Les synthèses du CLUSIF

Consumérisation de l'IT (BYOD) et la sécurité de l'information

Synthèse de la conférence thématique du CLUSIF du 3 mai 2012 à Paris

Le nouveau Président du CLUSIF, Lazaro Pejsachowicz ouvre la conférence en annonçant le nombre important d'intervenants lié à la complexité du sujet. Le BYOD (« Bring Your Own Device », littéralement « Apportez votre propre matériel ») prend de l'ampleur. De plus en plus de salariés apportent leurs équipements personnels au travail (smartphone, tablettes, PC etc). La question se pose pour les DSI de savoir comment exercer un contrôle sur ces appareils personnels puisqu'elles restent responsables de la sécurité du réseau de leur entreprise.

Chadi Hantouche, Solucom

Chadi Hantouche aborde le BYOD sous l'angle des risques et des solutions de sécurisation.

Devenu « buzzword » aujourd'hui la notion de BYOD existe pourtant depuis un moment. Au XXe siècle aux Etats Unis, on parle de BYOB (*Bring your own bottle*), l'idée étant d'apporter sa propre bouteille à une soirée par exemple. Dans le monde de l'IT, c'est Apple qui en 2005 accompagne la vente de son Mac mini d'un « BYODKM » (*Bring your own display, keyboard and mouse*). Apple vendait le boitier central et il fallait ajouter son écran, sa souris et son clavier. En 2006 enfin, BP ne fournit plus de poste de travail à ses collaborateurs et appelle ce projet « DIY IT » (*faites-le vous mêmes*). Entre juillet 2011 et avril 2012 le nombre de requêtes « BYOD » sur Google a doublé.

Trois grandes catégories de risque cohabitent :

- des risques pour les données professionnelles ou personnelles,
- des risques pour le système d'information de l'entreprise,
- des risques organisationnels, juridiques et réglementaires.

Ces risques se situent sur les terminaux, sur les liens entre les terminaux et le SI de l'entreprise (réseaux opérateurs et internet) et sur le SI lui-même. Ils doivent absolument être traités dans leur ensemble.

Les risques techniques ne sont pas des risques nouveaux, liés au BYOD en lui-même. Mais le fait que ces risques touchent des équipements qui sont la propriété du salarié, peut en modifier les types d'impacts.

Par exemple, un cas typique de problème lié au BYOD : celui d'un employé dont le terminal personnel est effacé entièrement parce qu'un administrateur de l'entreprise a fait une erreur de manipulation.

Pour protéger les données du SI, l'entreprise peut mettre en place des mesures de sécurité classiques : code PIN, chiffrement, versions d'OS autorisées etc.). Mais quand les postes de travail sont personnels, trop de contraintes dégradent l'ergonomie et exposent à un rejet de la part des utilisateurs. Ils peuvent craindre notamment une intrusion dans leur vie privée (géolocalisation etc.) et une limitation des usages de leur terminal.

Des solutions techniques sont disponibles et efficaces :

- Si possible, ne rien stocker sur les terminaux personnels, en utilisant le déport d'écran et les applications webisées (publier les applications en mode web).
- Sinon, sécuriser les postes de travail en se basant sur deux grandes méthodes de sécurisation :
  - ✓ le silo applicatif : le terminal est personnel mais l'entreprise y inclue une « bulle » professionnelle sécurisée et sur laquelle l'entreprise garde le contrôle. L'utilisateur étant libre par ailleurs de faire l'usage qu'il veut de son terminal.
  - ✓ La gestion de flotte : l'entreprise garde la main sur ses terminaux et les mesures de sécurité qu'elle y applique.

Actuellement, le déport d'affichage est plutôt réservé aux PC. Cette solution montre ses limites pour les terminaux plus petits et plus mobiles qui acceptent mieux les solutions de type silo applicatif.

La connexion des terminaux personnels doit également être prise en compte. Les terminaux mobiles par exemple n'ont pas forcément d'autres connexions que celles du wifi de l'entreprise. Certaines fonctionnalités de contrôle sur le réseau existent. En revanche leur mise en place nécessite un investissement dont il faut évaluer l'intérêt.

Mais au delà des aspects techniques, les vrais enjeux du BYOD sont organisationnels. Un encadrement s'impose :

- Sur les problématiques d'organisation du travail. Si un service est ouvert aux terminaux personnels des collaborateurs, certains vont l'utiliser et seront plus réactifs (par exemple en répondant à leurs mails plus rapidement que ceux qui ne l'utilisent pas). Cette discrimination éventuelle pose des problèmes de management.
- Sur les questions relatives à la traçabilité et au respect de la vie privée.
- Sur la fonction d'administrateur. Ce dernier peut-il par exemple accéder aux données personnelles ou effacer le contenu d'un terminal personnel ?
- Sur les usages. Quelle est la responsabilité de l'entreprise face à un accident ou le vol d'un terminal personnel utilisé à des fins professionnelles ?

Les DSI sont obligées de repenser leurs fondamentaux face aux utilisateurs. Alors qu'elles disposaient de postes de travail dont elles pouvaient restreindre les usages à leur gré, dans un mode BYOD leur travail de configuration laisse place à plus de responsabilisation de l'utilisateur.

Afin de lancer et sécuriser un environnement BYOD, un certain nombre d'étapes s'imposent :

- Commencer par les besoins les plus évidents en se basant sur des solutions techniques mûres et en lançant des POC de solutions innovantes. Des tests sont nécessaires dans son environnement propre afin d'adapter la démarche BYOD à la culture de l'entreprise : tout n'est pas applicable partout.
- Définir la cible, les usages, les terminaux concernés et le niveau de service offert.
- Ne pas négliger les aspects non-techniques. Définir des règles d'utilisation en collaboration avec les services RH et juridiques.
- S'assurer que les aspects réglementaires sont respectés (vis à vis des instances représentatives du personnel, de la CNIL etc.)

En conclusion, Chadi Hantouche se veut provocateur : « BYOD, l'avenir de la DSI ? ». Pas nécessairement selon lui, mais les DSI ne peuvent ignorer ce mouvement et doivent l'accompagner. L'interdiction n'est plus possible. Les DSI sont par ailleurs sensibles à la réduction des coûts liée au BYOD, bien qu'elle ne soit pas encore confirmée dans la durée.

La consumérisation, de son côté, est un phénomène qui va se poursuivre et entraîner une accélération de la fusion des sphères personnelles et professionnelles. De nouveaux usages apparaissent déjà : BYO Apps ou BYO Identity.

Loup Gronier, Devoteam,

Loup Gronier montre comment le BYOD va probablement passer d'un geste volontaire vers une le financement du matériel du salarié.

Le nouvel engouement pour le BYOD s'explique par :

- Un cycle permanent de nouveautés, qui entraîne une qualité d'équipements chez les particuliers, supérieure à celle qu'ils trouvent dans leur entreprise.
- Une génération Y qui cherche à rester en communication permanente.
- Un prix de ces nouveaux « devices » en baisse.
- Des budgets IT en diminution.
- La demande aux sous-traitants d'apporter leur propre matériel.

Le BYOD est souvent associé aux tablettes et aux smartphones. Pourtant, les premiers exemples de BYOD ont essentiellement concerné les PC et en particulier les Macintosh.

Les PC mais aussi les devices « annexes » (disques durs, cartes avec du réseau etc.) sont apportés dans l'entreprise par les particuliers. Une vision globale de la sécurité impose d'en tenir compte.

Avant 2010, la plupart des chartes informatiques prohibaient l'utilisation de « devices » personnels et très peu de requêtes sur Google concernaient « BYOD ».

Ce sujet est aujourd'hui d'actualité. Les autorisations d'usage de ces équipements, accordées par les équipes de sécurité, concernent encore souvent des populations ciblées (VIP, génération Y, IT etc.). Le BYOD est une démarche poussée par l'envie : envie d'utiliser son propre matériel plus récent, plus à la mode.

A l'horizon 2015, un nouveau BYOD pourrait voir le jour : « buy » (achetez) your own device. A l'envie succéderait l'obligation imposée par les directions financières pour des raisons de coûts. Ces derniers profitant de l'existence de la démarche pour donner une enveloppe aux employés et exiger qu'ils utilisent leur propre terminal dans l'entreprise. Ce BYOD, qui existait déjà pour la téléphonie, commence à apparaître à l'initiative de certaines directions financières.

La population visée concerne à ce jour une minorité de personnes dans la structure mais pourrait, à terme, concerner l'ensemble des collaborateurs. Or, si la population VIP et la génération Y peuvent se trouver dans une logique « d'envie » il est à craindre que d'autres populations vivent cette évolution plus difficilement.

Le principe consiste à allouer une enveloppe à un utilisateur qui doit alors apporter son terminal et l'entretenir. Même le support n'est plus dans l'entreprise.

L'analyse des risques d'une approche BYOD (qu'elle soit « bring » ou « buy ») impose d'étudier :

- Les populations qui sont ciblées (VIP, génération Y, ou une population large).
- Les équipements concernés (smartphone, tablette, PC etc.).
- Le type d'usage prévu (de la téléphonie jusqu'aux applications critiques de l'entreprise).
- Les informations mises à disposition (intranet, applications métier ou données critiques).

Les risques liés au BYOD sont :

- Les fuites d'information : ce risque existe déjà au sein des systèmes d'information avec par exemple la messagerie mais le BYOD augmente la surface d'attaque et le nombre de possibilités pour sortir de l'information.
- La réversibilité et la perte d'information (comment sont sauvegardées les données et comment les récupérer en cas de conflit avec le collaborateur ou sa famille).
- Les attaques, les infections, les intrusions (comment garantir l'innocuité des terminaux pour le SI de l'entreprise).

Il existe en revanche un sujet sur lequel « Bring » et « Buy » se différencient : grâce au nombre important de terminaux personnels à protéger qu'il va générer, le développement du BuyYOD, permettra sans doute de faire les investissements nécessaires pour protéger toutes les applications. Le BringYOD étant souvent trop anecdotique pour que toute

l'attention nécessaire y soit portée en terme de sécurité.

L'augmentation des risques liés au BYOD concerne également :

- Les aspects juridiques (à qui appartiennent les données, peut-on formater à distance un équipement personnel en cas de vol etc.).
- Les aspects RH (responsabilité d'un employé qui n'apporterait pas son terminal etc.).
- Les problèmes liés à l'IT (compatibilités des systèmes etc.).

En conclusion, le « Buy your own device » est inéluctable si l'on résout les dimensions RH et juridique. Il suivra le « Bring your own device » qui existe déjà dans toutes les entreprises. Les directeurs financiers pourraient accélérer sa mise en place avant l'horizon 2015. Chaque type de BYOD présente des risques spécifiques qui devront être traités différemment. **la SSI ne pourra pas interdire mais se devra d'accompagner voir d'anticiper ce changement comme elle accompagne l'externalisation, le cloud…**

Garance Mathias, avocate

Garance Mathias aborde les aspects RH et juridiques du BYOD.

Non seulement les individus apportent leur matériel sur leur lieu de travail mais en plus ils entretiennent avec lui un lien émotionnel.

En réalité les individus ont toujours apporté du matériel personnel au travail. Et pourtant aucune jurisprudence ne concerne encore l'enjeu spécifique du BYOD.

Or cette tendance se développe et doit être appréhendée par le Droit et par les RH. Les questions soulevées étant par exemple :

- L' « hyper-connectivité » comme facteur de stress pour le salarié. Pour cette raison il est déjà question de la mise en place au sein des institutions représentatives du personnel de cellules dédiées à la mise en place du BYOD. Plus particulièrement dans les entreprises qui ont plus de 50 salariés et qui ont un CHST.
- La discrimination : pourquoi autoriser par exemple une équipe IT à venir avec son propre matériel et le refuser à un autre service.

L'aspect juridique et RH doit être clairement défini et soulève de nombreuses questions, par exemple :

- L'entreprise peut-elle maîtriser le terminal personnel de l'utilisateur (le tracer, récupérer certaines données etc.)?
- Le salarié peut-il conserver les données de l'entreprise ?
- Qu'en est-il de la perte ou du vol de la partie matérielle et immatérielle ?
- Comment gérer les dommages causés par un bien personnel sur le système d'information de l'entreprise, les autres salariés, etc ?

Le Droit prévoit que l'employeur est responsable à l'égard des tiers pour les actes commis par son salarié « quand celui-ci agit sans excéder les limites de la mission qui lui a été impartie ». Concrètement cela signifie que, en cas de vol par exemple, l'employeur sera présumé responsable de la disparition du bien (il pourra cependant atténuer sa responsabilité en prouvant la faute du salarié).

Par ailleurs, en contre partie de la mission exécutée par le salarié, le Droit prévoit que l'employeur doit mettre à sa disposition tous les moyens pour lui permettre d'exécuter cette mission. Si l'employé vient avec son propre matériel une faille pourrait être relevée dans le respect du contrat de travail.

Plusieurs autres questions se posent :

- Si l'employé vient avec son matériel personnel sur le lieu de travail, doit-il demander une autorisation de l'employeur pour pouvoir se connecter ?
- L'employeur doit-il et peut-il demander à l'employé s'il est à jour de ses licences ? Et s'il n'a pas téléchargé des films ou des applications interdites (Hadopi, droits d'auteur de manière générale) ?
- L'employeur peut-il accéder au matériel personnel du salarié ? Peut-il lire les données ? Comment peut-il différencier les données personnelles et professionnelles ? La cour de cassation

autorise l'accès par l'employeur aux données présentes sur le poste de travail. Mais cette jurisprudence peut-elle être transposée en l'état lorsque les biens sont la propriété exclusive du salarié ?

Pour répondre à ces nombreuses questions les réflexions devront se faire en concertation avec les institutions représentatives du personnel. Elles porteront sur :

- les moyens utilisés,
- leur emploi,
- la démarche volontaire de l'entreprise (est-ce l'entreprise qui va donner une somme pour acheter les biens),
- la qualification ou non de ce matériel en « avantage en nature » (parallèle avec les voitures de fonction),
- l'obligation ou non de rendre le matériel financé en cas de départ de l'entreprise, etc.

Une autre question concerne la durée légale du temps de travail face à des individus connectés en permanence avec leur entreprise. L' «hyper-connexion » ne correspondant pas à la définition légale du télétravail.

L'accompagnement juridique et RH du BYOD est donc nécessaire et passe par la modification des chartes. Celle-ci s'accompagne automatiquement de la modification du contrat de travail pour les nouveaux salariés. La charte doit prévoir :

- les règles relatives à la sécurité du système d'information,
- les règles concernant la consultation de sites internet ou de réseaux sociaux dans le cadre professionnel,
- les règles de respect de la propriété intellectuelle,
- les modalités de contrôle et de sanction. Etc.

Le contrat de travail et la charte informatique peuvent permettre d'anticiper les litiges liés au BYOD. Enfin, la charte doit être intégrée au règlement intérieur afin de devenir un instrument disciplinaire le cas échéant.

Comme toutes les évolutions sociétales, le BYOD a des conséquences juridiques et RH. Si l'entreprise s'est toujours adaptée, le salarié, lui, a aussi toujours réfléchi et agi en son âme et conscience.

Pascal Sauliere, Microsoft France

Pascal Sauliere présente une réflexion sur la mise en œuvre de BYOD, entamée depuis un an chez Microsoft France pour répondre aux interrogations de ses clients. Il concentre son exposé sur les pistes technologiques.

Les DSI font face à des défis importants et doivent adapter leurs infrastructures à ce nouveau phénomène. D'une manière générale, les DSI savent que le BYOD est inévitable et l'idée n'est pas de le rejeter mais de s'y adapter le mieux possible.

L'approche de Microsoft France est basée sur deux piliers :

- Un pilier axé sur le terminal. Il concerne les risques liés au Jailbreak, au rooting, à la multiplication des OS, au mélange des données privées à celles de l'entreprise etc.
- Un pilier axé sur la protection de l'infrastructure et des applications. Y apparaissent les scénarios mis en œuvre par Microsoft, par exemple :
  - ✓ Comment permettre à un « device » personnel (un Ipad par exemple) de se connecter au réseau d'entreprise (ces appareils étant plutôt des appareils wifi que des appareils qui se branchent sur le câble) ?
  - ✓ Comment autoriser à certains terminaux l'accès à certaines données sensibles, en fonction de leur niveau de confiance ?
  - ✓ Comment classifier ces données sensibles ?
  - ✓ Quelles protections contre les fuites d'information ? Etc.

I. Concernant la sécurité du terminal, Microsoft a développé un protocole de management des terminaux mobiles : Exchange ActiveSync (EAS). Implémenté sur la plupart des fournisseurs de périphériques mobiles, IOS, Android, Windows Phone, WebOS (mais pas Blackberry), il permet l'accès à la messagerie, au calendrier, aux

contacts etc. mais aussi l'installation de systèmes de sécurité sur les appareils.

C'est une piste de solution basique mais utile pour « imposer » une politique de sécurité sur les appareils.

Cependant le constat est le suivant : les politiques de sécurité ne sont pas implémentées de manière homogène sur les périphériques. Pour aller plus loin dans la gestion spécifique des périphériques hétérogènes l'investissement dans des solutions « Mobile Device Management » (MDM) est indispensable.

Pour les risques de mélanges des données privées et professionnelles, les solutions apportées sont le chiffrement de messageries ou de documents ainsi que des solutions en silo.

Enfin, les marketplaces privées peuvent répondre aux risques de sécurité des applications du marketplace.

Les tests de mise en œuvre de ces solutions ont été réalisés avec un Ipad, une tablette Android, un Windows Phone etc.

II. Concernant l'infrastructure et les applications :

- La solution 802.1x permet de contrôler l'accès au réseau wifi de l'entreprise.
- La classification des données permet de déterminer leur niveau de sensibilité.
- IPSec permet la protection des données sensibles.
- La Gestion des Droits Numériques RMS (Rights Management Services) protège la fuite d'information en permettant de faire suivre avec le document lui-même, son mode d'utilisation, ses licences d'utilisation et ses autorisations.
- Les solutions d'accès à distance comme Activsync permettent à un périphérique portable d'être synchronisé à un ordinateur de bureau.
- Les passerelles (comme UAG) peuvent gérer les droits de connexion d'un device externe à une application interne. En fonction du type de device et en fonction de l'application.

Les produits Windows incluent déjà des fonctionnalités dédiées au BYOD. Mais les produits Windows 8 et Windows Server 2012 qui sortiront cette année proposent des solutions nouvelles, notamment pour les tablettes. Par exemple, Windows To Go est une solution très simple de boot sur Windows placé sur une clé USB. Elle permet à l'entreprise de distribuer à ses employés une clé USB qui contient Windows 8. Ces derniers peuvent alors démarrer leur environnement Windows à partir de n'importe quel PC.

Par ailleurs, Windows 8 intègrera Hyper-V. Ces deux solutions, Windows To Go et la virtualisation permettent d'avoir :

- soit un environnement totalement géré et isolé de l'environnement personnel,
- soit un environnement qui cohabite avec l'environnement personnel, qui est un peu moins isolé mais qui reste géré.

Le deuxième cas, le client de virtualisation permettant si on n'est pas passé à windows 8 de déployer des images windows 7, windows XP etc.

D'autres solutions vont voir le jour prochainement avec les tablettes Windows 8 ARM.

Questions et Réponses avec l'assistance.

Cette conférence comportait également un débat avec la salle, non retranscrit dans ce document mais disponible en vidéo à l'adresse suivante : http://www.clusif.fr/fr/production/videos/#video120503.

Retrouvez les vidéos de cette conférence et les supports des interventions sur le web CLUSIF http://www.clusif.fr/fr/infos/event/#conf120503.