Un programme « Apportez votre propre appareil » constitue-t-il le bon choix pour votre organisation?

Risques en matière de vie privée et de sécurité associés à l'utilisation par les employés de leurs propres appareils à des fins professionnelles

Commissariat à la protection de la vie privée du Canada

Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique

Commissariat à l'information et à la protection de la vie privée de l'Alberta

Août 2015

Table des matières

Objet

Au Canada, de nombreuses organisations du secteur privé optent pour la formule selon laquelle chaque employé apporte son propre appareil mobile au travail, communément appelée « AVPA ». Cette pratique estompe toutefois davantage la démarcation entre la vie personnelle et la vie professionnelle. Les employés s'inquiètent du risque d'atteinte à leur vie privée, et cette pratique soulève des questions par rapport à la sécurité des renseignements personnels des consommateurs.

Les organisations qui envisagent d'adopter cette pratique doivent protéger les renseignements commerciaux accessibles à partir des appareils mobiles des employés ou qui y sont stockés. Il est difficile d'élaborer une stratégie de mise en œuvre qui protège efficacement les renseignements de l'entreprise et respecte le droit à la vie privée dont bénéficient les clients et les employés en vertu des lois fédérales et provinciales. Cette démarche nécessite des solutions stratégiques, éducatives et techniques.

Afin de faciliter la tâche des organisations, le Commissariat à la protection de la vie privée du Canada et les commissariats à l'information et à la protection de la vie privée de l'Alberta et de la Colombie-Britannique[1] publient les présentes lignes directrices, qui portent sur les facteurs à prendre en compte au moment de déterminer s'il y a lieu d'adopter un programme AVPA et, le cas échéant, sur la façon de s'y prendre pour le faire.

Introduction

Les organisations qui optent pour un programme AVPA autorisent leurs employés à utiliser leurs propres appareils mobiles, comme un téléphone intelligent ou une tablette, tant à des fins personnelles que professionnelles. De nombreuses organisations permettent déjà à leurs employés d'utiliser à des fins personnelles des appareils qu'elles leur fournissent. Toutefois, dans le cadre d'un programme AVPA, ce sont leurs propres appareils que les employés utilisent à des fins personnelles et professionnelles. Cette pratique peut donc estomper la démarcation entre l'utilisation d'un appareil mobile dans le cadre du travail et de la vie personnelle et soulever de sérieuses préoccupations relativement à la vie privée et à la sécurité.

De nombreux facteurs peuvent dicter la décision d'opter pour cette pratique. Par exemple, les appareils mobiles permettent désormais de s'acquitter de tâches professionnelles qui étaient auparavant exécutées à l'aide d'un ordinateur de bureau. En outre, les gens ont de plus en plus tendance à utiliser toute une panoplie d'appareils mobiles, comme un téléphone intelligent ou une tablette, et souhaitent souvent utiliser l'appareil de leur choix dans le cadre de leur travail et dans leur vie personnelle. Le programme AVPA devient dès lors un moyen intéressant de gérer les coûts et un outil susceptible d'améliorer la satisfaction et la productivité des employés. La volonté d'utiliser ce type d'outil est souvent motivée par des caractéristiques propres à l'appareil, la maîtrise de l'appareil ou la compatibilité avec d'autres services utilisés par l'employé.

Même si l'utilisation par les employés de leurs propres appareils à des fins professionnelles peut s'inscrire dans la stratégie de réduction des coûts d'une entreprise, cette pratique peut s'avérer extrêmement onéreuse si la mise en œuvre ne se fait pas de façon adéquate et sécuritaire. Une atteinte à la vie privée pourrait causer d'importants dommages à une organisation, par exemple en occasionnant des pertes financières, en la privant d'un avantage concurrentiel ou en entachant sa réputation. C'est d'autant plus vrai que l'on peut stocker sur un appareil personnel utilisé par un employé à des fins professionnelles d'importants documents d'affaires, les renseignements personnels de consommateurs (y compris des renseignements sensibles comme les données financières des clients) et les renseignements personnels des employés.

Le présent document met l'accent sur les principaux risques d'atteinte à la vie privée et à la sécurité qui devraient être pris en compte au moment de décider s'il y a lieu d'adopter un programme AVPA, notamment en ce qui concerne la pertinence de ce programme pour l'organisation. Peu importe la province où elles exercent leurs activités, toutes les organisations doivent veiller à ce que les renseignements personnels sur leurs clients et leurs employés soient stockés de façon sécuritaire et qu'ils ne soient pas communiqués sans autorisation.

REMARQUE : Il existe d'autres possibilités que le programme AVPA, par exemple les appareils appartenant à l'entreprise et mis à la disposition des employés à des fins professionnelles et personnelles. Cette pratique vise à atténuer certains risques pour la vie privée et la sécurité associés à un programme AVPA, mais elle n'est pas nécessairement plus sûre, car elle repose encore sur l'utilisation d'un seul appareil dans le cadre du travail et dans la vie personnelle[2]. Le présent document ne porte pas sur les risques en matière de vie privée associés à cette pratique.

1. Obtenir de la haute direction qu'elle s'engage à traiter les risques en matière de vie privée et de sécurité

L'engagement de la haute direction est essentiel pour que l'organisation puisse se doter des compétences et des outils qui lui permettront de régler les problèmes particuliers que pose l'utilisation par les employés de leurs propres appareils à des fins professionnelles. La haute direction devrait montrer clairement qu'elle est déterminée à cerner et à éliminer complètement les risques pour la vie privée et la sécurité et évaluer les besoins et les ressources afin de déterminer les compétences et les outils requis pour s'attaquer aux risques particuliers d'atteinte à la vie privée susceptibles de nuire aux activités de l'organisation. Sans l'appui de la haute direction, il peut être difficile d'obtenir les ressources nécessaires, de mettre en œuvre des stratégies d'atténuation du risque appropriées et d'élaborer une politique et des procédures pertinentes.

2. Effectuer une évaluation des facteurs relatifs à la vie privée et une évaluation des menaces et des risques

Il y aurait lieu d'effectuer une évaluation des facteurs relatifs à la vie privée (EFVP) et une évaluation des menaces et des risques (EMR) pour cerner et éliminer les risques associés à la collecte, à l'utilisation, à la communication, au stockage et à la conservation des renseignements personnels. Ces évaluations devraient porter sur les risques associés à l'application de la technologie sous-jacente et à la mise en œuvre d'un processus opérationnel centré sur l'utilisation par les employés de leurs propres appareils à des fins professionnelles.

Par exemple, une organisation pourrait juger souhaitable de restreindre l'utilisation d'applications et les interactions avec des services d'infonuagique non approuvés. Elle pourrait également vouloir limiter à certains employés occupant des postes précis l'utilisation d'appareils dans le cadre du programme.

Différentes organisations recueillent, utilisent, communiquent et conservent des types et des quantités variés de renseignements personnels dont la sensibilité peut varier d'un secteur d'activité à l'autre, voire à l'intérieur d'un secteur. Ainsi, chaque organisation doit prendre en compte des risques précis pour la vie privée et la sécurité lorsqu'elle envisage d'adopter un programme AVPA. D'ailleurs, un examen de ces risques peut révéler que cette formule ne constitue pas nécessairement la bonne solution dans son cas.

Une organisation pourrait vouloir adopter un programme AVPA et le mettre en œuvre rapidement, mais il est important que la haute direction examine si cette formule est appropriée dans son cas. L'utilisation d'un seul appareil pour les activités personnelles et professionnelles peut entraîner des risques pour la vie privée et la sécurité qui pourraient compromettre les renseignements de l'employé et ceux de l'entreprise. Par conséquent, il est important d'évaluer l'ampleur et la portée de ces risques afin de déterminer s'il s'agit d'un programme approprié pour une organisation en particulier.

3. Élaborer, diffuser, mettre en œuvre et mettre en application une politique portant expressément sur l'utilisation par les employés de leurs propres appareils à des fins professionnelles

Bien que nombre d'organisations se soient dotées d'une politique sur les appareils mobiles et la sécurité, il est souhaitable d'élaborer, de diffuser, de mettre en œuvre et de mettre en application une politique portant expressément sur l'utilisation par les employés de leurs propres appareils à des fins professionnelles. Cette politique devrait énoncer clairement les obligations et les attentes de ces employés et celles de l'organisation.

La politique devrait être élaborée en concertation avec les services compétents de l'organisation, par exemple le service des technologies de l'information (TI), celui de la gestion de l'information, les services juridiques, les services financiers et le service des ressources humaines. La politique en découlant devrait être facile à comprendre et avoir force exécutoire. Elle devrait également être communiquée de façon appropriée à tous les employés utilisant leurs propres appareils à des fins professionnelles et tenue à jour.

Une organisation est responsable des renseignements personnels de ses clients et de ses employés, notamment de l'information recueillie, utilisée ou communiquée au moyen d'un appareil personnel utilisé par un employé à des fins professionnelles. La politique en la matière devrait aborder un certain nombre de points :

- les responsabilités de l'utilisateur;
- la possibilité de surveillance raisonnable et acceptable des renseignements personnels sous la responsabilité d'une organisation stockés dans l'appareil personnel d'un employé et la façon dont les utilisateurs sont informés des pratiques de surveillance;
- la question de savoir si l'organisation fera le suivi des données de géolocalisation générées par l'appareil mobile;
- les pratiques de protection des renseignements personnels adoptées par une organisation en lien avec l'utilisation par les employés de leurs propres appareils à des fins professionnelles;
- la formation des employés utilisant leurs propres appareils à des fins professionnelles;
- les utilisations acceptables et non acceptables des appareils personnels des employés;
- le partage des appareils avec des parents ou des amis;
- la gestion des applications;
- la responsabilité concernant le forfait données-voix;
- les exigences relatives à la sécurité de l'appareil et de l'information; et
- les demandes d'accès.

La politique relative à l'utilisation par les employés de leurs propres appareils à des fins professionnelles devrait également mentionner toute restriction à cette pratique, par exemple :

- les appareils, les systèmes d'exploitation et leur version ainsi que les services d'infonuagique approuvés;
- les fonctions et rôles des employés qui pourraient ne pas être de bons candidats pour l'utilisation de leurs propres appareils à des fins professionnelles;
- les classes, catégories ou types de renseignements pour lesquels cette pratique n'est pas appropriée;
- les contrôles d'accès permettant aux utilisateurs de récupérer des renseignements de classes, catégories ou types particuliers.

La politique devrait également aborder les questions de communication préalable, le mode de traitement des demandes d'accès reçues par une organisation, les pratiques relatives aux enquêtes ou aux litiges concernant l'information stockée sur un appareil et ce qu'il advient de l'information stockée sur l'appareil lorsqu'un employé quitte l'organisation. Elle devrait également faire état des responsabilités de l'organisation et de celles des employés relativement aux appareils personnels qui cessent d'être utilisés par les employés à des fins professionnelles (y compris en cas de remplacement, de perte ou de vol d'un appareil ou de départ d'un employé).

Compte tenu de tout ce qui précède, une organisation devrait adopter un programme AVPA trouvant un équilibre entre ses besoins de gestion de l'information et les attentes de confidentialité des employés utilisant leurs propres appareils.

4. Mener un projet pilote avant de mettre en œuvre un programme AVPA

Si une organisation opte pour un programme AVPA, il serait souhaitable qu'elle en fasse l'essai avant de le déployer dans l'ensemble de ses services. Elle pourra ainsi évaluer les risques et les avantages du programme et déterminer son incidence possible sur ses activités. Il serait peut-être bon de commencer par une seule plateforme mobile avant d'envisager d'étendre la mise en œuvre à d'autres plateformes. À la lumière des résultats du projet pilote, l'organisation devrait prendre les mesures qui s'imposent pour corriger les lacunes mises au jour avant la mise en œuvre à grande échelle et l'élaboration du matériel de formation.

5. Élaborer le matériel et les programmes de formation

La formation est un élément clé du succès d'un programme AVPA. Tant les professionnels des technologies de l'information que les utilisateurs doivent suivre une formation appropriée – celle des professionnels des TI portera sur la mise en œuvre et l'utilisation des contrôles de sécurité techniques adéquats, y compris des logiciels de gestion des appareils mobiles (GAM), tandis que celle des utilisateurs leur permettra de comprendre les attentes de l'organisation énoncées dans la politique appropriée. Entre autres choses, on devrait traiter adéquatement de la protection de la vie privée et de la sécurité dans le matériel de formation et offrir et mettre à jour régulièrement des possibilités de formation. Il faut offrir aux utilisateurs l'occasion de poser des questions sur l'utilisation de leurs appareils et mettre à leur disposition des ressources afin d'obtenir de l'aide s'ils ont des questions ou des préoccupations dans l'avenir.

La formation devrait porter sur de nombreux sujets visant à permettre aux intervenants du programme de gérer les risques, entre autres :

- administration des appareils mobiles;
- stockage et conservation de l'information;
- chiffrement;
- gestion des correctifs et des vulnérabilités logicielles;
- gestion et configuration des applications;
- authentification et autorisation;
- protection contre les maliciels et réaction;
- gestion des incidents;
- gestion des biens et contrôle des stocks.

6. Rendre des comptes

Lorsque les employés utilisent leurs propres appareils dans le cadre de leur travail, la gestion ou l'administration des appareils pose des défis de taille. Comme les propriétaires d'appareils mobiles détiennent les droits d'administration de leurs appareils, ils sont en mesure de les configurer, de modifier ou de changer les paramètres ou encore d'installer ou de désinstaller des logiciels ou des applications en tout temps. Cette situation peut être raisonnable lorsque le propriétaire utilise l'appareil uniquement pour ses propres fins, mais la question de l'administration de l'appareil devient plus complexe lorsqu'un appareil est utilisé à la fois à des fins professionnelles et personnelles.

Dans le cadre d'un programme AVPA, si l'employé détient tous les droits d'administration sur l'information stockée sur son appareil, il se peut que l'organisation ne puisse rendre compte de façon appropriée de l'information dont elle a la responsabilité ou la garde. En outre, le fait de relier un appareil personnel au réseau d'une organisation peut poser d'importants risques pour la vie privée et la sécurité, entre autres menacer l'intégrité et la sécurité du réseau.

Si une organisation souhaite toujours mettre en œuvre un programme AVPA, elle devrait envisager d'utiliser un logiciel de GAM pour gérer les appareils mobiles reliés à son réseau. Ce type de logiciel offre généralement les fonctions de distribution par radiocommunication des applications, des données et des paramètres de configuration. Les solutions de GAM devraient optimiser les fonctions de l'appareil et la sécurité des communications mobiles.

Avant d'installer un logiciel de GAM sur l'appareil personnel d'un employé, il faudrait documenter les attentes de l'utilisateur et celles de l'organisation dans une politique sur l'utilisation par les employés de leurs propres appareils à des fins professionnelles. Le propriétaire de l'appareil et l'organisation devraient conclure une entente signée qui énonce clairement les activités précises d'administration de l'appareil que l'organisation peut exécuter sur les appareils personnels des employés.

7. Atténuer les risques grâce à la conteneurisation

Dans le cadre d'une stratégie d'atténuation du risque, les organisations devraient envisager la « conteneurisation », c'est-à-dire la segmentation de chaque appareil en deux compartiments ou « conteneurs », soit un servant à des fins professionnelles et l'autre à des fins personnelles. L'information de

l'entreprise devrait être séparée par contrôle logique de l'information personnelle de l'employé et le flux d'information entre les deux conteneurs devrait être restreint.

Le logiciel de GAM retenu devrait permettre à l'organisation de gérer et de protéger efficacement le conteneur où est stockée l'information personnelle sous sa responsabilité ainsi que toute application approuvée par l'organisation. La conteneurisation peut réduire les risques d'atteinte à la vie privée et à la sécurité, mais elle ne les élimine pas. Les vulnérabilités du conteneur personnel pourraient s'étendre au conteneur de l'entreprise et le compromettre, et vice-versa.

Seules les applications approuvées et autorisées par l'organisation devraient être installées dans le conteneur de l'entreprise. Si un employé quitte l'organisation, qu'il met à jour son appareil personnel ou qu'un appareil est perdu ou volé, l'organisation devrait pouvoir effacer le conteneur où est stockée l'information de l'entreprise, peu importe qu'elle ait un accès direct ou à distance à l'appareil, conformément à la politique relative à l'utilisation par les employés de leurs propres appareils à des fins professionnelles.

Si un appareil mobile est « débridé » ou « enraciné », il est possible de contourner les contrôles en matière de vie privée et de sécurité. Par « débridage » ou « enracinement », on entend la suppression des restrictions sur un appareil mobile pour rehausser les privilèges d'administration de l'utilisateur. Ainsi, l'utilisateur peut alors installer et désinstaller des applications particulières, ce qu'il ne pourrait faire autrement. Par conséquent, il est important de s'assurer qu'un appareil n'a pas été débridé ou déraciné avant son utilisation ou qu'il ne le sera pas si l'organisation adopte un programme AVPA. Ce sujet devrait également être abordé dans la politique relative à l'utilisation par les employés de leurs propres appareils à des fins professionnelles.

8. Établir la politique et les procédures sur le stockage et la conservation de l'information

Une organisation devrait se doter d'une politique régissant le stockage et la conservation des renseignements personnels dont elle a la garde ou la responsabilité. Idéalement, les renseignements personnels sous sa responsabilité devraient être stockés dans le réseau de l'organisation ou sur des appareils approuvés, et non directement sur les appareils des employés. L'utilisation d'un environnement à « client léger »[3] permettrait de ne pas stocker l'information directement sur un appareil personnel. Un client léger est un système informatique (par exemple, un service d'ordinateurs de bureau à distance) où un appareil sert d'écran pour afficher – sans la stocker – l'information se trouvant sur les serveurs d'une entreprise.

Le client léger pourrait aider à apaiser les préoccupations concernant la conservation, puisque tous les renseignements personnels sous la responsabilité d'une organisation demeureraient dans ses serveurs et non sur plusieurs appareils mobiles apportés au travail. Le stockage de renseignements personnels dans ses serveurs permettra également à l'organisation de répondre aux demandes d'accès à l'information personnelle prévues en vertu des lois en vigueur.

9. Chiffrer les appareils et les communications

Toute politique relative à l'utilisation par les employés de leurs propres appareils à des fins professionnelles devrait énoncer clairement les exigences en matière de chiffrement. Elle devrait notamment porter sur le chiffrement de l'appareil, du conteneur et des canaux de communication entre les appareils ou les

applications mobiles et le réseau de l'organisation. Idéalement, l'accès à distance au réseau de l'organisation devrait se faire au moyen d'une connexion sécurisée, par exemple un réseau privé virtuel.

Pour toute les solutions de chiffrement, il faut utiliser à tout le moins les algorithmes de chiffrement standard de l'industrie et respecter les exigences législatives en matière de protection de la vie privée pour protéger les renseignements personnels.

Dans le cas du chiffrement activé par l'utilisateur, ce dernier gère la clé de chiffrement, ce qui peut poser problème si cette clé est compromise ou perdue. Il faut donner aux utilisateurs une formation appropriée sur la gestion de la clé. Afin d'atténuer ce risque, le chiffrement de l'appareil personnel des employés pourrait être géré de façon centralisée par le service des TI d'une organisation. En conteneurisant les appareils personnels utilisés par les employés à des fins professionnelles, une organisation peut gérer le chiffrement dans le conteneur de l'entreprise. Selon les ressources disponibles et les exigences opérationnelles, elle pourrait chiffrer tout son conteneur ou bien des données précises avant de les stocker dans chacun de ses conteneurs (chiffrement des fichiers).

10. Gérer les corrections et les vulnérabilités logicielles

La protection contre les vulnérabilités logicielles et les activités malveillantes est un autre volet du programme AVPA qui, s'il n'est pas bien géré, risque d'entraîner de graves problèmes de protection de la vie privée et de sécurité. Une organisation qui adopte ce type de programme doit établir clairement les responsabilités pour la gestion des corrections et les mises à jour. Si ces tâches incombent à l'utilisateur, il est possible qu'elles ne soient pas effectuées en temps opportun ou qu'elles ne le soient pas du tout.

Il faut se pencher à la fois sur le système d'exploitation et sur les applications mobiles utilisées sur l'appareil. Si l'appareil n'est pas conteneurisé, les applications installées par l'utilisateur et celles de l'entreprise partagent le même environnement. Même si les applications de l'entreprise contiennent des correctifs de sécurité, les vulnérabilités de sécurité des applications installées par l'utilisateur pourraient compromettre les renseignements personnels.

L'organisation doit déterminer s'il convient d'autoriser la connexion à son réseau d'appareils sur lesquels les corrections et les mises à jour appropriées n'ont pas été effectuées.

Toutefois, si l'organisation centralise la gestion des corrections et des mises à jour, elle pourrait devoir autoriser des connexions restreintes et contrôlées afin d'effectuer les mises à jour logicielles appropriées. Ces pratiques et exigences devraient elles-mêmes être mises à jour de façon périodique et communiquées clairement aux employés utilisant leurs propres appareils à des fins professionnelles et aux employés du service des TI.

En vertu des exigences liées à la sécurité des renseignements personnels imposées par la *Personal Information Protection Act* de la Colombie-Britannique, la *Personal Information Protection Act* de l'Alberta et la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) du Canada, les organisations doivent prendre des mesures raisonnables afin de protéger les renseignements personnels en leur possession ou dont elles ont la garde contre les risques d'accès, de collecte, d'utilisation, de communication, de reproduction, de modification, d'élimination ou de destruction non autorisés.

Les trois organismes ont élaboré ensemble la ressource intitulée *Protéger les renseignements personnels : Un outil d'auto-évaluation à l'intention des organisations* pour aider les organisations à examiner leurs normes et leurs pratiques de sécurité[4].

11. Gérer les applications et leur configuration

En ce qui concerne la gestion des applications, l'organisation qui met en œuvre un programme AVPA devrait avoir une liste des applications approuvées qui peuvent être installées ainsi qu'une politique et des procédures permettant de gérer l'installation, la mise à jour et la suppression des applications. Une gestion et une coordination centralisées de ce processus pourraient simplifier la conformité aux politiques de l'entreprise.

Les organisations devraient aussi examiner attentivement le fonctionnement des applications dans le cadre des évaluations du risque. Des applications mal configurées peuvent donner lieu à des fuites de données ou à la communication non autorisée de renseignements personnels par divers canaux, notamment le courriel, la messagerie texte, le registre des appels et les contacts. Certaines applications enregistrent automatiquement une copie des données dans un nuage, tandis que d'autres n'exigent pas l'authentification de l'utilisateur ou offrent la possibilité de garder les sessions ouvertes indéfiniment. En pareil cas, l'information peut facilement être compromise.

12. Appuyer des pratiques efficaces en matière d'authentification et d'autorisation

L'authentification est le processus consistant à vérifier l'identité avant de donner accès à une ressource. L'autorisation est donnée une fois l'identité confirmée, afin de permettre l'accès à des renseignements particuliers dans une application en respectant les permissions données. Une authentification et une autorisation efficaces sont essentielles pour assurer l'efficacité des contrôles de sécurité et la reddition de comptes. Chaque organisation doit chercher à établir un juste équilibre entre, d'une part, la sécurité et la protection des renseignements personnels et, d'autre part, la convivialité. Il faudrait examiner les facettes suivantes de l'authentification :

- **Authentification de l'appareil :** Si l'appareil personnel d'un employé peut se connecter au réseau de l'entreprise, cette connexion doit se faire au moyen d'une méthode d'accès à distance appropriée, par exemple un réseau privé virtuel. L'organisation devrait s'assurer que chaque appareil a été authentifié de façon appropriée et sécuritaire avant d'autoriser l'accès au réseau.

- **Authentification du conteneur :** Ce processus peut aider à réserver aux personnes autorisées l'accès au conteneur de l'entreprise. En mettant en œuvre des contrôles de l'authentification pour le conteneur de l'entreprise, une organisation peut atténuer le risque d'accès et de communication non autorisés de renseignements personnels.

- **Authentification de l'utilisateur :** Le logiciel de GAM peut exiger que l'utilisateur choisisse un mot de passe difficile à deviner. Les appareils personnels des employés devraient être configurés de façon à pouvoir authentifier l'identité de chaque utilisateur avant de lui donner accès à l'appareil au moyen d'un mot de passe difficile à deviner ou d'une autre forme d'authentification approuvée par l'organisation. Bien que les utilisateurs puissent choisir leurs mots de passe ou codes d'accès, la gestion et la coordination

centralisées de ce processus par une organisation peut faciliter la conformité à la politique de l'entreprise. L'organisation doit fournir aux utilisateurs les lignes directrices sur le choix et le remplacement du mot de passe et effectuer périodiquement des examens pour s'assurer qu'une authentification efficace des utilisateurs est en place conformément aux exigences. Par mesure de sécurité, les utilisateurs pourraient être authentifiés au moyen d'un processus multifactoriel. Ainsi, l'identification à deux facteurs pourrait faire appel à un élément d'information que l'utilisateur connaît (par exemple un mot de passe) et à un élément qu'il a en sa possession (par exemple un jeton, un certificat de clé publique ou un identificateur biométrique).

Les applications mobiles qui traitent des renseignements personnels provenant du conteneur de l'entreprise pourraient également être configurées de façon à exiger une authentification distincte de l'utilisateur. En outre, les applications pourraient être configurées pour se mettre en veilleuse après une certaine période d'inactivité de l'utilisateur et exiger une nouvelle authentification de l'utilisateur avant d'autoriser l'accès. Il faut désactiver les fonctions des applications qui permettent aux utilisateurs de garder une session ouverte indéfiniment.

13. Se pencher sur la protection contre les maliciels

Les attaques par maliciel ont évolué considérablement au fil des ans et elles ciblent des environnements variés, dont les appareils mobiles. Les appareils mobiles peuvent avoir une capacité limitée de détecter et de prévenir les attaques. En outre, les utilisateurs ont accès à l'information plus rapidement sur les appareils électroniques que sur les ordinateurs de bureau et ils ne prennent peut-être pas le temps de lire ou d'examiner l'information ayant trait à la sécurité et à la protection de la vie privée, particulièrement sur un écran de petite taille. Ces caractéristiques font de ces appareils des cibles attrayantes pour les maliciels.

Parmi les maliciels courants, mentionnons les vers, les virus, les rançongiciels, les logiciels publicitaires et les chevaux de Troie. Les maliciels peuvent se propager au cours de diverses utilisations courantes d'un appareil mobile, par exemple la messagerie texte, le courriel et les liens hypertextes.

Certains logiciels de GAM peuvent comporter une protection contre les maliciels, mais l'organisation doit s'assurer que le recours à ce type de protection est conforme à la politique et aux normes de sécurité de l'entreprise. La protection contre les maliciels devrait être abordée dans la politique sur l'utilisation par les employés de leurs propres appareils à des fins professionnelles et dans l'entente conclue entre le propriétaire d'un appareil et l'organisation.

Pour maîtriser les risques que posent les maliciels, une organisation doit s'assurer que la sécurité de son réseau est surveillée, testée et mise à jour régulièrement. S'il est compromis, le réseau pourrait compromettre à son tour tous les appareils qui y sont reliés – y compris ceux des employés utilisant leurs propres appareils à des fins professionnelles.

En outre, une organisation devrait expliquer aux utilisateurs comment atténuer les risques liés aux maliciels. Il faudrait leur rappeler de faire preuve de jugement quant aux sites Web qu'ils consultent et les sensibiliser au danger de cliquer sur des liens douteux ou de consulter des messages textes suspects.

Par exemple, on a constaté la présence de maliciels dans de nombreuses applications gratuites offertes sur le Web. Ce risque renforce l'importance pour l'organisation de s'assurer que seules les applications qu'elle a approuvées sont installées dans son conteneur et que l'installation est conforme à sa politique et à ses procédures.

14. Adopter un processus officiel de gestion des incidents liés à l'utilisation par les employés de leurs propres appareils à des fins professionnelles

Il est important de reconnaître que les choses peuvent mal tourner quelles que soient les mesures prises pour cerner les risques d'atteinte à la vie privée et à la sécurité et les maîtriser. Le processus de gestion des incidents permet de s'assurer que les incidents liés à la sécurité ou les atteintes à la vie privée sont détectés, circonscrits, déclarés, examinés et corrigés systématiquement et rapidement.

Chaque organisation devrait adopter un processus documenté pour la gestion des incidents. Elle devrait le tester ou le mettre à l'essai régulièrement pour s'assurer que les membres de l'équipe conservent leurs aptitudes et qu'il fonctionne efficacement. Le processus devrait énoncer clairement les attentes et les responsabilités de l'organisation et celles des employés relativement à la gestion des incidents. Il est essentiel que les incidents liés à la sécurité ou les atteintes à la vie privée soient déclarés au responsable de la protection des renseignements personnels de l'organisation dès qu'ils sont mis au jour. Le processus de gestion des incidents devrait être abordé dans le cadre de la formation sur le programme AVPA.

Gestion et inventaire des biens

Afin de bien maîtriser la gestion des appareils personnels utilisés par les employés à des fins professionnelles, il est important de tenir à jour une liste des appareils mobiles et des applications autorisés dans le cadre du programme AVPA. Cette liste est particulièrement importante en cas d'incident. Par exemple, si quelqu'un déclare la perte ou le vol d'un appareil, l'information qui figure sur la liste pourrait aider à prendre des mesures d'atténuation, notamment en limitant la connexion de l'appareil au réseau.

Cette liste pourrait aussi permettre d'empêcher l'accès des appareils indésirables au réseau ou à l'information de l'entreprise. Une liste bien tenue est le reflet d'une bonne reddition de comptes et facilite l'enregistrement et le désenregistrement des appareils personnels utilisés par les employés à des fins professionnelles.

Conclusion

L'utilisation d'appareils personnels en milieu de travail comporte certains avantages, mais l'élaboration et la mise en œuvre d'une politique en la matière présentent de nombreux défis, lesquels pourraient se multiplier dans un environnement multiplateformes. Il est donc important pour une organisation qui envisage d'adopter un programme AVPA de cerner et d'évaluer les risques d'atteinte à la vie privée et à la sécurité afin de déterminer dans un premier temps la pertinence d'adopter cette pratique.

L'évaluation ne devrait pas viser uniquement à déterminer si les avantages du programme pour l'organisation et ses employés l'emportent sur les risques. Elle devrait également prendre en compte les ressources humaines et financières à consacrer à la mise en œuvre, à la surveillance et à la mise à jour de tous les aspects du programme, y compris les facteurs ayant trait à la vie privée et à la sécurité.

De surcroît, aucune solution technologique ou stratégique ne permet à elle seule de maîtriser tous les risques, ce qui constitue un autre défi. Les solutions varient, comme c'est le cas dans le domaine de la gestion des données et de l'information. La complexité du programme AVPA réside dans l'intégration d'applications et de données des employés et de l'entreprise sur un seul appareil.

Si une organisation choisit de mettre en œuvre un programme AVPA, elle devrait le faire au cas par cas et être en mesure de montrer qu'elle peut résoudre de façon sécuritaire et responsable les problèmes particuliers de protection de la vie privée et de sécurité auxquels elle se heurte.

Ressources supplémentaires

Les documents intitulés Un programme de gestion de la protection de la vie privée : la clé de la responsabilité et *Protéger les renseignements personnels : Un outil d'auto-évaluation à l'intention des organisations ont été publiés conjointement par le Commissariat à la protection de la vie privée du Canada et les commissariats à l'information et à la protection de la vie privée de l'Alberta et de la Colombie-Britannique.*

Le Commissariat à la protection de la vie privée du Canada a conçu de nombreux outils qui renseignent les organisations sur les fondements de la protection de la vie privée et la législation sur la protection des renseignements personnels, entre autres *Trousse d'outils en matière de vie privée – Guide à l'intention des entreprises et des organisations*; et une vidéo à l'intention des petites et moyennes entreprises intitulée *Protégez la vie privée de vos clients : La LPRPDE pour les entreprises*.

Le Commissariat à l'information et à la protection de la vie privée de l'Alberta a élaboré les documents suivants, qui seront eux aussi utiles : *Guide for Businesses and Organizations on the Personal Information Protection Act, Information Privacy Rights* et *10 Steps to Implement PIPA*.

Le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique a élaboré des ressources similaires portant sur la législation provinciale applicable au secteur privé, entre autres *What are My Organization's Responsibilities Under PIPA?* et *A Guide for Business and Organizations to BC's Personal Information Protection Act*.

Annexe A : Éléments d'ordre stratégique pour l'utilisation par les employés de leur propres appareils à des fins professionnelles

Appui de la haute direction	- Obtenir l'appui de la haute direction afin de cerner les risques d'atteinte à la vie privée, de mettre en œuvre des stratégies d'atténuation du risque et d'élaborer une politique et des procédures appropriées.
Évaluation des facteurs relatifs à la vie privée et évaluation des menaces et des risques	- Déterminer si le programme AVPA constitue une solution appropriée que l'organisation peut adopter en toute sécurité. - Mener un projet pilote avant de mettre en œuvre le programme à grande échelle afin d'analyser les risques, de déterminer s'il s'agit du bon choix pour l'organisation et de combler toute lacune en matière de ressources.
Élaboration, diffusion, mise en œuvre et mise en application d'une politique portant expressément sur l'utilisation par les employés de leurs propres appareils à des fins professionnelles	- Élaborer une politique après avoir consulté les employés de l'ensemble de l'organisation. Déterminer le mode d'examen, de mise à jour, de diffusion et d'application de la politique et des procédures connexes.
Élaboration de matériel et de programmes de formation	- Déterminer les outils de formation particuliers nécessaires aux employés qui utilisent leurs propres appareils à des fins professionnelles et aux employés du service des TI. - Mettre à jour périodiquement la formation.
Administration des appareils mobiles	- Élaborer une stratégie faisant état des appareils, des systèmes d'exploitation et des versions de ces systèmes qui seront pris en charge. - Prendre en compte des pratiques telles que la conteneurisation des appareils ou le recours à un environnement « client léger ».
Transmission et stockage d'information	- Déterminer l'information pouvant être envoyée aux appareils personnels approuvés et stockée sur ces appareils. Déterminer les catégories et le degré de sensibilité de l'information autorisés.
Chiffrement	- Mettre en œuvre une politique et des procédures pour se pencher sur des questions comme le chiffrement des appareils, des conteneurs et des canaux de communication entre les appareils ou les applications mobiles et le réseau d'entreprise.
Gestion des corrections et des vulnérabilités logicielles	- Expliquer clairement comment les appareils et les logiciels seront mis à jour ainsi que les rôles et responsabilités des utilisateurs et ceux des employés du service des TI. - Élaborer des procédures et du matériel de formation portant sur les attaques techniques et attaques d'ingénierie sociale associées aux maliciels et sur d'autres types d'attaques.

Gestion et inventaire des biens	- Tenir à jour une liste des appareils et des applications mobiles autorisés dans le cadre d'un programme AVPA. - Élaborer une liste des applications approuvées aux fins d'installation ainsi qu'une politique et des procédures sur la gestion de l'installation, de la mise à jour et de la suppression des applications.
Authentification et autorisation	- Établir un processus d'authentification de l'utilisateur avant de donner accès à une ressource. - Cela inclut l'authentification au niveau de l'appareil, du conteneur et de l'utilisateur.
Processus de gestion des incidents	- Mettre en place un processus de gestion des incidents qui porte sur la déclaration, la détection, l'identification, l'enquête et les mesures correctives. - Mettre régulièrement à l'essai le processus de gestion des incidents et le mettre à jour au besoin.

Pour de plus amples renseignements :

Commissariat à la protection de la vie privée du Canada

Commissariat à la protection
de la vie privée du Canada
30, rue Victoria, 1er étage
Gatineau (Québec) K1A 1H3
Sans frais : 1-800-282-1376
Tél. : 819-994-5444
Télécopieur : 819-994-5424
ATS : 819-994-6591
www.priv.gc.ca

Office of the Information and Privacy Commissioner of Alberta

Commissariat à l'information et à la protection
de la vie privée de l'Alberta
9925, 109e rue N.-O., bureau 410
Edmonton (Alberta) T5K 2J8
Sans frais : 1-888-878-4044
Tél. : 780-422-6860
Télécopieur : 780-422-5682
Courriel : generalinfo@oipc.ab.ca
www.oipc.ab.ca

Office of the Information & Privacy Commissioner for British Columbia
Protecting privacy. Promoting transparency.

Commissariat à l'information
et à la protection de la vie privée
de la Colombie-Britannique
C.P. 9038, succ. gouv. prov.
Victoria (Colombie-Britannique) V8W 9A4
Tél. : 250-387-5629
Sans frais à Vancouver : 604-660-2421
Sans frais ailleurs en C.-B. : 1-800-663-7867
Télécopieur : 250-387-1696
Courriel : info@oipc.bc.ca
www.oipc.bc.ca

NOTES DE FIN DE DOCUMENT

[1] *Loi sur la protection des renseignements personnels et les documents électronique* (LPRPDE) et lois provinciales essentiellement similaires, y compris la *Personal Information Protection Act* de l'Alberta et la *Personal Information Protection Act* de la Colombie-Britannique. *Même si certaines dispositions peuvent varier d'une loi à l'autre, ces trois lois sont considérées comme très similaires sur le plan du contenu et reposent sur les mêmes principes fondamentaux*.

[2] Ryan Kalember, « Weighing COPE vs. AVPA? Don't Forget Key Security Factor: FILE », *Computerworld*, 24 juillet 2013.

[3] Pour obtenir une définition du concept de « client léger », voir la référence au modèle Software as a Service (SaaS) dans *The NIST Definition of Cloud Computing*, publication spéciale n° 800-145 du National Institute of Standards and Technology du U.S. Department of Commerce, page 2, septembre 2011.

[4] Commissariat à la protection de la vie privée du Canada, Commissariat *à l'information et à la protection de la vie privée* de l'Alberta et Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique, Protéger les renseignements personnels : Un outil d'auto-évaluation à l'intention des organisations.