FORTIFICATION DU SYSTÈME DE RETRAITE

Préparons les prochains 150 ans

CONGRÈS NATIONAL 2018 DE L'ACARR

ACPM | ACARR

Ville de Québec, QC

Fairmont Le Château Frontenac

DU 11 AU 13 SEPTEMBRE 2018

www.acpm-acarr.com

COMMANDITAIRE DIAMANT ›

Desjardins Assurances

Vie · Santé · Retraite

Atelier 6

À chaque Bitcoin ses deux faces :
Occasions et risques des avancées technologiques

Conférenciers :
Jean-François Allard, *KPMG*

Renée LaFlamme, *iA Financial Group*

Modératrice :
Danelle Parkinson, *Ontario Pension Board*

Les deux côtés de la médaille : les opportunités et les risques reliés à l'avancement de la technologie

Renée Laflamme, vice-présidente exécutive, iA Groupe financier

Jean-François Allard, associé, Services de cybersécurité, KPMG Canada

La technologie au service des gens : repenser l'expérience client

Renée Laflamme
Vice-présidente exécutive
iA Groupe financier


amazon
PrimeAir

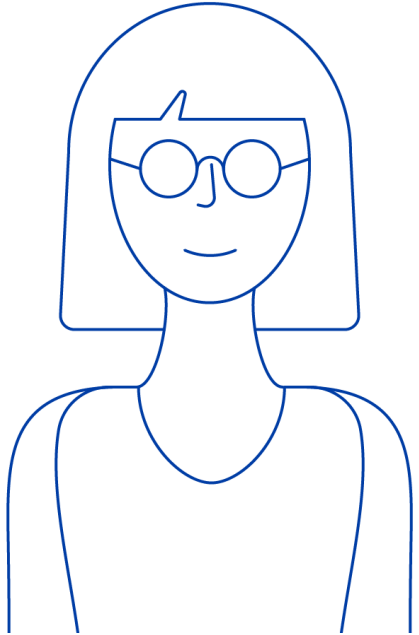
Le constat

ACPM | ACARR

KPMG

iA Groupe financier

La communication client : avant et après



Unidirectionnel ⇨ Interactif

Passif ⇨ Participatif

Standardisé ⇨ Personnalisé

Temps fixe ⇨ Temps réel

⇨ Interactif

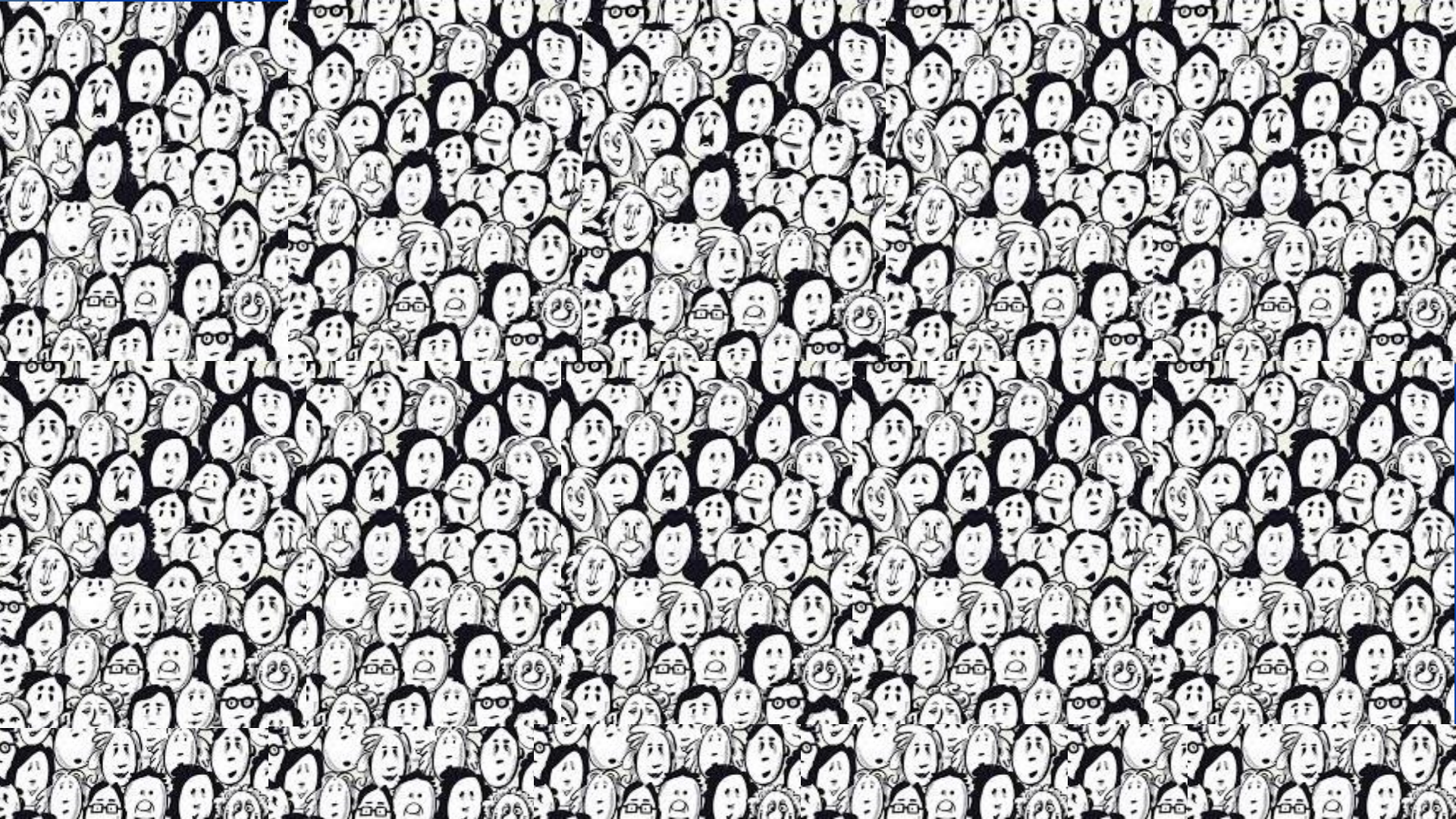
⇨ Participatif

⇨ Personnalisé

⇨ Temps réel

Proximité

Comment évolue la communication client?



Service personnalisé.


Google


amazon


Microsoft

L’apprentissage-machine

Technologie d’intelligence artificielle qui permet aux systèmes d’apprendre et de s’améliorer grâce à l’expérience.

ACPM | ACARR

KPMG

iA Groupe financier

Nouveau concept d’assistance virtuelle

Reconnaissance de la voix

Apprentissage-machine

Détection des émotions

Détection des intentions

Je viens de me marier

Je change d'emploi

J'attends un bébé!

Comment puis-je atteindre mon objectif de retraite?

Est-ce qu'il y a des tâches à compléter?

J'ai eu une promotion

J'achète une maison

ACPM | ACARR

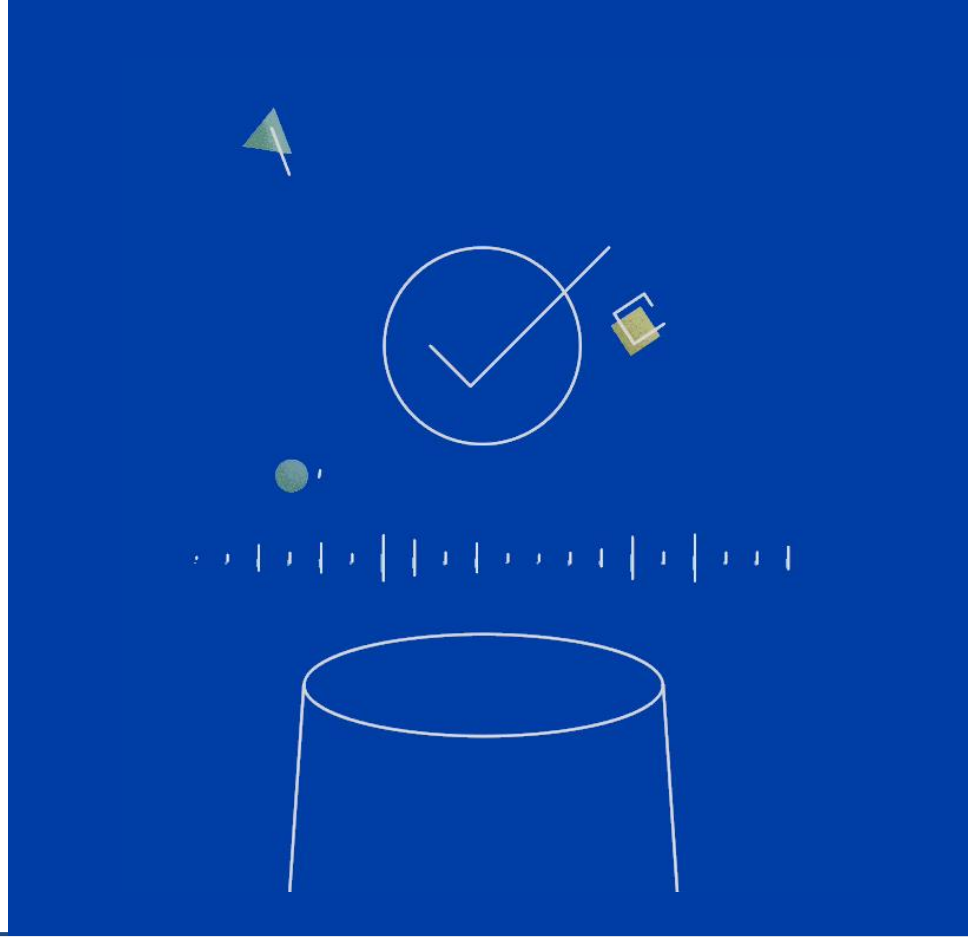
KPMG

iA Groupe financier

73 % des Canadiens

aimeraient compléter des tâches en **parlant avec un assistant virtuel.**

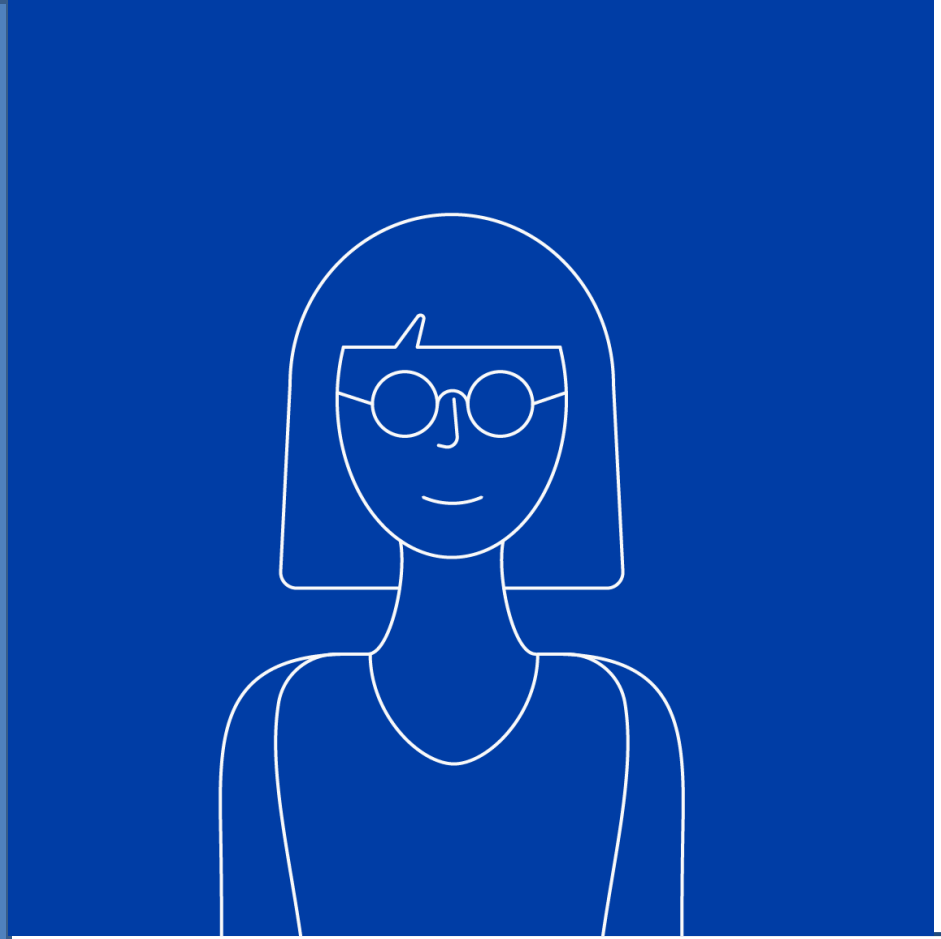
Google



ACPM | ACARR

KPMG

iA Groupe financier

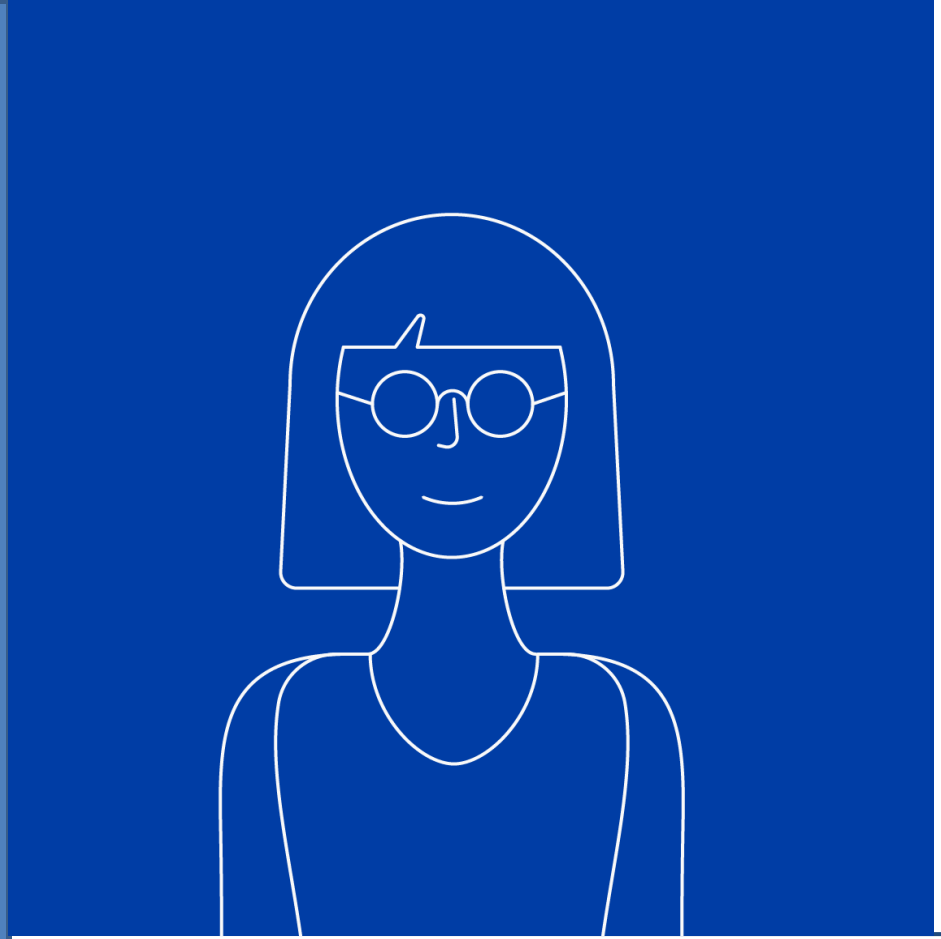


70 % des propriétaires de téléphones intelligents aimeraient accomplir des tâches **par commande vocale** au lieu de **taper** sur un clavier ou de **toucher** un écran.

ACPM | ACARR

KPMG

IA.A.I Groupe financier



D’ici 2020, les **algorithmes** auront **modifié le comportement** de milliards de travailleurs dans le monde.

Gartner

ACPM | ACARR

KPMG

iA Groupe financier

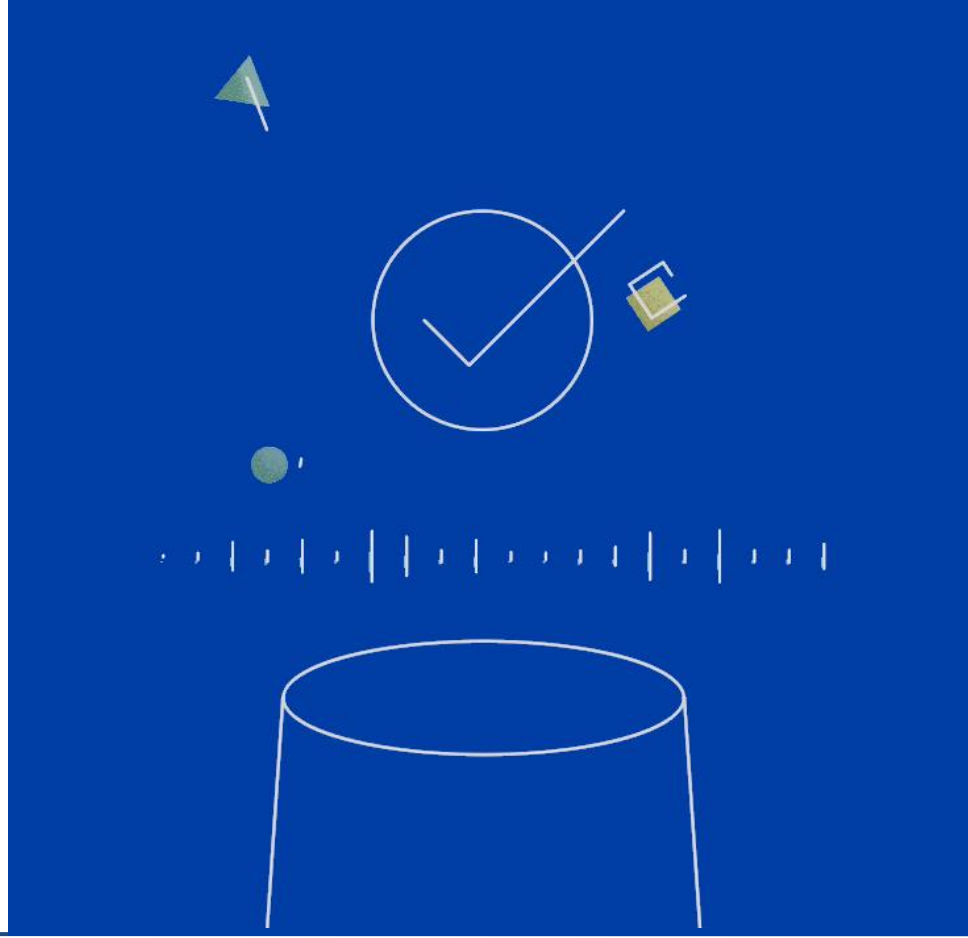
D’ici 2020,

30 % des visites

sur le Web se feront

sans écran.

Gartner

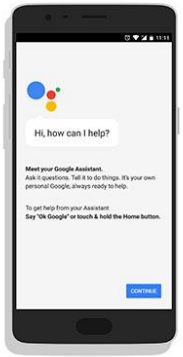


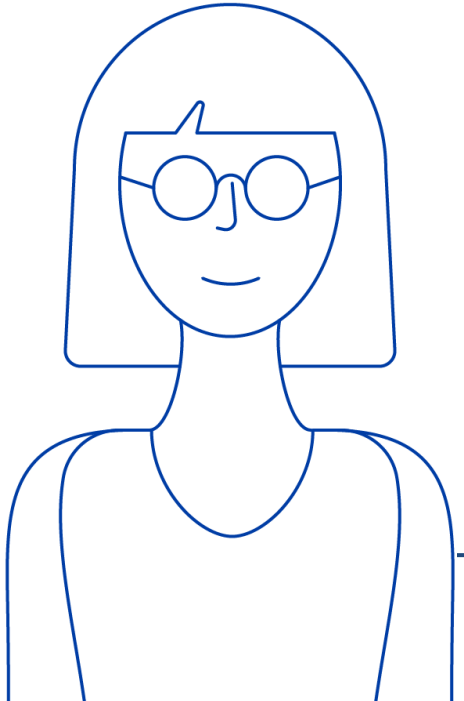
ACPM | ACARR

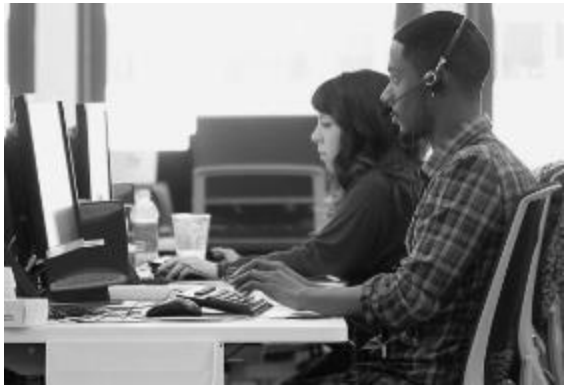
KPMG

iA Groupe financier

La technologie au service de l’humain







ACPM | ACARR

KPMG

iA Groupe financier

Faire face aux nouvelles menaces en cybersécurité

Jean-François Allard
Associé, Services de cybersécurité
KPMG Canada

Ordre du jour :

1. Évolution de la cybercriminalité
2. Les attentes du conseil d’administration

Définition

Qu'est-ce que la cybercriminalité?

– Selon la Gendarmerie Royale du Canada, elle se divise en deux types :

La cible est la technologie

- Piratage à des fins criminelles
- Réseaux zombies et installation de logiciels malveillants (*malware*)
- Dénis de services distribués (DDos)
- Rançonnage

La technologie est l'instrument

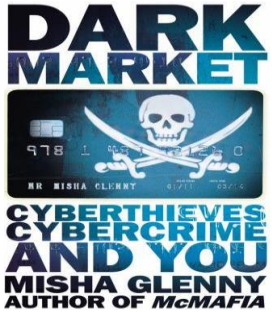
- Le vol et la fraude
- Le vol d'identité
- La violation de propriété intellectuelle
- Le blanchiment d'argent
- Le trafic de drogues
- La traite de personnes
- La cyberintimidation

Mise en contexte

Pourquoi y a-t-il recrudescence de la cybercriminalité?

– Essentiellement cinq phénomènes sont responsables :

1. Numérisation de l'économie
2. Dépendance importante aux infrastructures TI critiques
3. Habilité accrue des jeunes avec les TI
4. Apparition en 2010 d'un protocole de communication appelé « TOR » et anonymisation des échanges sur Internet
5. Apparition du marché noir électronique (*dark market*)



Qui sont les acteurs?

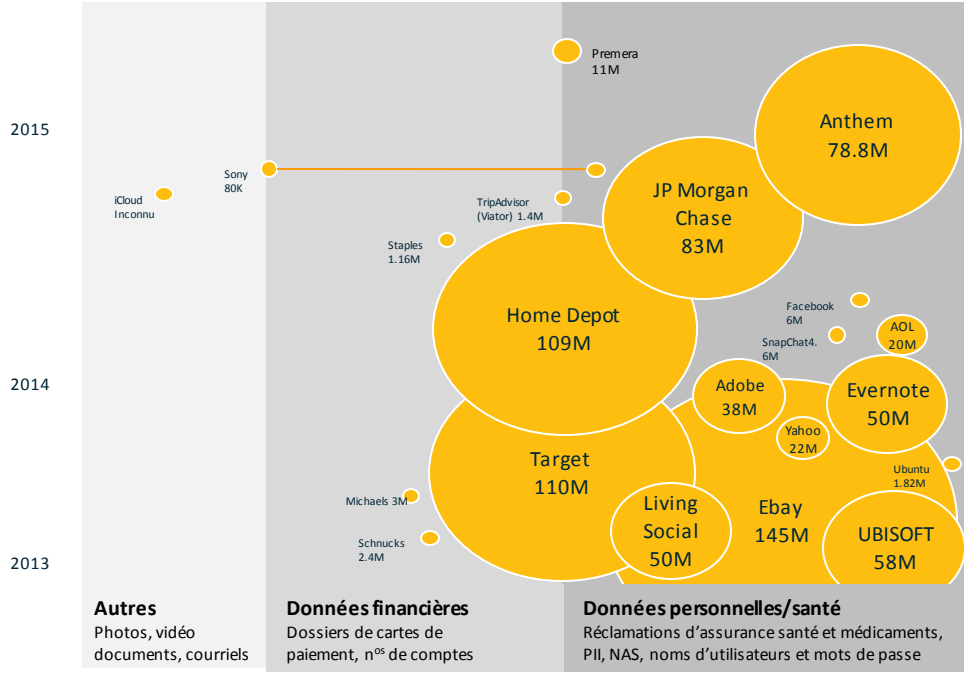
Petits criminels / Motifs : gains financiers

Hacktivistes / Motifs : soutien politique

Crime organisé / Motifs : gains financiers

États / Motifs : stratégie politique

Cybersécurité : les plus grands incidents



Les plus importantes fuites de données
2013 – aujourd'hui
Nombre de brèches par entreprise reconnue et par type de données (>1 M dossiers)

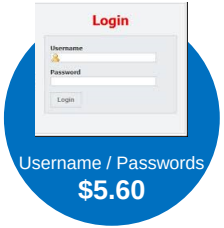
Références :
http://blogs.wsj.com/corporate-intelligence/2014/03/28/whats-more-valuable-a-stolen-twitter-account-or-a-stolen-credit-card/

http://blogs.wsj.com/riskandcompliance/2013/06/26/passwords-more-valuable-than-credit-card-data/

http://www.foxbusiness.com/technology/2014/01/15/e-bazaar-crooks-hawk-your-info-in-online-black-market/

Combien vaut votre identité sur Internet?

- Prix en dollars US de données volées dans le marché noir



Username / Passwords
$5.60

Debit Card (#)
$9.55

Health Record / SSN
$47.62

Loyalty Rewards
$.50 for 50k points

Social Media
$.05 - $8.00

Credit Card (#)
$.25 - $100

References:

- http://blogs.wsj.com/corporate-intelligence/2015/03/28/whats-more-valuable-a-stolen-twitter-account-or-a-stolen-credit-card/
- http://blogs.wsj.com/riskandcompliance/2013/06/26/passwords-more-valuable-than-credit-card-data/
- http://www.tripwire.com/state-of-security/vulnerability-management/how-stolen-target-credit-cards-are-used-on-the-black-market/
- http://www.foxbusiness.com/technology/2015/01/15/e-bazaar-crooks-hawk-your-info-in-online-black-market/
- http://www.theregister.co.uk/2015/11/05/hilton_honor_cards_breached/

Pourquoi est-ce un défi pour les organisations?

Stratégie de sécurité :

- La fonction sécurité opère de façon indépendante et isolé de la stratégie d'affaires de l'organisation. La sécurité est perçue comme un frein à l'innovation.

La base de la sécurité :

- Les organisations ne maîtrisent toujours pas les pratiques de base de la sécurité. Ces nouveaux enjeux s'ajoutent aux défis existants, ils ne les remplacent pas.

Veille sur les menaces :

- Ne pas rester au fait des dernières menaces et faire évoluer son approche de sécurité en conséquence.

  L'absence d'information sur les menaces les plus importantes empêche de prendre des décisions intelligentes.

Conformité globale :

- Ne pas considérer les lois et réglementations internationales même si vos activités sont locales.

  Ne pas respecter les exigences de conformité pourrait entraîner des sanctions financières, pouvant atteindre jusqu'à 5% de vos revenus, ou même des peines de prison. Adopter un approche réactive face aux enjeux de sécurité est toujours une erreur.

Pourquoi est-ce un défi pour les organisations?

Gestion des fournisseurs :

- Plusieurs incidents de sécurité incluent des fournisseurs.

  Un contrat comportant des clauses de sécurité n'est plus suffisant.

Seulement faire de la prévention :

- Le monde a changé, et la prévention n'est plus suffisante en matière de sécurité.

  Votre organisation doit être en mesure de détecter et répondre adéquatement à des incidents de sécurité.

Faillir à réagir adéquatement :

- Ne pas réagir adéquatement à une brèche de sécurité peut augmenter significativement les pertes financières, l'impact sur la réputation et même les probabilités d'une poursuite.

  Cela peut aussi créer une impression de faiblesse et vous rendre plus vulnérable à d'autres attaques.

La sécurité est vue comme un exercice de conformité :

- Plusieurs organisations qui ont subi des incidents de sécurité approchaient la sécurité comme un exercice de conformité, plutôt que d'appliquer des mesures de protection basées sur les risques. Soyez sécuritaire dès la conception.

Attentes du conseil d'administration

Le rôle du conseil d'administration est essentiel à l'efficacité de la cybersécurité :

- Obtenir et être d'accord avec les réponses aux trois questions fondamentales relatives à la cybersécurité :
  1. Où en sommes-nous?
  2. Où voulons-nous être (votre position de défense)?
  3. Comment pouvons-nous y arriver?
- Ceci ne devrait pas être un débat sur la cybersécurité, mais plutôt une discussion d'affaires sur la protection des actifs de l'entreprise.
- Comprendre la valeur des divers sous-ensembles de données, et s'assurer que les ressources appropriées sont consacrées à la classification et à la sécurisation des actifs les plus critiques.
- S'assurer que la cybersécurité reste un sujet d'actualité et le diviser en trois catégories d'éléments : Information, Action, Décision.
- S'assurer de l'obtention régulière des informations de gestion et indicateurs de performance de la sécurité.
- Demander des rapports périodiques d'incidents de cybersécurité afin de suivre les attaques et les tendances.
- S'assurer que tous les membres du conseil sont conscients qu'ils font partie du risque.
- Participer activement au plan d'intervention de votre entreprise pour les incidents de cybersécurité.
- Évaluer périodiquement les risques de cybersécurité et examiner la nécessité d'une évaluation indépendante.
- Finalement, si un cyber-risque est soulevé, atténuer ou accepter le risque; **ne pas l'ignorer**.

Questions

FORTIFICATION DU SYSTÈME DE RETRAITE

Préparons les prochains 150 ans

CONGRÈS NATIONAL 2018 DE L'ACARR

ACPM | ACARR

Ville de Québec, QC

Fairmont Le Château Frontenac

DU 11 AU 13 SEPTEMBRE 2018

www.acpm-acarr.com

COMMANDITAIRE DIAMANT ›

Desjardins Assurances

Vie · Santé · Retraite