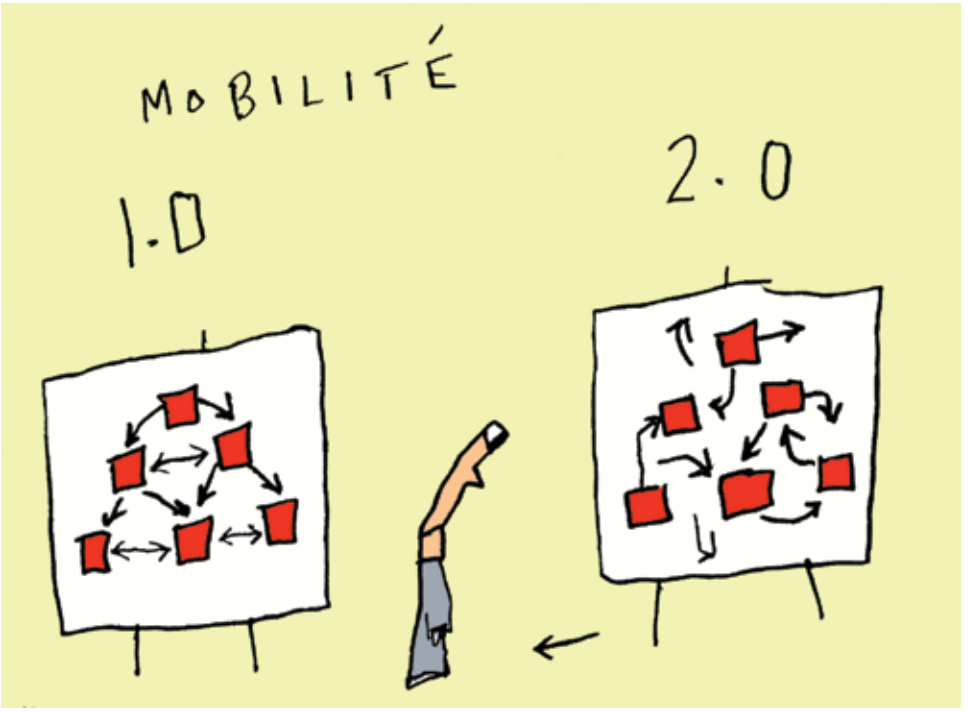
Par Guy-Marie Joseph et Pascale Dominique

La mobilité 2.0 (seconde partie)

Une saine gestion et une excellente compréhension des risques et contrôles permettent aux décideurs de tirer parti des nouvelles technologies



Le monde des technologies de l'information a connu des changements radicaux au cours des dernières décennies. En plus de l'évolution constante des technologies, nous devons faire face à l'avènement de la mobilité qui ne se limite plus à la réception d'un message via un PDA (*personal digital assistant*). Ce temps est maintenant révolu. Les innovations dans le domaine de la mobilité ou ce qu'on appelle le «virage 2.0», ont une incidence sur les mesures de contrôles internes et elles peuvent créer des difficultés pour les auditeurs du secteur de l'informatique. Ces problèmes sont souvent attribuables à une incompréhension de ces technologies, ce qui rend difficile la mise en place de contrôles adéquats.

Dans notre article du numéro d'octobre de *CAmagazine* (voir «Le virage de la mobilité 2.0» (p. 39) ou camagazine.com/archives), nous vous avons présenté les volets de la convergence voix et données, de l'informatique en nuage (*cloud computing*), et d'autres éléments qui ont accéléré la mise en place de réseaux sans fil dans les organisations, et contribué à redessiner le modèle traditionnel de l'usager mobile. Même si les gains économiques sont incontestables, les risques associés à ces nouvelles technologies demeurent un frein à leur adoption. Nous examinerons donc les risques et les mesures de contrôles internes à mettre en place, tout en tirant profit des avantages escomptés de ces technologies.

L'harmonisation des technologies de l'information avec les stratégies de l'entreprise et l'assurance que les systèmes sont adéquatement protégés et comportent un niveau acceptable de risques constituent un défi constant pour les équipes des TI. En outre, l'émergence des nouvelles technologies, comme l'informatique en nuage, accentue le besoin d'une bonne gouvernance. Enfin, de plus en plus de systèmes critiques, tant les actifs tangibles qu'intangibles, ne se situent plus entre les quatre murs de l'entreprise.

MIKE CONSTABLE

Par conséquent, les politiques internes d'utilisation doivent se fonder sur la mobilité évaluée et les risques qui y sont associés. Les employés doivent être informés et sensibilisés à la question, tout comme en ce qui a trait aux mesures de contrôle instaurées pour y remédier. Il est important que les auditeurs reconnaissent ces nouvelles technologies, qu'ils prennent connaissance des meilleures pratiques en la matière, et qu'ils comprennent les outils à mettre en place afin de réduire les risques associés à leur utilisation.

Dans le cadre de cet article, il serait impossible de procéder à une analyse exhaustive de ces sujets. Cependant, pour chacun de ceux-ci, nous décrirons les risques qui s'y rattachent, et les mesures de contrôles qui permettent d'atténuer ces risques.

Unités portables

Les appareils de type PDA ont de multiples systèmes d'exploitation qui supportent divers outils et beaucoup d'applications configurées spécifiquement pour ces environnements. Ils peuvent synchroniser avec les systèmes internes par les infrastructures câblées, en infrarouge et sans-fil. La plupart de ces appareils peuvent accepter des cartes mémoires de type Compact Flash, Smart Card, etc.

Risques physiques

• la perte de périphériques;
• le vol et la fraude résultant de l'utilisation de données stockées;
• le dommage pouvant nuire à la réputation de l'entreprise;
• le «piquage d'information par le surf d'épaule»;
• la surveillance clandestine du trafic, occasionnant des attaques sur ces unités et un accès illicite au réseau de l'entreprise;
• souvent exclue des politiques de gestion des actifs de l'entreprise, l'utilisation mixte d'outils personnels à des fins d'affaires oblige les gestionnaires à jongler avec des divergences;
• les appareils de type consommateurs sont moins bien conçus en matière de sécurité.

Risques applicatifs

• la complexité de ces nouvelles technologies rend difficile la mise en place d'un niveau de sécurité adéquat pour l'équipe des TI;
• la grande capacité à stocker des données, souvent non chiffrées sur les unités, augmente le risque;
• les autorisations d'accès de l'usager sont parfois excessives, permettant le téléchargement de données normalement interdites;
• les mises à jour de sécurité ne sont pas toujours contrôlées ou encore appliquées.

Les contrôles

Il faut prévoir l'établissement d'une gouvernance des TI en matière de mobilité 2.0. En regard des *risques physiques*, il s'agit :
• de mettre en place des politiques formelles quant à l'utilisation de ces appareils. Ces politiques feront la différence entre les unités personnelles régies par ces politiques et celles qui en sont exclues;
• de définir une politique de gestion et de classification des actifs;
• de s'assurer que les utilisateurs prennent formellement connaissance de la politique et qu'ils s'y conforment;
• de prévoir le droit, au gré, de pouvoir auditer ces unités;
• de former et d'éduquer les usagers en matière de prévention en les sensibilisant aux risques («surf d'épaule», pertes, vol).

En regard des *risques applicatifs*, il faut :
• identifier et définir un standard coopératif quant aux unités mobiles utilisées et acceptées en entreprise;
• s'assurer que ces unités utilisent des systèmes d'exploitation reconnus, documentés et supportés, car il est difficile de maintenir et de contrôler les risques émergents lorsque des plateformes mixtes sont déployées;
• intégrer des fonctions de sécurité aux applications;
• utiliser des mots de passe plus complexes;
• effectuer une libération sur temporisation (*time-out*) obligeant la saisie du mot de passe après une certaine période;
• faire la saisie du mot de passe lors de la synchronisation ou de la mise en marche de l'unité;
• renforcer et rajouter des éléments de sécurité aux applications développées en utilisant des outils offerts par des tiers, comme la biométrie (signature, voix, empreintes et reconnaissance de pictogrammes à titre d'identifiant du mot de passe); les jetons (authentification à deux facteurs); le chiffrement (un minimum de 128 bits) des données et des applicatifs, et le chiffrement du sans-fil WPA2 et plus, tel que recommandé par la norme 802.11; une infrastructure de PKI et l'utilisation de certificats (il est à noter qu'une telle infrastructure est complexe, et par le fait même, difficile à implanter et à gérer); l'utilisation du chiffrement entre la transmission des données des unités aux points d'accès; le déploiement d'antivirus et de murs coupe-feu sur les unités et enfin, une politique qui assure les mises à jour de sécurité.

La téléphonie IP (VoIP)

Le système téléphonique n'est plus qu'une extension des applications utilisant le protocole Internet (IP) menant à une gestion centralisée et consolidée.

De plus, l'utilisation de standards ouverts permet l'intégration d'équipements de différents fournisseurs, ce qui se traduit par un meilleur rapport sur le plan du coût.

Les risques

Qualité des services (QoS)
• perte de paquets;
• instabilité;
• délai de transit.

Sécurité
• vulnérabilité aux mêmes attaques que les réseaux IP (virus, DoS, reniflage de paquets comme le vol d'identité, la divulgation de renseignements confidentiels, et l'information circule en clair);
• difficulté de prévoir des temps d'arrêt des systèmes pour les entretiens préventifs;
• toute intrusion provenant de l'interne constitue aussi une menace.

Les contrôles

• la sécurité physique des équipements;
• le chiffrement des données transmises (chiffrement du trafic);
• la segmentation du réseau et la séparation du trafic voix et données sur différents VLAN;
• la mise en place de serveurs pour la téléphonie et les données;
• la configuration de murs coupe-feu dans le but de filtrer le trafic non autorisé.

Les réseaux sans fil

L'information est transmise dans les airs par fréquence radio. Elle véhicule les données d'applications critiques ainsi que la voix (VoWLAN). Bien qu'ils semblent simples à déployer, l'installation et le maintien de ces réseaux exigent un personnel qualifié.

Nous retrouvons les mêmes risques que ceux des réseaux câblés, mais nous devons mentionner d'autres vulnérabilités importantes comme l'écoute illicite, l'accès illicite au réseau, le déni de service (DoS) et l'utilisation de protocoles non ratifiés.

Les contrôles

• une approche multicouches est une de celles préconisées sur le plan des meilleures pratiques de contrôle pour l'accès, l'authentification et le chiffrement des données d'un réseau sans fil;
• le déploiement du réseau et les politiques;
• le déploiement d'un minimum de points d'accès (*access port* ou AP) pour une couverture adéquate;
• s'assurer que les AP transmettent au plus faible niveau;
• s'assurer de la couverture à l'intérieur et à l'extérieur du bâtiment;
• maintenir les politiques d'installation des AP, des NIC (*Network Interface Card*) ainsi que des groupes d'usagers des WLAN;
• supporter des protocoles 802.11 ratifiés (p. ex. : a/b/g/n).

Contrôle d'accès

• configurer en mode WPA ou WPA2 pour un niveau élevé de chiffrement des données;
• changer les SSID fréquemment lorsque cela est possible (à tout le moins, éviter une nomenclature affichant la nature de SSID);
• contrôler la diffusion des SSID;
• vérifier les adresses MAC (*Media Access Control*) de tous les périphériques se connectant au WLAN;
• maintenir les politiques d'accès et de déni d'accès pour tous les périphériques non reconnus.

Périmètre de sécurité

• installer un mur coupe-feu, des systèmes de détection et de prévention d'intrus;
•utiliser des VPN pour le chiffrement du trafic, et diriger le trafic par l'intermédiaire de ces serveurs;
• maintenir et appliquer les politiques d'accès et de routage du VPN;
• configurer ces accès clients de manière appropriée;
• installer un WIPS (*Wireless Intrusion Protection System*) dédié.

Sécurité des applications

• s'assurer des privilèges d'accès et de l'authentification des usagers en ce qui a trait aux applications;
• maintenir et appliquer les permissions d'accès et de gestion des mots de passe;
• installer les rustines du manufacturier dès le moment où elles sont disponibles.

L'informatique en nuage

Domaine en développement, l'informatique en nuage se définit «comme un modèle permettant un accès au réseau à la demande d'un regroupement de ressources informatiques configurables (réseau, serveurs, stockage, applications, services) qui peuvent être rapidement approvisionnés et libérés avec un minimum d'effort ou d'interaction de la part du prestataire de services», selon la définition du National Institute of Standards and Technology. Le Cloud Security Alliance (CSA) regroupe les risques de l'informatique en nuage dans les domaines de la gouvernance et des opérations :

La gouvernance

• conséquences légales;
• contenu du contrat;
• viabilité financière du pourvoyeur;
• aspects transfrontaliers;
• respect des lois et de la réglementation en cours;
• audit et conformité;
• sécurité et protection des données;
• migration des données vers un autre pourvoyeur;
• s'assurer d'agir conformément au *Patriot Act* en ce qui a trait aux données qui sont stockées aux États-Unis;
• lois sur la protection des renseignements personnels qui peuvent s'appliquer.

Les opérations

• authentification;
• intégration aux autres systèmes de l'entreprise;
• disponibilité des systèmes;
• continuité des opérations;
• plan de désastre;
• gestion d'incidents;
• accessibilité.

Les contrôles

• maintenir l'inventaire et la classification des actifs en impartition;
• s'assurer de l'existence d'un contrat des services (SLA) répondant aux besoins de l'entreprise;
• s'assurer que les données ne sont pas assujetties au *Patriot Act;*
• s'assurer que les lois sur la protection des renseignements personnels sont respectées;
• prévoir un audit annuel des sites des pourvoyeurs et une révision de leurs politiques en matière de sécurité, de plan de désastre, de gestion d'incidents ainsi que de maintien des compétences et certifications des techniciens chargés des systèmes.

Même si tous les éléments en matière de risques et de contrôles internes ne peuvent être couverts dans cet article, il s'agissait d'effectuer un survol de la gestion adéquate des risques qu'elle représente et de l'importance de la mise en place des contrôles internes. Bien qu'ils soient similaires aux méthodes traditionnelles, ces contrôles exigent, de la part des auditeurs en TI, une très bonne compréhension de ces méthodes. Une saine gestion permettra aux décideurs de tirer le maximum de ces nouvelles technologies.

Guy-Marie Joseph, MA, est président et responsable du secteur de la mobilité, sécurité et des TI chez ConnecTalk TM à Montréal. On peut le joindre à gjoseph@connectalk.com
Pascale Dominique, CA, CA•IT, CA•CISA, est vice-présidente finances et responsable du développement des applications à la même entreprise. On peut la joindre à pdominique@connectalk.com

---

Yves Godbout, CA•IT, CA•CISA, est directeur des services des TI au Bureau du vérificateur général du Canada et il dirige cette rubrique.