Auteur : Kamal HAJJOU
Consultant Manager sécurité systèmes d'information

"BYOD" Bring your own device
Enjeux, risques et bonnes pratiques de sécurité

La pratique du Bring Your Own Device « BYOD », littéralement, « apportez votre propre appareil », consiste à amener ses appareils informatiques personnels au sein de l'entreprise (smartphones, tablettes, portables, les lecteurs flash, etc.) et à les utiliser dans le cadre de ses activités professionnelles, certains préfèrent une description plus large « apportez votre propre technologie (BYOT) », puisqu'il s'agit non seulement de matériel (s), mais aussi de logiciels utilisés sur l'appareil.

L'Observatoire de l'informatique et des télécoms au service des nouvelles organisations du Travail à publier en mai 2012, une étude menée par IDC et Bouygues Telecom, qui révèle que l'équipement en appareils personnels dans un milieu professionnel progresse, soit 72% des salariés équipés d'un smartphone en profitent pour travailler avec sur leur temps personnel, elle prévoit un triplement de la fourniture en tablettes attendue d'ici à douze mois ou l'extension de la virtualisation des postes de travail. Une autre étude de **Fortinet**, menée dans 15 pays informe que près de 70 % des salariés, **de 20 à 29 ans,** considèrent que l'utilisation de leur appareil personnel au travail n'est pas un privilège, mais un droit.

Cependant, la pratique du BYOD introduit des risques en laissant les appareils grand public sur le réseau de l'entreprise, 61% des entreprises estiment que l'utilisation des appareils mobiles personnels sur leurs réseaux se traduit par une augmentation des incidents de sécurité, un sondage parrainé par **Check Point Software Technologies**, et effectué sur un panel de 750 professionnels des TI et de sécurité, l'enquête révèle que 78% des répondants ont vu le nombre d'appareils personnels qui se connectent à leurs réseaux doubler en deux ans. Un récent sondage **Harris Interactive**, sur un panel de 1.300 d'adultes d'Amérique, qui sont actuellement employés, a constaté que plus de 80% utilise un appareil BYOD, est plus de 50% des employés utilisent des portables personnels pour prendre des informations sensibles à l'extérieur des murs de l'entreprise.

Face à ces constats, certaines entreprises considèrent le « Bring Your Own Device » comme un facteur de productivité, d'autant plus que cela représente une économie non négligeable quant aux dépenses liées à l'acquisition et à la maintenance de leur équipement informatique, cette approche peut s'avérer risquée, en absence d'une vision claire sur la frontière entre vies privée et professionnelle, rendant la sécurité des données de l'entreprise dans une situation critique. D'autres entreprises ont choisi la voie de la proscription, en estimant que leur sécurité est plus importante, en interdisant à ses employés d'utiliser leurs appareils privés et en imposant une séparation stricte des usages privés et professionnels, cette vision peut être la plus simple et la plus efficace, car autrement il faudra adapter vos systèmes de sécurité informatiques mis en place au fil des années à la pratique du BYOD, le risque est d'aboutir à des comportements hors contrôle – plus ou moins conscient – qui contourne cette décision.

L'usage professionnel des appareils BYOD, en lieu et place des ordinateurs de bureau, probablement irréversible et présage d'une ère nouvelle…, de plus en plus d'employés ont adoptés cette « BYOD Attitude », ils préfèrent travailler sur une tablette ou sur un smartphone, la génération Y en tête, et ils estiment qu'être entravés par un manque de connectivité mobile, impact leur productivité. Les organisations savent que l'autorisation des appareils personnels satisfait les employés, et à ce titre, selon **Forrester**, près de 60% des organisations soutiennent un programme BYOD aujourd'hui.

La sécurité « BYOD » face aux risques technologiques:

L'émergence du « BYOD » s'inscrit parfaitement dans le concept « **Open Enterprise Architecture** », c'est l'architecture de l'entreprise qui prend avantages de l'adhésion aux normes ouvertes, ce qui lui permet d'interagir facilement et de se connecter à d'autres entreprises, d'autres réseaux, et d'autres clients. Ce nouveau modèle TI impose aux DSI d'adopter une stratégie de bout en bout de sécurité SI, avec pour vision un alignement de la sécurité SI de l'entreprise et de l'architecture TI avec les exigences d'un environnement plus ouvert.

Pour une organisation, qui peut être soumise à une réglementation avec des exigences juridiques que l'information soit disponible à chaque demande (les exemples du standard PCI DSS qui contrôle à la fois les données collectées et comment elles sont stockées, ou de la norme ISO 27001 qui oblige à inclure tous vos actifs dans le périmètre de certification, etc.), la pratique BYOD se présente comme un défi majeur de conformité SI, puisque les appareils personnels ne sont pas des actifs de l'entreprise, alors comment les intégrer dans votre stratégie de management des risques des systèmes d'information de l'entreprise. Au niveau de la DSI, adopter un accès mobile de type « Anywhere, Anytime » est antithétique des exigences de sécurité TI, on parle de « Bring Your Own Danger » et « Bring Your Own Disaster », et pour de bonnes raisons. Il est beaucoup plus fréquent de se faire voler un smartphone ou une tablette qu'un ordinateur de bureau. De même la pratique du « BYOD » amène le risque d'attaques d'ingénierie sociale, par exemple "man in the middle", qui permet de détourner du trafic ou d'usurper l'identité du propriétaire du terminal, ou le risque des applications malveillantes disponibles sur les "appstores" des principaux acteurs, etc., d'où la nécessité d'une protection contre ces failles de sécurité. Un autre défi majeur de la pratique du BYOD, est d'engendrer une arrivée massive de nouveaux terminaux sur le réseau de l'entreprise qui continue de mettre à mal le stock d'adresses IPV4 et les mécanismes de translation d'adresse qui doivent être capable de gérer plus de sessions. Ce qui impose une migration vers IPv6 comme unique solution viable pour assurer une parfaite compatibilité de votre réseau avec ces terminaux qui sont pour la plupart nativement IPv6, d'autant plus que IPv6 offre une itinérance transparente (sans coupures), une qualité des vidéos, une meilleure communication réseau et une meilleure protection de la sécurité IPv6 pour contrer les vulnérabilités de sécurité.

L'enjeu du « BYOD » pour la sécurité SI est organisationnel, ce qui nécessite une gouvernance de sécurité SI, et l'adoption d'un programme « **Enterprise Security Framework** », pour satisfaire les exigences de **sécurité Mobile**. D'où l'importance d'une politique de management des risques SI, un appareil BYOD doit être pris en considération comme n'importe quel autre actif, la direction de l'entreprise doit prendre les dispositions juridiques nécessaires, définir les exigences en matière de sécurité SI à exécuter, définir la politique de sécurité SI, et doit prendre en compte la problématique de la sécurité mobile, avec une mise œuvre d'une politique de sécurité BYOD qui expose clairement la position de l'entreprise. La DSI est responsable de sécuriser les données, si la politique traditionnelle consistait à bloquer les périphériques indésirables d'accéder au réseau, le phénomène « BYOD » force les responsables réseaux et sécurité à un changement majeur dans la façon de gérer la problématique, au lieu de penser d'abord, « Bloquer l'accès», ils sont en train de penser, « Activer l'accès en toute sécurité », c'est un nouvel état d'esprit qui nécessite d'adopter les meilleures pratiques de sécurité pour la mobilité au sein de votre organisation, par l'adoption d'une approche proactive et d'identifier les scénarios de sécurité TI efficaces pour satisfaire les demandes de ses employées, et pour contrer le contournent des employés des règles de sécurité.

Dans un environnement BYOD, l'inquiétude de perdre des données d'entreprise en raison d'une tablette ou d'un smartphone perdu, volé ou détruit, est réelle; l'enjeu technologique pour les responsables réseaux et de sécurité est de sécuriser un appareil personnel avec lequel l'utilisateur se

connecte dans les réseaux d'entreprises, et de comprendre la manière d'utilisation des appareils personnels (nombreux d'utilisateurs qui ont accès à des courriels d'entreprise, à des ressources de stockage des données et aux applications d'entreprise, etc.), pour minimiser les risques d'un code malveillant ou la fuite de données privées, une infrastructure technologique de sécurité est préconisée :

- La sécurité du terminal, par l'acquisition d'une solution « **Endpoint Control** », pour le renforcement du contrôle de l'appareil BYOD et pour la protection des applications, des réseaux et des données (antivirus, firewall personnel, authentification et contrôle des accès 802.1x, chiffrement …)
- La sécurité du réseau(s) mobile au sein des réseaux d'entreprises, par l'acquisition d'une solution « **Mobile Device Security Management** », qui permet de superviser, administrer, supporter les terminaux déployés dans une entreprise, et de sécuriser pour faire face aux vulnérabilités qui existe sur l'appareil (authentification locale, gérer les règles de protection des données, chiffrement des données stockées, géolocalisation, l'effacement à distance, etc …), mais également une intégration avec les services de sécurité de l'entreprise comme le SIEM, le DLP, les antimalwares, les VPN, les systèmes de filtrage des contenus, etc. Une solution intégrée MDM/ NAC « **Network Access Control** » pour permettre une politique de sécurité basée sur le contrôle d'accès des appareils BYOD et du réseau, est une approche à considérer.
- La sécurité des systèmes d'information de l'entreprise, par l'acquisition d'une solution « **SIEM** » pour permettre aux administrateurs de sécurité TI d'avoir une visibilité sur le trafic réseau mobile et le comportement des utilisateurs BYOD par périphérique, de superviser les informations de sécurité d'entreprise et la gestion des événements de sécurité. Egalement par l'acquisition d'une solution « **DLP** » pour la surveillance et la sécurité des données, le contrôle, la vérification de la conformité, cela peut aider les administrateurs à identifier les violations de conformité tels que l'accès non autorisé, les menaces internes et les fuites de données sensibles, ainsi que les armer avec les informations dont ils ont besoin pour remédier à la situation
- La sécurité des réseaux d'entreprises, par l'acquisition d'une solution « **Next-generation firewalls** » pour aider à surveiller la sécurité BYOD, à détecter automatiquement et à classer les différents OS (Apple iOS, Android, Windows, Mac OS, et autres). Grâce à l'App-ID pour l'identification du trafic applicatif, ce qui comprend l'inspection du trafic applicatif encrypté en dépit des ports et protocoles utilisés, il est possible d'avoir une visibilité pour appliquer une politique de sécurité BYOD (bloquer Facebook, jeux, vidéo, etc.), en s'appuyant sur la classification des applications, l'analyse du comportement sur le réseau, et l'association à l'utilisateur.

Il est conseillé de réaliser une étude, en lançant un POC « **proof of concept** » de solutions techniques innovantes autour du projet BYOD, pour tester et adapter l'infrastructure technologique de sécurité préconisée à l'environnement technique actuelle de votre entreprise (Wifi privé, VPN, Internet, etc.) avec des résultats mesurables afin qu'ils puissent être introduits dans le processus décisionnel.

Les responsables réseaux et sécurité doivent :

- Catégoriser les utilisateurs éligibles à un accès au réseau d'entreprise, le périmètre et les moyens d'accès
- Répertorier l'appareil BYOD de l'employé dans l'inventaire de l'entreprise
- Cartographier les technologies hétérogènes (marques, systèmes d'exploitation ou versions)
- Superviser et administrer à distance les terminaux mobiles

- Définir des politiques des codes de verrouillage, et des stratégies de déploiement des profils de configuration
- S'assurer de l'existence d'un emplacement professionnel dans l'appareil de l'employé
- S'assurer que les politiques sont conçues pour des appareils spécifiques de l'employé, en identifiants les rôles et les lieux
- Renforcer la gestion des identités (IAM), et appliquer des politiques granulaires (réseaux et des périphériques), sur la base de droits d'accès, en accord avec la politique de sécurité de l'entreprise
- Elaborer une stratégie de sauvegarde prenant en compte les appareils personnels de votre entreprise, et planifier des sauvegardes de données.
- Effectuer des audits périodique pour s'assurer que l'appareil personnel est en conformité avec la politique de l'entreprise en matière de sécurité BYOD, pour inspecter le trafic réseau, pour vérifier chaque adresse MAC afin de vérifier si elle se rapporte à un PC ou un périphérique mobile, pour appliquer des politiques d'accès au réseau en conséquence, etc.

Dans le cadre de votre politique de sécurité BYOD concernant les appareils personnels, des exigences de sécurité doivent être définies, pour chaque type d'appareil personnel qui est utilisé dans le lieu de travail et relié aux réseaux de l'entreprise, par exemple, exiger que les périphériques soit configurés avec des mots de passe d'une longueur déterminée, interdire certains types d'applications d'être installé sur l'appareil ou obliger à chiffrer toutes les données sur le périphérique, limiter les applications et/ou les fonctionnalités que les employés sont autorisés à effectuer sur les appareils BYOD, imposer d'activer l'option **verrouillage et effacement à distance** sur l'appareil BYOD. Cela signifie que si votre appareil est volé ou piraté, le service informatique peut verrouiller à distance l'appareil, puis supprimer les données de l'entreprise qu'il contient, etc.

Il est important de rappeler l'importance d'une politique de sécurité SI unifiée sur l'ensemble du réseau de l'organisation (filaire, réseau sans fil, cellulaires et VPN, etc.), mais également la nécessité d'établir et d'appliquer des politiques spécifiques à travers toute l'entreprise en fonction des rôles, des employées, des appareils, des réseaux, des applications et des informations qu'ils utilisent.

Ne pas oublier les aspects ressources humaines et juridiques générés par la pratique BYOD:

L'émergence d'une informatique mobile, n'est pas une nouveauté en soi, ce qui caractérise la pratique BYOD est **l'interactivité numérique privé-pro**, on parle d'une interaction mi-privée, mi-professionnelle d'un usager avec un appareil personnel, ce qui suscite une forte augmentation des risques informatiques, chaque fois qu'un appareil BYOD est autorisé dans un réseau informatique, il expose, par exemple, votre entreprise à une fuite de vos données sensibles. Cependant l'aspect le plus délicat dans une pratique BYOD n'est pas lié aux risques techniques mais bien aux risques humains et juridiques, ce qui implique une évaluation et une mise à jour du règlement intérieur, de la charte informatique et des contrats de travail. La sécurité mobile de votre organisation, si elle existe, doit prendre en compte la sécurité BYOD, selon une approche proactive et holistique qui couvre les aspects techniques, humaines et juridiques liés à la sécurité du système d'information, pour fixer des règles dans une logique d'anticipation afin d'éviter des éventuelles répercussions économiques ou une dégradation de l'image dans l'opinion publique.

Risques humains :

Dans le livre blanc de l'observatoire de l'informatique et des télécoms au service de nouvelles organisations du travail (vers le télétravail 2.0), il est question des nouveaux usages technologiques qui seront le vecteur de l'épanouissement et de la productivité des salariés si les entreprises mettent en place des politiques adaptées à cette nouvelle norme technologique.

Votre organisation, par l'adoption de la pratique BYOD, fait face à un mode de travail différent « télétravail caché », puisque l'employé à la possibilité de travailler n'importe où, n'importe quand, et à étendre son travail au-delà des heures de bureau. Cette pratique engendre l'apparition d'un nouvel écosystème numérique avec de nouveaux risques, par exemple **risque d'une « l'hyper-connectivité »** qui peut devenir addictive, également le **risque d'une « fracture numérique »** entre les employés, en fonction de la qualité de leur équipement personnel, etc. Au regard de ces faits, Il est de la responsabilité de votre direction RH de promouvoir des pratiques de management adaptées à cette situation, la **dimension humaine** doit prévaloir absolument, par un accompagnement au changement de l'ensemble des directions, puisque la lutte contre les risques de sécurité SI requiert plus des changements d'attitude (**en termes d'usage, d'utilisateurs, d'objectifs et de résultats attendus**) plutôt que des outils technologiques, elle nécessite également la formalisation d'une charte de bonne utilisation des appareils personnels dans un cadre professionnel, nécessaire pour sensibiliser les employés à l'usage des BYOD pour accéder au SI de l'entreprise. Cette charte doit décrire dans un langage clair, l'utilisation acceptable d'un appareil BYOD pour votre entreprise, et les risques encourus par l'employeur en cas de violation (l'avertissement, la suspension et la résiliation de contrat). Ce qui nécessite une formation de sensibilisation des employés, pour que les employés soit conscients de leurs responsabilités dans la sécurité BYOD, et pour aider leur entreprise à mieux gérer ces périphériques et d'assurer la sécurité des réseaux, des formations et des séminaires qui devront se faire régulièrement pour inclure des modules sur la politique de sécurité SI de l'entreprise, la cybersécurité BYOD, la sécurité physique, la sécurité Wi-Fi, la cybercriminalité (attaques d'ingénierie sociale), les bonnes pratiques de sécurité (l'auto-verrouillage, la protection par mot de passe fort..), etc.

En fait la sensibilisation des utilisateurs est un élément clé des meilleures pratiques de sécurité SI, puisque le manque de sensibilisation des employés est un facteur important dans les incidents de sécurité.

Votre direction RH doit initier une réflexion sur des thèmes :

- Qui est concerné par la pratique du BYOD au sein de l'organisation?
- Comment gérer l'interactivité numérique privé-pro au sein de l'organisation?
- Comment établir précisément ce qui relève de la sphère professionnelle ou de la sphère privée sur l'appareil BYOD de l'employé?
- Comment classifier les données (privées, professionnelles, confidentielles) sur l'appareil BYOD de l'employé?
- Comment assurer une protection effective de l'information professionnelle et confidentielle?
- Quelles sont les règles nécessaires pour protéger l'intégralité du patrimoine informationnel?
- Quelles sont les activités effectuées sur l'appareil BYOD de l'employé qui peuvent être jugées comme du temps de travail supplémentaire?
- Quels sont les changements profonds dans les modes d'organisation du travail, dû à la pratique BYOD ?

- Quelles sont les atteintes à la santé de l'employé par une utilisation excessif de l'appareil BYOD (stress, workaholisme, troubles anxio-dépressifs..), et quel est la responsabilité sociale de l'entreprise?
- Qui paye quoi "achat, assurance, licence, abonnement, remplacement en cas de perte ou de vol, dégâts causés sur du matériel privé dans le cadre d'un usage professionnel, etc." ?

La direction RH est garant du respect des règles générales applicables au BYOD pour chaque employé, elle doit s'assurer qu'une autorisation hiérarchique, ainsi qu'une validation par la DSI, avant une éventuelle pratique BYOD au sein de l'organisation.

Risques juridiques :

La politique de management des risques nécessite la mise en place d'une « **culture juridique** » au sein de l'entreprise, l'aspect juridique de la pratique BYOD doit être clairement défini, notamment au regard de la protection du patrimoine informationnel, mais également les questions du risque d'organisation (fuite de savoir-faire), du risque pénal (l'atteinte à la vie privée), et du risque de contentieux (rupture du contrat de travail), etc. En tant qu'employeur vous devrez vous s'assurer que les employés utilisent le réseau conformément à la législation sur la propriété intellectuelle (lois HADOPI), puisque légalement vous êtes responsable de tout acte illicite commis par votre employé.

Ce processus commence par une réflexion sur les règles judicieuses pour protéger les données. Il s'agit notamment de contrôler qui accède à quelles informations et de définir des règles applicables et en adéquation avec les opérations de l'entreprise. À partir de là, les employés doivent être informés sur ces règles, puis testées. Cette réflexion devra définir l'étendue du contrôle juridique que votre organisation pourra exercer sur l'appareil personnel de l'employé:

- Quelle est la responsabilité de chacun, aux yeux de la loi?
- Quelle est la responsabilité de l'employeur en cas d'utilisation illégale?
- Qui est propriétaire des données durant la collaboration de l'employé, mais également, au terme de cette collaboration?
- Est-il possible ou non de surveiller, d'auditer, ou saisir les appareils BYOD de l'employé?
- Est-il possible de contrôler l'appareil personnel de l'utilisateur (le tracer, effacer son terminal à distance, récupérer certaines données personnelles et/ou professionnelles …)?
- Quel sont les modalités de contrôle et les sanctions encourues?
- Quelles sont les activités professionnelles autorisées (messagerie, internet, applications, etc.)?
- Qui est responsable de la sécurité, du support, de la réparation ou du remplacement de l'appareil personnel en cas d'incident ?
- Est-il possible de verrouiller, supprimer ou récupérer des données professionnelles en cas de départ de la société ?
- Comment préserver le droit des employés, spécifié par la CNIL?

Il est conseillé aux entreprises pour régler ces questions, de formaliser une charte de bonne utilisation des appareils personnels dans un cadre professionnel signée par l'utilisateur, et par exemple annexée au règlement intérieur, ou bien effectué une mise à jour de la charte informatique. Néanmoins, il est nécessaire de mentionner qu'il demeurera un risque que la nouvelle charte se révèle finalement désuète, faute d'une jurisprudence.

Votre organisation évolue dans un cadre numérique complexe, qui est au cœur de la plupart des processus d'entreprisse, la pratique du BYOD doit être considérée comme un projet technique, humain et juridique, avec un fort impact sur l'organisation de l'entreprise et de la DSI, avec des risques de sécurité liés à l'utilisation à des fins professionnelles d'équipements informatiques personnels (BYOD, « Bring Your Own Device »), ce qui implique une insécurité économie, et qui nécessite une approche systémique de la cybersécurité pour anticiper les risques, éviter de subir les menaces, et protéger votre système d'information; cette démarche structure, organise, et améliore par la mise en œuvre des politiques, des stratégies, des actions et des solutions technologiques.

Gartner's 2012 Hype Cycle for Emerging Technologies, place Le BYOD au sommet d'espoir («Peak of Inflated Expecations») des technologies émergentes, le phénomène du BYOD n'est pas prêt de disparaitre, il correspond à une tendance de consumérisation de l'informatique, il représente un vrai défi pour les entreprises et les organisations, puisque l'informatique est à la veille d'un changement radical, est plus précisément, l'informatique côté utilisateur final qui se fera de plus en plus pour des usages professionnel et privé, en associant un hyperviseur à un appareil BYOD, pour fournir des postes de travail virtuels à partir d'un appareil personnel, pour accéder à un son propre Cloud privé. Ceci impose un nouveau modèle de sécurité pour ne pas laisser s'échapper hors de son périmètre des données sensibles, stratégiques, voire confidentielles. Il est également précurseur d'un prochain sujet brûlant pour les entreprises et les travailleurs mobiles, on parle du « Bring Your Own Network » (BYON), où l'employé apporte non seulement son propre appareil, mais également son réseau (par exemple réseaux Wifi et services VoIP d'un fournisseur télécom).

Face au BYOD, votre entreprise doit être proactive et holistique.

Pour tous ceux qui souhaitent me contacter, kamalhajjou@gmail.com

Vos suggestions, questions, réactions...qu'elles soient les bienvenues!