de l'information sensible (chambre d'hôtel, soute à bagages, train, ...)
- Adopter un profil bas : n'affichez pas plus que nécessaire l'appartenance à votre entreprise
- Éviter les indiscrétions : ne racontez pas votre vie !

- Sélectionner l'information transportée
- Verrouiller son PC avant de le quitter et utiliser des filtres sur les écrans.
- Chaque personne doit avoir et utiliser un câble antivol

Le passeport de conseils aux voyageurs

Afin de renforcer la sécurité en situation de mobilité, l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) avec la participation de ministères, du CIGREF et du CDSE (Club des Directeurs de Sécurité des Entreprises) ont publié un guide de bonnes pratiques, le «Passeport de conseils aux voyageurs » qui a pour but de donner des conseils avant, pendant et après les déplacements professionnels à l'étranger.

Figure 10 : Passeport de conseils aux voyageurs

Source : ANSSI

5. Normes

La normalisation établit des normes et standards à partir des usages et des bonnes pratiques d'un secteur afin d'en harmoniser l'activité.

Elle permet de garantir l'interopérabilité des produits, d'assurer une certaines transparence de la technique, et dans le domaine de la sécurité de limiter la présence de portes dérobées (« *backdoors* »).

Les différents normes

Lors de nos entretiens, nous avons demandé à nos interlocuteurs de citer quelques normes relatives à la sécurisation de la mobilité. Le graphique ci-dessous en présente les résultats consolidés.

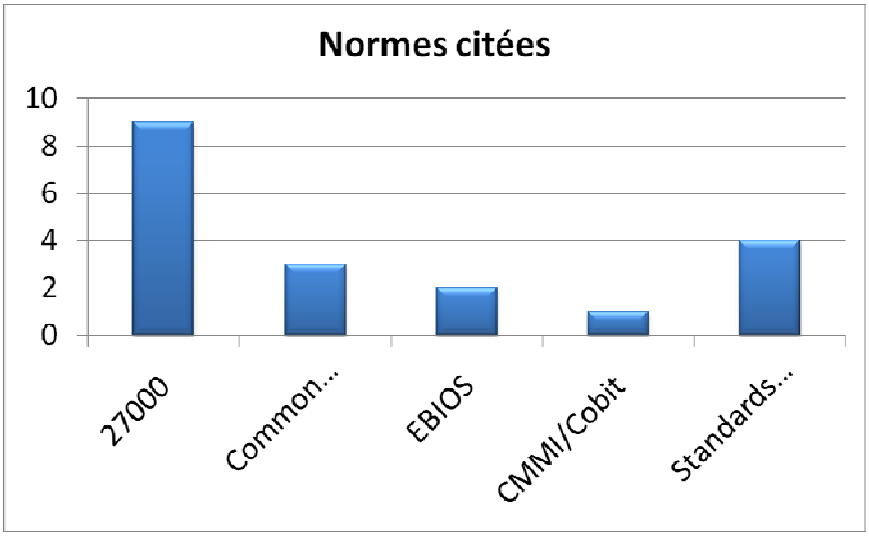

Figure 11 : Normes citées en entretien

Source : CIGREF

Suite 27000

La suite 27000 contient des standards et des bonnes pratiques de management de la sécurité de l'information. Elle est citée par la majorité des interviewés.

Cependant elle n'est pas propre à la mobilité, mais elle aide au management de la sécurité du SI.

Certification Critères communs (*Common Criteria*) – EAL

Common Criteria est un standard international pour les équipements et logiciels de sécurité.

L'Evaluation Assurance Level (EAL) possède 7 niveaux d'assurance d'évaluation. La certification EAL est coûteuse. Elle est surtout utilisée par les fournisseurs pour certifier le niveau de sécurité de leurs produits.

En France, l'ANSSI a certifié des produits dont la liste est disponible ici : http://www.ssi.gouv.fr/site_rubrique53.html

Méthode EBIOS

La méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) permet d'apprécier et de traiter les risques relatifs à la sécurité. Elle est citée par les entreprises du secteur de la défense.

Référentiels CMMI/Cobit

Ils ne sont pas propres à la sécurité ou à la mobilité, mais traitent du management des SI en général.

Standards techniques

Les standards techniques sont nombreux dans le domaine de la sécurité. On peut citer : PKI X509, VPN SSL, IPSEC, IPv6, …Ce sont ces standards qui permettent l'interopérabilité des produits.

Reproches concernant les normes

Toutes les entreprises suivent de près ou de loin certaines normes, et ont plusieurs reproches les concernant :

- La plupart des normes ont été conçues dans un monde pas encore très mobile (sans *Smartphones* par exemple)
- Leur mise en œuvre est longue et les normes ne sont pas toujours adaptées aux usages des grandes entreprises.
- Elles répondent d'abord aux enjeux des organismes de certification qui ont développé un écosystème autour de la mise en place de cette certification.
- Elles traitent du système de management de la sécurité, mais pas du niveau réel de sécurité

6. Recommandations

L'accroissement de l'usage de l'internet mobile, des technologies de l'information et de la communication ainsi que la volonté des entreprises d'augmenter leur agilité et leur réactivité par le biais de la mobilité font de la prévention du risque informationnel une priorité majeure de toutes les entreprises françaises.

Les recommandations du CIGREF en matière de sécurisation de la mobilité sont les suivantes :

1. **Créer un écosystème de fournisseurs français ou européens**
   - **Une liste d'acteurs français de la sécurité a été établie** afin de dresser un panorama de l'offre nationale actuelle en matière de sécurisation de la mobilité.
   - **Les grandes entreprises françaises souhaitent que les fournisseurs français ou européens « têtes de file » bâtissent une offre de sécurité de bout en bout**, alternative aux solutions essentiellement américaines.

2. **Continuer à sensibiliser les utilisateurs** – Au-delà des solutions techniques, une approche par des solutions comportementales et organisationnelles est indispensable. **Le passeport pour les voyageurs** élaboré par l'ANSSI avec le CIGREF est une première avancée sur ce sujet.

3. **Contribuer à l'émergence de véritables normes et standards spécifiques à la sécurisation de la mobilité** - La sécurisation de la mobilité doit également reposer sur l'utilisation des normes et des standards.

4. **Renforcer les partenariats avec l'Etat**
   - **Relayer les évaluations de l'Etat auprès des entreprises et faire part à l'Etat des contraintes des entreprises**. L'état enfin doit contribuer à stimuler et consolider l'offre française actuelle. Cela peut se traduire par une meilleure communication sur le processus d'évaluation de la performance des solutions de sécurité existantes ou nouvelles, ou encore la participation d'acteurs privés ou associatifs au processus d'évaluation public, afin d'aider les entreprises à choisir les meilleures solutions.
   - **Piloter l'innovation.** Afin de renforcer cette offre, l'état français doit soutenir les PME innovantes en matière de sécurité, intégrer de manière systématique le thème de la sécurité dans son dispositif de soutien aux PME innovantes. **Le thème de la sécurité de la mobilité doit être un des axes majeurs de la politique de soutien à l'innovation de l'Etat.**

5. **Le CIGREF peut servir de plateforme d'échange** et aider à renforcer les échanges entre l'industrie, les clients et l'état français, par exemple en contribuant via ses membres au processus d'évaluation de la performance des solutions de sécurité mis en place par les pouvoirs publics, **mais également de centre d'expertise** pour tout ceux qui veulent " ... mieux comprendre les enjeux de la sécurité des usages numériques" à l'image de la formation mise en place récemment en partenariat avec l'INHESJ.

6. **Les grandes entreprises doivent prendre conscience de leur rôle et animer leur écosystème.**
    - Les grandes entreprises ont-elles aussi **un rôle moteur à jouer dans l'animation de bout en bout de la sécurité au sein de leur écosystème**. Les grandes entreprises seules ont la capacité à créer et orienter un marché, de part leur volume d'achats et leur cahier des charges.
    - Les grands groupes et les PME pourraient **participer aux exercices nationaux de sécurité ou de gestion de crise** organisés par l'ANSSI ou l'élaboration de « Livres blancs » ou aux guides de bonnes pratiques en matière de sécurité.
    - Enfin les entreprises peuvent **se regrouper au sein de structures associatives** ad hoc, à l'instar de ce qui s'est fait en matière de ebusiness ou d'archivage, afin de bâtir des cahiers des charges communs, en vue de mieux structurer le marché et d'orienter l'offre.