



CPA

COMPTABLES
PROFESSIONNELS
AGRÉÉS
CANADA

Internet des objets

TENDANCE TECHNOLOGIQUE

« L'Internet des objets transforme les objets qui nous entourent en un écosystème d'information qui enrichit nos vies. Réfrigérateurs, espaces de stationnement, maisons... de plus en plus d'éléments s'ajoutent chaque jour à l'espace numérique, de sorte que l'Internet des objets constituera bientôt un secteur de plusieurs billions de dollars¹. »

Depuis un bon moment déjà, le Web permet la communication entre personnes, entreprises et marchés. Au départ, il fallait utiliser un ordinateur de bureau relié à des serveurs et à des centres de données. Les connexions réseau reposaient souvent sur des prises fixes, confinant les appareils dans des espaces précis.

La situation a bien changé. Plus personne n'est attaché à son bureau par des câbles branchés à des serveurs occupant des étages complets. Maintenant, tout appareil permettant la collecte et la transmission de données peut être connecté. La puissance d'Internet et les progrès en technologies sans fil ont permis le développement de l'Internet des objets.

Description

L'Internet des objets (IdO) fait référence à tout appareil informatique capable de transférer des données par réseau. Télévisions, caméras de surveillance, électroménagers, interrupteurs, capteurs de mouvement, capteurs industriels, étiquettes d'identification par radiofréquence (RFID) avancée, balises ou drones d'entreprises, par exemple, en font partie. Selon Gartner, l'IdO désigne un réseau d'objets physiques qui contiennent des technologies intégrées leur

¹ www.pwc.com/us/en/increasing-it-effectiveness/assets/future-of-the-internet-of-things.pdf

permettant de communiquer ou de détecter leur état interne ou leur environnement externe ainsi que d'interagir avec ceux-ci. En connectant ses actifs à ses processus et à son personnel, une entreprise peut saisir des données et des événements et ensuite les analyser afin d'apprendre un comportement ou un usage, de mettre en œuvre des mesures préventives ou encore d'améliorer ou de modifier ses processus².

Interactions dans un système IdO



Source : <https://securityledger.com/2014/04/will-ot-big-data-create-darwinian-struggle-for-insurance-carriers/iot-loop/>

Importance

L'IdO devrait comprendre 20 milliards d'appareils intelligents d'ici 2020³. Ces derniers feront donc partie intégrante de nos vies et de nos entreprises. Bien utiliser les appareils IdO est essentiel à la collecte et à l'analyse des données en temps réel, ou presque, en vue de l'amélioration et de l'accélération du processus décisionnel axé sur les données. L'IdO favorise aussi l'automatisation en plus d'encourager les entreprises à transformer leurs processus et à améliorer leur efficacité opérationnelle (notamment grâce à la maintenance

2 www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

3 www.zdnet.com/article/iot-devices-will-outnumber-the-worlds-population-this-year-for-the-first-time/

prédictive). Déjà, les entreprises et les consommateurs tirent parti d'applications concrètes. Et si certains secteurs (fabrication, agriculture, commerce de détail et santé) sont mieux placés pour en profiter, tous les domaines y gagneront.

Pour les CPA, la grande quantité de données disponibles en temps réel améliore la précision des travaux de planification et de prévision. Plus les objets sont aptes à communiquer, plus l'information (p. ex., les niveaux de stocks) devient précise et utile. La fraude devient plus difficile à commettre, mais aussi plus facile à détecter lorsqu'on réduit les interventions humaines. L'IdO permet aussi la maintenance prédictive des machines, grâce à laquelle les CPA pourront mieux savoir quand une machine a besoin d'entretien et prévoir le budget nécessaire. Les CPA doivent comprendre comment l'IdO transforme les entreprises qu'elles conseillent ainsi que les changements qui devront être apportés à leurs systèmes financiers.

Avantages et considérations pour les entreprises

Selon un sondage du Forum économique mondial, 68 % des répondants considéraient que l'IdO a joué un rôle stratégique ou transformateur pour leur entreprise.

En tête des avantages de ce nouveau phénomène, ils citent l'accroissement de la productivité, l'automatisation des processus et l'optimisation de la chaîne de valeur⁵.

EXEMPLES D'APPLICATIONS

L'utilisation de capteurs IdO **dans les milieux de la fabrication et du commerce de détail** améliore la gestion des actifs. Les données permettent en effet de réduire les pertes et le gaspillage, d'utiliser pleinement la chaîne d'approvisionnement et les tablettes, d'accroître l'efficacité de la main-d'œuvre et d'améliorer l'expérience client. Par exemple, dans une boutique, l'IdO servira à faire le suivi des stocks en temps réel, à diminuer le travail de tri nécessaire et à repérer facilement des articles manquants, améliorant ainsi l'expérience client.

À la ferme, des capteurs mesurent la luminosité, la température, l'humidité de l'air et celle du sol aux fins de l'automatisation des systèmes d'irrigation. Un système d'irrigation fondé sur l'IdO optimise l'utilisation de l'eau et le rendement des cultures tout en réduisant les charges et en augmentant les revenus.

Les capteurs **dans les avions commerciaux**, utilisés en parallèle avec l'analyse des journaux d'entretien et des messages de défaillance, permettent aux compagnies aériennes d'éviter des annulations et des retards onéreux, grâce à la maintenance prédictive. Par exemple, l'outil de maintenance prédictive de PwC peut prévoir de 15 % à 30 % des annulations et retards dus à la maintenance, améliorant de 0,3 % à 0,6 % le respect des horaires⁴. La maintenance prédictive pourra aussi être utilisée dans d'autres secteurs.

4 www.pwc.com/us/en/industries/transportation-logistics/airlines-airports/predictive-maintenance.html

5 www.weforum.org/agenda/2015/06/what-are-the-business-benefits-of-the-internet-of-things/

- **Accroissement de la productivité**

Le recours aux appareils intelligents appropriés permet aux entreprises de prévoir les bris d'équipement et d'effectuer les opérations de maintenance préventive nécessaires sans nuire à leurs activités, ce qui diminue les retards causés par la maintenance et améliore la rapidité de livraison des produits et services.

- **Automatisation des processus**

Programmés à réagir à certaines conditions, les appareils IdO peuvent lancer des processus, éliminant ainsi toute intervention humaine. Par exemple, des capteurs peuvent détecter l'arrivée de stocks à l'entrepôt et automatiquement recueillir l'information pertinente et l'envoyer au système de suivi des stocks.

- **Optimisation de la chaîne de valeur**

Les appareils IdO donnent un meilleur aperçu de l'ensemble de la chaîne de valeur (de la planification à l'ordonnancement des stocks), vue comme un système unifié. L'information précise obtenue et le suivi effectué en temps réel aident la direction à prendre des décisions axées sur les données, ce qui a pour effet d'améliorer la gestion des stocks et de réduire le gaspillage.

En plus de ces avantages, citons deux possibilités qu'offre l'IdO.

- **Amélioration de l'expérience client**

Les fabricants d'appareils intelligents peuvent fournir des mises à jour des microprogrammes intégrés aux appareils, en fonction des commentaires des clients, afin d'en améliorer le fonctionnement, ou encore fournir un soutien proactif pour tout bris imminent, favorisant une meilleure expérience client.

- **Création de nouveaux modèles d'affaires**

Comme toute nouvelle technologie, l'IdO peut perturber les modèles d'affaires existants ou permettre d'en créer de nouveaux. Des entreprises numériques comme Google ont mis au point des caméras et des capteurs de sécurité en réseau pouvant remplacer les systèmes d'alarme pour la maison.

Malgré tous les avantages que présente le recours à des appareils intelligents en entreprise, certains risques importants doivent être pris en compte afin de dégager toute la valeur de l'IdO.

Secteurs de risque	Stratégies d'atténuation des risques
<p>Les appareils IdO pourraient accroître les menaces à la sécurité pour les raisons suivantes :</p> <ul style="list-style-type: none">• Logiciels ou microprogrammes dépassés;• Absence de chiffrement des données transmises;• Processus d'authentification peu rigoureux;• Utilisation de mots de passe d'administrateur prédéfinis.	<ul style="list-style-type: none">• Les appareils IdO doivent être traités comme tout autre appareil en réseau, donc être protégés par un chiffrement adéquat et munis de mesures de sécurité aux endroits clés.• Si possible, l'équipement doit venir d'un fabricant ou d'un fournisseur de services IdO connu et digne de confiance. Les logiciels/microprogrammes doivent être mis à jour régulièrement.• Les mots de passe d'administrateur prédéfinis par le fabricant doivent être remplacés par des mots de passe qui respectent les politiques internes des TI.
<p>Les données stockées dans le nuage et gérées par un fournisseur de services IdO pourraient ne pas être adéquatement protégées.</p>	<ul style="list-style-type: none">• L'entreprise doit indiquer au fournisseur toute exigence particulière relative à la sécurité et à la protection des données, notamment les contrôles relatifs au stockage et à la transmission des données, ainsi que l'accès à celles-ci ou les exigences concernant les avis à fournir en cas d'atteinte à la sécurité.• Le fournisseur de services doit accepter, par contrat, les exigences précises relatives à la sécurité infonuagique.• Le fournisseur de service doit fournir un rapport de certification établi par un tiers sur la sécurité infonuagique et, au besoin, sur la confidentialité des données et le respect des obligations contractuelles.• Afin de réduire le nombre de données sensibles transmises, l'informatique en périphérie peut servir à traiter les données sur un appareil local. Par exemple, les données relatives aux fonctions Face ID ou Touch ID d'Apple sont conservées dans votre appareil; la vérification est faite localement sans qu'aucune donnée soit transmise aux serveurs d'Apple ou traitée par ceux-ci.

Secteurs de risque	Stratégies d'atténuation des risques
Les infrastructures de réseau pourraient ne pas répondre aux besoins des appareils IdO en bande passante.	<ul style="list-style-type: none">• Tous les appareils intelligents utilisent une partie de la bande passante disponible sur le réseau. Devant l'augmentation du nombre d'appareils intelligents sur leur réseau, les entreprises doivent s'assurer d'avoir suffisamment de bande passante pour soutenir les échanges d'information entre les appareils IdO et leurs applications principales. Autrement, des pannes de réseau pourraient nuire à la productivité des employés ou à l'expérience client.• Le recours à l'informatique en périphérie permet de transférer le traitement des données générées par les appareils IdO du nuage à l'appareil, réduisant ainsi les besoins en bande passante.
Une atteinte à la sécurité des données de l'IdO pourrait toucher des renseignements permettant d'identifier une personne.	<ul style="list-style-type: none">• Règle générale, les données stockées doivent être chiffrées et ne pas comprendre de renseignements personnels afin de minimiser les conséquences des vols d'information résultant d'une atteinte à la sécurité des données.• Si des renseignements permettant d'identifier une personne doivent être recueillis et stockés, il faut s'assurer de se conformer aux lois applicables, par exemple la <i>Loi sur la protection des renseignements personnels et les documents électroniques</i> (LPRPDE), au Canada, ou le Règlement général sur la protection des données, en Europe.• Un plan d'intervention en cas d'atteinte à la sécurité des données doit être en place et comprendre la marche à suivre pour :<ul style="list-style-type: none">— limiter l'incident;— évaluer les risques liés à l'incident;— avertir les personnes touchées;— éviter tout autre incident semblable.
Les employés pourraient accéder, sans autorisation, aux appareils IdO à l'aide de leurs appareils mobiles personnels.	<ul style="list-style-type: none">• Les appareils IdO doivent être sur un réseau privé, séparé du réseau auquel les employés ont accès pour leur appareil personnel.• Pour assurer la sécurité des appareils IdO, les mots de passe prédéfinis par le fabricant doivent être remplacés par des mots de passe conformes aux politiques internes des TI.

Secteurs de risque**Stratégies d'atténuation des risques**

Les employés pourraient accéder physiquement, sans autorisation, aux appareils IdO.

- La revue périodique des appareils IdO permet de s'assurer que le matériel n'a pas été altéré.
- Les appareils IdO devraient être conservés dans un endroit dont l'accès est sécurisé et limité aux personnes autorisées.
- Il est conseillé de passer périodiquement en revue l'historique des opérations des appareils et de pousser les analyses si l'appareil a été mis hors ligne. Habituellement, l'altération d'un appareil de façon malveillante nécessite de le mettre hors ligne et de le redémarrer.

La présente publication s'inscrit dans la [série Tendance technologique](#), qui porte sur les grandes tendances du domaine touchant le milieu comptable. Les documents de cette série sont disponibles sur notre site Web.

AVIS DE NON-RESPONSABILITÉ

Le présent document, préparé par Comptables professionnels agréés du Canada (CPA Canada), fournit des indications ne faisant pas autorité. CPA Canada et les auteurs déclinent toute responsabilité ou obligation pouvant découler, directement ou indirectement, de l'utilisation de ce document.

© 2019 Comptables professionnels agréés du Canada

Tous droits réservés. Cette publication est protégée par des droits d'auteur et ne peut être reproduite, stockée dans un système de recherche documentaire ou transmise de quelque manière que ce soit (électroniquement, mécaniquement, par photocopie, enregistrement ou toute autre méthode) sans autorisation écrite préalable.

Pour demander cette autorisation, veuillez écrire à permissions@cpacanada.ca.