SUJET NATIONAL POUR L'ENSEMBLE DES CENTRES DE GESTION ORGANISATEURS

CONCOURS EXTERNE DE TECHNICIEN PRINCIPAL TERRITORIAL DE 2ème CLASSE

SESSION 2012

EPREUVE

Rédaction d'un rapport technique portant sur la spécialité au titre de laquelle le candidat concourt. Ce rapport est assorti de propositions opérationnelles.

Durée : 3 heures
Coefficient : 1

SPECIALITE : Ingénierie, Informatique et Systèmes d'information

A LIRE ATTENTIVEMENT AVANT DE TRAITER LE SUJET

Ce document comprend : un sujet de 2 pages, un dossier de 24 pages.

- **Vous ne devez faire apparaître aucun signe distinctif ni dans votre copie, ni dans tout document à rendre (nom ou nom fictif, signature ou paraphe, numéro de convocation...)**
- **Aucune référence (nom de collectivité, nom de personne, ...) autre que celle 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, 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.**

De plus en plus d'agents souhaitent pouvoir utiliser leurs outils informatiques personnels (tablette, smartphone, mobile ...) pour le travail. Ce phénomène, connu sous le nom de BYOD (Bring Your Own Device) illustre la porosité de plus en plus importante entre vie professionnelle et personnelle.

Vous êtes technicien principal territorial de 2ème classe dans la commune de Techniville (2000 agents, budget annuel, tous postes confondus, supérieur à 230 millions d'euros, 150.000 habitants)

Dans un premier temps, le DGA en charge des Moyens Généraux et Systèmes d'Information vous demande de rédiger à son attention, exclusivement à partir des documents ci-joints, un rapport technique portant sur l'utilisation des outils personnels pour le travail. **8 points**

Dans un deuxième temps, vous proposerez un plan d'action visant à rendre techniquement possible l'utilisation, par les agents de la collectivité, de leurs outils personnels. **12 points**

Pour traiter cette seconde partie, vous mobiliserez également vos connaissances

Document 1 : Fiche n°5 « Comment sécuriser l'informatique mobile ? » Guide de la CNIL, Sécurité des données personnelles (extrait) - Edition 2010 – www.cnil.fr - 1 page

Document 2 : « BYOD : la charte informatique encore plus nécessaire » - www.blog-lamon-associes.com - 22 février 2012 - 1 page

Document 3 : « Six questions sur le phénomène "Bring your own device" » - www indexel.net -15 juin 2011 - 2 pages

Document 4 : « L'instantané devient-il la nouvelle norme ? » - www.focusrh.com – 7 mars 2012 - 2 pages

Document 5 : « Le CG13 virtualise et sécurise ses postes de travail » - www.lemagit.fr – 25 novembre 2011 – 2 pages

Document 6 : « Le "bring your own device" gagne du terrain » - www.decision-achats.fr mai 2012 - 1 page

Document 7 : « En quête de liberté : pourquoi les entreprises ont tout intérêt à suivre les nouvelles tendances de la mobilité » - www.cio-online.com - 7 mai 2012 - 2 pages

Document 8 : « BYOD : comment transformer son Smartphone en outil professionnel ? » - www.telcospinner-solucom.fr - 16 août 2011 – 4 pages

Document 9 : « Les outils de mobilité : les dernières évolutions et leurs impacts » - cercleducrm.wordpress.com - 2 mars 2009 - 1 page

Document 10 : « Bring your own device : quels risques ? quelles règles ? » - www.feral-avocats.com - novembre 2011 – 2 pages

Document 11 : Formulaire de demande d'installation d'un client messagerie + agenda professionnel sur un équipement personnel – Document interne émanant d'une collectivité territoriale – 2011 - 1 page

Document 12 : « Le Mobile Device Management : enjeux, outils et perspectives en entreprise » - http://iseeds.fr - 2 septembre 2010 - 3 pages

Document 13 : « Avantages et inconvénients du MDM face au MAM » - http://iseeds.fr - 24 mai 2012 - 2 pages

Ce document comprend : un sujet de 2 pages, un dossier de 24 pages.

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

DOCUMENT 1

Guide de la CNIL. Sécurité des données personnelles (extrait)

www.cnil.fr

Fiche n° 5 - COMMENT SÉCURISER L'INFORMATIQUE MOBILE?

Fiche n° 5 - Comment sécuriser l'informatique mobile ?

La multiplication des ordinateurs portables, des clés USB et des smartphones rend indispensable d'anticiper la possible perte d'informations consécutive au vol où à la perte d'un tel équipement.

Les précautions élémentaires

• Prévoir des moyens de chiffrement pour les espaces de stockage des matériels informatiques mobiles (ordinateur portable, périphérique de stockage amovible tel que clés USB, CD-ROM, DVD-RW, etc.).

Parmi ces moyens, on peut citer :
- le chiffrement du disque dur dans sa totalité au niveau matériel ;
- le chiffrement du disque dur dans sa totalité à un niveau logique via le système d'exploitation ;
- le chiffrement fichier par fichier ;
- la création de conteneurs chiffrés.

Parmi les outils disponibles, des logiciels libres tels que TrueCrypt (www.truecrypt.org) permettent de créer des conteneurs chiffrés dont la sécurité repose sur un mot de passe.

De nombreux constructeurs de PC portables vendent des solutions avec disque dur chiffré : il convient de privilégier ces équipements et de s'assurer que le chiffrement est bien mis en oeuvre par les utilisateurs.

Ce qu'il ne faut pas faire

• Conserver des données personnelles dans les équipements mobiles lors de déplacement à l'étranger. On peut consulter à ce sujet les préconisations formulées dans le document Passeport de conseils aux voyageurs publié par l'ANSSI disponible à l'adresse http://www.securite-informatique.gouv.fr/IMG/pdf/Passeport-de-conseils-aux-voyageurs_janvier-2010.pdf.

Pour aller plus loin

• Lorsque des appareils mobiles servent à la collecte de données en itinérance (ex : PDA, Smartphones ou PC portables, etc.), il faut sécuriser les données qui y sont stockées et prévoir un verrouillage de l'appareil au bout de quelques minutes d'inactivité. Prévoir aussi de purger ces équipements des données collectées sitôt qu'elles ont été introduites dans le système d'information de l'organisme.
• De plus en plus d'ordinateurs portables sont équipés d'un dispositif de lecture d'empreinte digitale. La mise en oeuvre de tels dispositifs est soumise à l'autorisation de la CNIL.

DOCUMENT 2

BYOD : la charte informatique encore plus nécessaire

www.blog-lamon-associes.com

La tendance actuelle pour les salariés est d'utiliser leurs interfaces numériques personnelles dans l'exécution de leurs fonctions professionnelles. Cette tendance porte le nom de BYOD (Bring Your Own Device) et soulève de nombreuses interrogations sur le plan légal.

Quelles sont les précautions juridiques que doit prendre l'employeur face au développement du BYOD ?

L'employeur doit être conscient des obligations légales qui lui incombent s'il encourage ou tolère une telle pratique dans son entreprise.

D'après les lois HADOPI, l'employeur doit s'assurer que les employés utilisent le réseau conformément à la législation sur la propriété intellectuelle. Si le salarié télécharge un contenu contrefaisant via le réseau Internet de l'entreprise, l'employeur sera responsable.

L'employeur doit veiller à respecter la vie privée de ses employés. Le matériel appartenant au salarié, toute saisie nécessitera une autorisation judiciaire. Pour la même raison, le salarié qui subit le vol de son matériel au sein de l'entreprise pourra dans certaines situations, demander réparation à son employeur.

Si le contrat de travail et/ou la charte informatique de l'entreprise ne règlent pas ces questions, les juridictions françaises ont tendance à favoriser la protection des salariés.

Les difficultés que soulève le BYOD se traitent efficacement grâce à l'introduction d'une charte informatique en annexe du règlement intérieur. Cette charte organise l'utilisation du matériel numérique personnel par le salarié dans l'exercice de ses fonctions. Elle doit appréhender un certain nombre de points importants :

- Imposer des conditions de sécurité au salarié (antivirus, protection matérielle des terminaux contre le vol...) ;

- Désigner la propriété des données professionnelles contenues dans l'interface personnelle (au cours de l'exécution du contrat de travail et à son terme) ;

- Etablir précisément ce qui relève de la vie personnelle ou de la vie professionnelle du salarié ;

- Préciser les modalités de contrôle et les sanctions encourues...

Pour être efficace, cette charte doit être rédigée sur-mesure selon les besoins de l'entreprise.

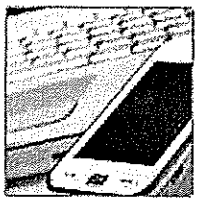
DOCUMENT 3

Six questions sur le phénomène "Bring your own device"

www.indexel.net

Initialement subi par l'entreprise, le phénomène "Bring your own device" ou "apportez votre appareil personnel" devient une opportunité, à condition de l'encadrer aux niveaux sécurité, financier et juridique.

1. Quelle est l'origine du BYOD ?



Le phénomène "bring your own device" ou "apportez votre propre appareil", est né de l'engouement du grand public pour les smartphones et les tablettes. Il a été accentué par la crise. *"Nombre d'employeurs ont restreint l'usage personnel du mobile professionnel ou ont arrêté de fournir gratuitement des smartphones"*, explique Antoine Marcou, expert practice télécoms & innovation chez Solucom. Dès lors, les employés, frustrés par l'écart entre l'ergonomie du mobile fourni par l'entreprise et celle de leur iPhone personnel, ont utilisé ce dernier pour un usage professionnel. *"Pris de court par ce phénomène fulgurant, nos clients s'inquiètent de l'arrivée massive d'objets incontrôlés dans leur entreprise"*, constate Jean-Michel Craye, responsable de la stratégie pour les services à l'utilisateur chez Orange Business Services.

2. Comment détecter le phénomène ?

Certains utilisateurs insèrent, dans leur smartphone personnel, la puce du téléphone professionnel. *"L'entreprise constate alors une évolution des usages et une augmentation de la consommation, donc de la facture mobile"*, explique Jean-Michel Craye. D'autres demandent en toute innocence au support technique comment se connecter à la messagerie à partir de leur smartphone. Enfin, les jeunes générations paramètrent eux-mêmes ce smartphone pour accéder aux applications de l'entreprise, parfois en contournant les protections. *"Cela se voit par l'analyse du trafic"*, ajoute Jean-Michel Craye.

3. Est-ce une opportunité pour l'entreprise ?

Le phénomène permet l'introduction, pour des usages professionnels, de terminaux sophistiqués et d'applications pouvant apporter une réelle valeur à l'entreprise. *"Les employés assurent un rôle de prescripteur auprès de leur management, par exemple en proposant de tester la tablette, en réunion pour la prise de notes, ou lors de présentations chez des clients"*, cite Antoine Marcou (photo).D'autre part, l'entreprise a longtemps reproché aux utilisateurs de ne pas être formés aux technologies de l'information. *"Depuis qu'ils les utilisent pour leur usage personnel, les problèmes de formation sont en partie réglés"*, explique Antoine Marcou. De plus, le BYOD incite à décloisonner les sphères professionnelles et personnelles, ce qui peut être source de nouveaux partenariats ou de prospection. Enfin, l'utilisateur prend davantage soin du terminal, puisque c'est le sien.

4. Les entreprises doivent-elles le craindre ?

Le BYOD pose des questions de sécurité de l'accès au système d'information, de risque d'introduction de codes malveillants et de fuites de données. À ce titre, la crainte principale, c'est que des informations stratégiques soient stockées en local sur l'appareil. *"Les tablettes posent des questions supplémentaires car elles permettent un accès plus large aux documents stockés sur les serveurs"*, explique Antoine Marcou. Très classiquement, la maîtrise de la sécurité impose l'identification et l'authentification des utilisateurs, le contrôle des configurations et le chiffrement des données stockées et les flux. Or, l'hétérogénéité inhérente au BYOD complique ces tâches. Il est donc conseillé d'établir une liste de terminaux autorisés et d'adopter une solution sur étagère multi-OS, comme Afaria de Sybase, ou Good de Good Technology.

5. Quelles sont les questions juridiques ?

Il existe d'autres craintes, comme celle d'usages illicites de l'accès internet à partir du réseau de l'entreprise, donc sous la responsabilité de celle-ci. À l'inverse, l'employé peut craindre pour sa vie privée. *"Sans créer une barrière franche entre usage professionnel et personnel, il faut définir un cadre juridique pour éviter de faire courir des risques à l'entreprise ou à l'employé"*, met en garde Jean-Michel Craye (photo). Il s'agit de préciser si l'entreprise a le droit de tracer ses employés, d'assurer la protection de ses données personnelles, ou encore de dégager la responsabilité de l'entreprise en cas d'usage illicite. Cela passe notamment par une modification de la charte d'utilisation de l'informatique ou du contrat de travail.

6. Comment répartir les coûts ?

Même si l'utilisateur finance son propre terminal, le BYOD est source de coûts, que ce soit au niveau de la facture télécom ou de l'impact sur l'infrastructure de l'entreprise. Dès lors que celle-ci considère que le phénomène représente une valeur ajoutée ou qu'il faut le canaliser, elle doit réfléchir au partage des coûts. *"Soit l'entreprise dédommagera l'utilisateur en considérant qu'il apporte le terminal, soit l'utilisateur participera aux frais télécom car il utilisera partiellement le forfait professionnel pour son usage personnel"*, analyse Jean-Michel Craye. Certaines entreprises règlent le problème en achetant le smartphone de l'employé qui en fera officiellement un usage mixte, ce qui permettra d'en faciliter le contrôle.

DOCUMENT 4

L'instantané devient-il la nouvelle norme ?

www.focusrh.com

L'urgence c'est fini ! Aujourd'hui on vit dans l'immédiateté. Parce que les « nouvelles » technologies nous permettent d'être de plus en plus réactif et de communiquer toujours plus rapidement, nos modes de vie et de travail changent et s'accélèrent. L'instantané va-t-il pour autant devenir la nouvelle norme ?

Dans une société où tout va très vite, où tout va de plus en plus vite, la relation à l'autre tendrait à disparaître tout comme la notion de temps. Aujourd'hui, on n'a plus le temps. Il est en effet devenu insupportable de devoir attendre quelques instants pour faire un achat à un guichet, ou inacceptable de ne pas être livré dans la journée d'une commande passée sur le web.

Dans l'entreprise, il n'est plus concevable de ne pas répondre au téléphone, dès la première sonnerie de son portable, que l'on soit en réunion, à son domicile le soir, ou en congés. L'incompréhension est identique, pour un mail posté le week-end qui resterait sans réponse jusqu'au lundi matin.

Ce ne sont pas tant les comportements qui changent, mais les comportements qui ne changent pas face à des outils incroyablement plus performants qui nous laissent imaginer pouvoir devenir beaucoup plus performants nous-mêmes. Et là se posent à nous de réelles questions.

Sommes-nous pressés ou stressés ?

Répondre à tout, n'importe où, tout le temps, symbolise une époque où les barrières entre le personnel et le professionnel deviennent de moins en moins lisibles. La multiplication des outils de communication participe totalement à cette situation nouvelle. Quand le téléphone devient mobile et qu'un collaborateur le conserve en permanence, cela induit qu'il devienne joignable à tout moment. Quand on utilise au bureau son smartphone personnel pour communiquer sur des réseaux sociaux, alors la sphère privée s'invite dans celle de l'entreprise.

Développer la capacité de traiter à la fois le perso et le pro, dans des proportions variables, autant sur son lieu de travail qu'à domicile, permet une plus grande disponibilité et réactivité. Cela permet peut-être de travailler plus et plus vite. Mais cela explique aussi souvent la multiplication de risques psychosociaux, que la loi impose désormais aux entreprises de prévenir.

Oui, les temps de l'action, de la réaction voire de la production sont plus rapides avec de nouveaux outils de communication, mais celui de la réflexion reste celui de l'humain et sa croissance n'est pas décuplée grâce à la technologie.

Oui, le stress peut être positif et moteur, porteur d'une forte motivation à réaliser son travail, mais il peut aussi être négatif, être un poids, un frein, et causer un stress finalement nuisible à l'activité professionnelle.

Qu'est-ce que je connais du temps de l'autre ?

L'abus de « nouvelles » technologies, avant de risquer de nous faire perdre tous nos repères, pourrait nous rendre égoïstes voire idiots.

N'oublions pas de rester des humains car nous ne serons jamais des machines. Ne confondons pas rythmes de vie et cadences. Et surtout, restons attentifs à l'autre et notamment au temps de l'autre. Notre agenda professionnel, notre charge de travail ou nos obligations ne répondent pas toujours aux mêmes exigences, à commencer par celle du temps. Et, cela se respecte.

Quand un mail est envoyé la nuit par un expéditeur insomniaque, le destinataire ne doit pas se sentir obligé d'y répondre sur le champ. Il doit être capable d'accepter, sans se culpabiliser, de profiter de sa soirée entre amis, ou de sa nuit.
Le manager qui décide de travailler le week-end, peut aussi enregistrer ses messages pour ne les diffuser que le lundi, évitant de pousser ses collaborateurs à travailler sur leur temps de repos.
Quand la machine devient de plus en plus performante, l'humain aussi doit devenir de plus en plus performant, pas dans sa capacité à produire, mais dans celle à maintenir un niveau relationnel soutenu, contrepoids nécessaire et indispensable à son équilibre et à sa capacité à vivre l'expérience !
L'instantané est probablement déjà devenu la norme. Il faut donc nous adapter à cette situation à laquelle nous ne sommes peut-être pas suffisamment préparés. Optimiser l'écoute, l'attention, et de façon générale la relation humaine pour favoriser l'harmonie entre développements technologiques et humains, devient alors certainement une des clefs de la réussite du monde de l'entreprise de demain.

DOCUMENT 5

Le CG13 virtualise et sécurise ses postes de travail

Le MagIT

Marc Dovero, RSSI du Conseil Général des Bouches du Rhône, a expliqué, à l'occasion des Assises de la Sécurité, comment ses équipes ont commencé à virtualiser les postes de travail des milliers d'agents du CG avec XenDesktop.

Marc Dovero, RSSI du CG13, plante d'emblée le décor, soulignant les contraintes de la DSI : le Conseil Général est une collectivité territoriale aux prérogatives vastes, avec de nombreux métiers. En tout, il compte 7000 agents pour 6500 postes de travail, le tout éclaté sur un grand nombre de sites. Certes, un site principal - l'hôtel du département - centralise environ 2500 personnes. Un second, à côté de la tour CMA, à Marseille, en rassemble 800, mais la problématique demeure. Et la multiplication des métiers propres à une collectivité territoriale induit celle des applications, «peu d'architectures Web, surtout des logiciels achetés avec des architectures client/serveur ». Les serveurs étant essentiellement concentrés sur l'hôtel du département.

L'allocation de locaux à proximité de la tour CMA a été l'occasion de mettre en place un socle technique adapté aux besoins des métiers, explique Marc Dovero : «il a fallu intégrer les nouveaux terminaux - tablettes et smartphones (personnels et fournis par la collectivité) -, et des ordinateurs dits personnels », même si le *Bring Your Own Device* n'a pas encore cours. Toutefois, il s'agissait de permettre à des prestataires de pouvoir utiliser leur propre matériel sur le réseau du CG. Plus globalement, le projet devait permettre à l'administration de gagner en agilité et de réduire les coûts associés aux postes de travail : «oui, cela représentait un investissement mais nous calculons le retour sur investissement sur la base de la réduction des coûts de maintenance, sur le poste de travail et sur le réseau, ainsi que sur l'exploitation des serveurs », explique le RSSI.

La place limitée sur les bureaux du nouveau bâtiment a poussé à l'adoption de clients légers. «Il y avait deux risques pour nous : la lenteur et l'acceptation des utilisateurs. Mais cela s'est bien passé », se rappelle Marc Dovero. Pour éviter les risques de ralentissement par rapport à des postes lourds, « on a fait simple en mettant tous les serveurs concernés dans le même bâtiment ». Et l'appropriation des terminaux s'est également bien déroulée : «la mobilité est la plus appréciée, cette capacité à se connecter depuis n'importe quel terminal. Ça a pris le pas sur le fait d'avoir son propre PC et ses propres personnalisations.» Les machines virtuelles sont sous Windows 7, avec Exchange et Lync; les serveurs sont virtualisés avec Hyper-V et les postes de travail, produits avec XenDesktop et XenApp.

Pour la sécurité, le CG13 voulait traçabilité et authentification : «il fallait au moins pouvoir tracer les demandes de connexion et les actions sur les applications. Les solutions de F5 Networks nous ont été assez utiles pour faire ça: nous les avons déployées en coupure de beaucoup de choses. En authentification, NAC et 802.1X nous permettent de procéder à l'authentification à la connexion du poste. [...] Nous sommes partis du principe de recentrer la sécurité sur le centre de calcul, après avoir enlevé l'information du poste de travail. Le poste peut alors se permettre d'être hors de la zone de confiance.» Ce qui permet, au passage, d'aborder sereinement la question des accès

distants, via Internet, « en OTP sur un VPN. Tous les utilisateurs n'y ont pas encore accès; nous sommes un peu frileux et en phase d'audit de sécurité ».

Le Conseil Général a également mis en place un dispositif de partage de fichiers par Internet : «nous en avions un peu assez que les gens utilisent des services externes comme réceptacles des données de l'administration. Nous devions proposer une alternative, un équivalent plus industriel chez nous.» Sur le réseau local, les «clients légers sont connectés avec NAC, et authentifiés par certificat numérique. C'est vrai également pour les téléphones IP et pour les PC. On espère que ce sera vrai pour les iPad mais nous n'avons pas encore testé. Accessoirement, cela renforce la sécurité et cela réduit les coûts d'exploitation avec l'assignation automatique des VLAN ». Bien sûr, Marc Dovero avait dû conduire, au préalable, «un projet de PKI : 800 certificats pour les postes; autant pour les téléphones ».

Pour sécuriser les données, «les flux entre postes et applications sont contrôlés selon les profils ActiveDirectory ». Un étage de contrôle du trafic applicatif est assuré par les équipements F5 dont sont également activées les fonctionnalités d'équilibrage de charge. «Le cluster d'équipements F5 a été configuré en actif/passif sur un seul site, initialement. Dans le cadre du plan de continuité de l'activité, il a vocation à évoluer vers une configuration actif/actif sur deux sites », pour assurer l'équilibrage de charge, toujours, mais aussi la haute disponibilité. Le filtrage des flux applicatifs est quant à lui «en cours de renforcement : entre les machines virtuelles et les applications. Avec la solution F5, on peut encore affiner, en marquant certaines activités. Nous n'avons pas encore essayé mais nous allons y venir.»

Marc Dovero souligne la flexibilité et l'évolutivité des solutions F5 : «nous les avons choisies en raison de leur ouverture et des capacités de personnalisation.» Mais il conserve un regard réaliste dessus. Heureusement que son partenaire - Telindus - était là pour le déploiement : «ils connaissent bien le produit et la réécriture de règles hors de l'interface Web est complexe.» Toutefois, passée cette première phase, «l'exploitation est facile.»

DOCUMENT 6

Le "bring your own device" gagne du terrain

www.decision-achats.fr

L'Observatoire de l'informatique et des télécoms au service des nouvelles organisations de travail, publié annuellement par [...] IDC, s'intéresse aux environnements mobiles que les salariés possèdent et utilisent, de plus en plus systématiquement, sur leur lieu de travail.

[...] Une enquête a été menée au cours du mois de mars 2012 auprès de deux populations, issues d'entreprises de plus de 50 salariés : des responsables informatiques (240 entretiens téléphoniques) et des salariés possédant au moins un outil mobile, à titre privé ou professionnel (795 répondants, par web-enquête).

Le phénomène "bring your own device"

Séduits par l'ergonomie, l'esthétique et la flexibilité offertes par les outils de dernière génération, notamment les smartphones, les salariés les adoptent rapidement dans leur vie personnelle et les utilisent dans le cadre de leur travail (une tendance souvent désignée par l'expression anglaise "bring your own device") :

- 61 % des salariés interrogés possèdent au moins un smartphone. Parmi ceux-ci, un agent sur deux a son smartphone personnel et **seuls 22 % des salariés en ont un fourni par l'entreprise**
- 52 % des salariés équipés utilisent leurs outils personnels dans leur entreprise alors que 65 % des responsables informatiques interrogés déclarent ne pas autoriser la connexion au système d'information via les outils personnels des salariés (principalement pour des raisons de sécurité).

Un travail qui déborde de plus en plus sur la vie personnelle

Ce décalage entre la position officielle des responsables informatiques et la pratique réelle des salariés a pour conséquence la montée d'un "télétravail" non formalisé, aux pratiques non encadrées. En effet, si les salariés perçoivent bien les avantages de ces outils de mobilité pour mieux équilibrer leurs vies personnelles et professionnelles, **72 % d'entre eux reconnaissent travailler sur leur temps personnel**.

[...] Si elle présente des avantages [...], cette abolition progressive de la frontière entre vies personnelle et professionnelle nécessite un encadrement des usages afin de ne pas conduire le salarié à une situation de connexion permanente (et donc à un risque de sur-sollicitation). Face à cette forte volonté d'équipement [...], de plus en plus d'entreprises intègrent peu à peu la mobilité dans leur stratégie informatique :

- **L'équipement en outils nomades progresse**, avec plus de PC portables fournis au détriment des PC fixes et un triplement des équipements en tablettes média
- Un tiers des entreprises ont initié la **virtualisation des applications et du poste de travail** qui permet d'offrir un environnement de travail accessible via un navigateur internet ;
- 34 % des entreprises ont prévu à court terme la **convergence fixe-mobile**, en s'appuyant sur le haut débit des réseaux fixes et mobiles 3G+ et 4G, ce qui a pour avantage une meilleure accessibilité des collaborateurs.

52 % des responsables informatiques interrogés déclarent néanmoins n'avoir encore rien prévu en la matière. Ils devront alors faire face aux enjeux de financement (principal frein pour 38 % des interrogés) et de sécurité. Sans oublier les enjeux d'encadrement des usages...

DOCUMENT 7

En quête de liberté : pourquoi les entreprises ont tout intérêt à suivre les nouvelles tendances de la mobilité

www.cio-online.com

Si vous êtes [...] à la recherche de jeunes talents, vous aurez sans doute remarqué que les nouveaux candidats prennent en compte des critères bien plus variés que le salaire [...].

Parmi les facteurs déterminants pour la nouvelle génération d'actifs: la possibilité de conserver une part de liberté dans leur manière de communiquer. Pour les employeurs, cela revient à laisser leurs nouvelles recrues communiquer selon le mode qu'ils ont adopté naturellement dans leur vie privée, en tant que génération ayant grandi dans le monde numérique.

Cela comprend bien évidemment l'utilisation des réseaux sociaux, mais également, et plus que jamais, l'utilisation de certains périphériques bien connus des jeunes. Ils préfèrent encore ne pas communiquer du tout plutôt que de s'encombrer d'un périphérique « has-been »

C'est ainsi qu'est né le mouvement « BYOD » (« Bring your own device », apporte ton propre périphérique) il y a quelques années aux Etats-Unis. Comme beaucoup d'autres tendances, celle-ci a réussi à s'imposer.

A première vue, permettre aux employés de connecter leurs propres périphériques au réseau professionnel peut sembler risqué et ouvrir la porte aux fuites de données et à d'autres menaces pour l'entreprise. En y regardant de plus près, cependant, il s'agit déjà d'une réalité [...].

L'heure est venue de fixer les règles

Pratiquer la politique de l'autruche serait malvenu. Au contraire, il est temps pour les entreprises de définir des règles strictes pour cadrer le mouvement BYOD. Ce sera le seul moyen pour les responsables informatiques d'assurer un contrôle de tous les périphériques appartenant aux employés et étant connectés au réseau d'entreprise, et ainsi éviter que le réseau ne soit investi dans l'ombre.

Cela est préférable pour tous, d'autant plus que, dans les environnements qui prévoient une procédure d'autorisation pour que les employés puissent connecter leurs propres périphériques, cette solution permet de pallier le caractère relativement anarchique de la situation actuelle.

En tant que responsable informatique, quels éléments prendre en considération avant d'adopter le système BYOD ? D'après moi, le système BYOD séduit les responsables informatiques car il peut leur épargner la gestion complexe du matériel.

[...] Malgré tout, le système BYOD s'accompagne de deux risques : la fuite des données et l'accès frauduleux au réseau d'entreprise.
Le premier problème est loin d'être nouveau : les responsables informatiques se heurtent déjà à la difficulté de gérer les capacités de mémoire élevées des périphériques ultra mobiles comme les smartphones et les tablettes.

Comme avant, avec les clés USB, l'un des défis rencontrés par les responsables informatiques consiste à contrôler les données copiées depuis le réseau sur des périphériques portables, sur des sites de partage ou par e-mail. Aujourd'hui, de nombreuses solutions permettent aux entreprises de s'attaquer à ce problème en particulier.

La menace d'un accès non autorisé au réseau d'entreprise inquiète particulièrement les responsables informatiques lorsque la fraude est localisée à l'intérieur du pare-feu, c'est-à-dire lorsqu'elle est réalisée depuis un périphérique (PC ou tablette) non autorisé et simplement connecté au réseau. Là aussi, la plupart des entreprises utilisent déjà des outils de protection contre ce type de risque.
[...]

Une nouvelle perspective
Nous assistons à une redéfinition des priorités : ce qui comptait le plus auparavant était la gestion des périphériques physiques tels que les ordinateurs portables et de bureau.

Désormais, les responsables informatiques s'intéressent uniquement à l'image de l'entreprise fonctionnant en tant que machine virtuelle hôte.

Le meilleur moyen de gérer et de sécuriser tous les périphériques BYOD est de définir une limite très nette entre les technologies placées sous la responsabilité de l'employé et celles étant gérées par l'employeur. Certaines entreprises utilisent déjà des smartphones comme machines virtuelles, ce qui signifie que chaque périphérique (ordinateur portable, tablette, smartphone, etc.) peut fonctionner en tant que machine virtuelle appartenant au réseau professionnel : on a donc, sur un seul et même périphérique, un environnement sécurisé indépendant de l'environnement privé.

En bref, même si le système BYOD peut faire peur, il s'avère très bénéfique s'il est utilisé correctement. [...]

DOCUMENT 8

BYOD : comment transformer son Smartphone en outil professionnel ?

www.telcospinner-solucom.fr

La révolution mobilité est en marche dans les entreprises. **Le BYOD (Bring You Own Device)** consiste à se servir de son terminal mobile personnel (Smartphone, Tablette) comme d'un outil professionnel. On retrouve principalement des outils utiles améliorant le confort de travail des salariés. (Contact, mail, Communication…)

Nous constatons ces dernières années que les progrès réalisés sur les technologies mobiles en termes d'équipements sont tirés par le marché grand public. Les smartphones ainsi que les tablettes par leur accès internet sont devenus de véritables terminaux d'accès au SI.

On parle alors de la « consumérisation » de l'informatique. L'impulsion est donnée par **les VIP de l'entreprise** et par la « **génération Y** » qui tolèrent mal d'être moins bien équipés au bureau qu'à la maison.

Motivées par les employés, de plus en plus d'entreprises sont prêtes à franchir le pas. Selon **IDG Survey, 60 % des entreprises** pensent qu'il est important de supporter le BYOD pour satisfaire le besoin fonctionnel des salariés. En entreprise, **89% des applications mobiles utilisées aujourd'hui sont dédiées à la messagerie** et **74 % à la gestion de contacts et l'agenda** selon le cabinet d'étude Forrester.

La technologie mobile avance à grand pas, les usages des utilisateurs professionnels également. Cette forte poussée des salariés équipés de smartphones oblige les directions à accélérer le déploiement des applications mobiles professionnelles. Nous allons tenter d'expliquer ce phénomène par une brève étude de 2 corps de métier : le consultant que je représente et un médecin libéral.

Prenons le cas de ce consultant corporate et technophile équipé d'un IPhone 4 et d'une suite professionnelle Office et tâchons de lister ses besoins professionnels :

- Accéder aux outils de communications professionnels (Mails, synchronisation calendrier, contacts)
- Prise de notes
- Visualisation de documents compatible avec la suite Office
- Éditer un document de la suite Office avec un émulateur
- Aide à la navigation routière
- Gestionnaire d'appel en fonction des types d'appels et correspondants
- Outils d'impression

Afin de répondre à ses usages nous avons sélectionné des applications disponibles sur les plates-formes de téléchargement mobile. Dans le cadre de notre étude nous évaluons les coûts perçus par l'utilisateur et non les dépenses que cela engendre pour l'entreprise.

Usages	Applications	Android	IOS	Prix	Description
Accéder aux outils de communication interne	Good Technology	✓	✓	Free pour l'employé	Application: Push mail/ Partage Calendrier Pro / Contacts entreprise
	Airwatch	✓	✓	Free pour l'employé	Application : Push mail/Partage Calendrier Pro/ Contacts entreprises
Prise de note	Evernote	✓	✓	Free	Application : Prise de note/ Prise de photos / Prise de Vidéo/Enregistrement sonore
	OneNote	✗	✓	Free	Application: Création de mémos, Dresser des listes en insérant diverses sources (textes images sons vidéo)
Visualiser et éditer des logiciels bureautique	Iwork	✗	✓	7,99€ / Application	Application: Création et partage de documents professionnels(Keynotes, Pages and Numbers)
	Document to go	✓	✓	10,55€	Application: Modification, création et affichage des fichiers Word, Excel, Power Point.
Imprimer	Printcentral pro	✗	✓	7,99€	Application: Impression vers les imprimantes Wifi, Impression via le réseau 3G.
	Print	✓	✓	3,51€	Application : Impressions vers les imprimantes Wifi et le réseau 3G.
Aide à la navigation routière	Navigon	✓	✓	49,99€ IOS / 49,95€ Android	Application: Navigation GPS, Aide à la navigation routière
	Tom Tom	✗	✓	59,99€ IOS	Application : Aide à la navigation routière
Gérer les appels	Mute o Matic	✓	✗	1,99€	Application: Mise sous silencieux du téléphone en fonction des évents du calendrier synchroniser
	Calendar Mute	✗	✓	Free	Application: Configuration du téléphone en mode silencieux ou vibreur en fonction des évènements planning

Figure 1 : Le Toolkit applicatif du consultant

Ainsi notre consultant devra-t-il débourser environ 71€ pour s'équiper, pour avoir fait le choix d'un mobile compatible avec 2 des 3 OS mobiles les plus vendus sur le marché. Il faut compter également l'abonnement Data nécessaire pour un tel usage dont le coût, lui, est de l'ordre de 35€ aujourd'hui sur le marché pour les 1ers prix.

Prix annuel : 420€/an + 71€ d'application.

À présent penchons-nous sur les usages auxquels fait face un médecin de nos jours :

- Gestionnaire de planning
- Accès simplifié à un guide thérapeutique
- Aide à la consultation par enregistrement audio
- Aide au diagnostic
- Prise de mesures sur le corps humain (Tension, électrocardiogramme)
- Accès aux logiciels bureautiques mobiles
- Impression

Les applications orientées santé connaissent un succès florissant. Voici quelques applications indispensables à notre praticien :

Usages	Applications	Android	IOS	Prix	Description
Prise de mesure sur le patient	Alivecor	✗	✓	100€	Application: Coque associée à un programme afin d'obtenir l'électrocardiogramme d'un patient
	Withings	✗	✓	129€	Application : Dispositif pour prendre la tension sur iPhone/ iPad
Information	Arrêt cardiaque	✓	✓	Free	Application: Localisation du défibrillateur le plus proche
	Doctor 2.0	✗	✓	Free	Application: Liste conférences, Agenda composé de Cv intervenants + thème Actus.
Aide au diagnostic	Urgences 1clic	✗	✓	29,99€	Application: e-book de langue française regroupant tout les domaines de la médecine d'urgence.
	Fiches preuves et pratiques	✗	✓	Free	Application: Guide de référence de plus de 200 situations cliniques présentées sous forme d'aide mémoire
Accès simplifié à un guide thérapeutique	Vidal Mobile	✓	✓	29,99€ / An	Application: Base de données de 10000 fiches médicaments. Fonction recherche par nom/substance/indication/laboratoires
	iMédiGuide	✗	✓	4,99€	Application: base de données thérapeutique à développée à partir des données de la banque Claude Bernard (BCB)
Accès aux logiciels bureautiques	Iwork	✗	✓	7,99€	Application: Création et partage de documents professionnels (Keynotes, Pages and Numbers)
	Document to Go	✓	✓	10,99€	Application: Modification, création et affichage des fichiers Word, Excel, Power Point.
Impression	Printcentral pro	✗	✓	7,99€	Application: Impression vers les imprimantes Wifi, Impression via le réseau 3G.
	Print	✓	✓	3,51€	Application: Impressions vers les imprimantes Wifi, impression via le réseau 3G
Aide à la navigation routière	Navigon	✓	✓	49,99€ IOS / 49,95€ Android	Application: Navigation GPS, Aide à la navigation routière
	TomTom	✗	✓	59,99€ IOS	Application: Aide à la navigation routière.
Aide à la consultation	Voice recorder	✓	✓	free	Application native
	Voixie Pro	✗	✓	1,59€	Application: Différents mode d'enregistrement, en mode archive ou en mode rapide. Envoie possible de la note via Email ou via les contacts ou téléphone.
Gestion de planning	Google Agenda	✓	✓	free	Application : GoogleSync
	Executive Assistant	✓	✗	6,99€	Application: Visibilité en clavier verrouillé des notifications mail, SMS, Messages manqués, évènements calendriers, Tâches

Figure 2 Trousse applicative du médecin

Ainsi notre praticien aura une facture de 330 € en plus d'un abonnement comme vu précédemment. Ceci se traduit par **un coût annuel de 420€ + 29,99€ (Vidal) = 450€/An + 330€ Application**

Quels sont les coûts cachés d'une solution de mobilité en entreprise? Nous prenons pour évaluer ces coûts l'une des solutions disponibles sur le marché, Good Technology for Enterprise , et effectuons le calcul pour une entreprise de 500 collaborateurs.

Cet exemple nous permet de noter, que, dans le cas de figure du consultant, les usages permettant l'accès aux communications professionnelles de l'entreprise sont transparents en termes de coûts vis-à-vis de l'employé mais pas de l'employeur. Les solutions du type de celle prise en exemple sont vendues selon le modèle suivant :

- Serveur licence (1430€ dans le cas de Good Technology)
- Licence par utilisateur (152€)
- Maintenance annuelle (430€/An)
- Support standard par licence utilisateur (24€/ An)

Soit un coût d'investissement **CAPEX : 77 430€**

Coût exploitation **OPEX : 12 430€**

L'ensemble des prix proposés sont des prix HT.

Au final, en se plaçant uniquement côté utilisateur nous constatons que les solutions associées au BYOD sont certes plus riches mais plus chères pour un médecin libéral que pour notre consultant, qui peut au final voir une partie des coûts prise en charge par son entreprise.

Ces coûts plus attractifs confirment bien la tendance selon laquelle les collaborateurs d'entreprise deviennent des éléments moteur dans cette démarche associant le confort personnel et l'utilité professionnelle pour une productivité accrue. Ne sommes-nous pas en train de changer nos outils de travail et notre manière de travailler ? Ce changement se traduira probablement par la capacité de nos DSI à innover de manière structurée afin de répondre à ce nouveau besoin.

DOCUMENT 9

Les outils de mobilité : les dernières évolutions et leurs impacts

cercleducrm.wordpress.com

Wi-Fi, carte 3G, Pocket PC, Blackberry ... Autant de solutions et de technologies qui permettent d'établir des accès permanents au système d'information de l'entreprise.
Les solutions dites « mobiles » permettent au collaborateur distant d'accéder à sa propre base de données clients, de rechercher et de mettre à jour des informations, de communiquer (via les SMS notamment) et d'optimiser ses tâches grâce à des solutions comme :

- **L'assistant numérique personnel** – ou **PDA** – qui est à l'origine un agenda électronique. Il s'est, depuis, beaucoup enrichi en fonctionnalités communicantes (push mail, carte 3G, connexions Bluetooth, etc.).
- **Les blackberry,** la différence avec l'utilisation d'un PDA réside dans le mode de transmission : les messages sont envoyés en temps réel au terminal, en mode "push", sans qu'il soit nécessaire de composer un code ou d'initialiser une connexion. On peut donc accéder sans fil aux comptes de messagerie existants et aux bases de données de l'entreprise, via le réseau mobile GPRS
- **Le smartphone**, un téléphone intelligent, où la communication et la navigation sur Internet priment. Les dernières fonctionnalités ajoutées font que cet outil se rapproche désormais du PDA
- **Le tablet PC**, qui se rapproche plus d'un ordinateur. Le clavier est presque inexistant puisque la plupart des commandes s'effectuent sur l'écran
- Enfin, **l'Ultra Portable**, intermédiaire entre l'encombrement d'un ordinateur et sa richesse applicative et les PDA, plus mobiles mais moins efficaces. Les Ultra Portables pèsent moins de 2 kg et se montrent relativement faciles à transporter.

La mobilité : des impacts sur la sécurité et la résistance des utilisateurs...

On reproche souvent aux solutions mobiles l'augmentation du risque sécuritaire (vol de données confidentielles en cas de vol du matériel). Aujourd'hui les dernières évolutions font que des solutions existent pour maîtriser ces risques : Cryptage des données et des communications, accès à une zone tampon protégée par des pare-feu ou pré-paramétrage de la connexion Bluetooth ou Wi-Fi du terminal.
En revanche, les technologies mobiles représentent un lien supplémentaire, rattachant – bon gré mal gré – le collaborateur à sa sphère professionnelle et c'est précisément ça qui peut rendre le déploiement des solutions mobilité plus complexe sur certain profils.
L'accroissement de la productivité individuelle a sans doute des conséquences sur les relations entretenues entre le collaborateur, plus particulièrement dans le cadre de Force de Vente mobile, et son entreprise, comme la sensation "piège" lié à la mise à disposition d'un matériel à des fins d'accroître en réalité son temps de disponibilité. Notons aussi que certains collaborateurs peuvent se sentir gênés par le fait que cet outil les met parfois dans l'obligation de répondre immédiatement et en permanence (tard dans la soirée ou pendant le week-end) aux sollicitations qui leur sont faites.

...mais une solution réellement efficace

Ces outils sont cependant dans bien des cas réclamés par les collaborateurs eux-mêmes. Tout réside dans l'utilisation que l'on souhaite qu'ils fassent de cet outil, et de la manière dont le déploiement va être mené. Doit-on revenir à certains critères de déontologie (par exemple en accordant au collaborateur des délais de réponse raisonnables malgré le caractère immédiat de l'outil) et mettre en évidence de façon plus claire les bénéfices de ce genre de solution afin de leur donner les meilleures chances de succès ?

DOCUMENT 10

« Bring your own device » : quels risques ? quelles règles ?

www.feral-avocats.com

Le salarié dispose aujourd'hui de deux excroissances indispensables à sa survie numérique : son smartphone et son ordinateur portable. A mesure que les sphères privées et professionnelles se mélangent, que le temps de travail mord sur le temps de repos et qu'une partie du temps de travail est consacrée à des activités personnelles, l'intérêt d'utiliser le même ordinateur portable, tant au bureau que chez soi, est évident.

Les intérêts du salarié, qui regroupe sur un même appareil toutes ses données, et de l'entreprise, qui n'a plus à en financer l'acquisition et la maintenance, peuvent ici se rejoindre. Chacun peut, cependant, avoir à souffrir de la situation.

Des risques réciproques à anticiper

L'ordinateur peut être une source de risques pour l'entreprise : c'est la porte d'entrée de virus et chevaux de Troie, c'est le lieu de stockage de contenus parfois illicites : musiques, vidéos, etc., c'est également un moyen pour sortir de l'entreprise de l'information confidentielle. Mais l'usage de son ordinateur dans le cadre du travail peut également être source de dommage pour le salarié : l'ordinateur peut être volé sur le lieu du travail ou même endommagé accidentellement par un autre salarié.

En l'absence de toute règle, quelques grands principes de droit de la responsabilité trouveront à s'appliquer. Le propriétaire d'un bien - donc le salarié - est responsable des dommages que le bien dont il a la garde cause à autrui, ce peut être son employeur mais également un autre salarié. Les cas de blessures physiques causées par un PC portable à un autre salarié sont des cas d'école. Dans cette hypothèse, comme pour tout dommage subi par une personne sur son lieu de travail, le régime juridique des accidents de travail s'appliquera, que l'employeur soit propriétaire ou non de l'appareil ayant causé le dommage.

L'hypothèse que l'on peut plus facilement imaginer est celle où le PC d'un salarié, mal paramétré ou non doté d'un antivirus performant et à jour, est à l'origine de la dissémination de virus ou d'une intrusion frauduleuse dans le système de l'entreprise. Le salarié verra-t-il sa responsabilité engagée ? Rien n'est moins sûr. Il n'y a pas aujourd'hui d'obligation pesant sur tout individu d'assurer la sécurité de son matériel informatique, c'est peut-être son intérêt, mais ce n'est pas son obligation. On peut penser que l'entreprise, par essence dans une situation de compétence supérieure à celle du salarié sur ces questions techniques, accepte le risque de voir connectés sur son réseau des matériels hétérogènes, à la sécurité non avérée. En outre, la jurisprudence constante de la Cour de cassation considère que la responsabilité civile du salarié envers son employeur suppose « non une simple erreur involontaire, mais une faute lourde assimilable au dol ». Cette faute lourde doit être caractérisée par une intention de nuire à l'employeur. Ce n'est que sur le terrain du droit disciplinaire que l'employé pourra être sanctionné, à condition que les règles de conduite qui lui ont été imposées aient clairement été spécifiées dans le règlement intérieur.

Mieux valant prévenir que guérir, l'entreprise sera avisée d'imposer aux salariés des outils de protection à l'état de l'art mais en assistant le salarié dans cet usage : quel logiciel ? quel paramétrage ? quelles mises à jour ? etc. Si l'entreprise fournit elle-même les antivirus, elle devra s'assurer auprès des éditeurs que les licences acquises lui permettent cette mise à disposition sur des postes dont elle n'est pas propriétaire.

Imaginons maintenant que ce soit l'ordinateur du salarié qui soit victime du dommage : son ordinateur peut faire l'objet d'un vol, il peut être accidenté par un autre salarié. Quelle sera la responsabilité de l'entreprise ? Ici, encore, en l'absence de toute règle, nous devons utiliser les principes généraux du droit de la responsabilité.

En cas de vol, c'est l'employeur qui sera présumé responsable de la disparition de l'ordinateur. Il sera tenu d'indemniser le salarié. Il pourra atténuer sa responsabilité en prouvant la faute du salarié.

L'entreprise devra s'aviser de vérifier que sa police d'assurance couvre tous ces types de dommages et de responsabilités.

Des règles claires à fixer

Il existe manifestement un intérêt réciproque, entre le salarié et l'entreprise, de fixer la règle du jeu de l'usage professionnel d'un bien privé. En l'absence actuelle de tout texte ou jurisprudence sur ces questions, il est préférable d'anticiper les risques [...]. Beaucoup d'entreprises disposent [...] d'une « charte » d'utilisation des moyens informatiques. Celles qui n'en ont pas encore ont un intérêt pressant à en adopter une.

Ces chartes sont des adjonctions au règlement intérieur de l'entreprise. Même si des juridictions ont accordé une certaine valeur juridique à ces « chartes », il est préférable de s'assurer de l'efficacité des interdictions et des sanctions qui y seraient édictées en les soumettant au régime juridique du règlement intérieur [...].

Les ordinateurs personnels utilisés par les salariés dans le cadre de leur activité professionnelle, sur le lieu de travail, connectés au réseau et aux ressources de l'entreprise doivent être inclus dans le périmètre de cette charte.

La charte devra notamment veiller à fixer les règles relatives à l'accès par l'employeur aux données présentes sur l'ordinateur du salarié.

En une décennie, la jurisprudence de la Cour de cassation s'est formée concernant l'accès par l'employeur aux données, mails ou documents, qui sont stockés sur le poste d'un salarié. Il est aujourd'hui admis par les tribunaux que les données présentes sur les postes de travail mis à disposition des salariés par l'employeur sont présumées être des données professionnelles. Il en résulte que l'employeur peut librement en prendre connaissance, les conserver, les recopier, etc, sauf si ces données sont clairement identifiées comme personnelles. Et même dans ce dernier cas, en cas de circonstances exceptionnelles, l'employeur peut obtenir un accès aux courriers électroniques et documents identifiés comme personnel par le salarié.

Cette jurisprudence, établie pas à pas au cours de la dernière décennie, devra nécessairement être revisitée à l'aune du « bring your own device ». En effet, s'il est aujourd'hui acquis que l'employeur à un accès « de plein droit » aux données présentes sur les postes de travail de ses salariés, qu'en sera-t-il lorsque ces ordinateurs seront la propriété des salariés ? Doit-on s'attendre à un renversement de la présomption : les données de l'ordinateur personnel du salarié seront-elles considérées par les juges comme présumées personnelles ? Dans ces circonstances, comment l'employeur aura-t-il accès aux données professionnelles, notamment lorsque le salarié est absent ou quitte l'entreprise ? Il y a là un champ d'incertitude que la charte informatique doit absolument combler. Des procédures techniques de recopie ou d'effacement automatique des informations de l'entreprise, lorsque le poste informatique du salarié est connecté au réseau ou lorsqu'il quitte l'entreprise, sont à étudier.

DOCUMENT 11

Formulaire

Objet : demande d'installation d'un client messagerie + agenda professionnel sur un équipement personnel.

Prénom et nom du demandeur :	
Service :	
Equipement personnel (iphone 3 / 4, galaxy ...) :	
Version logiciel (ios, android ...) :	
Justification du besoin :	

En acceptant cette installation, je m'engage à :

- En faire une utilisation conforme à la charte informatique
- Alerter le service support utilisateur en cas de perte ou de vol de mon équipement personnel le premier jour suivant le constat
- Utiliser l'agenda électronique professionnel
- Ne pas tenir la collectivité ou la DSI responsable d'un éventuel dysfonctionnement de mon équipement personnel
- Informer, par écrit, la DSI en cas de non utilisation de la solution
- Tenir à jour la version logicielle de la solution
- Ne solliciter le support utilisateur que pour des demandes concernant directement la solution installée.

Je suis également informé(e) que :

- Les demandes d'assistance concernant la solution ne sont pas prioritaires
- La DSI se réserve le droit de la suspendre sans accord préalable de l'utilisateur pour des raisons techniques (changement de solution, problème de sécurité, de licence ...), en cas d'utilisation non conforme à la charte informatique, ou sur décision hiérarchique en cas de non respect des engagements précédents.

Date :

Signature du demandeur : Signature du Directeur :

DOCUMENT 12

Le Mobile Device Management : enjeux, outils et perspectives en entreprise

http://iseeds.fr

C'est une tendance assez récente, mais il apparaît que les salariés imposent de plus en plus leur choix de smartphone au sein de leur entreprise.

Selon Good Technology, les Smartphones personnels sont de plus en plus utilisés dans la sphère professionnelle. Le succès grand public de l'iPhone et des smartphones sous Android constitue un facteur susceptible d'expliquer ce changement : « Plus que jamais, les usagers influencent fortement les décisions du SI en se basant sur leurs usages personnels" a commenté John Herrema, chef marketing de Good Technology le 5 Août dernier.

Aujourd'hui et selon le Gartner, 50% des cadres effectuent 80% de leurs opérations sur des PC non standardisés par l'entreprise. La vague touchera inévitablement le segment de la mobilité.
Cette situation peut être analysée selon deux perspectives :

- Tout d'abord, si l'utilisateur choisit d'utiliser son propre smartphone plutôt que celui proposé par l'entreprise, c'est qu'il perçoit des avantages d'utilisation et qu'il s'estime peut-être plus efficace avec.
- D'un point de vue plus mercantile, cela permet de limiter le TCO (Total Cost of Ownership) de l'entreprise : plus besoin de financer une flotte complète de smartphones si l'utilisateur possède déjà son propre terminal.

Si ce phénomène perdure, le cabinet Deloitte prévoit que le DSI risque de perdre une partie de son pouvoir, et que l'achat de matériel devra se faire en concertation avec les effectifs.

Duncan Stewart, directeur du centre de recherche chez Deloitte, nous explique donc qu'il est vain de chercher à imposer des smartphones s'ils ne sont pas utilisés, mais qu'il est préférable d'individualiser les achats, quitte à rallonger la note de 10%, afin que le matériel soit effectivement utilisé et que les employés soient satisfaits.

Cet état de fait implique qu'un collaborateur est susceptible d'utiliser un appareil personnel à des fins professionnelles et cela entraîne inévitablement des risques.

Par exemple, l'iPhone qui a été utilisé pour accéder à un service géolocalisé ou de partage de photos viendra se connecter au wifi de l'entreprise. Et inversement, après import des contacts de travail sur son smartphone, celui-ci sera utilisé sur un réseau social.

Ce mélange des genres peut logiquement favoriser des fuites d'information. Le smartphone représente donc une brèche supplémentaire dans la sécurité de l'entreprise. Il peut être vecteur de virus, (par exemple des virus cachés dans des jeux) et il est facile à voler ou égarer. S'il contient des données considérées comme sensibles par l'entreprise, cela peut s'avérer très problématique. Ne parlons pas des autres tracas qui peuvent se poser suite au jailbreaking (déverrouillage de l'OS) de l'appareil.

Quelles solutions pour l'entreprise ?

Comme nous venons de l'observer, le smartphone est devenu une composante inhérente du SI, source de nombreux risques qu'il faut pouvoir limiter. Il faut donc penser, tout comme pour un ordinateur portable, à y intégrer les politiques de sécurité de l'entreprise..s'il y'en a…

En effet, malgré le risque que soulève l'utilisation de smartphones en entreprise, SyBase nous apprend dans l'une de ses études que 2/3 des entreprises ne savent pas précisément quels types de données sont stockées sur ces terminaux, 40% ne connaissent pas la nature des applications installées, et plus préoccupant encore, 15% seulement estiment être protégées contre le vol ou la perte de ces mobiles (en utilisant des solutions de remote-wipe/lock).

Fort heureusement, il existe des outils permettant d'optimiser les fonctionnalités et la sécurité des communications mobiles, tout en réduisant les coûts et le downtime.

Il s'agit du MDM pour Mobile Device Management. Cette notion et les outils qui lui sont associés permettent de sécuriser, monitorer, gérer et supporter les terminaux déployés dans une entreprise.

Les principales fonctionnalités que doit offrir un outil MDM sont :

- FOTA – Firmware Over The Air : pour mettre a jour instantanément le logiciel interne du smartphone.
- Monitoring: analyse des dysfonctionnements.
- Prise de contrôle à distance: pour le support
- Gestion d'inventaire: dénombrement, terminaux actifs, cassés…
- Securité
- Backup/Restore: Essentiel pour réduire le TCO. Il doit être possible de restaurer un appareil lors d'un problème majeur.
- Blocage et effacement à distance.
- Software Installation (OTA). Performance & Diagnostics: information sur la "vie" de votre terminal, telle que la batterie, les informations réseaux…
- Gestion du Roaming : pour bloquer l'installation d'applications sur des terminaux se trouvant hors d'un territoire géographique donné.

Parmi les solutions MDM que l'on trouve sur le marché, on distingue deux types d'offres :

- Les offres ne supportant qu'un seul type d'OS mobile. Par exemple RIM avec BlackBerry Enterprise Server, ou encore Microsoft avec son System Center MDM 2008.
- Quant au second type d'offre, il prend en charge l'ensemble des principaux d'OS, tel que iOS4, Windows Mobile, Palm OS, Symbian, Android.

Le tableau comparatif des principales offres du marché

	OS supportés	Inventaire, provisioning, monitoring et prise de contrôle à distance	Tunneling applicatif AES 256bits
Good Technologies / GFE	iPhone OS 4, Android 2.2, Windows Mobile 6.5, Palm OS et Symbian v3	Inventaire, provisioning et monitoring	AES 192bits
Microsoft / SCMDM 2008	Windows Mobile 6.1	Ok	Ok
RIM / Enterprise BlackBerry Server et Express	BlackBerry OS 5	Ok (Enterprise BlackBerry Server)	Ok
SAP-Sybase / iAnywhere Afaria	BlackBerry OS 5, iPhone OS 4, Android 2.2, Windows Mobile 6.5, Palm OS et Symbian v3	Ok	Ok
Sparus Software / EveryWAN Mobile Manager	iPhone OS 4, Android 2.2 et Windows Mobile 6.5	Ok	Ok (Advanced Edition)

Source : JDN Solutions

Source : http://www.journaldunet.com/solutions/systemes-reseaux/gestion-de-flottes-de-smartphones-panorama/les-solutions-au-crible.shtml

Notons que les solutions MDM ne s'adressent plus uniquement aux grands comptes, mais s'ouvrent aussi progressivement aux TPE / PME qui peuvent posséder des flottes réduites composées de quelques dizaines d'appareils.

Du coté de l'iPhone

Apple, avec la sortie de son iOS 4.0, vise clairement le marché des entreprises.

Pour se faire, Apple a opté pour une stratégie d'ouverture de certaines de ses API à des éditeurs tiers comme MobileIron (Entreprise américaine proposant une solution pour gérer des flottes de smartphones) dont le vice-président a affirmé récemment : « iOS 4.0 augmente la valeur des plateformes de gestion comme MobileIron car nous pouvons à présent prendre en charge des API supplémentaires (comprendre celles de l'iPhone)" .

Conscients de l'énorme potentiel de l'iPhone en entreprise, gageons que les éditeurs proposant des solutions de MDM orientées vers ce smartphone vont monter en puissance dans les mois qui viennent, en attendant qu'Apple propose ses propres outils : cette hypothèse est plus que probable sur le moyen terme.

CONCLUSION :
La récente et soudaine irruption des smartphones en entreprise offre de nouveaux challenges à la DSI et par ricochet à l'ensemble de l'entreprise : le sujet est relativement complexe et pose des problèmes de sécurité qui ne peuvent plus être négligés.
Plutôt que d'occulter cette problématique, des outils et des process existent pour gérer efficacement des déploiements de smartphones. Encore faut-il en avoir une connaissance approfondie et savoir les paramétrer en bonne intelligence.
Une entreprise pourra donc avoir tout intérêt à faire appel à une société spécialiste du sujet afin d'auditer son parc de smartphones, de décider des règles à mettre en place et des outils à déployer. C'est le métier d'iSeeds. N'hésitez pas à prendre contact avec nous si vous êtes impliqué dans un projet de cette nature.

DOCUMENT 13

Avantages et inconvénients du MDM face au MAM

http://iseeds.fr

Comment faire face au phénomène BYOD ?

Les DSI sont à la croisée des chemins. D'un côté, ils connaissent le modèle classique, celui du Mobile Device Management (MDM). De l'autre, ils sont confrontés à l'émergence progressive du Mobile Application Management (MAM), notamment à cause du développement de la tendance à amener son équipement numérique au travail (Bring Your Own Device ou BYOD) et à télécharger des applications sur les différents stores existants.

Cette seconde tendance semble inéluctable : c'est le sens de l'histoire. Les utilisateurs ont pris le pouvoir : ils ont inventé leurs modes de production et de consommation de l'information. Et ils maîtrisent leurs outils numériques qui, rappelons-le, ont souvent la puissance d'un ordinateur d'il y a seulement 4 ans. Pour les DSI, le défi technique et organisationnel est de tirer le meilleur parti de toutes ces évolutions et des changements de comportement !

Quels sont les avantages du Mobile Application Management et du BYOD ?

Le BYOD est une ressource mise à la disposition de l'entreprise. En laissant ainsi le choix à l'employé, on augmente son autonomie, son efficacité au travail et in fine sa motivation à communiquer avec des outils numériques. Ce modèle, de plus en plus plébiscité par les collaborateurs, a tendance à perturber les DSI. Or, l'expérience montre qu'il est créateur de valeur à condition d'être bien piloté. De plus, il permet de réduire les coûts de mise à disposition des terminaux ainsi que les coûts de support pour l'entreprise.

Le modèle MAM (User Centrics) s'appuie résolument sur ce constat : il considère l'utilisateur comme actif, en recherche constante des informations et des solutions qui lui permettent d'améliorer sa productivité. Cette approche est évidemment centrée sur l'utilisateur et s'oppose au modèle antérieur du MDM (Enterprise Centrics), dans lequel la DSI décide de tout, imposant équipements et logiciels. Bien au contraire, le modèle MAM se place au service des utilisateurs et installe la DSI dans une relation client-fournisseur.

Suivant ces modèles, la DSI devrait donc se remettre en cause. Par où commencer ?

La bonne attitude consiste à sortir du cadre habituel, presque «culturel» des DSI, pour adopter une approche d'écoute. L'entreprise ayant fait ses grands investissements en ERP et CRM, par exemple, comment en tirer parti, surtout en mobilité ? Comment créer de la valeur au niveau de l'interfaçage avec les grands outils de l'entreprise ? Quid des problèmes de sécurité ? Comment redéfinir les chartes informatiques en fonction de ce nouveau mode de consommation des données de l'entreprise ?

Pour capter les vrais besoins et les attentes des utilisateurs – considérés comme des clients -, il est recommandé de constituer des groupes. On adopte ainsi la position d'un éditeur de logiciel qui met en place une dynamique d'innovation participative à la recherche de nouveaux usages.

Il faut ensuite concentrer son analyse sur l'interface utilisateur, en s'appuyant éventuellement sur les méthodes du Business Process Management ou BPM, et en gardant à l'esprit que l'utilisateur n'exploite généralement qu'à 5% les outils dont il dispose. A un instant donné, surtout en mobilité, il veut obtenir vite l'information qui lui est nécessaire, et pas plus ! Un bon interfaçage permet de répondre à ce besoin, en mettant l'info à disposition, généralement grâce à une appli métier bien conçue et donc simple.

Comment conduire l'étude des besoins et les développements nécessaires ?

Il convient d'être réaliste et de constater que, dans beaucoup d'entreprises, les utilisateurs ont court-circuité le SI de l'entreprise et se sont fabriqués leurs outils. Combien de vos utilisateurs se sont fait des classeurs Excel dans lesquels ils placent les infos qui leur sont effectivement utiles ? Combien ont-ils déjà téléchargé des applications sur leurs propres smartphones sur lesquelles transitent les informations de l'entreprise (par exemple sur dropbox) ? L'entreprise a t-elle vraiment créé une base de données ou d'expertise que chacun exploite et contribue à remplir chaque jour de manière naturelle? Les données clés de l'entreprise sont-elles réellement à jour ? N'a t-on pas créé une forme de big data non maîtrisé à l'intérieur de l'entreprise ?

Pour développer des applis métier rentables, il vaut mieux investir sur les groupes, aller vers les métiers, comprendre leurs objectifs à un instant T. Il semble aussi préférable d'externaliser les développements. Ceci apporte de l'agilité au projet de construction progressive du bouquet d'applications ou de l'app store de l'entreprise. On se donne des objectifs limités qui répondent à une attente identifiée des utilisateurs (une-appli-qui-fait-juste-ça).

L'expérience montre en effet qu'il vaut mieux faire simple, quitte à apporter des compléments quelques mois plus tard. Avec cette approche, on se donne aussi les moyens de mesurer avec précision le ROI.

Quelles sont les options pour déployer un app store dans l'entreprise ?

L'approche des éditeurs de solutions MDM semble aujourd'hui très limitative. Elle a tendance à être liée au terminal, se montre assez complexe et pas suffisamment adaptable. On reste dans une logique de contrôle de l'utilisateur et de son terminal. Selon nous ce n'est plus le sens de l'histoire !

En ce qui nous concerne nous avons été attirés par une autre approche, née aux Etats-Unis avec une pure logique MAM, et développée par APPERIAN : leur solution EASE, que nous avons choisi de distribuer, est vraiment centrée sur l'utilisateur et sur sa productivité. Elle est simple à mettre en oeuvre (cloud), s'appuie sur les LDAP et l'architecture de l'entreprise, et permet le téléchargement des applications par les collaborateurs sur les OS principaux (iOS, Androïd ou Windows).

Nous avons déjà des premiers clients qui nous sollicitent sur cette nouvelle approche et nous pensons que ce n'est que le début des stores d'entreprise.