BYOD: LA GESTION DU RISQUE JURIDIQUE

Me Amina Khaled
Me Benoît Rast

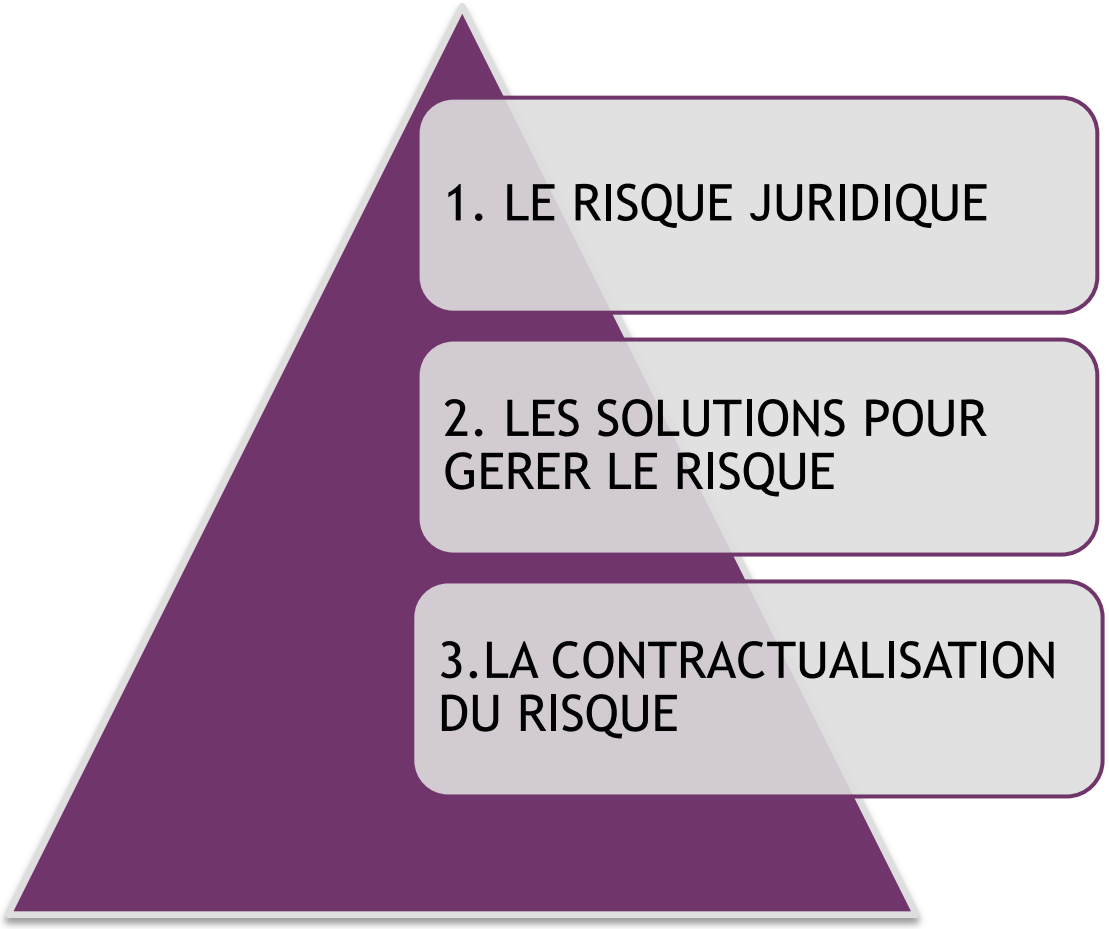
Club EBIOS
Réunion du 11 juin 2013

Beam
Avocats

Introduction

- Postulat : le matériel a été acheté par l'employé : il lui appartient = plus efficace et plus puissant
- Risques techniques évidents : sécurité et fuites de données mais également risques indirects tel que perte de certification ISO 27001
- Risques juridiques : nombreux et variés
- Sur le BYOD, vide légal et jurisprudentiel
- Auparavant, les tendances arrivaient par l'arrivée d'une nouvelle technologie (télétravail avec les ordinateurs portables par exemple). Maintenant, elles arrivent par les usages qui sont fait des outils par leurs utilisateurs
- « BYOD » = « AVEC » en fr (Apportez Votre Equipement personnel de Communication)

BYOD: LA GESTION DU RISQUE JURIDIQUE



1. LE RISQUE JURIDIQUE

1. Accès aux terminaux et aux contenus
2. Données personnelles
3. Propriété intellectuelle
4. Responsabilité civile
5. Ressources humaines
6. Confidentialité et secret professionnel

1.1 Accès aux terminaux et aux contenus

- Hypothèse: accès par l'employeur au matériel du salarié lorsqu'il soupçonne un comportement déloyal, ou simplement si le salarié est absent pour assurer la continuité d'un dossier
- Risques d'atteintes à la vie privée des salariés
- Nécessité de trouver un juste équilibre entre vie privée du salarié et contrôle de l'activité des salariés
- Aujourd'hui, la jurisprudence n'a pas tranché pour le cas spécifique du BYOD
- Mais des pistes existent ….

1.2 Données personnelles

- Toutes les obligations « classiques » de la loi I&L
  - Formalités administratives
  - Mise en place de procédures internes (mise à jour, durées de conservation, etc.)
  - Mesures de sécurité
  - Etc.

- Sanctions pénales : art. 226-16 Code pénal (5 ans/300K euros) : ICO/Glasgow City Council = 150k£

- Particulièrement concerné :
  - Notification de faille de sécurité (champ limité aux fournisseurs de services de communications électroniques)
    - Prochainement étendue !!! Projet de Règlement UE

1.3 Propriété intellectuelle

Risques de contrefaçon : 2 aspects

Applications métiers

- Application métier installé sur l'équipement
  - Risque de copie = contrefaçon
  - si le logiciel = savoir-faire de l'entreprise
    - Perte de compétitivité
    - Perte de clientèle
- Risque de perte de chiffre d'affaire, voire survie de l'entreprise

Logiciels tiers

- Logiciel tiers installé sans droits sur l'équipement
  - Logiciels « crackés »
  - Licence d'entreprise détournée (dépasse le nombre de licences accordées)
- Risque de contentieux =
  - Risque financier
  - Risque pénal
  - Risque en terme d'image

1.4 Responsabilité civile

- Hypothèse: un salarié qui utilise son propre matériel cause un préjudice à l'entreprise ou à un tiers (introduction d'un malware par exemple)
- L'entreprise est en principe responsable, en sa qualité de « commettant », des actes « commis » par le salarié dans le cadre de l'exécution de son contrat de travail
- Exception: faute lourde ou intention de nuire du salarié (mais dans la majorité des hypothèses, il s'agira de simple négligence, inadvertance ou méconnaissance)
- Dans ce domaine, la propriété du *Device* importe peu, la société engagera sa responsabilité dans les mêmes conditions pour son matériel ou dans la cas du BYOD

1.5 Ressources humaines

- Augmentation du risque lié à la question de la durée légale du temps de travail
- Risque d'augmentation des contentieux liés au harcèlement moral
- Risque de discrimination
- Gestion de la question du remboursement des frais professionnels liés à l'exécution du contrat de travail

1.6 Confidentialité et secret professionnel

- Secret médical, Secret professionnel des avocats, des experts-comptables, etc.
  - Sanctions = art. 226-13 du Code pénal = 1 an/15k euros)
- Secret de la défense nationale: obligations techniques !
  - Ex: Instruction générale interministérielle sur la protection du secret de la défense nationale du 23 juillet 2010
    - Sanctions du dépositaire : art. 413-10 Code pénal (7 ans/100K euros)
    - Sanctions du possesseur sans droit du secret : art. 413-11 ibid (5 ans/75k euros)
- Risque financier et pénal = qui est redevable ?
- « Confidentiel entreprise » : projet de loi de 2011 abandonné mais reviendra

2. LES SOLUTIONS POUR GERER LE RISQUE

1. Refuser le BYOD

2. Limiter le BYOD

3. Accepter et encadrer le BYOD

2.1 Refuser le BYOD

- Possible et même recommandé par l'ANSSI
  - Note technique « Recommandations de sécurité relatives aux ordiphones » du 15 mai 2013
- Particulièrement déconseillé quand données sensibles
- Ne pas céder aux sirènes du BYOD :

> *« La sécurité, c'est aussi le courage de dire non. »*
>
> Patrick PAILLOUX, DG de l'ANSSI

2.2 Limiter le BYOD

- COPE : Corporate Owned, Personally Enabled
  - Propriété de l'équipement = employeur
  - Choix donné à l'employé parmi les meilleurs équipements du moment

- Conserver le meilleur des deux mondes :

2.3 Accepter et encadrer le BYOD

- Avantages : baisse des coûts et augmentation de la productivité

- Etude CISCO 2012 *Internet Business Solutions Group*
  - 40% des DSI française pour le BYOD
  - 80% des DSI en asie, aux US et en amérique latine pour le BYOD

- Inconvénients : complexification de la sécurité et obligation de mettre en place un MDM (Mobile Device Management)

3. LA CONTRACTUALISATION DU RISQUE

1. Les outils

2. Le contenu

3. La procédure

3.1 Les outils

3.2 Le contenu

- La charte Informatique doit fixer les règles d'utilisation du *device* du salarié et ***sanctionner leur non-respect***

- La charte doit a minima fixer :

  - Les pré-requis techniques et organisationnels à respecter par le salarié avant d'utiliser son *device* dans le cadre de son activité professionnelle et les règles relatives à l'accès au SI de l'entreprise (configuration du terminal personnel par l'installation de logiciels, mots de passe...)
  - Les modalités d'accès par l'employeur aux informations professionnelles qui y sont stockées
  - Les modalités de reprise et nettoyage des données en cas de départ de l'employé, perte ou vol du *device*
  - Les règles d'utilisation dans le cadre du travail (horaires) et pour les besoins du travail
  - Les modalités de participation financière éventuelle de l'entreprise
  - Les conditions d'entretien, d'assistance, de maintenance et de remplacement applicables

3.3 La procédure

- La charte informatique, insérée au règlement intérieur, a la même valeur et devient opposable juridiquement aux salariés

- Toutefois pour être opposable, elle doit respecter des règles d'adoption et de mise en œuvre strictes qu'il faut également anticiper :

  - Information et consultation des IRP
  - Communication à l'Inspection du travail
  - Dépôt au Conseil des Prud'hommes
  - Affichage et communication au sein de l'entreprise...

MERCI !

Avez-vous des questions ?