ifaci
institut français de l'audit et du contrôle internes

BYOD

Quels risques et enjeux pour l'audit et le contrôle internes ?

Le *Bring Your Own Device* (BYOD)[1] consiste à utiliser des équipements personnels à des fins professionnelles.

Cet usage connaît un succès grandissant avec la démocratisation des terminaux évolués à la portée de tous. Les utilisateurs, cherchant à retrouver le même niveau de souplesse et de confort rencontré dans leur quotidien, peuvent souhaiter utiliser leurs outils personnels pour accéder au Système d'Information (SI) de l'organisation.

Il peut prendre une multitude de formes, par exemple l'usage de smartphones ou de tablettes personnels pour accéder à la messagerie, ou encore l'usage d'ordinateurs personnels comme matériel professionnel. Le BYOD impacte la gouvernance et la sécurité du SI ainsi que le modèle de sécurité de l'organisation. Cette pratique amène les organisations à envisager autrement leur système d'information. Il en découle des risques et des opportunités que les auditeurs et contrôleurs internes doivent appréhender et évaluer.

[1] *Apportez Vos Outils Personnels (AVOP)*

1- En quoi consiste le BYOD ou « consumérisation »[2] ?

Le *Bring Your Own Device* est un phénomène récent résultant de l'utilisation de dispositifs de communication personnels pour effectuer des tâches professionnelles. Avant le BYOD, les organisations fournissaient des smartphones, des ordinateurs portables, et, plus récemment, des tablettes à certains de leurs collaborateurs. Ces appareils mobiles étaient la propriété de l'organisation et donnaient généralement accès au système d'information par l'intermédiaire d'une interface de gestion rigoureuse souvent spécifique et sécurisée pour le type de terminal proposé aux collaborateurs.

Avec le BYOD, les équipements mobiles personnels variés (smartphones, tablettes tactiles et ordinateurs portables) sont, dans certaines organisations, autorisés à accéder aux systèmes d'information de l'organisation. Les collaborateurs apprécient cette flexibilité et la possibilité de combiner leurs équipements privés aux équipements nécessaires à leur vie professionnelle.

La réduction des coûts liée aux économies réalisées par l'achat des appareils appartenant aux collaborateurs n'est pas le seul avantage. En effet, l'accès immédiat et en toutes circonstances au SI grâce au BYOD améliore notamment **la réactivité** et **la productivité** des collaborateurs.

La notion de BYOD est limitée à l'utilisation de terminaux personnels. Néanmoins, l'on observe également les usages suivants :

- Le BYOA « *Bring Your Own Application* » : utilisation d'applications grand public. La percée du modèle SaaS *(Software as a Service)* a fortement contribué au développement de ce genre de pratique. Ces applications ont leur utilité dans la vie professionnelle. Elles concernent :
  - les réseaux sociaux (Twitter, Linkedin, Facebook, etc.) ;
  - le stockage et la synchronisation (Skydrive, Gdrive, Box, Hic, Evernote, etc.) ;
  - le travail collaboratif (Skype, Office web apps, GoogleDocs, Azendoo, Prezi, etc.).
- Le BYOS « *Bring Your Own Software* » : utilisation, par le collaborateur, de logiciels n'appartenant pas à l'organisation. Ces logiciels peuvent être des types suivants :
  - Multimédia (I-tunes, Spotify, etc.) ;
  - Partage de documents (Dropbox, GoogleDocs, etc.) ;
  - Logiciels libres à usage professionnel (Dia, R, etc.).
- Le BYOT « *Bring Your Own Technology* » : utilisation d'appareils électroniques tels que des disques durs, des clés USB, etc.

Les entreprises peuvent tirer profit du BYOD en adoptant une stratégie leur permettant de réduire les risques financiers et de sécurité, et le chaos organisationnel.

En outre, une nouvelle tendance pour allier les avantages du BYOD en évitant certains de ses inconvénients consiste en la solution du COPE *(Corporate Owned, Personally Enabled)*. Dans cette approche, l'organisation fournit elle-même les terminaux et accepte leur utilisation à titre personnel. Cette solution s'apparente plus au modèle classique de gestion des terminaux avec une liste de matériels définie et validée par la DSI, ce qui permet d'avoir un contrôle sur la flotte des terminaux mobiles, tout en laissant au salarié

[2] *La « consumérisation » est la tendance croissante selon laquelle les utilisateurs professionnels choisissent les périphériques, les applications et les services pour leur travail.*

la possibilité de faire son choix. Ceci limite les problèmes juridiques, notamment liés à la vie privée et réduit également les risques liés à la sécurité.

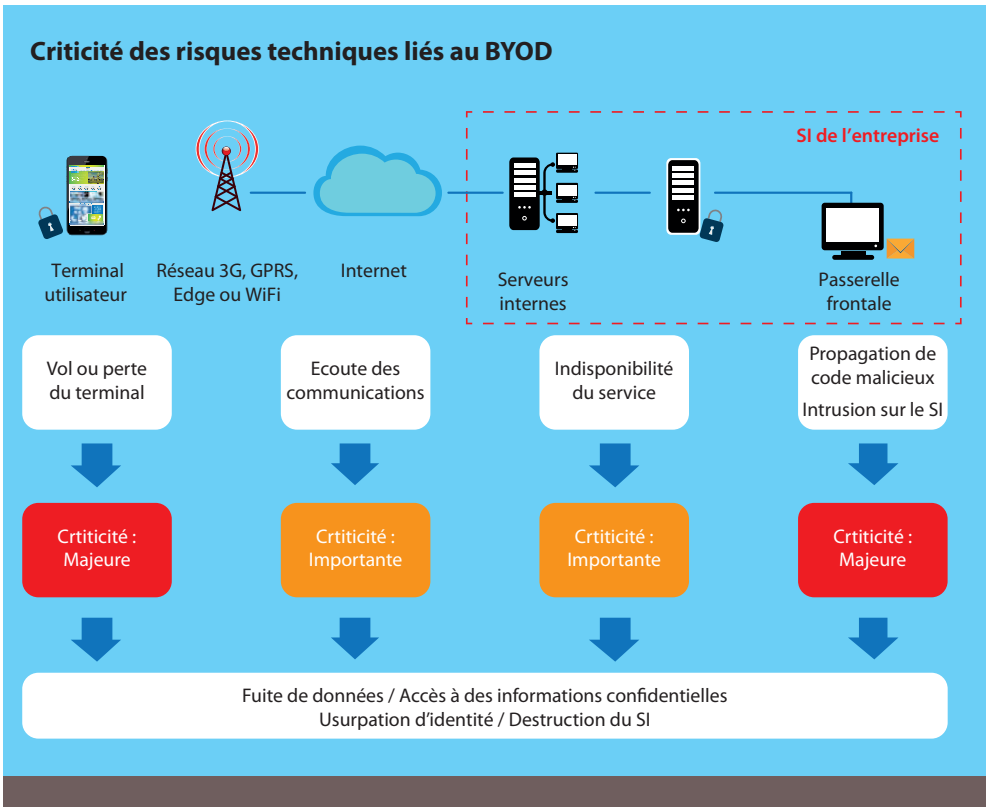
Les DSI et les managers sont donc confrontés aux enjeux et à la maîtrise des risques liés au BYOD. Compte tenu des attentes des salariés, il ne s'agit plus de juguler cette pratique, mais il convient de l'encadrer dans le cadre d'un projet BYOD structuré en ayant correctement identifié les risques et opportunités de ces nouveaux usages.

2- Quels sont les risques liés à la mise en place du BYOD ?

Le BYOD implique des risques de sécurité auxquels l'organisation doit faire face. L'enjeu est de maintenir la sécurité et la confidentialité des données sur des dispositifs qu'elle ne possède pas et qu'elle ne contrôle que très partiellement.
Les risques liés au BYOD sont de nature technique et opérationnelle.

Les risques techniques de sécurité sont similaires à ceux de l'informatique mobile, notamment :

- la fuite de données sensibles et l'impact sur la propriété intellectuelle ;
- la perte de données de l'organisation à partir d'appareils appartenant aux collaborateurs lors de la cessation de l'emploi ou encore lors de la perte ou du vol du terminal ;
- l'indisponibilité du système d'information par contamination du BYOD (propagation de malware) ;
- l'usurpation d'identité par une utilisation malveillante du terminal (intrusion).



Ces risques techniques sont généralement dus :

- au manque de sécurisation des terminaux personnels des collaborateurs et au manque de contrôle d'accès sur les appareils mobiles personnels ;
- à l'accès injustifié depuis ces terminaux à des applications critiques de l'organisation ;
- à l'incapacité technique et organisationnelle à maintenir l'ensemble des postes ;
- à l'augmentation de la surface d'attaque et d'intrusion ;
- au manque de sauvegarde des dispositifs de BYOD appartenant aux collaborateurs.

Le BYOD comporte également des **risques plus opérationnels**. Bien que régulièrement oubliés, ces risques peuvent tout autant affecter la productivité et la réputation de l'organisation :

- Risques de non-conformité réglementaire et juridique :
  - Non déclaration à la CNIL ;
  - Supervision par l'organisation des communications (emails, navigation sur Internet) professionnelles voire personnelles ;
  - Problématique de conservation des fichiers des traces de connexion au SI ;
  - Engagement de la responsabilité de l'organisation versus responsabilité personnelle du salarié.
- Risques liés aux ressources humaines, notamment l'impact sur les fiches de poste et le temps de travail ;
- Risques liés à l'atteinte à la vie privée des salariés (les données personnelles étant mélangées avec les données professionnelles) et l'impact sur le « poste de travail » du salarié et le temps de travail (en lien avec les problématiques suivies par le Comité d'Hygiène, de Sécurité et des Conditions de Travail - CHSCT) ;
- Risques liés aux licences (piratage, utilisation de licences privées dans le domaine professionnel) ;
- Propriété et usage des données ;
- Risques liés à la maitrise des coûts (cf. encart p.11).

Quelques chiffres liés à l'évolution du BYOD :

- **30 %** des salariés consultent, stockent, transmettent ou modifient des documents professionnels sur leur mobile ou leur tablette personnels.
- **30 %** des sondés se disent décidés à quitter leur société s'ils ne peuvent utiliser leur mobile ou leur tablette personnels pour travailler.
- **32 %** des salariés sont prêts à contourner la DSI pour utiliser leur mobile ou leur tablette personnels.
- **49 %** des organisations sondées déclarent avoir subi des pertes (vol ou oubli) de terminaux mobiles contenant des données professionnelles en 2012.
- **60 %** de leurs terminaux mobiles ont subi des incidents de sécurité durant la même année.

Source : Vanson Bourne 2012, UBM 2013

Zoom sur quelques risques juridiques

Outre les risques techniques liés à la sécurité dans le cadre de la mise en place du BYOD, il convient d'être attentif aux risques juridiques. Ainsi, la perte ou l'altération de données à caractère personnel dans le cadre de l'utilisation du BYOD, peut provoquer des dommages économiques non négligeables pour l'entreprise mais également engager sa responsabilité.

A ce titre, l'article 34 de la Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dispose notamment que *« le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès ».*

Par ailleurs, la mise en œuvre de mesures techniques et organisationnelles afin d'assurer la protection des données à caractère personnel est prévue par l'article 226-17 du Code pénal selon lequel : *« Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans de prison et de 300 000 euros d'amende ».*

De fait, les tribunaux sanctionnent la divulgation d'informations couvertes par le secret professionnel. Ex : TGI Versailles 18/12/2007, affaire Valéo : Condamnation d'une stagiaire chinoise qui a copié sur son disque dur des fichiers confidentiels de la société Valéo (condamnée pour abus de confiance à un an de prison, dont 2 mois ferme, et 7 000 euros d'amende).

Il peut être utile de s'interroger sur les dispositions de La loi Warsmann du 22 mars 2012 qui inclut dans le code du travail une section intitulée « Télétravail » dont les trois articles, L1222-9 à L1222-11, comportent plusieurs dispositions importantes qui peuvent impacter le BYOD (« forme d'organisation du travail qui se fait dans le cadre d'un contrat de travail ou d'un avenant à celui-ci »).

3- Quels mesures et dispositifs l'organisation peut-elle déployer ?

Au regard des différents risques évoqués, l'organisation se doit de mettre en place des dispositifs de maîtrise des risques, notamment fondés sur un système de sécurité cohérent avec ces nouvelles menaces.

Les entreprises doivent en effet encadrer l'utilisation du BYOD et garder en toutes circonstances le contrôle de l'accès au réseau et des données y étant accessibles.

Il pourrait notamment être utile de prévoir :

- que le salarié soit obligé, préalablement à la connexion de son terminal au réseau de son entreprise, d'avertir le DSI et de faire contrôler son équipement afin de s'assurer de sa conformité en termes de sécurité ;
- que le salarié s'engage à disposer d'un équipement en état de fonctionnement, à télécharger les mises à jour proposées par les éditeurs, etc. ;
- des systèmes de cryptage de données, des outils de sauvegarde journalière, etc.

Seule une analyse de risques propre à chaque organisation permet de déterminer des mesures correspondant au niveau de risque acceptable qu'elle a défini. Cependant, vous trouverez ci-dessous des exemples de bonnes pratiques dans le cadre du déploiement d'un projet de gestion du BYOD.

Exemples de mesures organisationnelles

- Politique et procédures :
  - Définition claire et précise du contexte dans lequel le BYOD peut être appliqué.
  - Mise à jour de la charte d'usage des moyens informatiques en étroite collaboration avec les instances représentatives du personnel.
  - Mise à jour des politiques de sécurité et formalisation d'une politique de sécurité BYOD.
  - Revue de la gestion des problématiques d'identification et d'accès.
- Autorisation de l'augmentation des usages à condition qu'ils soient systématiquement référencés pour mieux les contrôler.
- Ressources et compétences :
  - Développement de compétences pour la sécurité des applications mobiles.
  - Veille accrue sur les nouveaux systèmes d'exploitation (iOS, Android) et sur les risques associés.
  - Formation du support utilisateurs à la remontée et à la gestion des alertes de sécurité pour les équipements personnels.
  - Veille technologique sur les vulnérabilités.
- Gestion du changement et communication :
  - Implication formalisée et régulière de la direction dans le cadre du projet de mise en place des solutions de BYOD.
- Gestion des identités : seuls les utilisateurs BYOD authentifiés peuvent se connecter aux réseaux de l'organisation.

- Gestion des périphériques mobiles : l'organisation utilise un logiciel de gestion des périphériques mobiles *(Mobile Device Management – MDM)* pour gérer tous les appareils mobiles BYOD.
- Tests de sécurité : l'infrastructure BYOD doit avoir fait l'objet de tests d'intrusion et revues de sécurité.
- Prévention de logiciels malveillants, de détection et de correction : des antivirus et antimalware doivent être présents sur les différents éléments de l'infrastructure BYOD :
  - Création d'un plan d'action sur le court terme et long terme (la connaissance et la compréhension des évolutions des écosystèmes mobiles).
  - Sensibilisation des collaborateurs aux bons usages.
  - Diffusion régulière d'une newsletter (ou rubrique intégrée dans l'intranet) sur la mobilité et le BYOD en présentant les menaces et les bonnes pratiques aux utilisateurs.

Exemples de mesures techniques

- Renforcement de la sécurité du terminal et du réseau :
  - Authentification forte.
  - Supervision des flux (à réaliser en conformité avec les directives de la Loi Informatique et Liberté).
  - Mise en place d'un outil de gestion des paramétrages de sécurité et des mises à jour de flotte hétérogène.
  - Mise à disposition d'un outil permettant l'acquisition d'applications (AppStore, Google Play, etc.).
- Protection contre la fuite d'informations[3] :
  - Recensement et classification des données sensibles.
  - Protection et ségrégation forte des données sensibles.
  - Investissement dans un outil de *Data Loss Prevention* (DLP) pour prévenir la fuite des données.
- Réalisation d'audit de sécurité :
  - Audit de l'infrastructure serveur.
  - Audit des applications accédées par les terminaux personnels.
  - Audit d'intrusion sur les terminaux personnels.

L'organisation peut avoir recours à deux solutions majeures et satisfaisantes pour encadrer l'utilisation du BYOD :

- La première option consiste à imposer une suite minimale d'applications permettant de sécuriser chacun des terminaux mobiles. Cette suite devra inclure, notamment, les éléments suivants :
  - Chiffrement du terminal ;
  - Antivirus ;
  - Firewall ;
  - Effacement à distance des données sur les terminaux.
- La deuxième option est d'imposer la virtualisation des postes de travail de l'organisation. Cela permet d'enfermer les données professionnelles dans une bulle technique et hermétique à l'équipement personnel.

[3] *Le document « Cloud et protection des données : guide pratique à l'attention des directions opérationnelles et générales », ouvrage collectif coédité par le Cigref, l'IFACI et l'AFAI traite aussi des notions et des enjeux en termes de protection des données.*

Zoom sur la protection des données

Il convient de distinguer les données sensibles au sens de l'entreprise (qui peuvent, selon le cas, être des données confidentielles ou dont l'intégrité ou la conservation sont particulièrement critiques) des données sensibles au sens de l'article 8 de la Loi Informatique et Libertés et la CNIL, définies comme *« les données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci ».*

La jurisprudence interprète de façon large la notion de donnée sensible *« L'indication du fait qu'une personne s'est blessée au pied et est en congé de maladie partiel constitue une donnée à caractère personnel relative à la santé au sens de l'article 8, § 1, de la directive 95/46 »* (CJCE, 6 nov. 2003).

La distinction entre données sensibles de l'entreprise et données sensibles CNIL est importante car seul le traitement de données à caractère personnel sensibles au sens de la Loi informatique et libertés est interdit par principe.

4- Impacts du BYOD sur le contrôle interne et la démarche d'audit interne

La mise en place du BYOD induit des changements dans les missions et les travaux d'audit et de contrôle internes, qui devront désormais prendre en compte les risques et les enjeux du BYOD. Le défi du contrôle et de l'audit internes sera d'évaluer les risques et les mesures prises pour sécuriser les données de l'organisation et minimiser les conséquences d'une fraude, d'une intrusion, etc.

Exemple de mission d'audit BYOD

Objectifs d'une mission d'audit sur le BYOD :

- Fournir à la direction une évaluation des politiques et des procédures BYOD et une option sur l'efficacité de leur exploitation ;
- Identifier les manquements réglementaires qui pourraient affecter l'organisation ;
- Identifier les faiblesses de sécurité qui pourraient nuire à la fiabilité, à l'exactitude, à la disponibilité et à l'intégrité des données de l'organisation.

Exemples de thèmes à traiter :

- Politiques BYOD : les politiques BYOD ont été définies, documentées, approuvées, mises en œuvre et sont maintenues.
- Questions juridiques : les procédures BYOD sont conformes aux exigences légales et juridiques.

- Support Utilisateurs : un service d'assistance ou de support a été mis en place pour traiter les questions des utilisateurs.
- Gouvernance : le BYOD est soumis à la surveillance et au suivi de la direction.
- Formation : les utilisateurs BYOD suivent une formation et une sensibilisation est régulièrement réalisée.
- Sécurité du terminal : les utilisateurs BYOD sont tenus de respecter une politique de sécurité.
- Gestion des identités : seuls les utilisateurs BYOD authentifiés peuvent se connecter aux réseaux de l'organisation.
- Gestion des périphériques mobiles : l'organisation utilise un logiciel de gestion des périphériques mobiles (MDM) pour gérer tous les appareils mobiles BYOD.
- Tests de sécurité : l'infrastructure BYOD doit avoir fait l'objet de tests d'intrusion et revues de sécurité.

Prévention de logiciels malveillants, de détection et de correction : des antivirus et anti-malware (logiciel malveillant) doivent être présents sur les différents éléments de l'infrastructure BYOD.
L'appel à des experts peut s'avérer utile, comme pour tout audit, pour s'assurer de mettre en évidence les risques liés au BYOD et proposer des recommandations adaptées.

Exemple d'un plan de sécurité spécifique au BYOD

- Le BYOD fait partie des analyses de risques.
- Existence d'un « comité BYOD » dans lequel chacune des parties prenantes (métier, DSI, RH et sécurité) participe dans le but d'identifier et d'évaluer les risques.
- Existence de politiques et de procédures pour renforcer la connexion au réseau d'organisation lors de l'utilisation des périphériques personnels.
- Existence d'un plan projet regroupant les principaux thèmes de sécurité liés au BYOD (contrôles des applications, respect de la politique de sécurité, révocation des droits, chiffrement des données et des appareils, suppression des données, etc.).
- Evaluation des critères de choix du BYOD en prenant en compte les besoins mais également le seuil de tolérance au risque défini par l'organisation, l'impact sur le réseau existant et l'amélioration des technologies existantes.
- Déploiement de la solution de manière progressive via des parties prenantes pilotes de chaque département.
- Revue périodique de la solution choisie, des pratiques des salariés et des mesures de contrôle.

Le BYOD permet-il de réduire les coûts de maintenance autant qu'escompté ?

Comme nous l'avons constaté précédemment, le BYOD permet aux organisations de dégager des gains partiels mais cette pratique recèle de nombreux coûts cachés :

- L'achat du terminal par le collaborateur : Subvention ? €
- La création de nouvelles règles de sécurité : Surcharge des procédures €
- Nouveaux outils de surveillance et de monitoring des accès €€
- Des problématiques de sécurité (vol de matériel, etc.) €€
- Un effort pédagogique : formation des utilisateurs €
- Des problématiques juridiques et de conformité : Changement des chartes RH, CE, etc. €€
- Augmentation des capacités réseau €€
- Des accès plus ouverts aux réseaux de l'organisation €
- Veille technologique : Menaces, terminaux, usages, … €
- Surcharge du support Helpdesk €€€

Total projet BYOD : €€€

* *
*

En guise de conclusion, quelques questions clés que doivent se poser les auditeurs et les contrôleurs internes dans le cadre de l'appréciation des risques liés au BYOD au sein de leur organisation :

- Où en est mon organisation sur le sujet du BYOD ? Un projet a-t-il été lancé ? Quel est le stade d'avancement de ce projet ? Qui sont les principaux acteurs ?
- Les opportunités, les gains escomptés et le retour sur investissement ont-ils été appréhendés ?
- Les impacts sur la sécurité informatique et notamment sur la protection des données professionnelles et personnelles ont-ils été évalués ?
- Existe-t-il un plan clair pour gérer et maîtriser de manière anticipée les enjeux liés au BYOD dans l'organisation ?
- Quels sont les effets sur le référentiel de contrôle interne et quels tests réaliser lors des missions d'audit interne ?

Bibliographie

Vous trouverez d'autres références sur les enjeux du BYOD publiés par l'ISACA et l'IIA notamment :

- BYOD security audit/assurance program. ISACA. 2012, p. 39
- Auditing the BYOD program. IIA, Internal auditor, Février 2013, p. 23-27
- BYOD business issues. IIA, Internal auditor, Février 2014, p. 21; 23

Remerciements

L'IFACI tient à remercier les personnes qui ont contribué à la conception et à la rédaction de ce document :

- José Bouaniche, Auditeur, Caisse des dépôts, Président du groupe professionnel Système d'Information
- Benoît Herment, Manager IT Advisory, KPMG SA
- Agathe Nadeau, Direction juridique et fiscale, Caisse des dépôts
- Yohann Vermeren, Director IT Advisory, KPMG SA

Réalisation : Ebzone Communication (www.ebzone.fr) - Crédit photo : © Syda Productions - Fotolia.com

© IFACI – Paris – mai 2014

ISBN : 978-2-915042-61-0

Toute représentation ou reproduction, intégrale ou partielle, faite sans le consentement de l'auteur, ou de ses ayants droits, ou ayants cause, est illicite (loi du 11 mars 1957, alinéa 1er de l'article 40). Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait une contrefaçon sanctionnée par les articles 425 et suivants du Code Pénal.