Sujet national pour l'ensemble des centres de gestion organisateurs

INGENIEUR TERRITORIAL

EXAMEN PROFESSIONNEL DE PROMOTION INTERNE

SESSION 2014

Etablissement d'un projet ou étude portant sur l'option choisie par le candidat au moment de son inscription.

Durée : 4 heures
Coefficient : 5

INFORMATIQUE ET SYSTEMES D'INFORMATION

OPTION : SYSTÈMES D'INFORMATION ET DE COMMUNICATION

À LIRE ATTENTIVEMENT AVANT DE TRAITER LE SUJET :

- Vous ne devez faire apparaître aucun signe distinctif dans votre copie, ni votre nom ou un nom fictif, ni votre numéro de convocation, ni signature ou paraphe.

- Aucune référence (nom de collectivité, nom de personne, ...) **autre que celles figurant le cas échéant sur le sujet ou dans le dossier** ne doit apparaître dans votre copie.

- Seul l'usage d'un stylo soit noir soit bleu est autorisé (bille à encre non effaçable, plume ou feutre). L'utilisation d'une autre couleur pour écrire ou souligner sera considérée comme un signe distinctif, de même que l'utilisation d'un surligneur.

- Le non-respect des règles ci-dessus peut entraîner l'annulation de la copie par le jury.

- Les feuilles de brouillon ne seront en aucun cas prises en compte.

Ce sujet comprend 30 pages
Il appartient au candidat de vérifier que le document comprend le nombre de pages indiqué

- Vous préciserez le numéro de la question et le cas échéant de la sous-question auxquelles vous répondrez.
- Des réponses rédigées sont attendues et peuvent être accompagnées si besoin de tableaux, graphiques, schémas...

Vous êtes recruté comme ingénieur territorial à la Direction des systèmes informatiques du Conseil Général de X, 7 000 agents, rattaché au Directeur des Systèmes d'Information en tant que chargé de mission « informatique innovante ».

Depuis quelques années, de nombreux agents du département ont peu à peu pris l'habitude d'utiliser leurs outils informatiques et téléphoniques personnels (PC, tablettes, smartphones...) pour se connecter au système d'information de la collectivité, pratique connue sous le nom de BYOD (Bring Your Own Device). Ce phénomène s'est développé au fil de l'eau sans réel contrôle d'opportunité, les ouvertures d'accès s'effectuant à la demande et sans vérification des moyens utilisés pour se connecter. Un inventaire a été effectué et il s'avère qu'environ 150 personnes de tous horizons (élus, personnel de la DSI, décideurs...) accèdent de manière plus ou moins fréquente au système d'information de la collectivité via leurs outils personnels.

Nouvellement arrivé, le Directeur des Systèmes d'Information s'inquiète du développement anarchique de ces connexions et souhaite formaliser davantage l'accès au système d'information de la collectivité.

Pour appuyer sa démarche, le Directeur des Systèmes d'Information vous demande, à l'aide des documents joints et de vos connaissances personnelles, de répondre aux questions suivantes :

Question 1 (5 points) :

Rédigez une note sur les caractéristiques comparées du BYOD et du CYOD.

Question 2 (5 points) :

Détaillez les contraintes techniques et juridiques afférentes au BYOD.

Question 3 (10 points) :

Proposez un plan de refonte concerté des accès au sein du département en expliquant votre choix (BYOD ou CYOD) et en détaillant les étapes du projet.

Liste des documents joints

Document 1 :	« Après le BYOD, voilà le CYOD » - *demainlemail.com* - 18 novembre 2013 - 1 page
Document 2 :	« BYOD et enjeux de sécurité » - *demainlemail.com* - 17 janvier 2013 - 2 pages
Document 3 :	« Les enjeux du BYOD : avantages ou risques» - *it-expertise.com* - 5 décembre 2012 - 8 pages
Document 4 :	« BYOD, COPE, CYOD ou comment satisfaire les demandes des utilisateurs en minimisant les risques pour l'entreprise » - *netetcom.wordpress.com* - 25 novembre 2013 - 3 pages
Document 5 :	« Pour ou contre la pratique du BYOD : quelques réponses juridiques »- www.dwavocat.com - 18 novembre 2013 - 3 pages
Document 6 :	« Le CYOD : le juste milieu entre BYOD et fourniture de l'appareil ? » - *zdnet.fr* - 18 novembre 2013 - 1 page
Document 7 :	« BYOD, BYOA : quel encadrement juridique ?» - *sfrbusinessteam.fr* - 5 décembre 2012 - 2 pages
Document 8 :	« Polémique DSI : Faut-il interdire l'usage des outils personnels à des fins professionnelles ? »- *Pro.01net.com* - 4 avril 2013 - 2 pages
Document 9 :	« Les précautions à prendre pour passer en mode BYOD » - *Pro.01net.com* - 4 octobre 2013 - 3 pages
Document 10 :	« BYOD : définition, enjeux et impacts » - *demainlemail.com* - 27 mars 2012 - 2 pages

Documents reproduits avec l'autorisation du CFC

Certains documents peuvent comporter des renvois à des notes ou à des documents non fournis car non indispensables à la compréhension du sujet

DOCUMENT 1

Après le BYOD, voilà le CYOD

Le **BYOD**, nous vous en avons déjà parlé, consiste à ce que les employés utilisent leur terminaux personnels (mobile, tablette ou même ordinateur) dans un cadre professionnel. Cette pratique, qui se démocratise de plus en plus, est source d'économies substantielles pour les entreprises et évite un temps précieux de formation, les employés étant tout à fait capables d'utiliser leurs propres outils.
Malgré cela, le **BYOD** effraie encore un grand nombre de **DSI**. Leurs plus grandes craintes concernent la sécurité des données, l'écroulement de la barrière vie privée/vie personnelle et la disparité d'équipement entre les différents employés.
Pour pallier ces problèmes, une nouvelle tendance se développe : le **CYOD** pour Choose Your Own Device. Petit frère du BYOD, le **CYOD** permet aux employés de choisir le terminal qu'ils souhaitent parmi une gamme approuvée par la direction.
Si les avantages économiques sont nettement moindres par rapport aux **BYOD**, la sécurité en est elle renforcée. En effet, les **DSI** gardent le contrôle de leur flotte mobile et peuvent s'assurer de la bonne utilisation des terminaux. Pour l'employé, c'est un confort de choisir le modèle qui lui convient le mieux et on peut ainsi noter un certain gain de productivité. De plus, cet avantage en nature est généralement très apprécié.
Certes, le système n'est pas encore parfait mais il semble être un bon compromis pour les entreprises ainsi que pour les employés et semble être une réponse adaptée à la plupart des craintes évoquées à ce jour par les DSI.

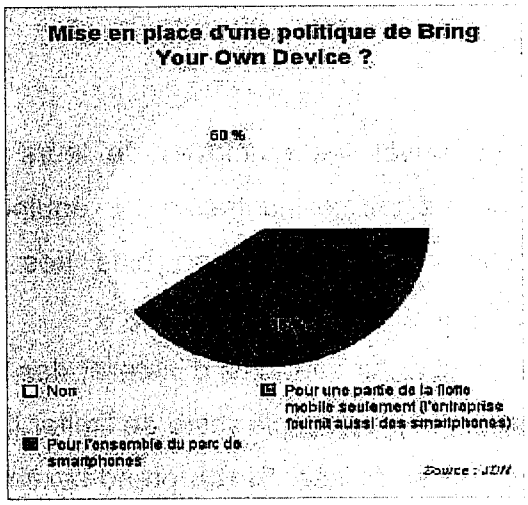
18 novembre 2013 - demainlemail.com

DOCUMENT 2

BYOD et enjeux de sécurité

Nous vous avions présenté il y a quelque temps, le phénomène du BYOD, Bring Your Own Device. Cette tendance grandissante reflète le fait que les employés se servent de plus en plus de leurs outils personnels (ordinateurs, smartphones, tablettes, ...) comme outils de travail. La messagerie en est une composante essentielle car l'email est l'application la plus utilisée dans les entreprises.

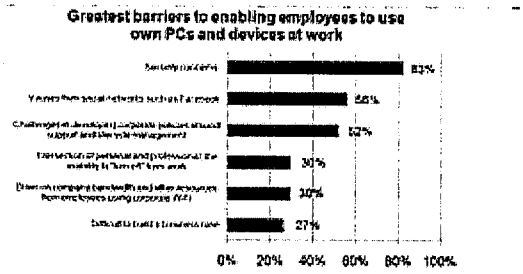
A l'heure où les smartphones sont de plus en plus la cible des attaques virtuelles, le BYOD inquiète nombre de DSI. En effet, en France, seuls 40% des DSI voient le BYOD (total ou partiel) comme un élément positif de développement pour l'entreprise là où ils sont 80% aux Etats-Unis.



Les avantages de ce système sont pourtant nombreux : augmentation de la productivité, satisfaction au travail mais surtout réduction importante des coûts (de 10 à 25%). Sans compter le temps de formation, les employés étant la plupart du temps parfaitement opérationnels sur leur propre matériel. Ils sont, de plus, plus enclins à en prendre soin étant donné qu'ils les ont financés eux-mêmes.

Malgré ces avantages, la sécurité reste le souci principal de 83% des DSI. En autorisant les employés à utiliser leurs terminaux personnels dans un cadre professionnel, beaucoup d'entre eux craignent pour la sécurité des données de

l'entreprise, que ce soit au sujet de leur diffusion ou à l'entrée de virus ou logiciels malfaisants dans le système informatique de l'entreprise.



Les principaux risques proviennent des pertes et vols du matériel. En France en 2010, 630 000 téléphones portables ont été dérobés. Si se faire voler son téléphone est déjà gênant, cela devient réellement problématique si des données relatives à l'entreprise y sont contenues. Comptes emails, documents confidentiels, contacts, agendas, autant de raisons pour les DSI de craindre la montée du BYOD.

Il ne faut pas non plus oublier le danger que représente l'espionnage industriel. Octobre rouge par exemple, la dernière menace d'espionnage industrielle détectée par Kaspersky, est capable de voler des données des terminaux mobiles tels que les smartphones (Apple et Windows phone).

Quelles solutions ?

Il paraît évident qu'il est impossible de priver les employés de leurs outils de communication et que les empêcher de les utiliser au travail, ou équiper tout le monde avec des modèles de fonction ne sont pas non plus des solutions envisageables pour tout le monde. Alors que faire ?

Si certains fournisseurs sont aujourd'hui tout à fait capables d'installer des systèmes personnels et professionnels indépendants, le plus simple reste de limiter l'utilisation des principales applications à des systèmes sécurisés. Si l'on prend l'exemple de la messagerie, qui est un des usages principaux du BYOD avec la consultation de documents, il est tout à fait possible d'utiliser des systèmes sécurisés, tels qu'Alinto Motion pour la messagerie. L'accès peut être sécurisé grâce à une connexion SSL et les messages n'ont pas à être téléchargés localement. Ainsi, en cas de pertes ou de vol, les données ne sont pas perdues. De plus, l'accès peut être contrôlé par les entreprises. De tels systèmes permettent une mise en place sécurisée du BYOD et donc de réduire grandement les risques liés à cette pratique.

17 janvier 2013 - demainlemail.com

DOCUMENT 3

Les enjeux du BYOD : avantages ou risques ?

Aux Etats-Unis, environ 35% des employés achètent personnellement le smartphone qu'ils utiliseront pour leur travail selon une récente étude de Forrester Research. **Cette tendance présente des défis certains pour l'entreprise. Devons-nous contrôler ou encadrer ce phénomène ? Faut-il l'ouvrir aux tablettes ? Comment aborder le sujet ? Quelles sont les risques pour la propriété intellectuelle de l'entreprise ? Quels sont les outils disponibles et comment les utiliser ?**

Le mouvement a commencé il y a une dizaine d'années avec l'arrivée des smartphones. Les collaborateurs étaient équipés de façon standard avec des terminaux dont la marque et le modèle avait été décidés par l'IT de l'entreprise selon des critères reposant principalement sur leurs fonctionnalités et leur capacité à être administrés (là encore par l'IT). La standardisation de fait des protocoles de communication mobile a bouleversé ce mode de fonctionnement et a permis aux collaborateurs d'acheter leur propre smartphone au look sexy et à la mode à des fins professionnelles. Les premiers pas du « Bring Your Own Device » (BYOD) étaient effectués. Ce phénomène s'accompagne ou est amplifié avec l'arrivée en entreprise de collaborateurs non seulement habitués à utiliser les outils informatiques mais aussi souhaitant personnaliser et s'approprier les outils qui sont mis à leur disposition. (http://download.microsoft.com/documents/France/Entreprises/2009/Reference-des-Usages-IT-au-travail.pptx).

Avantages ou risques ?

C'est la première démarche qu'il faut avoir sur le BYOD. Autant les risques sont souvent très vite identifiés (parfois amplifiés) par le département IT autant les avantages peuvent être plus difficiles à cerner.

Les risques ou les défis qui vont être rencontrés par un département IT vont être autant techniques qu'organisationnels. Ils concernent les sujets suivants :

- **Le matériel** : au lieu d'avoir à supporter un nombre limité de types de matériels, si les employés ne peuvent pas gérer leur propre support, l'entreprise peut se retrouver à devoir supporter des centaines de modèles différents avec des problèmes très variés. Il arrive fréquemment qu'une entreprise signe un contrat global avec un fabriquant et les employés peuvent sélectionner leur modèle au sein d'une gamme prédéfinie afin de limiter la multitude de modèles de PC.
- **Le coût de l'infrastructure** : un programme BYOD robuste implique que l'entreprise puisse supporter et forcer un standard comme par exemple un anti-virus. Il est alors nécessaire de mettre en œuvre et de maintenir une infrastructure très robuste pour des sujets comme les accès distants, le déploiement d'application…

- **La sécurité** : ce défi ne concerne pas seulement les anti-virus mais aussi la sécurité, confidentialité, protection des informations de l'entreprise et la capacité à éviter leur fuite.
- **Les politiques du département IT** : une démarche de type BYOD entraine une perte de contrôle du département IT sur certains aspects de la sécurité du poste de travail. Cette perte de contrôle doit s'accompagner d'une révision certaine et approfondie des politiques de sécurité. Ces modifications doivent être communiquées auprès des différents ayant-droits, des entités métier et bien sûr signées par les participants au programme BYOD.
- **Les considérations légales et humaines** : dans une démarche BYOD, les données personnelles et professionnelles vont être amenées à coexister sur le même matériel. Le bon sens veut que l'entreprise ne finance que les applications qui sont nécessaires à la réalisation de l'activité de l'employé. Cependant, il faut définir les implications et responsabilités notamment légales si du contenu inapproprié est découvert sur le périphérique de l'employé ou si des applications illicites y sont installées. La situation où le périphérique en question est volé ou perdu doit aussi être prise en considération.
- **L'exposition aux risques divers de l'IT sera accrue**. Le Gartner estime que 4 à 8% des PC d'entreprise (Gartner Report ID : G00206248) sont compromis par des malwares divers incluant les botnets alors que ce taux est de 20 à 30% selon Microsoft sur l'ensemble des PCs des consommateurs. Avec la mise en œuvre d'une démarche BYOD il faut s'attendre à une augmentation du taux d'infection des machines.

Les risques exposés sont à prendre en compte mais ne doivent pas faire perdre de vue les bénéfices liés à la mise en place d'un tel projet :

- **Redonner du pouvoir aux employés**: le simple fait de laisser les employés d'une entreprise pouvoir choisir et utiliser le périphérique qu'ils souhaitent leur donne le sentiment de propriété. Ce sentiment va faciliter la prise en main, réduire le temps lié à l'adoption, et à l'apprentissage des interfaces tout en augmentant le niveau global de satisfaction.
- **Réduire les coûts**: les utilisateurs sont plus à même de comprendre le fonctionnement de leur équipement et de supporter ou d'effectuer de simples opérations de maintenance. De la même façon qu'ils le font avec les équipements qu'ils possèdent à la maison. Les services et les garanties des constructeurs viennent en support de cette démarche qui peut, en quelque sorte, s'apparenter à de l'outsourcing du support du matériel informatique. L'organisation IT peut alors se recentrer sur les éléments qui sont critiques pour le succès d'un projet BYOD à savoir l'infrastructure et la sécurité.
- **Flexibilité**: en utilisant le même périphérique pour leurs activités personnelles et professionnelles, les employés ont un maximum de flexibilité pour organiser leur emploi du temps. Avec l'effacement que l'on constate des frontières entre vie professionnelle et vie personnelle, il est ainsi possible d'avancer sur un projet à la maison comme, par exemple, permettre de répondre à un mail personnel lors du temps de présence au bureau.
- **Mobilité des employés**: avec les évolutions économiques actuelles, la mobilité des employés est une force pour les entreprises. Que ce soit avec la réduction du temps de présence au bureau, la réduction des déplacements ou au contraire les « road warriors » de plus en plus au contact des clients, une démarche BYOD facilitera ce mode de travail à distance ou en mobilité en permettant l'accès à l'information en toute sécurité depuis n'importe quel réseau connecté à Internet.

- **Réutilisation des anciens équipements**: les technologies qui sont mises en œuvre pour soutenir une démarche BYOD vont permettre de réutiliser les anciens matériels comme un simple terminal pour se connecter à une infrastructure de type VDI (Virtual Desktop Infrastructure).
- **Technophiles** : les employés technophiles vont pouvoir utiliser dans leur environnement professionnel les mêmes outils que ceux qu'ils utilisent à la maison. Le BYOD est un des éléments qui permet d'attirer (et de retenir) ce type de population au sein des entreprises. Ces outils concernent les smartphones, les PC, les tablettes mais aussi les réseaux sociaux ou les différents services en ligne.

Le vrai défi pour le département IT est au final de faire en sorte que, quel que soit le propriétaire du périphérique, tout fonctionne de façon fluide TOUT EN GARANTISSANT le respect de la propriété intellectuelle de l'entreprise. Face à ces risques et bénéfices, faut-il implémenter un projet BYOD au sein de son entreprise ou faut-il au contraire tout mettre en œuvre pour éviter ce mouvement ? Faut-il contrôler ou encadrer cette « consumérisation de l'IT » ?
L'entreprise doit prendre une position claire pour l'une ou l'autre de ces deux approches. La responsabilité de l'IT est de vérifier que la politique choisie est bien suivie et de fournir aux équipes de direction, pour chaque plate-forme, une liste des périphériques non-autorisés y accédant et évaluer le risque associé. Toute zone d'ombre sera un risque d'intrusion illicite ou de fuite d'informations confidentielles.
A l'occasion de cette démarche d'encadrement de la consumérisation de l'IT, il est important de considérer l'usage de périphériques mais aussi l'utilisation de services en ligne fournis par exemple par Facebook, Google ou encore Microsoft. Les contrats d'utilisation de ces services ayant des implications juridiques qui peuvent mettre en cause l'entreprise.

Quelle démarche faut-il adopter pour un projet BYOD ?

Pour réussir son projet BYOD, il est important d'adopter une démarche structurée qui ne concerne pas seulement la technique mais aussi les populations qui seront impactées. La démarche peut se résumer en cinq grandes étapes :

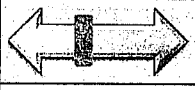
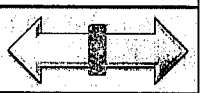
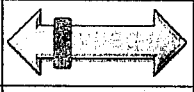
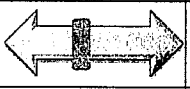
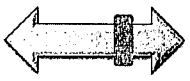
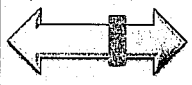
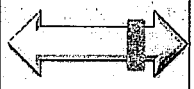
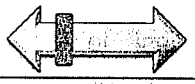
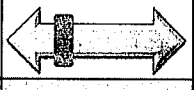
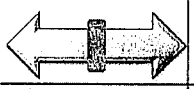
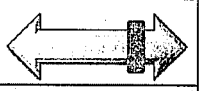
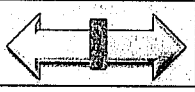
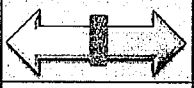
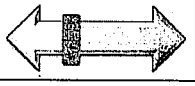
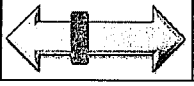
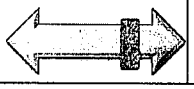
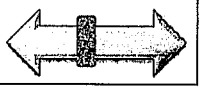
- Identifier les drivers, objectifs et périmètre du projet.
- Comprendre et évaluer les profils au sein de votre organisation
- Mesurer l'impact du projet sur l'IT
- Mise en place conjointe du plan au sein de l'IT, des Ressources Humaines et du département juridique
- Communication et adoption

Il est important de comprendre la population qui sera affectée par le projet. En fonction de leur profil de travail et de consommateur, ces utilisateurs auront des attentes différentes face au projet. En fonction de ces attentes, il sera alors possible de classifier les utilisateurs selon quatre modèles. Le graphique ci-dessous présente ces modèles selon le degré de liberté permis pour l'utilisateur et le niveau de risque associé à un modèle.

Selon le modèle choisi les politiques appliquées seront :

- **Strictes**, **option « voici le vôtre »,** le principe est relativement proche de ce qui est en place dans la majorité des entreprises à savoir un device prédéfini pour chaque rôle.
- **Flexible, options « choisir le sien » ou « apporter le sien »** qui consiste à choisir le périphérique dans une liste pré-approuvée. L'IT peut soit procéder aux achats ou laisser les employés acheter un matériel approuvé.
- **Sans politique, option « indépendance »**. Tout périphérique est accepté.

Lors de cette étape d'évaluation des différents modèles d'implémentation du BYOD il faut, pour chaque modèle, estimer les points suivants : risque business, utilisation des applications métier, niveau de collaboration, degré de mobilité, engagement envers la technologie.
Par exemple, une population d'ingénieurs aura a priori une appétence pour des systèmes puissants et performants qu'ils maintiendront eux-mêmes, alors qu'une population de commerciaux cherchera à avoir un périphérique très mobile sans vouloir se préoccuper de la maintenance.
On obtient ainsi une matrice qui permet de définir les facteurs de productivité pour chacun des modèles BYOD. Cette matrice sert de base pour choisir un modèle plutôt qu'un autre pour un profil de population donnée.

	Juriste	**Executif**	**Ingénieur**	**"Task Worker"**
Besoins de collaboration				
Mobilité				
Accès aux applications métiers				
Données classifiées				
Adaptabilité aux innovations				
Utilisateur "consommateur"				

Pilotes de productivité et Stratégie BYOD

L'impact du projet BYOD sur l'IT de l'entreprise est certain. Au minimum ces quatre domaines seront impactés:

- **Support** : en fonction du modèle adopté le support technique de l'entreprise ne sera pas impliqué de la même façon. Dans le cas d'une approche où l'utilisateur choisit son propre matériel, ce dernier sera peut-être amené à contacter le support du constructeur du matériel en question.

- **Infrastructure** : certains changements seront à effectuer au niveau de l'infrastructure pour laisser un accès réseau complet seulement aux périphériques complètement gérés et mettre en quarantaine ceux non gérés tout en leur laissant la possibilité d'accéder aux applications web ou à une infrastructure de type VDI.
- **Applications** : les applications doivent être repensées pour pouvoir être déployées simplement sur des environnements très diversifiés.
- **Licences** : certains modèles d'implémentation imposeront une révision de la gestion des licences. En effet si le PC est couvert pas une licence OEM, il n'est pas nécessaire d'avoir une licence en volume pour ce périphérique mais si l'utilisateur accède à une application déployée en tant que « RemoteApp », une CAL (Client Access License) sera toutefois nécessaire. Il faut aussi prendre en compte les licences nécessaires pour une architecture autour de postes clients virtualisés.

Finalement, la mise en œuvre du projet nécessite une bonne synchronisation avec les équipes des ressources humaines, du département juridique et les équipes de direction.
Les nouvelles règles qui seront mises en œuvre avec ce projet doivent intégrer des paramètres techniques comme les spécifications techniques minimales d'un périphérique accepté (aussi bien sur un plan matériel que logiciel) ou encore qui paye (et combien) pour le support. Il est aussi nécessaire de revoir les politiques d'accès distant, de conformité des périphériques ou encore de stockage des données sensibles de l'entreprise.
Il faut aussi penser à adresser la procédure à suivre dans le cas d'une rupture du contrat de travail. Comment gérer le nettoyage des données d'un poste de travail qui n'appartient pas à l'entreprise ? Quelle est la responsabilité de l'entreprise et de l'utilisateur ?

Quelles sont les solutions techniques ?

Aucun projet BYOD ne peut réussir sans une bonne préparation voire une mise à jour sérieuse de l'infrastructure IT de l'entreprise. Plusieurs technologies complémentaires peuvent être mises en œuvre pour adresser ou limiter les risques associés à chaque domaine :

- Périphérique
- Données
- Réseau
- Applications

La gestion des périphériques est un sujet adressé depuis plusieurs cycles d'évolution de l'IT. Actuellement plusieurs solutions comme System Center Configuration Manager de Microsoft existent sur le marché permettant de gérer tout type de périphérique. Que celui-ci utilise un OS pour mobiles (type iPhone, Android ou Windows Phone), un OS client plus traditionnel comme Windows, Linux ou Mac OS. Ces solutions permettent d'appliquer des politiques sur ces périphériques ayant accès à des données de l'entreprise.
Comme l'accès au réseau d'entreprise peut être limité pour certains périphériques, il peut être judicieux d'évaluer l'intérêt d'implémenter une solution de type Cloud qui offre la même capacité que la solution d'entreprise évoquée ci-dessus. Cette approche permet ainsi de gérer les périphériques clients qui sont dans le projet BYOD, sans que ceux-ci ne soient nécessairement sur le réseau de l'entreprise. Cette gestion permet entre autres

d'évaluer le niveau de conformité des postes de travail utilisés par les employés par rapport à un niveau de référence défini par l'IT.
Le sujet des données est probablement le plus sensible pour une entreprise en ce début du 21ième siècle. Ces données peuvent souvent être classifiées en catégories, par exemple : LBI – Low Business Impact / MBI – Medium Business Impact / HBI – High Business Impact. A chaque classification peuvent être appliqués des critères de diffusion au sein de l'entreprise et à l'extérieur de l'entreprise. Les documents de format Office peuvent être chiffrés automatiquement en fonction de classifications appliquées par les utilisateurs ou automatiquement en fonction de critères définis par l'entreprise. Par exemple si un fichier contient des numéros de carte de crédit il ne pourra ainsi ni être imprimé ni lu à l'extérieur de l'entreprise par une personne non autorisée.

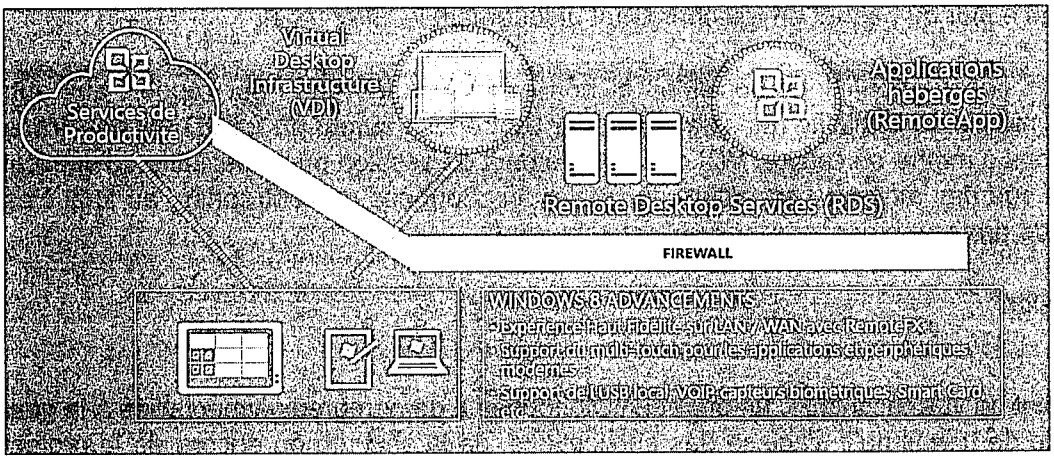
Avec l'arrivée du BYOD, la simple gestion des accès à un document ou à une ressource sur le réseau ne suffit plus. Il faut prendre en compte un paramètre supplémentaire : le périphérique depuis lequel on accède aux données. Le concept *d'accès dynamique à l'information (Dynamic Access Control)*, se basant sur un contrôle d'accès à base de *claims*, permet d'intégrer ce nouveau paramètre. Par exemple, un utilisateur peut avoir accès à un fichier depuis un système membre du domaine, mais n'aura plus accès au même document depuis un système non membre du domaine.

Avec la mise en œuvre d'un tel projet, l'accès principal au réseau ne sera plus le réseau local de l'entreprise mais Internet. Ce changement de paradigme veut dire que l'architecture réseau actuellement en place sera à faire évoluer pour mettre en œuvre des solutions permettant de segmenter et simplifier les accès réseaux des différents types de périphériques. Un PC membre du domaine, à jour en terme de correctif de sécurité et de mises à jour pourra bénéficier d'un accès de type Direct Access lui donnant ainsi un accès sécurisé à l'ensemble des ressources de l'entreprise. Pour les postes non membre du domaine, un accès VPN limité à certaines ressources pourra par contre s'avérer être un choix judicieux.

Lors de la présence sur site, sur le réseau local de l'entreprise, la mise en place de solutions de type NPS (Network Policy Server) peut permettre de laisser un accès libre au réseau aux machines du domaine mais rediriger les périphériques non gérés dans un réseau spécifique avec accès uniquement aux services de publication d'application ou d'accès aux données que nous allons détailler ci-après.
Reste à définir comment déployer les applications sur des postes de travail qui n'appartiennent pas à l'entreprise. Dans le cas d'une rupture du contrat de travail, comment récupérer la licence associée ? Il faut raisonner non plus sous la forme de déploiement de l'application mais plutôt de mise à disposition de celle-ci. Plusieurs technologies modernes permettent de répondre à ce besoin :

- Applications de productivité
- Poste de travail virtualisé
- Virtualisation de présentation ou de session
- Virtualisation d'application

Mise en oeuvre du BYOD



Comme la connectivité principale des postes BYOD est Internet, pour les applications de productivité, comme Office, un accès aux solutions de productivité en ligne, comme Office 365 de Microsoft, est à prendre en considération, car elle simplifie grandement le déploiement et la mise à jour des applications utilisées par tous. La double disponibilité sous la forme d'application web et disponibles à la demande sur le poste de travail permet aux utilisateurs de cette solution de choisir l'outil le mieux adapté à leur mode de travail.

Le poste de travail virtualisé permet de mettre à disposition des utilisateurs un poste de travail complet personnalisé ou standardisé. Dans les deux cas, le système d'exploitation tourne dans un pool de machines virtuelles qui sont allouées lors de la connexion des utilisateurs. Ces machines tournent sur un ou plusieurs hôtes au sein du datacenter de l'entreprise. Cette approche présente l'avantage de sécuriser les données de l'entreprise mais ne doit pas être considérée pour simplifier la gestion du parc. Les opérations de maintenance et de mise à jour doivent toujours être effectuées et supervisées surtout dans le cas de postes personnalisés.

La virtualisation de présentation consiste à déporter non plus l'affichage du bureau mais uniquement l'affichage lié à une application. Celle-ci en question s'exécute soit sur un pool de postes de travail virtualisés soir sur un hôte de sessions. Ces applications peuvent être publiées sur un portail d'entreprise interne ou externe (via un accès sécurisé) au réseau de l'entreprise ou dans le menu de démarrage de Windows 7, écran de démarrage de Windows 8. L'utilisateur lance l'application sans avoir à se préoccuper où celle-ci s'exécute. Les politiques de sécurité et de protection des données de l'entreprise sont ainsi respectées et le risque de fuite est minimisé.
L'authentification peut se faire en utilisant la session ouverte localement dans le cas où le poste est membre d'un domaine approuvé ou simplement via un portail d'authentification dans les autres situations.

La dernière approche consiste à fournir un socle de virtualisation à une application. Le code sera alors exécuté dans un environnement virtuel et les accès aux composants du système (registry, librairies système, exécutables) seront émulés. Par exemple, l'application lit ou écrit une valeur de la registry alors que le code est en fait en train d'accéder à une base de

données. Les valeurs qui ne sont pas dans cette base sont réellement lues depuis la registry du poste de travail. Initialement un séquencement de l'application est nécessaire pour créer le paquet qui sera déployé puis utilisé par la couche de virtualisation. Cette étape permet de virtualiser pratiquement n'importe quelle application. Les mises à jour se font en effectuant une mise à jour du paquet en téléchargeant uniquement le différentiel.

Plusieurs options sont donc possibles et non exclusives les unes par rapport aux autres. C'est le niveau de flexibilité qui sera choisi par l'entreprise autour du BYOD qui définira la ou les options à mettre en œuvre. VDI ou hébergement de session ou virtualisation d'application ne sont que des moyens permettant d'accéder aux données de l'entreprise, au final c'est le niveau de protection des données qui est important.

Conclusion

D'un point de vue technique, un projet BYOD touche à de nombreux aspects liés à la gestion du poste de travail qu'il s'agisse des applications, de la sécurité ou encore de la protection des données. Un projet de type BYOD implique de nombreux acteurs au sein de l'entreprise, en particulier les départements des ressources humaines, juridique et bien entendu IT.
La réalisation d'un tel projet permet non seulement d'améliorer la satisfaction des utilisateurs face à l'outil informatique au sein de l'entreprise mais aussi d'augmenter leur flexibilité tout en réduisant les coûts associés au poste de travail. L'image de l'IT en sera alors modernisée à condition que l'infrastructure soit correctement mise à jour.
Au final, la réussite d'un tel projet dépend de la bonne coordination des équipes de direction, des métiers et de l'IT. Il peut être judicieux de considérer les membres exécutifs pour les phases pilotes du projet

IT-expertise.com
05 déc 2012

DOCUMENT 4

BYOD, COPE, CYOD ou comment satisfaire les demandes des utilisateurs en minimisant les risques pour l'entreprise

Si le BYOD a fait beaucoup couler d'encre ces derniers mois, force est de constater que la réalité de son usage est bien en deçà de ce que pourrait laisser supposer sa couverture médiatique. En fait, la majorité des entreprises exerce une résistance plus ou moins importante à l'utilisation par leurs employés de leurs propres terminaux pour des raisons qui tiennent aux coûts engendrés sans oublier les questions de sécurité et de responsabilité juridique. Face à ces freins, une alternative dénommée COPE ou CYOD semble s'imposer comme une voie de compromis permettant de concilier les exigences légitimes des entreprises avec les aspirations des utilisateurs.

Il est indéniable que le BYOD a fait le « buzz » dans les médias ces derniers temps, ce phénomène étant présenté comme une prise de pouvoir des utilisateurs revendiquant la liberté de travailler avec leur propre terminal contre les diktats de la DSI. La réalité est comme souvent plus prosaïque. Selon différentes études publiées sur les pratiques des entreprises européennes en matière de BYOD, il apparait que l'ampleur du phénomène se réduit souvent à autoriser quelques dirigeants influents de grandes entreprises ou du secteur de la finance à utiliser leur iPad, leur Galaxy pour se connecter au système d'information. Ces mêmes études montrent clairement qu'une grande majorité d'entreprises mettent un veto pur et simple à ces pratiques renforcées en cela par les déclarations l'année dernière du directeur de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) qui se prononçait « Contre le BYOD, sans ambiguïté ! ».

Définitions préalables :

- BYOD « Bring Your Own Device » ou apporter votre propre outil, l'acronyme le plus usité dont la signification consiste à permettre l'utilisation de tout terminal personnel au sein de l'entreprise.
- COPE « Corporate Owned, personnaly enabled » que l'on peut traduire par appartenant à l'entreprise et utilisable personnellement, une approche consistant à fournir au collaborateur un terminal que l'utilisateur pourra utiliser à des fins personnelles.
- CYOD «Choose Your Own Device », un concept similaire au précédent donnant au collaborateur le choix entre plusieurs terminaux validés par l'entreprise.

Les limites du BYOD

Sur le papier, le BYOD présente de nombreux atouts : ses avantages tiennent notamment à ce que le collaborateur effectue l'achat du terminal sur ses fonds propres, qu'il n'a pas besoin de formation et qu'il peut l'utiliser en toutes circonstances (au bureau comme dans sa vie privée). Les gains de productivité sont souvent mis en exergue pour pousser à son adoption.

A contrario, ses inconvénients sont encore plus nombreux : problèmes de sécurité, support de terminaux hétérogènes dans l'accès aux applications métiers, considérations juridiques

complexes, impact sur la vie privée de l'employé sont autant de questions difficiles et particulièrement coûteuses à adresser.

Pour toutes ces raisons et en dépit de la publicité qui l'entoure, on constate en Europe de l'Ouest que la plupart des entreprises sont fermées au BYOD. Dans une majorité d'entreprises, cette pratique est tout simplement interdite !

Les risques liés à la sécurité

Concernant plus spécifiquement la sécurité, le BYOD implique de se reposer sur l'utilisateur pour la sécurisation de son terminal et les différentes études menées dans ce domaine montrent qu'environ un tiers des terminaux ne sont pas mis à jour par leurs propriétaires et se prêtent ainsi à des risques de compromission.

Une solution consisterait à faire en sorte que l'entreprise fournisse les outils de sécurité adaptés à ses employés mais cela nécessiterait de mettre à disposition autant d'outils que de types de terminaux utilisés et de variante de système d'exploitation (particulièrement pour les terminaux sous Android), sans garantie pour autant que chacun les utilise effectivement.

Ce problème est d'autant plus important que certains employés amènent sur leur lieu de travail non pas un mais souvent deux terminaux (smartphone et tablettes notamment).

L'autre problème consiste à donner accès, en situation de mobilité, aux applications métiers de l'entreprise pour une multitude de terminaux hétérogènes tout en respectant des standards de sécurité draconiens. Cela revient à revoir en profondeur l'architecture de sécurité du système d'information pour en élargir considérablement les moyens d'accès.

La question de la responsabilité juridique

Les risques juridiques représentant souvent des considérations plus importantes que celles liées à la sécurité pour de nombreuses entreprises.

Quid de l'effacement des données personnelles sur un terminal géré par l'entreprise ?

Un employé recevant des emails sur son terminal personnel ne pourrait-il pas demander la requalification de son temps passé hors de l'entreprise en temps de travail considérant la réception d'emails urgents à toute heure ?

Quid de la propriété des travaux réalisés par un employé sur son temps personnel et sur son propre matériel ?

Quid de la responsabilité de l'entreprise en cas d'utilisation d'un terminal personnel utilisant le réseau de l'entreprise pour se livrer à des malversations ?

Quid de la réparation du terminal chez un prestataire et de la protection des données de l'entreprise ?

Quid de l'utilisation de logiciels sans licence ?

Quid du prêt du terminal à des amis, membres de la famille ?

Le CYOD ou COPE comme solution de compromis

CYOD et COPE sont de fait très similaires.

Le principe consiste pour l'entreprise à définir une liste finie de terminaux agréés permettant l'utilisation des outils de MDM (Mobile Device Management) pour le déploiement d'applications autorisées, la spécification de paramètres de sécurité, voire la géolocalisation de l'appareil et son contrôle à distance.

Les appareils homologués sont gérés et sécurisés par l'entreprise tout en étant dotés des applications nécessaires à l'accomplissement des missions du collaborateur. On revient ici à un schéma classique dans lequel l'entreprise fournit à son employé le terminal dont il a besoin pour exercer ses fonctions. Cela permet également d'inclure les employés qui ne sont pas équipés d'un terminal personnel.

Le CYOD / COPE peut être perçu comme un avantage en nature à contrario du BYOD dans lequel certains utilisateurs voient d'un mauvais œil le fait d'avoir à utiliser leur terminal propre pour travailler. Cette pratique permet surtout de traiter les problèmes cités plus haut liés à la sécurité et la responsabilité juridique de l'entreprise.

On peut enfin considérer ces pratiques comme un premier pas en attendant une ouverture progressive tendant vers le BYOD.

POSTE PAR NETETCOM.WORDPRESS.COM - 25 NOVEMBRE 2013

DOCUMENT 5

Pour ou contre la pratique du BYOD : quelques réponses juridiques

La pratique du BYOD (Bring Your Own Device) ou le fait d'apporter et d'utiliser ses propres appareils numériques (smartphone, ordinateur, tablette) au travail tend à se répandre. Certains prônent la flexibilité, la mobilité et la facilité d'utilisation d'appareils auxquels les collaborateurs sont déjà habitués. D'autres rappellent les inégalités entre les collaborateurs qui peuvent (ou doivent) utiliser leurs propres appareils et les autres. Au-delà de ces prises de position se posent de réelles questions, en termes de sécurité, mais également en termes juridiques.

Nous aborderons le sujet du BYOD selon trois axes : celui de la sécurité informatique, celui relatif à la nécessaire distinction entre les données professionnelles et les données privées, et enfin, l'axe "pédagogique" de la charte informatique.

1. BYOD et sécurité

La question de la sécurité concerne non seulement la sécurité des systèmes informatiques de l'entreprise, mais également, la sécurité de l'information.

La sécurité des systèmes informatiques de l'entreprise est, à juste titre, au coeur de la préoccupation des Directions informatiques.

L'entreprise qui tolère l'utilisation par ses collaborateurs de leurs propres équipements numériques à des fins professionnelles, sans mettre en place les procédures de sécurité appropriées pour assurer la fiabilité de ces supports (logiciels devant être utilisés, anti-virus à installer, etc.), se met en situation de précarité. Hormis les coûts engendrés en cas d'atteinte au système informatique, un système mal sécurisé et vulnérable aux intrusions peut engager la responsabilité de l'entreprise, ou au moins, si l'on se réfère aux dernières jurisprudences dans ce domaine, entraîner un allègement de la responsabilité de la personne coupable de l'atteinte au STAD.

Les risques liés au BYOD concernent également les accès à distance aux serveurs et données, particulièrement si l'entreprise n'a pas déployé une politique de gestion des équipements BYOD, avec des pré-requis techniques avant d'autoriser l'accès à son système informatique, que ce système soit géré en interne, hébergé par un tiers ou exploité en mode Cloud.

En outre, en matière de traitements de données à caractère personnel, les entreprises sont responsables en cas d'atteinte à la sécurité des systèmes, en leur qualité de responsable de traitement. La loi Informatique et Libertés impose en effet au responsable de traitement de prendre toutes précautions utiles (mesures de sécurité technique et physique) pour empêcher que les données personnelles de leurs salariés et clients ne soient erronées, modifiées, effacées par erreur, ou que des tiers non autorisés y aient accès.

Enfin, le BYOD requiert de mettre en place une politique spécifique relative au traitement des documents de l'entreprise et à leur confidentialité, afin d'éviter que d'autres personnes n'y

aient accès, notamment si l'ordinateur personnel ou la tablette sont utilisés par ailleurs par d'autres membres de la famille.

2. BYOD et distinction entre données professionnelles et données privées

La frontière entre vie privée et vie professionnelle tend à se brouiller pour certaines catégories de salariés (télétravail, et mobilité notamment).

La jurisprudence relative aux droits de l'employeur à accéder aux documents et emails sur l'ordinateur du salarié est désormais relativement bien établie. Ainsi, l'employeur peut avoir accès aux fichiers informatiques créés, reçus et envoyés par les salariés, que ce soit dans le cadre de la réalisation normale de leur mission, ou dans une finalité de contrôle pour protéger les intérêts de l'entreprise ou sauvegarder les preuves en cas de faute disciplinaire du salarié.

Jusqu'à présent, la jurisprudence concernait les accès aux fichiers et emails sur les ordinateurs professionnels mis à la disposition des salariés par l'employeur. En résumé, l'employeur peut accéder aux fichiers numériques et emails du collaborateur, même en son absence, à l'exception des fichiers et emails identifiés comme "personnel" ou "privé". La jurisprudence a récemment étendu cette faculté d'accès par l'employeur pour les documents se trouvant sur une clé USB appartenant au salarié, mais connectée à l'ordinateur professionnel.

Alors qu'un appareil fourni par l'entreprise a pour finalité première d'être utilisé à des fins professionnelles et que l'utilisation à des fins privées est tolérée à la marge, un appareil personnel est censé être utilisé d'abord à des fins personnelles.

La jurisprudence relative à l'accès par l'employeur au contenu de l'ordinateur professionnel du salarié nous paraît difficilement transposable, telle quelle, au BYOD. En effet, le salarié a droit au respect de l'intimité de sa vie privée. Son employeur ne saurait librement accéder à ses équipements pour en contrôler le contenu. Afin de rétablir un équilibre entre données privées et données professionnelles, il est donc indispensable de définir les "règles du jeu" par la mise en oeuvre d'une charte technologique au sein de l'entreprise.

2. BYOD et charte technologique

Chaque entreprise devrait avoir déployé une charte informatique (également dénommée charte technologique ou charte utilisateur). (4) Cependant, même lorsqu'une charte est en vigueur dans l'entreprise, celle-ci doit être régulièrement revue et mise à jour pour tenir compte de l'évolution des usages et des technologies.

La charte informatique a une dimension pédagogique, à la fois pour les responsables informatique et sécurité qui doivent faire l'effort de poser les bonnes questions pour l'entreprise, la sécurité des systèmes et des données afin de rédiger une charte pertinente, et pour les collaborateurs qui auront à leur disposition les lignes de conduite à suivre dans ce domaine.

Ainsi, l'objet de la charte n'est pas nécessairement d'interdire mais de tracer les limites entre ce qui est autorisé et ce qui ne l'est pas : les collaborateurs sont-ils autorisés à utiliser la messagerie électronique pour échanger des emails privés, peuvent-ils consulter et utiliser les

réseaux sociaux pendant leurs heures de travail, enfin sont-ils autorisés à utiliser leurs propres équipements pour l'exécution de leur travail, etc.

L'entreprise devra prendre une position claire sur le fait d'autoriser ou d'interdire l'utilisation par les collaborateurs de leurs propres équipements à des fins professionnelles. Si l'entreprise décide d'autoriser la pratique du BYOD, les règles d'utilisation devront alors être clairement définies afin de pallier les risques identifiés ci-dessus.

En cas d'autorisation du BYOD, la charte devra déterminer les types d'équipements autorisés, les logiciels et mesures de sécurité qui doivent être adoptés par les collaborateurs concernés, les règles de distinction ou de partition entre sphère privée numérique et sphère professionnelle numérique sur les équipements, et les règles d'accès aux données professionnelles par l'employeur.

Enfin, il conviendra de gérer rigoureusement le départ du collaborateur de l'entreprise. En principe, les équipements sont restitués à l'entreprise au moment du départ du collaborateur. Dans le cas du BYOD, il conviendra de prévoir une procédure d'effacement des données professionnelles, avec un engagement de confidentialité renforcé de la part du salarié sur le départ, sans oublier de fermer ses accès à distance au système informatique de l'entreprise (blocage des identifiants et mots de passe).

La question du BYOD ne laisse pas indifférent, à tel point que certains détournent cet acronyme en "buy your own device" (achetez votre propre appareil) ou "bring your own disaster" (apportez votre catastrophe) ! Il n'en demeure pas moins que le BYOD est source de risques en matière de sécurité informatique et juridique. Toute entreprise, quelle que soit sa taille, doit prendre position sur le fait d'interdire ou d'autoriser à ses collaborateurs l'utilisation de leurs équipements numériques. L'interdiction a le mérite d'écarter ces risques, a fortiori si l'entreprise intervient sur des domaines sensibles. Elle permet de conserver le contrôle et de rationaliser le parc informatique et les budgets y afférents ainsi que de gérer les risques de sécurité, compte tenu des composantes matérielles et logicielles. En revanche, l'autorisation du BYOD doit être accompagnée par le déploiement d'une politique de sécurité renforcée et d'une charte informatique adaptée, comprises par les collaborateurs et régulièrement contrôlées et mises à jour.

www.dwavocat.com du lundi 18 novembre 2013

DOCUMENT 6

Le CYOD : le juste milieu entre BYOD et fourniture de l'appareil ?

Quelques avantages du BYOD, sans tous ses défauts

Si le **BYOD** a bien des atouts, il a aussi quelques inconvénients qui ont tous été abordés sur ce blog. Entre la sécurité, la problématique juridique, l'impact sur la vie privée de l'employé, etc., le BYOD n'est pas sans souci. Mais il a aussi certains atouts indéniables, notamment le fait que l'employé connait l'appareil comme sa poche, qu'il n'a pas besoin de formation spécifique et qu'il peut l'utiliser avant et après son arrivée au « bureau » (ou ailleurs).

Mais comment allier les avantages du BYOD tout en évitant certains de ses défauts ? Le CYOD, pour « Choose Your Own Device », a ainsi été inventé. Le concept est simple : l'entreprise fournit les matériels qui conviennent à la fois à ses préoccupations de fonctionnement et de performance mais aussi aux souhaits des utilisateurs.

Certes, ce n'est pas du BYOD : l'employé n'apporte pas son propre appareil. En réalité, il s'agit donc d'un fonctionnement classique où l'entreprise fournit les employés. Il n'y a donc pas l'avantage de l'économie liée au non-investissement des appareils. La différence fondamentale repose donc sur le choix donné aux salariés.

En offrant des alternatives, mais dans une liste fermée, bien définie et donc approuvée par le DSI, l'entreprise permet à la fois à l'employé de choisir l'appareil qui lui correspond le plus, ce qui devrait accroître sa productivité, tout en ayant le contrôle sur la flotte de smartphones, de tablettes ou de PC en fonctionnement. En résumé, cela a l'avantage d'un BYOD limité à certains appareils, sans exclure les employés non équipés.

Des atouts évidents pour les entreprises européennes

Si financièrement, l'intérêt du CYOD est effectivement limité en terme d'investissement initial, ses atouts n'en restent pas moins gigantesques. Cela supprime de facto tous les problèmes juridiques et ceux liés à la vie privée, mais cela réduit aussi fortement les risques de sécurité. Qui plus est, cela implique bien plus les employés, qui ne se verront pas forcés d'utiliser un iPhone, un Samsung, un BlackBerry ou un Nokia.

Si dans les pays où le BYOD est ultra généralisé, le CYOD n'a qu'un intérêt limité, il est certain qu'en Europe de l'Ouest, où les questions juridiques et de sécurité sont centrales, cette méthode peut avoir un succès évident. Cela a le mérite à la fois de rassurer les DSI et de contenter les employés. Que vouloir de plus ? Sachant que de nombreuses entreprises ont pour le moment opté pour du 0 % BYOD du fait de leurs multiples inquiétudes sur le sujet, pourquoi ne pas tenter l'approche du CYOD pour commencer ?

Le CYOD implique toutefois d'offrir un catalogue suffisamment large pour ne pas déplaire aux salariés, sans pour autant aller trop loin bien entendu. Il faut aussi développer les applications adéquates afin de relier tous les employés.

Notons enfin que le CYOD, contrairement au BYOD, a l'avantage d'être perçu comme une augmentation indirecte du salaire. C'est un argument quand on sait que certains salariés voient d'un mauvais œil l'exploitation de leur propre appareil au travail.

Zdnet.fr| Lundi 18 Novembre 2013

DOCUMENT 7

BYOD, BYOA : quel encadrement juridique ?

Deux usages récents ont été introduits dans l'entreprise par les salariés eux-mêmes : le BYOD (bring your own device) et le BYOA (bring your own application). Autorisés, tolérés, interdits... ils ont des statuts différents dans les entreprises et présentent quelques risques. Explications et conseils de Maîtres Wéry et Breteau, avocats aux barreaux de Paris et Bruxelles (cabinet Ulys).

Comment définir le BYOD et le BYOA ?
Ces expressions désignent la pratique, pour les membres d'une entreprise, d'utiliser à des fins professionnelles leurs outils technologiques personnels, appareils (BYOD) et applications (BYOA), hors du contrôle de l'employeur ou des autres responsables (informatique, achats, juridique, etc.). Ce phénomène s'insère dans le mouvement dit de consumérisation des nouvelles technologies dans l'entreprise, augmenté par l'apparition des services accessibles dans le cloud, et génère des questionnements juridiques sérieux.

Quelles questions l'entreprise doit-elle se poser ?
Principalement des questions liées à la sécurité du système d'information de l'entreprise et de ses données. Par exemple :
• Que se passe-t-il si une application personnelle utilisée à des fins professionnelles est infectée par un virus ?
• Un salarié peut-il librement revendre un smartphone qu'il utilise pour consulter ses mails professionnels depuis des années, pour acheter le modèle dernier cri ?
• Une application téléchargée par un salarié est-elle assortie des garanties adéquates en terme de propriété intellectuelle pour un usage professionnel ?

Quels sont les risques liés ?
Dans ces situations, l'entreprise encourt un risque de violation de données et d'atteintes à son système d'information, outre les risques de responsabilité en cas d'atteinte à des intérêts légitimes de tiers.
Il convient aussi de délimiter la frontière entre personnel et professionnel afin de déterminer dans quelle mesure l'employeur peut accéder, saisir ou conserver les appareils, et dans quelle mesure un salarié peut s'y opposer sans commettre de faute.

Dans quels cas peut-on interdire ces pratiques ?
Comme pour toute pratique nouvelle, il n'y a pas de solution standard : la réponse la plus adaptée sera le plus souvent trouvée après une analyse de risques. Il peut être préférable d'interdire le BYOD/BYOA en présence de risques trop importants, notamment lorsque l'entreprise est sujette à des obligations particulières, issues de la réglementation ou de contrats. Cela peut être le cas en présence de réglementations sectorielles, ou en présence d'une activité générant un risque spécifique (par exemple, recours à des outils sous licences de propriété intellectuelle, ou partenariats assortis d'obligations de confidentialité spécifiques, etc.).

Comment encadrer ces pratiques dans l'entreprise ?
Il existe plusieurs moyens : limitation à certaines ressources ou données de l'entreprise (exclusion d'accès, par exemple aux dossiers ressources humaines ou autres dossiers

personnels, etc.), sécurisation technique (codes d'accès, chiffrement, etc.) et, bien entendu, moyens juridiques.
En premier lieu il s'agit du contrat de travail et du règlement intérieur. En outre, l'entreprise peut définir et mettre en œuvre une politique de sensibilisation des équipes aux impératifs de sécurité et de confidentialité.
L'utilisation des outils informatiques est fréquemment prévue dans une charte informatique, la tendance actuelle étant à l'élaboration de chartes spécialisées par usage ou par thème, afin de disposer de documents facilement identifiables, lisibles et à jour.

Comment établir ces documents et ces règles ?
Les règles applicables en la matière sont, pour la plupart, à créer. De plus, la jurisprudence sera amenée à évoluer sur ces sujets, de même qu'elle l'a fait pour définir le périmètre du privé et du professionnel au sujet des courriers électroniques ou des fichiers sauvegardés sur les ordinateurs des salariés.
Les contrats et règlements intérieurs ou chartes d'utilisation doivent être rédigés avec soin, d'abord pour ne pas subir complètement la relative incertitude sur les solutions qui seront dégagées par les tribunaux à l'avenir. À cet égard, il convient de noter que les clauses d'une charte informatique risquent de s'imposer à l'employeur, même en présence d'une jurisprudence plus souple. D'autre part, les obligations définies en interne, pour être efficaces, ne peuvent pas imposer des pratiques qui ne refléteraient pas le « raz-de-marée » des évolutions de la société de l'information, et ne pas contraindre excessivement les relations de travail.

DOCUMENT 8

Polémique DSI : Faut-il interdire l'usage des outils personnels à des fins professionnelles ?

La percée du BYOD semble inévitable. Pour les uns, ce modèle accorde une plus grande flexibilité d'usage en mobilité. Pour les autres, il fait le lit d'un parc de terminaux hétérogènes ingérable.

La nouvelle formule du magazine 01 Business introduit un nouveau rendez-vous : « la polémique des DSI ». La rédaction recueille l'opinion des membres du Club 01 DSI sur des questions liées aux grandes tendances du marché informatique. Les deux DSI ayant livré les avis les plus argumentés seront publiés dans le magazine. Mais, pour ne rien perdre de la richesse des propos récoltés, les meilleures réponses à nos questions feront l'objet d'un article diffusé sur 01business.com.

« Faut-il bannir les équipements personnels au sein de l'entreprise ? ». Telle est la nouvelle question soumise aux DSI. Les adeptes du BYOD (Bring your own device) voient dans cette approche un moyen pour l'entreprise de dégager une image d'innovation auprès de ses collaborateurs. Lesquels apprécient la flexibilité d'un accès en mobilité au SI de leur employeur depuis leur terminal personnel. Mais ce modèle compte aussi ses réfractaires, qui estiment que la grande variété des marques et des configurations des postes personnels débouchera sur une maintenance de ce parc relevant du casse-tête.

Les partisans du oui

- **Yann Jouveneaux, DSI de Sakata EMEA**. "Nous privilégions l'achat et l'exploitation par l'entreprise de nos équipements pour plusieurs raisons. D'abord, nous souhaitons garantir à nos utilisateurs un support de qualité respectueux d'un contrat de service interne (SLA). Si nous acceptions le BYOD (Bring Your Own Device), il nous faudrait des compétences sur tous les terminaux. En outre, nos procédures d'aide doivent être universelles. Il n'est donc pas question de les adapter pour chaque solution de mobilité. Nos collaborateurs n'ont pas à assurer leur support technique, ce n'est pas leur métier. Enfin, nous voulons garantir la sécurité de nos applications mobiles et, à ce titre, administrer nos propres protections sur des plates-formes connues et identifiées. Ce qui serait impossible ou inutilement coûteux en mode BYOD. Certains systèmes, comme Android, vont à l'encontre des fondements de la gestion de la sécurité des systèmes d'information. Le business model de Google étant de monnayer, plus ou moins directement et de manière totalement opaque, toutes les données disponibles sur ses utilisateurs."
- **Vincent Leaux, DSI, Ville de Vélizy-Villacoublay**. "Le BYOD me semble relativement ingérable. D'un point de vue de la politique RH, si l'on permet aux salariés de travailler chez eux, en particulier le week-end, il est logique que l'entreprise leur mette à disposition le matériel."
- **Michel Juvin, DSI, Lafarge Ciments**. "Le BYOD est relativement complexe et d'un coût qui n'est pas forcément inférieur à la mise à disposition de ressources internes. [...] La variété des marques et des configurations des équipements personnels des collaborateurs rend leur support plus difficile. [...] Il est moins compliqué de proposer des matériels modernes adaptés à l'utilisation professionnelle. [...]"
- **Laurent Bérenguier, DSI, Université d'Auvergne** "[...] Le BYOD est certes une évolution des usages, peut contribuer au confort, mais ne répond véritablement à aucune nécessité

professionnelle. Tolérer qu'un terminal accède à des données métier sensibles sans être totalement sous contrôle me semble suicidaire."
- **Thierry Lepiez, DSI, Hoya France**. "[...] Nous privilégions plutôt l'achat par l'entreprise des nouveaux terminaux mobiles, comme les tablettes et les smartphones, dans un mode « COPE » (Corporate Owned, Personally Enabled). Mais, la mise en place prochaine par le groupe d'un outil de « mobile device management » (MDM) destiné à renforcer la sécurité des connexions, devrait favoriser le BYOD puisque l'usage personnel des IPhone et autres iPad sera réservé aux seules applications autorisées."

Les partisans du non

- **François Charpe, Group CIO d'Altran**. "Chez Altran, la politique de gestion du BYOD a été mise en place de facto. De par notre métier ? l'externalisation de R&D ?, nombre de nos collaborateurs travaillent hors de nos murs. Pour qu'ils se connectent au système d'information de l'entreprise, un moyen efficace et flexible était d'autoriser cet accès depuis leurs terminaux personnels. Aujourd'hui, nos 20 000 salariés possèdent un smartphone ou une tablette, voire les deux, alors que nous gérons 13 000 postes de travail fixes en interne. Mais les outils personnels, contrairement aux ordinateurs de bureau, restent à la charge de nos collaborateurs. Cette stratégie BYOD est grandement facilitée par le caractère 100 % Web de notre système d'information. Il suffit d'une connexion internet et d'un navigateur pour consommer nos services applicatifs (messagerie, gestion de la relation client, demande de voyage...). Cette approche s'accompagne de mesures de sécurité. A chaque connexion distante, nous contrôlons l'intégrité du terminal utilisé. Et nous sensibilisons régulièrement nos employés au danger lié à des comportements trop permissifs."
- **Michel Lami, ICT Manager, American School of Paris**. "Nous développons le BYOD au lycée. Nous demandons aux élèves d'installer un anti-virus avec mise à jour régulière. L'accès au wifi se fait par l'intermédiaire d'un portail captif. Par contre, nous fournissons les ordinateurs portables aux collégiens. Nous assurons l'administration des postes et nous nous réservons le droit d'intervenir si nous en estimons le besoin. Dans les deux cas, les utilisateurs signent une charte et sont pleinement responsables de leurs données. Nous n'assurons aucune sauvegarde. [...]"
- **Hélène Sol, DSI, CH d'Avignon**. "Nous favorisons le BYOD. Et cela, même si les smartphones ou les tablettes sont peu adaptés aux applications médicales. Celles-ci nécessitent de fréquentes saisies en chiffres avec virgules (prescriptions), et de grands écrans, les applications étant riches en informations ou très visuelles (imagerie médicale en haute définition). Aujourd'hui, nous avons placé la messagerie sur certains postes personnels, et nous allons ouvrir l'accès aux plannings des rendez-vous patients depuis l'extérieur de manière sécurisée."
- **Pascal Viginier, Group CIO, Orange**. "Depuis 2011, notre politique favorise le BYOD. 2500 employés en ont déjà bénéficié et 57% d'entre eux ont accès en mobilité au système d'information et aux intranets du groupe. Depuis leur équipement personnel, ils peuvent utiliser notre réseau social interne déployé depuis deux ans, ainsi que les réseaux sociaux externes, dont l'usage a été ouvert à l'été 2012."
- **Guillaume Ors, Directeur informatique et nouvelles technologies, Ville de Clichy la Garenne**. "[...] Il est utopiste de penser, en tant que DSI, pouvoir interdire le BYOD au sein de l'entreprise. Il est donc préférable de l'accepter et de l'encadrer. Ce modèle peut permettre de réaliser des économies sur l'achat des terminaux, mais il faut alors veiller à ce que l'utilisateur n'ait pas l'impression que son employeur cherche à faire des économies à ses dépens. [...]"

Pro.01net.com – 04/04/2013

DOCUMENT 9

Les précautions à prendre pour passer en mode BYOD

En utilisant leur propre équipement, vos collaborateurs sont plus productifs et améliorent leur confort de travail. A condition que vous les aidiez à protéger leurs données professionnelles.

Depuis 2012, le géant pétrolier Royal Dutch Shella, progressivement, a incité ses collaborateurs à exploiter leur propre équipement. Une opération concluante : outre une économie de 350 à 1 300 dollars par an et par personne, la productivité générale et les performances se sont considérablement accrues. Aujourd'hui, 81 % des employés estiment travailler plus efficacement sur le matériel qu'ils ont choisi. La généralisation du BYOD (Bring Your Own Device) dans les entreprises semble inéluctable. Largement adoptés à titre personnel par des salariés férus de technologies, les smartphones et les tablettes domestiques sont souvent plus performants que les vieillissants PC bridés installés dans les entreprises. Mais attention. Connectés en permanence, ces utilisateurs accèdent à leurs messages et données professionnelles sans grande connaissance des questions de sécurité informatique. Le passage au BYOD ne peut donc s'effectuer sans un encadrement rigoureux. Parmi les points auxquels vous devrez absolument veiller : la protection de vos données, mais aussi les aspects juridiques et sociaux liés à l'imbrication des sphères professionnelle et privée.

1. Évaluez le budget à prévoir

Pour avoir une idée du coût du BYOD, répertoriez d'abord les collaborateurs qui disposent d'un PC, d'un smartphone ou d'une tablette à titre personnel et, surtout, ceux qui souhaitent l'exploiter dans le cadre de leurs activités. Ce n'est pas le cas de tout le monde. Comptez 2,38 euros par mois et par appareil pour les solutions de prise en charge BYOD que nous préconisons dans ce dossier. Cette liste vous donne, de plus, le nombre de terminaux à gérer et leur répartition entre les divers systèmes du marché.
A partir de ces informations, énumérez les applications mobiles et les services dans le cloud dont auront besoin les salariés pour travailler, afin de calculer le coût des licences logicielles indispensables au travail en mode BYOD. En faisant la différence entre le coût des postes que vous n'aurez plus à déployer et le prix du BYOD, assurez-vous de dégager une économie suffisante pour que le jeu en vaille la chandelle.

2. Définissez une charte d'utilisation

La bonne marche du BYOD tient avant tout à l'établissement d'un contrat entre l'employeur et le collaborateur. Ce document définit le plus clairement possible les actions autorisées ou non. En particulier, indiquez que les données professionnelles restent dans tous les cas la propriété de l'entreprise, listez les seules tranches horaires et applications qui pourront être considérées comme de l'activité professionnelle, le reste relevant de la vie privée. Puis précisez les modalités de contrôle et les sanctions encourues. Vous trouverez un exemple de charte informatique pour le BYOD, à compléter et à adapter selon le profil de votre entreprise, à l'adresse tinyurl.com/chartebyod. Reportez-vous également à notre encadré consacré au cadre juridique afin de n'oublier aucun aspect du sujet.

3. Fournissez un support technique

Déployer une politique BYOD en entreprise suppose de renforcer le niveau technique de vos collaborateurs, qui devront choisir et mettre à jour leur propre équipement. Ne cherchez pas à répondre à toutes les questions. Rédigez des procédures pour les problèmes les plus courants, mais établissez dans le même document toutes les tâches qui ne relèvent pas du département informatique.

Attention cependant à ne pas vous retrouver avec des salariés abandonnés face à leurs problèmes techniques. Sur la base du volontariat et contre une compensation financière à définir (de l'ordre de quelques centaines d'euros par an), certaines entreprises confient à des salariés-référents le soin d'aider leurs collègues face à une panne ou un souci. Mettez en place un tel service, avec la taille qui correspond le mieux à votre culture d'entreprise.

4. Améliorez votre réseau Wi-Fi

A l'origine, les réseaux sans fil ne sont pas prévus pour gérer une flotte importante de smartphones et de tablettes aux caractéristiques différentes. Vous serez peut-être dans l'obligation de renforcer le vôtre. Le constructeur français Netinary propose une gamme de multibox, des boîtiers que vous connectez à votre modem et qui gèrent les connexions sans fil de manière sécurisée. Pour moins de 2 000 euros hors taxes, ce produit crée un point d'accès sans fil qui distingue les connexions temporaires, réservées aux invités, des accès permanents, destinés aux employés. Sa mise en place est simple : il suffit de lister dans son interface d'administration, accessible à travers un navigateur Web, l'annuaire de vos salariés. Chacun dispose ainsi d'un accès personnel pour tous ses appareils. Accessoirement, vous avez la possibilité de surveiller son activité réseau, comme vous avez indiqué le faire dans votre charte informatique, au point 2.

5. Offrez-vous un logiciel de gestion de flotte mobile

Plusieurs solutions logicielles prennent depuis peu en charge le déploiement et le suivi d'une flotte d'appareils mobiles hétérogènes. Il s'agit des Mobile Device Management (MDM). Ils savent contrôler les appareils à distance et, si besoin, effacent leurs données, surveillent leur activité et veillent au respect des règles de bonne conduite que vous aurez définies vous-même (ne pas utiliser la 3G en roaming, taper un code Pin pour activer l'appareil, etc.). Airwatch, Citrix Xen-mobile et MobileIron, qui gèrent les appareils de toutes les marques et de tous les types, comptent parmi les références du genre. Ces solutions coûtent environ 3 dollars par mois et par appareil, ou 50 dollars par appareil une fois pour toutes.
Dans les trois cas, vous pilotez votre parc mobile depuis votre navigateur Web. Sur leur appareil, les utilisateurs installent une application gratuite qui leur permet d'intégrer votre flotte professionnelle en s'authentifiant avec les identifiants que vous leur communiquez. La configuration de l'appareil est analysée, et seuls les équipements autorisés sont susceptibles de se connecter.
La fonction de base de ces logiciels ? Configurer d'un coup le courrier électronique et le partage de documents sur tous les appareils. Il suffit d'indiquer l'adresse Internet de votre serveur de messagerie et de préciser sa nature (Lotus Notes, Microsoft Exchange, Novell Groupwise...), puis de faire de même avec votre espace de stockage en ligne. A noter qu'Airwatch accompagne son offre d'un espace de partage en ligne de 25 gigaoctets.

6. Élaborez un annuaire du BYOD

Définir quels périphériques personnels sont utilisables en BYOD n'est pas compliqué, mais nécessite un peu de temps pour tout saisir dans le logiciel de MDM, soit environ trois minutes par utilisateur. Connecté à la console d'administration d'Airwatch, qui nous sert ici d'exemple, déroulez le menu Ajouter et cliquez sur Terminal. Saisissez le nom d'un employé dans le champ supérieur, puis cliquez sur Créer un nouvel utilisateur. Indiquez son adresse électronique, son identifiant et son mot de passe.
Choisissez ensuite le propriétaire de l'appareil (salarié, société...) et sa plate-forme (Android, Apple, Windows Phone...). En cliquant sur Enregistrer, vous adressez automatiquement un courriel à l'utilisateur : depuis son appareil mobile ou son ordinateur portable, il lui suffit de suivre un lien pour installer les applications et les certificats nécessaires à la connexion. Après avoir saisi son identifiant, votre collaborateur apparaît dans votre tableau de bord. Cliquez sur son intitulé afin d'accéder aux options essentielles.
Pour un iPhone, par exemple, vous contrôlez plusieurs dizaines de fonctionnalités, de l'obligation d'ajouter un code de verrouillage à la désactivation de la caméra ou de la synchronisation avec iCloud. Parcourez l'ensemble des sections et définissez des règles (mot de passe absent, application spécifique installée, l'utilisation du réseau cellulaire dépasse un certain montant, etc.). Si un utilisateur viole une règle de sécurité ainsi définie, le logiciel de MDM peut prendre plusieurs mesures. Elles vont de l'envoi d'une alerte à l'effacement total des données professionnelles contenues dans l'appareil.

7. Définissez les applications autorisées

Vous choisissez également depuis le logiciel le nom des applications à installer sur les mobiles. Son interface répertorie les catalogues des app store d'Apple, d'Android et consorts. Vos choix se répercutent immédiatement sur votre parc de mobiles, en fonction des utilisateurs que vous avez sélectionnés. Mais les applications ne s'installent pas automatiquement sur les appareils de vos utilisateurs.
Ceux-ci reçoivent juste un message leur indiquant de cliquer sur tel lien pour installer telle application recommandée ou les prévenant que tel logiciel n'est pas autorisé, sans pour autant parvenir à interdire son installation. La console de surveillance du logiciel de MDM vous indiquera en temps réel qui a bien déployé les logiciels recommandés et qui a installé un logiciel interdit.
Le cas des logiciels interdits est le talon d'Achille du BYOD. En effet, l'entreprise court le risque de se faire attaquer par les fournisseurs pour l'usage, par un salarié et dans un cadre professionnel, d'un logiciel dont elle n'a pas elle-même acheté la licence.
De fait, vous devez, dès la rédaction de votre charte, interdire le recours aux logiciels sans licence ou de ceux dont la licence n'est pas compatible avec un usage professionnel, ce qui protégera votre entreprise vis-à-vis des fournisseurs. Dans le logiciel de MDM, mettez en liste noire les logiciels qui entrent dans cette catégorie. Si un utilisateur en installe néanmoins un, prenez les dispositions que vous avez indiquées dans votre charte.
Les précautions juridiques à prendre :
L'introduction du BYOD implique l'accord des salariés et du comité d'entreprise, la mise à jour de la charte informatique et l'indication claire des règles d'usage et des sanctions encourues. définissez ce qui relève de l'usage personnel et professionnel. en France, il n'existe pas encore de réelle jurisprudence autour du BYOD. Aux Etats-Unis, en revanche, une société a été condamnée pour avoir effacé l'intégralité des données du mobile d'un employé, dont ses photos personnelles. Le BYOD estompant la frontière entre les activités privées et professionnelles, les questions du temps de travail se posent. Pouvez-vous bloquer le matériel pour faire respecter cette durée ? Vous ne devez alors pas entraver le bon fonctionnement du terminal personnel du collaborateur en dehors des heures de bureau. les questions liées aux compensations financières sont également primordiales. Par usage, on s'inspire souvent du défraiement des véhicules personnels. l'entreprise peut ainsi prendre en charge une partie du forfait téléphonique ou proposer un remboursement annuel.
Vos outils pros dans un appareil perso :
VMware Player, gratuit, exécute le PC de bureau avec toutes ses informations professionnelles dans la fenêtre d'un ordinateur personnel.
VMware Converter, gratuit, transforme un PC de bureau en PC virtuel, à savoir un fichier exécutable par VMware Player.
VMware Horizon Mobile, sur devis, sépare sur un mobile les données personnelles et professionnelles.
Optez pour une transition en douceur :
Si le passage au BYOD intégral vous effraie pour des raisons de sécurité ou de coût, envisagez d'assouplir la gestion de votre parc informatique au travers du CYOD (Choose Your Own Device, choisissez votre propre appareil). Il s'agit de ne pas autoriser les employés à se servir de leur équipement personnel, mais de leur proposer de choisir leur matériel professionnel parmi un catalogue de matériels prédéfinis. D'après une étude de Bouygues Telecom conduite en mars 2012, 65 % des responsables informatiques ne permettent pas aux salariés de se connecter au système d'information via leurs outils personnels, pour des raisons de sécurité. Elargir votre gamme d'appareils professionnels en incluant les périphériques que les employés sont susceptibles de posséder à titre personnel améliore leur confort et leur productivité. Vous encadrez ainsi le phénomène en maîtrisant davantage les questions de support et de sécurité. D'après une étude interne menée par Intel en juillet 2012, 72 % de ses salariés sont davantage favorables à ce système dans la mesure où les investissements financiers et les compensations sont plus clairement établis.

"pro.01.net.com" - le 04/10/13

DOCUMENT 10

BYOD: définition, enjeux et impacts

«BYOD», cet acronyme est depuis quelque mois de plus en plus visible sur le web, mais que cachent ces quatre lettres ? Le terme « Bring Your Own Device » ou en français « apportez votre appareil personnel », traduit la disparition de la frontière entre les univers « pro » et « perso ». En effet, le BYOD repose sur l'utilisation par le salarié de son matériel informatique personnel (tablette, PC portable, smartphones) dans le cadre professionnel. Le cabinet Gartner *(cabinet de conseil et de recherche spécialisé dans le domaine des techniques avancées)* explique ce phénomène par deux points : la consumérisation de l'informatique et l'arrivée de la génération Y dans les entreprises. En premier lieu, les smartphones, netbooks et autres tablettes connaissent une réelle explosion et vont continuer à évoluer et pénétrer dans les entreprises. L'explosion de leur utilisation brouille ainsi la barrière entre équipement personnel et professionnel. En effet, les utilisateurs séduits par la simplicité d'usage de leurs nouveaux terminaux ne peuvent plus s'en passer. Les appareils « grand public » sont considérés comme moins « austères » que les terminaux professionnels : qualité du graphisme, ergonomie...plusieurs critères entrent en jeu. De plus, le nomadisme des salariés a accéléré le mouvement : dans un contexte d'ultra mobilité il est plus simple de n'utiliser qu'un terminal. Enfin, les individus sont de plus en plus accros à leur terminal mobile et souhaitent que ce dernier combine messagerie, accès à des services Cloud, accès aux données et applications professionnelles, au multimédia etc... En second lieu, cette génération de technophiles (jeunes ayant entre 18 et 30 ans aujourd'hui, la génération "Y" ou "Why"), est devenue experte dans l'art d'utiliser quotidiennement les réseaux sociaux, la mobilité, le Cloud...que ce soit au niveau professionnel ou personnel, pour eux les frontières entre ces deux univers n'ont jamais vraiment existé. Cet afflux d'appareils personnels dans l'entreprise ne réjouit pas forcément les dirigeants et responsables informatiques. En effet, ces appareils «non contrôlés» par la société peuvent être source de multiples menaces concernant la sécurité des données.

Quels enjeux et solutions ?

Le BYOD doit permettre l'accès aux applications du Système d'information de l'entreprise via un terminal étranger à celle-ci et ceci sans avoir à investir dans une flotte de terminaux ni même de s'occuper du support du périphérique. L'objectif du DSI est donc de proposer un service compatible avec la plupart des terminaux et facilement paramétrable par l'utilisateur final. Nombreuses applications sont accessibles au moyen d'un simple navigateur et pour les autres la virtualisation du poste de travail peut s'avérer une alternative efficace. Le BYOD amène une réelle réflexion concernant l'organisation de l'entreprise, sur la manière d'assurer la sécurité de celle-ci et de ses données mais également sur l'intégration des nouveaux terminaux dans le cadre professionnel...

Avec le BYOD, la politique de gestion et de sécurité est totalement remise en cause: le DSI n'est plus le seul décideur et la « flotte » mobile de la société devient hétérogène. Certaines entreprises ferment les yeux, d'autres dépensent des sommes considérables dans la gestion de systèmes d'exploitation mobiles et dans la mise en œuvre de logiciels capables de protéger et d'isoler automatiquement les informations et applications de l'entreprise, et enfin certaines sociétés interdisent tout simplement l'utilisation du matériel personnel dans le cadre du travail. Il s'agit du problème majeur soulevé par le BYOD.
Au niveau organisationnel, la gestion de nombreux systèmes doit être aussi aisée que celle d'un seul. Cela permet à l'utilisateur d'accéder facilement aux données et au DSI de faciliter le support. L'enjeu futur est ainsi la gestion des identités (unification des multiples profils du titulaire d'un terminal et cohabitation des contacts et messageries pro et perso).
Enfin, des questions juridiques et RH sont également soulevées. Que faire si le matériel contenant des informations professionnelles est endommagé ou volé avec des informations confidentielles ? Comment séparer sphère privée et professionnelle? Comment empêcher les employés de tomber dans l'hyper-connectivité?
La place de la messagerie dans le BYOD
Une étude annuelle menée par Dresner Advisory Services en octobre dernier auprès d'un panel d'entreprises mondiales (tous secteurs d'activités confondus) nous explique que l'email est naturellement l'application mobile prioritaire dans les entreprises dont la «mobilisation», et donc le développement du BYOD est une priorité. Avec un indice de 3,5 (sur une échelle de 0 à 4), suivi de près par les outils de gestion d'informations personnels (3,1) l'accès aux comptes de messagerie et emails professionnels sur le matériel personnel ainsi que son contrôle est une priorité.
Une autre étude de Avenade "The Consumerization of IT" (menée auprès de 605 décideurs, responsables métier et informatiques de 17 pays en Amérique du Nord, en Amérique du Sud, en Europe et dans la zone Asie-Pacifique) nous montre que les entreprises déploient de plus en plus d'applications "cœur de métier" pour les rendre accessibles aux équipements mobiles, et donc aussi aux terminaux personnels. Par ordre d'importance, les entreprises permettent aux équipements personnels d'accéder à :

- la messagerie, l'agenda et les contacts (85 %),
- les réseaux sociaux (46 %),
- le CRM (45 %),
- la gestion du temps et des dépenses (44 %),
- l'ERP (38 %).

Soit des applications "utiles" à la productivité de l'employé et donc de la société. A noter, 79 % des entreprises sondées ont planifié des nouveaux investissements pour supporter l'intégration des équipements personnels sur 2012.De plus, 25% du budget informatique des entreprises sera utilisé pour gérer l'accès aux « terminaux BYOD ».
Ainsi, le phénomène BYOD commence à être accepté et se démocratise même avec l'investissement accru des sociétés dans les solutions mobiles. Quant à la future étape du BYOD, on parle déjà d' "App Stores d'entreprises" dans lesquelles ces dernières pourront proposer aux salariés des applications liées à leurs postes.

demainlemail.com – 27 mars 2012