



Pour l'avenir : Un balado de KPMG sur la cybersécurité

Série 1 : Destination : Identité numérique

Épisode 3 : Passer aux choses sérieuses



Imraan Bashir

[extrait]

L'identité numérique changera bien des choses pour les entreprises.

Sylvia Kingsmill

[extrait]

Tout repose sur la confiance. Les entreprises ont une responsabilité unique – assurer la sécurité des données de leurs clients.

Narrateur :

Quelque part à la croisée des chemins entre ce qui est juste et ce qui est rentable, les entreprises canadiennes auront une nouvelle vision des promesses de l'identité numérique.

[SFX – Chanson thème]

Hartaj Nijjar

Voici le balado « Pour l'avenir », qui explore la cybersécurité dans les entreprises d'aujourd'hui, de demain et de l'avenir.

Je m'appelle Hartaj Nijjar et je suis le leader national du groupe Cybersécurité de KPMG au Canada. Parcourez avec moi le monde de la cybersécurité, découvrons ce que l'avenir nous réserve et comment nous pouvons travailler ensemble pour le protéger.

[SFX - Crescendo et chanson thème]

Narrateur :

Je m'appelle Tamara Stanners et je suis votre hôte. Au cours des deux derniers épisodes, nous avons discuté du rôle important des pièces d'identité dans la vie quotidienne des Canadiens, et nous avons souligné l'impact que pourrait avoir l'émergence de systèmes d'identité numérique sur les citoyens.

Mais qu'est-ce que le passage à l'identité numérique signifiera pour les entreprises? C'est ce que nous explorerons dans cet épisode.

Avec la numérisation des services publics et privés et les attentes croissantes des clients, les organisations du monde entier ont accès à plus de données que jamais auparavant. Et à mesure que les préoccupations en matière de confidentialité augmentent et que la surveillance réglementaire s'intensifie, il est primordial de

connaître et de comprendre vos données.

Dans le but d'apprendre quels types de données nécessitent une protection, examinons deux cas d'utilisation clé des données relatives à l'identité dans une entreprise typique.

Marc Chaput – 1

Les entreprises utilisent actuellement les renseignements personnels de deux façons principales.

Narrateur

Voici Marc Chaput, spécialiste, Gestion des identités et des accès de KPMG.

Marc Chaput – 2

Le premier cas d'utilisation est celui de toute organisation engagée dans une relation d'affaires avec un client et qui doit gérer ses renseignements personnels.

Le deuxième cas d'utilisation très important – la gestion des effectifs d'une organisation. Il y a beaucoup de processus RH qui sous-tendent le traitement de données personnelles sur les employés.

Narrateur :

Peu importe le type de données d'identité, il est important de les recueillir de façon éthique et de les stocker de façon sécuritaire.

Imaginez que vous magasinez sur Internet et que vous tombez sur une nouvelle boutique en ligne fantastique qui vend, disons, des arrangements floraux. Comme le shower pour bébé de votre cousine s'en vient, vous choisissez le bouquet parfait et commencez à remplir le bon de commande. Vous fournissez vos renseignements de paiement, nom, adresse et courriel. Ça semble assez inoffensif. Mais, avec le recul, pensez-y : Où vont toutes ces données personnelles? Où sont-elles stockées? Qui y a accès? Dans quelle mesure sont-elles protégées?

Les entreprises ont une responsabilité importante dans la sécurité des données de leurs clients.

Sylvia Kingsmill

Du côté du client, il y a d'énormes risques en ce qui concerne la collecte excessive et l'utilisation ultérieure des renseignements personnels.

Narrateur :

Voici Sylvia Kingsmill, leader mondiale, Cybersécurité chez KPMG.

Sylvia Kingsmill

Donc le problème, c'est de savoir qui a accès à quoi et en vertu de quels règlements sur la protection des renseignements personnels. Le client a-t-il l'occasion de fournir un consentement éclairé? Le client doit comprendre le but pour lequel vous recueillez ses renseignements personnels. L'utilisation ultérieure de ces données est très restreinte; elles ne devraient l'être qu'à des fins professionnelles autorisées par la loi.

Si les données ne sont pas stockées et protégées au moyen de mesures de sécurité adéquates, il y a un risque de violation. Le défi réside aussi dans la gestion des identifiants des clients. Vous pouvez faire beaucoup de choses avec des renseignements personnels – des utilisations inappropriées ou contraires à la loi. Il est donc vraiment important que les organisations protègent l'information qu'elles recueillent.

Narrateur :

L'expression à retenir ici est « collecte excessive ». Non seulement cette pratique comporte-t-elle des risques, elle est aussi la cause de nombreux problèmes. Les utilisateurs se retrouvent dans une situation où ils doivent partager les mêmes données, encore et encore, avec différentes organisations. Ces dernières doivent investir davantage en cybersécurité pour protéger l'information sensible qui est stockée à différents endroits. Il en résulte une hausse des risques de violation de la vie privée et une exposition accrue à des procédures inutiles de profilage et de suivi.

L'établissement de relations solides avec vos clients suppose de gagner et de conserver leur **confiance**, ce que l'avènement de l'identité numérique est appelé à renforcer.

Sylvia Kingsmill

Pour les propriétaires d'entreprise, il s'agit d'offrir aux clients une expérience optimale et transparente. Ils veulent des clients heureux. C'est aussi une question de confiance. Les entreprises auront confiance que les renseignements obtenus sont authentiques; leur exposition au risque sera donc réduite. En fait, elles n'auront pas à se soucier du coût et des conséquences d'une violation. C'est donc non seulement plus facile pour le client, c'est aussi plus facile pour les entreprises d'avoir une identification numérique plus sécurisée, parce que les solutions actuelles, comme numériser votre permis de conduire et l'envoyer par courriel, ne sont pas pratiques, ni pour vous, ni pour le destinataire, et aussi vraiment peu sûres.

Les clients auront l'impression d'être en contrôle, n'est-ce pas? Parce qu'ils peuvent partager des données au besoin, ils peuvent aussi révoquer leur consentement. Et pour l'organisation, gardienne des données, la collecte de l'information est non seulement conforme à ses obligations et à la loi sur la protection des renseignements personnels, mais elle fait la bonne chose pour ses clients.

Narrateur :

Clients fidèles, transactions de confiance et importantes réductions de coûts.

Réfléchissez-y, lorsque toutes les pièces d'identité pourront être liées à une source fiable plutôt que de dépendre de multiples solutions individuelles, cela permettra aux entreprises de se débarrasser de la responsabilité de vérifier constamment l'identité de leurs clients, ce qui signifie plus de temps libre et plus de ressources pour se concentrer sur la prospérité de leur entreprise.

De plus, le fait d'accélérer la mise en œuvre de l'identité numérique pourrait présenter un avantage concurrentiel important, comme l'explique Imraan Bashir dans l'épisode 1.

Imraan Bashir

L'identité numérique changera les choses pour les entreprises. Entre une entreprise qui offre un accès instantané et plus transparent à ses services parce qu'elle accepte les pièces d'identité numériques, et une entreprise qui envoie un code par la poste pour que vous puissiez utiliser ses services en ligne par la suite – ou qui vous demande de passer en personne – laquelle choisirez-vous? Dans tous les cas, la première entreprise.

Narrateur :

Comme Marc Chaput l'a mentionné, en plus des données sur les clients, un autre type d'information clé que les entreprises mettent à profit est l'information sur leurs employés – un processus assorti d'un ensemble de considérations uniques.

Marc Chaput – 3

La gestion des données sur les employés pose quelques défis.

Narrateur :

C'est encore Marc.

Marc Chaput – 4

Le premier défi se pose quand une organisation veut embaucher de nouveaux talents dans ce monde nouveau créé par la pandémie. Certaines organisations embauchent des personnes sans qu'elles aient à se présenter sur place. Donc elles doivent être capables de vérifier leur identité.

Un autre défi très important se présente lors du processus d'embauche, où de nombreux renseignements nécessaires et doivent être vérifiés. Par exemple, les antécédents et les renseignements bancaires et autres pour la paie. Il y a plusieurs processus qui impliquent la collecte, la manipulation et le stockage des renseignements personnels des employés.

Et le troisième défi, tout aussi important, réside dans l'accès à vos systèmes. Vous devez accorder les droits d'accès nécessaires pour le poste du nouvel employé, pas plus.

Narrateur :

Bien sûr, il existe aujourd'hui de nombreuses mesures de protection pour s'assurer que les nouveaux employés et les employés actuels sont bien ceux qu'ils affirment être. Les équipes des RH de partout au Canada déploient des efforts considérables pour simplifier les processus d'embauche, d'accueil et de cessation d'emploi.

Mais ces processus demeurent en grande partie manuels et répétitifs. Ainsi, l'identité numérique prend tout son sens. Examinons un scénario.

Dramatisation 3.1 – Nouvel employé

FONDU :

SFX – Bureau. Clavier. Conversations. Gobelets pour refroidisseur d'eau.

NATASHA

As-tu entendu parler de l'employé qui s'est fait prendre par les RH?

JUNG

Oui, j'ai entendu dire que c'était le deuxième cette semaine, depuis le lancement du nouveau système d'identification.

NATASHA (CHOQUÉE)

Vraiment? J'avais évidemment entendu parler de gens qui embellissent leur CV, mais je ne savais pas que c'était si courant!

JUNG

Honnêtement, je ne suis pas si surpris. Avant la mise en place du système centralisé, qui prenait le temps de vérifier si un diplôme était authentique? Je pourrais me créer un diplôme d'Harvard en cinq minutes avec Photoshop.

(ton feutré)

Ne le dis à personne, mais pour mon premier emploi chez Purple Juice quand j'avais 16 ans, j'ai menti sur mon CV; j'avais inscrit que j'avais déjà travaillé dans un café auparavant. Ils m'ont embauché et j'ai quand même fait des suuuuper jus...

NATASHA

(rires) Ton secret est en sécurité avec moi.

Mais évidemment, ici c'est bien différent. Je n'arrive pas à croire qu'il ait non seulement menti sur son université, mais aussi sur son expérience de travail en tant que cadre!

JUNG

Imagine qu'on lui ait offert le poste de directeur principal; il n'aurait pas su quoi faire.

NATASHA

Ce que les gens font quand ils pensent qu'ils ne se feront pas prendre me fascine.

JUNG

Sauf que maintenant, ils se font prendre.

Fin de la scène

Narrateur :

Lorsque nous disposons de sources fiables et de moyens de validation continus, la fraude devient beaucoup plus facile à détecter. Cela peut dissuader les fraudeurs.

En plus de favoriser l'attraction des talents, l'identité numérique améliorera d'autres facettes des RH.

Marc Chaput

Il y a un moyen d'être plus efficace dans la façon dont nous nous accueillons les nouveaux employés. Nous disposerons d'un outil source fiable qui éliminera la nécessité de stocker des fichiers temporaires ou des copies des pièces d'identité papier des

employés.

Cela permettra également de mieux évaluer les droits d'accès à accorder en fonction des besoins.

Narrateur :

Pensez à un scénario où la gestion des accès pourrait être le point de rupture d'une interaction avec le client.

Dramatisation 3.2 – Le plancher sécurisé

FONDU :

SFX – Bureaux occupés. Sons de clavier. Des pas qui se rapprochent.

HARJIT

Meredeth, c'est fait!

Le contrat est signé. Halper et son équipe se dirigent à l'étage sécurisé en ce moment même.

MEREDETH (EXCITÉE)

Épatant! Vous avez réussi! C'est une nouvelle incroyable. C'est un énorme contrat, qui fait aussi l'objet d'une grande visibilité.

HARJIT

Oui, et le grand patron veut que tu fasses partie de l'équipe du client.

MEREDETH (SURPRISE)

Tu plaisantes! C'est incroyable! Merci beaucoup d'avoir parlé de moi.

HARJIT

Bien sûr, tu es la meilleure personne pour le poste et tu l'as mérité. As-tu une réunion de prévue maintenant? Si oui, annule-la et viens avec moi.

MEREDETH

Bien sûr!

SFX – Les deux commencent à marcher. On voit des personnes qui marchent (homme et femme). Sonnerie d'ascenseur, les portes s'ouvrent. Les deux y entrent. Les portes se referment.

VOIX DE L'ASCENSEUR

Nous montons.

MEREDETH

Attends, as-tu dit qu'ils se rencontrent à l'étage sécurisé?

HARJIT

Oui, au 28e.

MEREDETH

Oh, mais mon habilitation de sécurité n'a pas encore été transférée de mon ancien service.

HARJIT

C'est déjà fait. Il n'a fallu qu'une minute pour obtenir les approbations.

Il y a un an, ce transfert aurait été un cauchemar. Maintenant, c'est presque en temps réel.

VOIX DE L'ASCENSEUR

Vingt-huitième étage.

SFX – Les portes d'ascenseur s'ouvrent. Les deux sortent.
Balayage de la carte. Bip d'approbation. La porte s'ouvre.

MEREDETH

Clairement une amélioration! Je suis contente de pouvoir être là pour le client sans avoir à lui expliquer qu'une habilitation de sécurité m'a retardée...

[Fin de la scène]

Narrateur :

Il n'y a pas de deuxième chance de faire une première impression. Pour établir de solides relations avec les clients, il faut adopter des technologies qui accélèrent les processus administratifs en toute sécurité et qui permettent de s'assurer que vos employés

sont là où ils doivent être au bon moment.

Dans cet épisode, nous avons exploré quelques façons dont l'avènement de l'identité numérique pourrait profiter aux entreprises. Comme pour toute technologie, l'identité numérique ne sera pas la solution magique qui aplanit toutes les difficultés et résout tous les problèmes d'accès internes. Elle offre toutefois la possibilité d'améliorer la sécurité des données, de réduire les coûts d'acquisition, d'accroître l'efficacité et de renforcer les relations avec les clients. Mais concrétiser ce potentiel dépendra de la façon dont nous construisons le pont entre aujourd'hui et demain.

Écoutez le quatrième et dernier épisode de cette série pour en savoir plus.

Je suis Tamara Stanners, votre hôte, et vous venez d'écouter Pour l'avenir : Un balado de KPMG sur la cybersécurité. À bientôt.