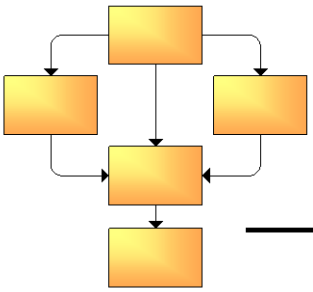

Club EBIOS

BYOD

Éléments de réflexion pour gérer les risques

Date	:	11 février 2014
Statut	:	Approuvé
Classification	:	Public
Nombre de pages	:	17
Responsable des travaux	:	Matthieu GRALL
Approbation	:	Conseil d'administration

Club EBIOS, 72 avenue Gaston Boissier, 78220 VIROFLAY

Ce document a été réalisé par le Club EBIOS avec l'aimable participation du Club des experts de la sécurité de l'information et du numérique (CESIN).

Responsable des travaux :

- Matthieu GRALL

Contributeurs :

- Membres du Club (réunions du 11 juin et du 5 août 2013), avec les présentations de Loïc BOURNON (MORPHO), d'Amina KHALED et Benoît RAST (BEAM AVOCATS), et de Vincent TOUBIANA (CNIL).
- Bruno OLLIVIER (BULL) et de Joseph GRACEFFA (ADVENS), du Club des experts de la sécurité de l'information et du numérique (CESIN).

Historique des modifications

Date	Objet de la modification	Auteur(s)	Statut
06/11/2013	Création du document sur la base de la réunion du 11 juin 2013 et du séminaire du 5 août 2013.	Matthieu GRALL	Document de travail, pour commentaires de la part du Club EBIOS et du CESIN
19/01/2014	Prise en compte des commentaires des membres du Club EBIOS et du CESIN.	Matthieu GRALL	Soumis à approbation du Conseil d'administration
11/02/2014	Finalisation pour publication.	Matthieu GRALL	Approuvé

Sommaire

Avant-propos

Ce document ne répond pas à la question « Puis-je faire du BYOD en toute sérénité ? ». Il aurait en effet été illusoire, voire dangereux, d'y répondre dans l'absolu. Les contributeurs espèrent juste que les éléments de réflexion fournis dans ce document aideront ceux qui se posent cette question à trouver leurs propres réponses, appropriées à leur contexte spécifique : « *Au Club EBIOS, on ne cherche pas savoir qui a raison, mais ce que pensent les membres !* ».

Comment faire AVEC le BYOD ?

Ce document a pour objectif de fournir des éléments utiles pour gérer les risques liés à l'utilisation du BYOD. Il n'a pas pour vocation à donner des solutions miracles, mais juste une vision du BYOD basée sur les risques, afin d'aider les responsables de la sécurité des systèmes d'information (RSSI)[1], les directeurs des systèmes d'information (DSI)[2] et les juristes[3].

Depuis quelques années, le BYOD est en forte évolution. C'est même devenu un phénomène sociétal qui s'impose à la plupart des organismes. Évolution technique ou évolution de société ? Les usages poussent-ils les offres ou est-ce l'inverse ?

Quoi qu'il en soit, des salariés, notamment aux États-Unis, considèrent aujourd'hui la possibilité de faire du BYOD comme un critère de choix de l'endroit dans lequel ils vont travailler. Et face à l'invasion d'équipements personnels en leur sein, les organismes doivent trouver des solutions.

On entend souvent ces questions :

- Le RSSI : « *un salarié peut-il venir avec un équipement qui n'est pas de confiance sans mettre le système en danger ?* »
- Le DSI : « *comment gérer une flotte d'équipements dont je n'ai pas la maîtrise ?* »
- Les juristes : « *comment rester conforme au droit du travail ?* »
- L'employeur et les décideurs : « *vont-ils enfin me simplifier la vie, au lieu de me la compliquer ?* »
- Les salariés : « *croient-ils sérieusement que je vais utiliser ce vieux téléphone au lieu de mon smartphone de dernière génération ?* »

Le BYOD soulevant une grande variété de problèmes techniques, juridiques et sociaux, on peut être tenté de répondre non, par précaution[4]. Mais beaucoup estiment également qu'il faut faire « AVEC », car sinon, les salariés contourneront les mesures qui leur seront imposées.

Une réflexion sur les risques liés au BYOD apparaît donc nécessaire afin d'apporter des éléments utiles aux décideurs.

Qu'est-ce que le BYOD ?

« BYOD » est l'acronyme anglais de « *Bring Your Own Device* ». Il peut être traduit en français par « AVEC » : Apportez Votre Équipement personnel de Communication.

Qu'est-ce qui est BYOD, et qu'est-ce qui n'est pas BYOD ? Le périmètre semble flou et les visions des experts diffèrent. Une réflexion sur les termes permet de le délimiter, tout en constatant que celui-ci est sujet à interprétation.

« *Bring* » (en français « apportez ») : avec l'ouverture actuelle des réseaux, on ne peut raisonnablement pas se limiter à une vision physique des locaux de l'organisme (ce qui est apporté dans les locaux) ; « Bring » implique une connexion avec le système d'information de l'organisme via n'importe quel canal de communication (lecteur de supports électroniques, USB, Ethernet, Wifi, Bluetooth, 3G, etc.) ; toutefois, on note que certains ne considèrent ici que les interfaces réseaux ;

« *Your Own* » (en français « votre propre ») : cette notion implique la possession, et par opposition aux systèmes que l'employeur possède, il s'agit ici de biens possédés par le salarié ; certains élargissent cette interprétation à ce qui est utilisé à titre personnel ou géré par le salarié (achat, configuration, maintenance, etc.) même s'il ne possède pas le bien ;

« *Device* » (en français « équipement ») : derrière ce terme pourraient se cacher toutes sortes d'équipements ; il convient toutefois de limiter son champ, pour écarter les stylos et autres machines à café ! Il semble en effet pertinent de ne considérer que les technologies de l'information et de la communication (TIC) ; dans cette catégorie d'équipements, tous ne s'accordent pas sur le fait que les équipements passifs (sans « intelligence »), tels que des clés USB, doivent être considérés dans le cadre du BYOD.

[1] D'une manière générale, toute personne en charge de la sécurité des systèmes d'information (SSI).

[2] D'une manière générale, les services en charge des systèmes d'information (SI).

[3] Le correspondant informatique et libertés (CIL), le directeur des affaires juridiques (DAJ) ou d'une manière générale, tout juriste travaillant sur les traitements de données à caractère personnel (DCP) ou dans le domaine du droit du travail.

[4] Le Directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) disait justement que « *La sécurité, c'est aussi le courage de dire non* » ! (position qui a ensuite été nuancée aux Assises de la sécurité de 2013).

1 Les spécificités du contexte du BYOD

1.1 Les principaux cas d'usages : de la messagerie à l'accès total aux ressources internes

En observant la manière dont le BYOD est intégré dans les organismes, les différents cas d'usages se distinguent généralement[5] par l'étendue des ressources de l'organisme qui peuvent être utilisées via des équipements BYOD : l'accès à la messagerie, au calendrier et aux contacts, puis l'accès à un choix limité de services internes[6], et enfin l'accès total à l'intranet et aux ressources internes.

La problématique pour le service en charge de l'informatique est le suivant : comment gérer une flotte d'équipements dont on n'a pas la maîtrise initialement ?

1.2 Les enjeux : gagner en confort et réduire les coûts

Le principal enjeu de la mise en place du BYOD réside dans la satisfaction conjointe des besoins des salariés et des employeurs.

Dans le contexte du BYOD, les enjeux pour le salarié viennent généralement de besoins n'étant pas, ou mal, pris en charge par l'employeur ou de besoins de confort et de liberté, avec des motivations personnelles, rationnelles et pratiques. Il s'agit souvent d'une envie de disposer d'un équipement, en substitution de l'ordinateur, qui démarre plus vite, qui est plus performant, plus léger, qui a une meilleure autonomie, une meilleure esthétique ou une meilleure ergonomie[7].

Pour l'employeur, les enjeux sont avant tout financiers, l'objectif étant de baisser les coûts et d'augmenter la productivité.
On note déjà que le BYOD peut être facilement choisi pour les activités ne nécessitant pas d'ordinateur, telles que la fabrication, ou bien en clientèle. Par ailleurs, le recours au BYOD peut diminuer les charges de support, dans la mesure où la casse, la perte, le vol, et l'entretien, voire l'utilisation des équipements, peut revenir à la charge des salariés[8]. Attention toutefois à l'augmentation d'autres coûts, du fait de la diversification des équipements utilisés[9]. Enfin, pour le service en charge de l'informatique, un autre enjeu réside dans le fait de rester compétitif par rapport au marché, et donc de réduire ses coûts et de créer de la valeur.

C'est au regard de ces enjeux que l'on acceptera ou non les risques résiduels à l'issue de l'étude.

[5] Une autre manière de présenter les cas d'utilisation consiste à différencier les accès nomades (équipements BYOD connectés depuis l'extérieur du réseau interne) des accès internes (équipements BYOD en connexion directe au réseau interne).

[6] Certaines applications, certains lecteurs réseaux…

[7] C'est aussi le confort de n'avoir qu'un appareil au bureau, en déplacement et à la maison, pour ne pas avoir en permanence à changer de système et de clavier et faciliter le transfert de fichiers. S'agissant des tablettes et smartphones, l'équipement peut être jugé plus léger, moins encombrant, avec des manipulations plus simples lors de voyages ou de présentations, une meilleure ergonomie (ex : écran tactile), une connectivité native en 3G ou en Wifi, la possibilité de ne disposer que d'un seul terminal et une notion de tout en un… On observe aussi que ce besoin est culturel, et qu'il est, généralement, inversement proportionnel à l'âge des salariés.

[8] Laisser à la charge du salarié la maintenance de l'appareil présente toutefois pour l'entreprise le risque de perdre la maîtrise de ses données. Par ailleurs, le salarié ne saurait assumer seul le coût d'achat et d'entretien d'un outil nécessaire à l'accomplissement de ses tâches, en l'absence d'alternative offerte par l'employeur, sans mettre à mal l'obligation de bonne foi de ce dernier.

[9] Coûts de développements, d'opération et de maintien en conditions opérationnelle des applications informatiques et des accès aux applications, interopérabilité.

1.3 Intégrer le BYOD dans l'amélioration continue de la sécurité

Le principal objectif de la gestion des risques liés au BYOD est de prendre en compte la problématique de manière objective et proactive, plutôt que de la subir. Toute démarche mature de management de la sécurité repose en effet sur une amélioration continue de la perception des risques et de la manière de les traiter, en considérant toute évolution du contexte de l'organisme.

Les besoins métiers, les stratégies possibles, puis les modalités pratiques de la mise en œuvre de la stratégie de réduction des risques choisie, devraient être identifiés et discutés avec les parties prenantes pertinentes selon le contexte : l'employeur, le service en charge des ressources humaines, les instances représentatives du personnel, le service en charge des questions juridiques, etc. Le facteur clé du succès consiste à trouver l'équilibre le plus satisfaisant pour toutes les parties.

En cela, l'étude des risques liés au BYOD devient un véritable projet d'entreprise.

1.4 Une coexistence de données professionnelles et privées

Même s'il est déjà toléré que des données privées soient stockées sur les systèmes internes, les équipements BYOD sont par nature porteurs de données privées et sont amenés à traiter des données professionnelles. Par nature, depuis 2010, les traitements de données effectués dans un cadre professionnel soulevaient la question d'une possible qualification d'espaces de stockages mis à disposition par l'employeur en espaces privés du salarié. Le BYOD matérialise en fait une inversion de principe : les espaces de stockage mis à disposition par le salarié pour traiter des données professionnelles peuvent-ils être qualifiés d'espaces de stockage professionnels, c'est-à-dire sous le contrôle direct de l'employeur ?

Coexistent donc au sein d'un même équipement, des données professionnelles, y compris des DCP dont l'organisme est le dépositaire, et des données privées, qui appartiennent au salarié.

1.5 Des équipements qui ne sont pas de confiance

Par définition, les équipements BYOD n'appartiennent pas à l'employeur. Certains considèrent donc qu'ils ne sont pas des biens supports, mais uniquement des interfaces du système d'information de l'organisme avec l'extérieur. Mais qu'ils soient considérés comme biens supports ou comme interfaces, il convient de les étudier afin de déterminer des mesures appropriées.

Leur principale spécificité réside dans le fait que les équipements concernés sont moins connus, et surtout moins maîtrisés, que les matériels et systèmes traditionnels.

Bien que les systèmes informatiques et de téléphonie des organismes puissent être variés, leurs vulnérabilités sont généralement bien identifiées, les risques gérés en toute connaissance de cause, et des mesures appliquées et contrôlées. Dans le contexte du BYOD, les supports considérés peuvent être des *smartphones*[10], des tablettes, voire tout autre « intrus » électronique plus ou moins intelligent[11]. D'ordinaire, ils ne sont pas sécurisés, et leurs caractéristiques et fonctionnalités particulières[12] peuvent être contraires à la politique de sécurité de l'organisme. Ils peuvent même accroître les risques sur le réseau interne s'ils sont compromis et y sont connectés.

En outre, les équipements appartiennent et sont généralement gérés par le salarié, et non par l'employeur. Cela peut comprendre l'approvisionnement et le paramétrage, mais aussi la maintenance, la vente, ou la mise au rebus. On ne peut pas protéger un équipement BYOD de l'utilisation personnelle du salarié (surf sur des sites inconnus, installation de jeux ou logiciels non vérifiés, insertion de clés USB ou CD-Rom d'origine non contrôlée, etc.), ni même de s'assurer des mises à jour des correctifs de sécurité et de la base antivirale.

[10] Appelés « ordiphones » par l'ANSSI.

[11] Imprimantes, bornes Wifi, et pour ceux qui les considèrent comme relevant du BYOD, les ordinateurs et clés USB personnels, ou encore les équipements connectés tels que Google glasses, l'iWatch, FitBit, Nike+…

[12] Notamment grâce à de nombreuses interfaces (téléphonie, Internet, connexions directes…) et à de nombreux capteurs (écran tactile, microphone, appareil photo, caméra…).

1.6 Des mesures souvent inefficaces

Les mesures de sécurité traditionnelles peuvent ne pas fonctionner, ou moins bien fonctionner, dans le contexte du BYOD. En outre, selon l'ANSSI, à l'heure actuelle, « *les fabricants et les éditeurs spécialisés multiplient les solutions* », mais « *ces solutions sont insuffisantes* » ([ZDNet]).

En effet, les mesures existantes ne s'appliquent pas toujours bien au BYOD : il est généralement plus difficile de sécuriser les systèmes, de maîtriser la gestion des accès, le branchement de clés USB, ou l'application des mises à jour et des correctifs de sécurité, de centraliser la gestion des produits de sécurité[13], de trouver des solutions de chiffrement portables, de filtrer la navigation web dans un contexte d'utilisation professionnelle et personnelle, d'inventorier le contenu des équipements, de contrôler les adresses IP, d'utiliser le NAC[14] quand celui-ci n'est pas prévu, et qu'il est nécessaire d'utiliser des VPN[15] pour accéder aux applications, des interfaces spécifiques pour faire fonctionner certains services et d'isoler les réseaux à l'aide de VLAN spécifiques.

1.7 De « nouvelles » sources de risques

Dans une étude des risques liés au BYOD, on retrouve, selon le contexte de l'organisme, n'importe quelle source humaine ou non humaine[16], interne ou externe, agissant de manière accidentelle ou délibérée, avec des capacités variables. La spécificité du BYOD réside notamment dans de plus grandes capacités des salariés et des vendeurs d'équipements.

Concernant le salarié, les équipements étant souvent choisis et utilisés à titre personnel par lui-même, cela a plusieurs conséquences : d'un côté le salarié apporte plus de soin à des équipements qui lui plaisent, mais d'un autre côté il peut davantage les exposer en les transportant partout avec lui, et en y installant plus d'applications ou d'accessoires que sur des systèmes professionnels ; en outre, les équipements liés au BYOD peuvent être davantage exposés à l'environnement du salarié[17] et c'est le salarié qui peut les choisir, les configurer, les prêter à des tiers, les vendre, les mettre au rebus, etc.
S'agissant des fournisseurs, on note qu'ils ont potentiellement plus de maîtrise sur les équipements que l'organisme et le salarié, qu'il s'agisse des matériels, des logiciels ou des canaux de communication. Ce sont eux qui peuvent les concevoir, les assembler, y installer des systèmes d'exploitation et logiciels, les configurer, les vendre, ou encore assurer leur maintenance.

Selon le contexte, il peut également être souhaitable de mettre les sources de risques suivantes en évidence : l'employeur, des codes malfaisants, des attaquants externes, ou les tiers autorisés.
En revanche, on se rend compte que, pour une fois, les administrateurs informatiques auront sans doute moins de capacités en tant que sources de risques !

1.8 Un impératif : assurer la sécurité

Le recours au BYOD ne doit pas mettre en péril la sécurité de l'employeur[18]. L'étude des risques devra donc démontrer que les solutions retenues tiennent compte de ses impératifs. S'agissant des salariés, il convient notamment de trouver des solutions respectueuses de la vie privée et conformes au droit du travail, alors que le BYOD peut remettre en question cette conformité s'il n'est pas convenablement géré. D'un point de vue métier, la conformité aux références applicables[19] peut être remise en cause par de nouveaux risques mais doit être assurée. Enfin, concernant la sécurité, le cadre normatif[20] requiert de tenir compte des évolutions du contexte pour une amélioration continue.

Le respect de ces impératifs devra être démontré lors du traitement des risques.

[13] Pare-feux, détection d'intrusion, lutte contre les codes malfaisants…

[14] *Network Access Control* (contrôleur d'accès au réseau).

[15] *Virtual Private Network* (réseau privé virtuel).

[16] Numérique, animale, naturelle, environnementale…

[17] Famille, entourage amical, ennemis…

[18] Sécurité de l'information, juridique, financière, continuité…

[19] Dans tous les cas la [Loi I&L], et selon le contexte le [RGS], [PCI-DSS], la [LSF], [SOX]…

[20] [ISO/IEC 27001], [ISO 22301], [ISO 31000]…

2 Les risques spécifiquement liés au BYOD

2.1 Le BYOD ne change ni les événements redoutés ni leur gravité

A priori, les événements redoutés sont identiques à ceux que l'on considère dans toute étude qui n'est pas liée au BYOD. En effet, les atteintes à la disponibilité, à l'intégrité et à la confidentialité des informations, ainsi que la gravité de leurs impacts sur l'organisme ou sur les personnes concernées[21], ne changent pas en cas de recours au BYOD.

Toutefois, certains peuvent vouloir considérer les données privées qui peuvent être impactées, alors que d'autres n'étudient même pas ces aspects, dans la mesure où ils estiment que ces données ne sont pas traitées par les systèmes de l'organisme. Pourtant, ces données privées pourraient constituer un moyen de pression sur un salarié afin d'obtenir des données professionnelles.

En outre, une réflexion devrait être menée sur les risques juridiques encourus par l'organisme du fait du recours au BYOD. Devraient notamment être considérées les violations de données à caractère personnel[22], la violation du secret[23], la responsabilité civile[24] et la perte de conformité à des référentiels légaux, règlementaires, normatifs, sectoriels ou internes[25].

Quoi qu'il en soit, l'estimation de la sensibilité des biens essentiels reste un élément crucial de l'étude.

2.2 Des scénarios de menaces et des vraisemblances qui diffèrent

Les scénarios de menaces à considérer sont globalement les mêmes, qu'il s'agisse de BYOD ou non, mais leur vraisemblance peut être différente : tous les cas habituels de détournement d'usage, d'observation, de détérioration, de modification, et de disparition d'un matériel, d'un logiciel, d'un canal informatique ou de téléphonie, d'une personne, et d'un canal interpersonnel, devraient être étudiés.

C'est la vraisemblance de ces menaces qui change dans le cadre du BYOD.

D'une part, la vraisemblance de certaines menaces dont les salariés peuvent être la source peut être diminuée par le fait qu'ils peuvent porter plus d'attention à un équipement qu'ils possèdent.

A contrario, la vraisemblance de plusieurs menaces augmente généralement : les menaces liées au fait que le salarié expose davantage ses équipements, ainsi que celles liées au manque de maîtrise dans le cycle de vie des équipements[26], et enfin celles liées aux facilités et aux capacités de communication.

Concernant le fait que le salarié expose davantage ses équipements, on pourra notamment considérer des menaces telles que l'observation et une utilisation détournée par son entourage, la saisie d'un équipement[27], ainsi que toutes les menaces liées aux conditions d'utilisation et de stockage des équipements et des données[28], l'installation d'applications non conformes à la politique de sécurité ou porteuses de logiciels malfaisants, mais également l'infection virale du réseau d'entreprise par un équipement personnel[29]. L'utilisation de réseaux sociaux, ou d'une manière plus

[21] Sur leur vie privée, par les traitements de données à caractère personnel qui reposeraient sur des équipements BYOD.

[22] Atteintes à la disponibilité, l'intégrité ou la confidentialité.

[23] Médical, des correspondances, d'une enquête…

[24] Dommage causé à l'entreprise par le salarié au moyen d'un équipement BYOD.

[25] Loi Informatique et libertés, PCI DSS, SOX…

[26] Achat, conception, maintenance, rebus…

[27] Enquête, contrôle aux frontières (un salarié ne peut prétendre ne pas connaitre les codes de déverrouillage de son propre terminal, ce qui peut entrainer la saisie de données professionnelles)…

[28] Elles peuvent aussi être stockées ailleurs que sur l'équipement (ex. : via un service en *cloud*).

[29] Pour voler des données, tenter un déni de service ou une prise de contrôle à distance…

générale de services d'échanges ou d'applications, peut également être la source de pertes de confidentialité.

S'agissant du manque de maîtrise du cycle de vie des équipements, on peut citer la transmission ou la vente d'un équipement à quelqu'un d'autre, y compris la simple possession[30], le changement d'organisme d'un salarié qui garde son équipement personnel, le dépannage ou l'entretien confié à un magasin, la limitation des possibilités de logiciels installés sans déverrouillage du fait du fournisseur, le refus d'actualiser le système d'exploitation ou des logiciels avec une mise à jour payante, etc.

Enfin, les grandes facilités et capacités de communication peuvent favoriser le branchement des équipements ou le branchement de périphériques à ces équipements, la capture du son et de l'image[31], l'exploitation par un attaquant des canaux et ports potentiellement ouverts[32], les difficultés en cas d'absence de réseau téléphonique, etc.

2.3 Au bilan, des risques habituels, mais plus vraisemblables

Au sujet des *smartphones*, l'ANSSI estime qu'ils engendrent « *des risques accrus de sécurité et de fuite de données* ». Cela vient surtout du fait que les vulnérabilités sont plus importantes dès lors qu'on a moins de maîtrise et qu'on ajoute des portes par lesquelles entrer dans l'organisme.

D'une manière générale, on constate que l'usage du BYOD engendre des risques similaires à ceux engendrés par des équipements de l'organisme, bien que certaines menaces soient plus vraisemblables.

Les mesures choisies pour traiter ces risques seront donc certainement différentes.

[30] Par exemple, s'il appartient à son conjoint.

[31] Capturés à l'insu de l'utilisateur ou volontairement par l'utilisateur, Bluetooth, Wifi…

[32] Intrusion, déni de service…

3 Le traitement des risques liés au BYOD

Au regard des risques appréciés, du contexte de l'organisme, notamment culturel et économique, plusieurs stratégies sont possibles pour les traiter.

Plusieurs mesures déjà en place contribuent au traitement des risques liés au BYOD. Toutefois, il convient de déterminer les éventuelles mesures complémentaires selon la stratégie retenue.

Le tableau suivant présente les mesures caractéristiques selon la stratégie choisie :

Stratégie de traitement des risques	Mesures caractéristiques
Refuser le BYOD (refuser le risque)	✓ Équipement de l'organisme, dédié ou non ✓ Justification aux utilisateurs finaux
Gagner la maîtrise de l'équipement (réduire le risque)	✓ Classification des informations ✓ Liste de matériels supportés ✓ Limitation et contrôle des usages via un MDM[33] ✓ Fourniture de services spécifiques ✓ Chiffrement de flux ✓ VPN
Maîtriser une bulle professionnelle (réduire le risque)	✓ Classification des informations ✓ Liste de matériels supportés ✓ Accès par un environnement sécurisé cloisonné (application spécifique) ✓ Contrôle d'accès logique ✓ Chiffrement de flux ✓ Chiffrement des données stockées le cas échéant ✓ VPN le cas échéant
Laisser l'équipement sans maîtrise (réduire le risque)	✓ Classification des informations ✓ Accès par une interface web (*webmail* uniquement, ou tout service accessible via le web) ✓ Contrôle d'accès logique ✓ Chiffrement de flux
Le BYOD en aveugle (prendre le risque)	✓ Aucune mesure particulière

3.1 Refuser les risques : éviter le BYOD

Une première stratégie consiste à ne pas permettre le BYOD. L'ANSSI a justement jugé que « *la sécurité, c'est aussi le courage de dire non* ». C'est en effet une stratégie envisageable, dans la mesure où les règles sont connues et acceptées par les salariés. Elle se justifie notamment dans le cas de systèmes traitant des données particulièrement sensibles. Cette stratégie devrait faire l'objet d'une justification auprès des salariés, voire d'une consultation des instances représentatives du personnel, afin qu'ils y adhèrent au lieu de tenter de la contourner !

Concernant les *smartphones*, les [Reco ANSSI] indiquent que « *les terminaux permettant d'y accéder doivent impérativement être dédiés et avoir fait l'objet d'une évaluation de sécurité, idéalement être labellisés par l'ANSSI* ».

Par ailleurs, on note que l'exemple du COPE[34] va dans ce sens, en tentant de conserver le meilleur des deux mondes, c'est-à-dire des équipements séduisants pour les salariés qui choisissent leurs

[33] *Mobile Device Management*. Un tel système permet de contrôler les applications installées et leur configuration, les fonctions et services utilisés, les éventuels *jailbreaks* de téléphones portables… Ce contrôle doit toutefois respecter la frontière entre vie professionnelle et vie privée du salarié.

[34] *Corporate Owned, Personally Enabled*.

équipements et une meilleure sécurité pour l'employeur. Il peut ainsi constituer une alternative à considérer. Dans ce cas, il convient évidemment de gérer la réintégration des biens en cas de départ.

3.2 Réduire les risques : accepter et encadrer le BYOD

Une autre stratégie peut consister à réduire les risques liés au BYOD. Pour ce faire, distinguons trois exemples qui correspondent à trois logiques différentes, plus au moins « intrusives ».

3.2.1 Exemple 1 – Gagner la maîtrise de l'équipement

La solution qui pourrait être jugée comme la plus « intrusive » consiste à appliquer des mesures sur les équipements. Elle peut grandement améliorer la confiance de l'employeur, mais n'est envisageable que si le salarié est également rassuré[35].

Concernant les *smartphones*, les [Reco ANSSI] prônent un cloisonnement efficace de chaque environnement, ainsi que la mise en œuvre de bonnes pratiques : « *l'utilisation de solutions centralisées de gestion de terminaux mobiles (MDM), la réduction des durées de vie des mots de passe ou du délai de verrouillage du terminal, l'interdiction d'accès aux boutiques d'applications, aux fonctions de géolocalisation liées aux applications, le chiffrement du stockage internet…* »

Quoi qu'il en soit, les mesures ne doivent pas être envisagées unitairement. Elles se complètent pour créer un dispositif de sécurité à la fois cohérent et proportionné aux risques. Par exemple, une bonne pratique peut consister en une gestion efficace, d'une part de la classification des informations, d'autre part des équipements, et enfin des services fournis.

Tout d'abord, la classification devrait non seulement consister à définir des critères et des règles de gestion associées, mais aussi à les appliquer techniquement, par exemple en attachant une marque sur les documents dès leur création, en détectant les potentielles transgressions, en avertissant les salariés et en journalisant leurs actions, dès lors que celles-ci sont réalisées dans le cadre professionnel[36].

Concernant la gestion des équipements, une bonne pratique consiste à recourir à un système centralisé de gestion de flottes d'appareils mobiles. Cette solution devrait permettre d'offrir le même niveau de sécurité et de contrôle pour les équipements BYOD que celui appliqué aux équipements gérés par la DSI, en les configurant conformément à la politique de l'organisme avant tout accès au réseau.
Attention cependant, tout l'enjeu réside ici dans le fait de ne gérer que ce qui est nécessaire et suffisant. Il est en effet inutile et difficilement légitime d'être trop invasif. Le système doit permettre d'effectuer des vérifications proportionnées à leur finalité et de pousser des configurations sans pour autant bloquer le salarié dans son usage courant ni surveiller toutes ses actions[37]. Le service en

[35] Voir notamment les limites des contrôles effectués, les obligations, et les messages à adresser aux utilisateurs de la [FDC-FAQ].

[36] Il est impensable de compter sur la technique pour empêcher quelqu'un de faire sortir de l'information (quelqu'un qui veut réellement faire sortir de l'information y parviendra d'une manière ou d'une autre), d'autant plus que cela peut être légitime (le métier, fort heureusement, prime sur la technique !). En revanche, la technique peut utilement détecter (sans interdire), prévenir et tracer, en excluant de ce contrôle les utilisations privées de l'équipement.

[37] Vérification que l'équipement n'a pas fait l'objet d'un *jailbreak*, que les applications installées ne permettent pas de détourner les fonctionnalités ou la stratégie de sécurité (l'interdiction pour les salariés de bénéficier du service *iCloud* se justifie par le fait que des informations de la société peuvent être confidentielles et qu'*iCloud* permettrait trop aisément des duplications de ces informations, sans qu'un contrôle efficace ne puisse-t-être opéré), qu'un logiciel de lutte contre les logiciels malfaisants est installé, que les applications sont à jour, que le déverrouillage de l'équipement requiert un code (l'activation du code de verrouillage des téléphones portables est une mesure à considérer, mais souvent les utilisateurs préfèrent que seul un container destiné à stocker ou à accéder aux données professionnelles nécessite un mot de passe), possibilité de neutraliser l'équipement à distance à sa demande (on note que cette fonctionnalité peut s'avérer être un intérêt pour le salarié également) ou d'isoler l'équipement qui ne respecte pas la politique de l'organisme… mais pas besoin de surveiller les sites Internet visités, un tel contrôle étant a priori trop intrusif).

charge de l'informatique pourrait enfin prévoir des recommandations précises aux salariés en fonction des équipements utilisés.
S'agissant de la gestion des services fournis, il s'agit de permettre aux salariés d'utiliser des applications sélectionnées ou spécifiquement développées pour qu'elles correspondent à leurs besoins métiers, voire également à leurs besoins dans la vie quotidienne. Cela peut requérir de mettre à disposition une plateforme de téléchargement et de concevoir et distribuer des outils adaptés. Il est toutefois difficile de développer des applications pour tous les systèmes et la confiance envers des systèmes très ouverts est trop faible pour apporter des garanties suffisantes en matière de sécurité. Ainsi, il peut être nécessaire de limiter le choix des équipements et des systèmes d'exploitation utilisables dans le cadre du BYOD, ou de gérer également la fourniture de packs de sécurisation.

La principale limite de cet exercice réside dans le fait que certains équipements ne permettent pas d'apporter une maîtrise et une confiance suffisantes. Il peut ainsi s'avérer nécessaire de limiter le choix des marques et des modèles, ou d'exiger que certaines caractéristiques soient requises.

3.2.2 Exemple 2 – Maîtriser une bulle professionnelle

Une autre stratégie peut consister à créer une « bulle » de confiance sur un équipement non maîtrisé. Cette stratégie a pour avantage de cloisonner les données et les usages professionnels et privés.

Parmi les solutions généralement évoquées, on peut citer le recours à plusieurs environnements[38] sur un ou plusieurs systèmes d'exploitations en général, ou à des machines virtuelles en particulier, à des coffres-forts numériques pour les données, au *cloud computing* pour les données et les applications.

Ces solutions reposent notamment, encore une fois, sur la classification des informations et sur le contrôle d'accès logique aux données ou aux services. Il convient donc de porter une attention particulière à la gestion des identités et aux moyens d'authentification.

La question fondamentale reste celle du stockage des données. Il convient en effet de déterminer si l'on accepte que des données professionnelles soient stockées sur le terminal, auquel cas il conviendra de protéger leur confidentialité[39], notamment du fait que les sauvegardes faites par le salarié pourraient concerner des données professionnelles[40]. Elles peuvent notamment être chiffrées séparément[41], sur un support amovible dédié. Une bonne pratique pourrait consister à considérer que tout ce qui n'est pas explicitement défini comme professionnel est une donnée privée. Toutefois, la Cour de cassation a finalement qualifié une clé USB privée, amenée par un salarié, de professionnelle[42]. Peut également se poser la question de l'accès aux données en mode déconnecté et de la manière de les synchroniser au retour de la connexion.

Là également, une liste des matériels, voire des logiciels, autorisés et non autorisés[43] pourraient être proposée pour éviter les cas où les solutions choisies ne soient pas compatibles ou rendues ineffectives.
La limite de cette solution réside dans le fait qu'il n'existe que peu de dispositifs pour gérer ces bulles de confiance, et encore moins de dispositifs dont la sécurité a été évaluée.

[38] Des solutions de cloisonnement de contextes sont en cours d'élaboration et permettent d'offrir plusieurs environnements d'utilisation a un seul terminal.

[39] Minimisation, anonymisation, chiffrement…

[40] Problématique de sécurité de l'information) et inversement (problématique Informatique et libertés.

[41] Par exemple, lors d'un contrôle aux frontières, un salarié devant divulguer les codes de déverrouillage de son propre terminal peut éviter que des données professionnelles ne soient saisies.

[42] « *Attendu cependant qu'une clé USB, dès lors qu'elle est connectée à un outil informatique mis à la disposition du salarié par l'employeur pour l'exécution du contrat de travail, étant présumée utilisée à des fins professionnelles, l'employeur peut avoir accès aux fichiers non identifiés comme personnels qu'elle contient, hors la présence du salarié* » (12 février 2013).

[43] Base, obsolescence…

3.2.3 Exemple 3 – Laisser l'équipement sans maîtrise

Depuis longtemps, de nombreux organismes permettent à leurs salariés de travailler depuis chez eux et d'accéder aux ressources internes au travers les équipements personnels des salariés. Ils accèdent ainsi à leurs courriers, voire au réseau de l'organisme. C'est la solution qui laisse le plus de liberté au salarié.
En considérant que tout équipement connecté n'est pas de confiance, la sécurité vient essentiellement du choix des services et données accessibles, du contrôle d'accès logique, de la protection du canal de communication, et des mesures de détection appliquées aux services choisis.

Dans ce cadre, il convient encore une fois d'estimer la sensibilité des données et de leur appliquer une classification, pour définir les conditions d'utilisation[44] et les mesures applicables à chaque niveau. Cela doit notamment permettre d'assurer le cloisonnement et la sécurité des données pour isoler autant que possible les données du salarié et les données professionnelles, et pour protéger les échanges d'informations. Pour ce faire, les bonnes pratiques souvent citées sont notamment l'utilisation de sessions différentes quand le terminal le supporte, un accès à des données internes en mode terminal uniquement, voire avec un CD-ROM démarrable et un bureau à distance, le filtrage et le chiffrement des flux à l'aide de réseaux privés virtuels (VPN), ou le contrôle des adresses MAC. S'agissant de l'accès au courrier électronique, s'il est envisagé de l'autoriser en dehors des accès évoqués, il conviendrait au moins qu'ils ne soient accessibles que via un *webmail* sécurisé[45].

Le stockage des données étant centralisé sur un système de l'organisme, la limite de cette stratégie réside dans le fait qu'elle requiert une connectivité permanente.

3.2.4 Conséquences liées à la stratégie de réduction des risques

Concernant la gestion des systèmes informatiques, la manière d'assurer le service offert aux utilisateurs peut devoir fortement évoluer, en termes :

- de développement : méthodes de développement, intégration, déploiement, etc.
- de gestion du parc d'équipements : ordinateurs, tablettes, téléphones, etc.
- d'architecture : on peut passer d'une architecture station-réseau interne-serveur à une architecture équipement BYOD-passerelle-serveur ;
- de sécurité : classification, stockage en mode *cloud computing*, isolation des réseaux, authentification forte, contrôle des équipements, effacement ou désactivation à distance, etc.
- d'assistance : maintien d'une fourniture d'équipements de secours non BYOD, question de la responsabilité de l'entretien et des réparations, etc.

Une attention particulière devrait être portée à une gestion efficace des interfaces avec les équipements BYOD, et à la fourniture de services et applications à la fois ergonomiques et de confiance.

En termes de sécurité, il convient de garder la maîtrise du système interne et de ses interfaces avec les équipements BYOD. Dès lors, les points d'attention concernent principalement les compétences en sécurité, la gestion des identités et des accès, l'isolation des réseaux et la traçabilité, mais aussi la veille et la capacité à mesurer la robustesse des mécanismes utilisés.

En termes d'organisation, les points d'attention concernent notamment la compétence des salariés et leur formation, ainsi que la surveillance du respect des règles définies dans différents documents (règlement intérieur, charte informatique, autres)[46].

3.3 Prendre les risques : le BYOD en aveugle !

Une blague ? Oui, une blague ! Cette option semble juste suicidaire, au tout du moins complètement irresponsable. Elle s'apparente à laisser la porte de chez soi ouverte et à ne même pas la surveiller afin de ne pas savoir si quelqu'un y rentre. Elle ne semble raisonnablement viable que dans le cas où l'organisme ne dispose pas de système d'information.

[44] Limitation des données accessibles et des services utilisables, aucun stockage sur l'équipement…

[45] Authentification, canal chiffré…

[46] Voir également les processus et organisation à renforcer dans la [FDC-FAQ].

La limite de cette « stratégie » est qu'elle repose sur la chance de ne pas être victime du moindre incident ou du miser sur le fait que l'organisme pourra s'en remettre.

Au minimum, il conviendrait dans ce cas de sensibiliser les salariés sur les risques que cette stratégie engendre sur l'organisme et sur eux-mêmes, ainsi que sur les bonnes pratiques à mettre en œuvre.

3.4 Couverture des impératifs : BYOD & conformité

Une bonne pratique consiste à élaborer une « déclaration d'applicabilité ». Celle-ci devrait dresser la liste des points dont on veut absolument tenir compte ou auxquels on veut se conformer[47] à partir des impératifs identifiés dans l'étude du contexte. Elle devrait permettre soit d'expliquer comment chacun de ces points est traité, soit de justifier pourquoi il ne l'est pas. Les mesures déterminées pour traiter les risques seront ainsi complétées par des mesures d'encadrement de la solution choisie.

Tout d'abord, il convient de distinguer clairement le « BYOD sur la base du volontariat » et le « BYOD par nécessité du service ». Dans la mesure où le salarié est libre de s'enrôler ou non, s'il considère cette restriction trop contraignante, il peut décider de ne pas bénéficier du BYOD.

Du point de vue juridique, on se soucie principalement de la conformité aux exigences du droit du travail, du droit de la protection des données personnelles et de propriété intellectuelle. Les questions à traiter peuvent notamment concerner le fait que l'employeur est tenu de fournir les moyens de travail[48], les avantages en nature[49], l'usage d'un logiciel sur le terminal sans en avoir acquis les droits ou le dépassement du nombre de licences acquises, que ce soit par utilisation professionnelle de licences ou services grand public, ou bien par utilisation de licences « internes » sur terminal personnel[50], l'augmentation du temps de travail et le travail en dehors des heures légales, la discrimination[51], le remboursement des frais, la protection de la vie privée.

Concernant les moyens mis en œuvre pour contrôler les équipements BYOD en termes d'applications, de configuration, de journalisation, voire de blocage ou d'effacement, il convient d'informer les salariés des dispositifs mis en place et de leur finalité. Il convient également de les informer que, potentiellement, si le matériel utilisé est présumé utilisé « *à des fins professionnelles, l'employeur peut avoir accès aux fichiers non identifiés comme personnels qu'elle contient, hors la présence du salarié* »[52]. De même, les instances représentatives du personnel devront être informées, voire consultées, dès lors que l'introduction du BYOD modifie les conditions de travail des salariés et implique la création d'un nouveau mode de contrôle de leur activité.
Une attention particulière devait être portée à la localisation des données et au prestataire retenu dans le cas d'un recours à des services de *cloud computing*. En effet, selon le pays où les données sont stockées et/ou accédées, ainsi que les obligations de la société de répondre positivement aux réquisitions émanant de certains pays dont elle dépend, il peut être nécessaire d'effectuer des démarches particulières pour rester conforme aux lois françaises, telles que la mise en œuvre des recommandations adoptées par la CNIL le 7 juin 2012[53].

[47] Dans le contexte du BYOD, on retrouve généralement le droit du travail, la loi "Informatique et Libertés" (notamment pour définir l'étendue du contrôle de l'employeur sur les appareils personnels, pour anticiper les risques de violation de données ou encore pour encadrer les éventuels transferts de données hors Union européenne).

[48] Cas particuliers : traitement du vol, casse, assurance…

[49] URSAAF, impôts…

[50] Extension de l'usage copie licence sur poste personnel.

[51] La condition de tenue de poste d'un salarié doté d'un terminal et acceptant de l'utiliser à des fins professionnelles est-elle la même que celle d'un salarié non équipé ou refusant cette usage ? N'y a-t-il pas trop de déséquilibre dans l'activité professionnelle entre ceux qui peuvent se payer un smartphone haut de gamme, un abonnement très performant, etc., et les autres ? Par ailleurs, ont-ils tous la capacité à utiliser les outils ?

[52] Une clef USB, comme vu par la Cour de cassation (12 février 2013), ou tout équipement susceptible de se connecter à un autre équipement ou réseau professionnel.

[53] http://www.cnil.fr/english/news-and-events/news/article/cloud-computing-cnils-recommandations-for-companies-using-these-new-services/.

De même, s'agissant de chiffrement, il convient de garder à l'esprit que certains pays ou ambassades ont une réglementation particulière à laquelle il faudra se conformer.
Les cas d'usages particuliers doivent également être traités : la localisation des données stockées, les transferts de données en dehors de l'Union européenne, la géolocalisation des utilisateurs, etc.

L'encadrement juridique de l'utilisation du BYOD passe principalement par le contrat de travail, la charte informatique[54] et la politique de sécurité. Il est généralement conseillé que cette charte, qui fixe notamment les responsabilités du salarié dans son périmètre personnel, couvre au minimum les pré-requis techniques[55], les modalités d'accès par l'employeur aux informations, les modalités de reprise et nettoyage des données, les règles d'utilisation[56], les éventuelles modalités de participation financière, les conditions d'entretien, d'assistance, de maintenance et de remplacement applicables. Elle devrait être annexée au règlement intérieur pour avoir la même valeur juridique, sous réserve du respect de certaines conditions de mise en œuvre, et notamment l'information et la consultation des instances représentatives du personnel, la communication à l'Inspection du travail, le dépôt au Conseil des Prud'hommes, l'affichage et communication au sein de l'entreprise. On note qu'une bonne pratique consiste à utiliser un questionnaire pour vérifier que le salarié a bien compris la charte.

4 L'acceptation des risques liés au BYOD

L'acceptation des risques consiste à faire valider la manière dont on a décidé de les traiter, et notamment les risques résiduels, au regard des enjeux des différentes parties prenantes. Cette étape constitue le cœur décisionnel de la gestion des risques.

Ainsi, l'argumentaire devrait mettre en balance les risques qui subsistent à l'issue de leur traitement avec les résultats attendus, tels que l'amélioration de la liberté des salariés et les gains de productivité pour l'employeur, afin de permettre une prise de décision éclairée[57]. On constate en effet que les gains de productivité vont souvent de paire avec une augmentation des risques. Et inversement ?

[54] Pour fixer les règles et sanctionner leur non-respect.

[55] En termes de configuration par exemple.

[56] En termes d'horaires par exemple.

[57] Par l'employeur, mais aussi par les instances représentatives du personnel et la CNIL.

Conclusion

Le BYOD est le reflet de phénomènes sociétaux actuels. Il concrétise notamment l'atténuation des frontières, qu'elles soient géographiques, ou qu'elles soient entre le domaine professionnel et le domaine privé. Il témoigne également du besoin grandissant pour l'*homo sapiens modernicus* d'une simplicité accrue, d'être connecté en permanence avec le monde, et de se distinguer des autres.

Face à ces phénomènes, les questions qu'il soulève offrent peut-être l'opportunité de remettre en cause les schémas habituels. Comment faire pour permettre aux salariés de se connecter de n'importe où, avec n'importe quel appareil, avec une confiance suffisante pour ne pas nuire, ni à l'organisme, ni aux salariés ? Les solutions que nous imaginions jusqu'à présent ne devraient-elles pas également évoluer ? Notre manière même de voir la sécurité ne devrait-elle pas changer ?

En partant du principe que ce qui peut se connecter aux ressources internes n'est pas de confiance, et en adoptant une logique centrée sur l'information et le salarié, des solutions existent. Certaines ne sont pas nouvelles. En effet, pour beaucoup, le BYOD n'apporte même rien de nouveau aux problématiques préalablement rencontrées et gérées. D'autres le sont davantage. Passer d'un modèle où le service en charge de l'informatique assure l'architecture, le choix, la fourniture, la préparation et la maintenance, et une défense périmétrique de son parc informatique avec son lot d'interdictions[58], à un modèle où il devient fournisseur et gestionnaire de services de confiance, avec une logique centrée sur l'information, où il agit surtout en prévention et en traçabilité, peut apparaitre comme quelque peu novateur ! De ce fait, la manière de gérer les systèmes d'information et leur sécurité devra sans doute être complètement repensée, mais cette rupture pourrait également apporter de nouvelles manières de gérer les équipements non BYOD du fait qu'il conduit à une amélioration de la prise en compte technologique de la sécurité.

Les risques mis en évidence ne doivent pas pour autant être négligés. Sans une réflexion préalable, conjointe entre les parties prenantes, basée sur la gestion des risques, il est communément admis que l'intégration du BYOD ne peut se faire.

Véritable projet d'entreprise, l'intégration du BYOD soulève des questions avant tout juridiques et liées aux ressources humaines, mais également organisationnelles et techniques, et ce, de manière cohérente. Pour ce faire, tous s'accordent sur les clés du succès : le sponsoring des métiers et l'accompagnement des salariés. En termes de tactique, beaucoup semblent préférer commencer par introduire le BYOD dans leur organisme via les *smartphones* des salariés, en ne leur permettant que l'accès au serveur de messagerie, au calendrier et aux contacts, pour ensuite étudier l'ouverture à d'autres services et d'autres équipements.

Pour finir, on note que ce document peut être utile dans le contexte de technologies connues aujourd'hui et aux utilisations répertoriées. De nouvelles utilisations du BYOD ou des technologies plus ouvertes pourraient modifier sensiblement certaines conclusions.

[58] On note à ce sujet que plus il y a de mesures coercitives, plus l'introduction du BYOD nécessite des adaptations aux équipements spécifiques, ce qui peut grandement compliquer sa mise en place.

Annexes

Acronymes

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
AVEC	Apportez Votre Équipement personnel de Communication
BYOD	*Bring Your Own Device*

Bibliographie

Les références suivantes apparaissent entre crochets dans le présent document.

[Loi I&L] Loi n° 78-17 du 6 janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux libertés.
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460

[LSF] Loi n° 2003-706 du 1 août 2003 de sécurité financière.
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000428977

[SOX] Loi fédérale américaine de 2002 sur la réforme de la comptabilité des sociétés cotées et la protection des investisseurs (loi Sarbanes-Oxley).
http://fr.wikipedia.org/wiki/Loi_Sarbanes-Oxley

[PCI-DSS] PCI Data Security Standard (PCI-DSS), Security Standards Council.
https://www.pcisecuritystandards.org/security_standards/pcidss_agreement.php?association=pcidss

[RGS] Référentiel général de sécurité.
http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/

[Reco ANSSI] Recommandations de sécurité relatives aux ordiphones de l'ANSSI.
http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-des-solutions-de-mobilite/recommandations-de-securite-relatives-aux-ordiphones.html

[EBIOS] *Expression des Besoins et Identification des Objectifs de Sécurité*, méthode de gestion des risques de l'ANSSI.
http://www.ssi.gouv.fr/fr/bonnes-pratiques/outils-methodologiques/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite.html

[FDC-FAQ] Les terminaux personnels en entreprise – FAQ, Forum des compétences.
http://www.forum-des-competences.org/index.php?action=download_resource&id=579&module=resourcesmodule&src=%40random5198dba8b1f0b

[ISO 22301] ISO 22301, *Sécurité sociétale – Système de management de la continuité de l'activité*, Organisation internationale de normalisation.

[ISO 27001] ISO/IEC 27001:2013, *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences*, Organisation internationale de normalisation.

[ISO 31000] ISO 31000:2009, *Gestion des risques – Principes et lignes directrices*, Organisation internationale de normalisation.

[ZNDet] *L'Anssi déconseille aux entreprises d'accepter le BYOD*, ZDNet, 23 mai 2013.
http://www.zdnet.fr/actualites/l-anssi-deconseille-aux-entreprises-d-accepter-le-byod-39790633.htm