



The Next 150  
**FORTIFYING**  
RETIREMENT FOR THE FUTURE

2018 ACPM  
**NATIONAL**  
CONFERENCE



**Québec City, QC**  
**Fairmont Le Château Frontenac**  
**SEPTEMBER 11-13, 2018**

[www.acpm.com](http://www.acpm.com)

DIAMOND SPONSOR >



**Desjardins**  
Insurance

Life • Health • Retirement

# Workshop 6

## Two Sides to Every Bitcoin: The Opportunities and Risks of Advances in Technology

*Speakers:*

**Jean-François Allard**, *KPMG*

**Renée LaFlamme**, *iA Financial Group*

*Moderator:*

**Danelle Parkinson**, *Ontario Pension Board*

# Two Sides to Every Bitcoin: The Opportunities and Risks of Advances in Technology

Renée Laflamme, Executive Vice-President, iA Financial Group  
Jean-François Allard, Partner, Cybersecurity Services, KPMG Canada

# Technology serving people: reshaping customer experience

**Renée Laflamme**  
**Executive Vice-President**  
**iA Financial Group**

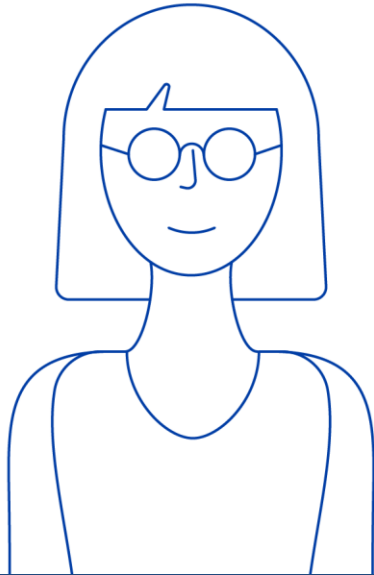




A  
not-so-quick  
reality check



# Client communication: then and now



Unidirectional ⇨ Interactive

Passive ⇨ Participative

Standard ⇨ Personalized

Fixed time ⇨ Real time

⇒ **Interactive**

⇒ **Participative**

⇒ **Personalized**

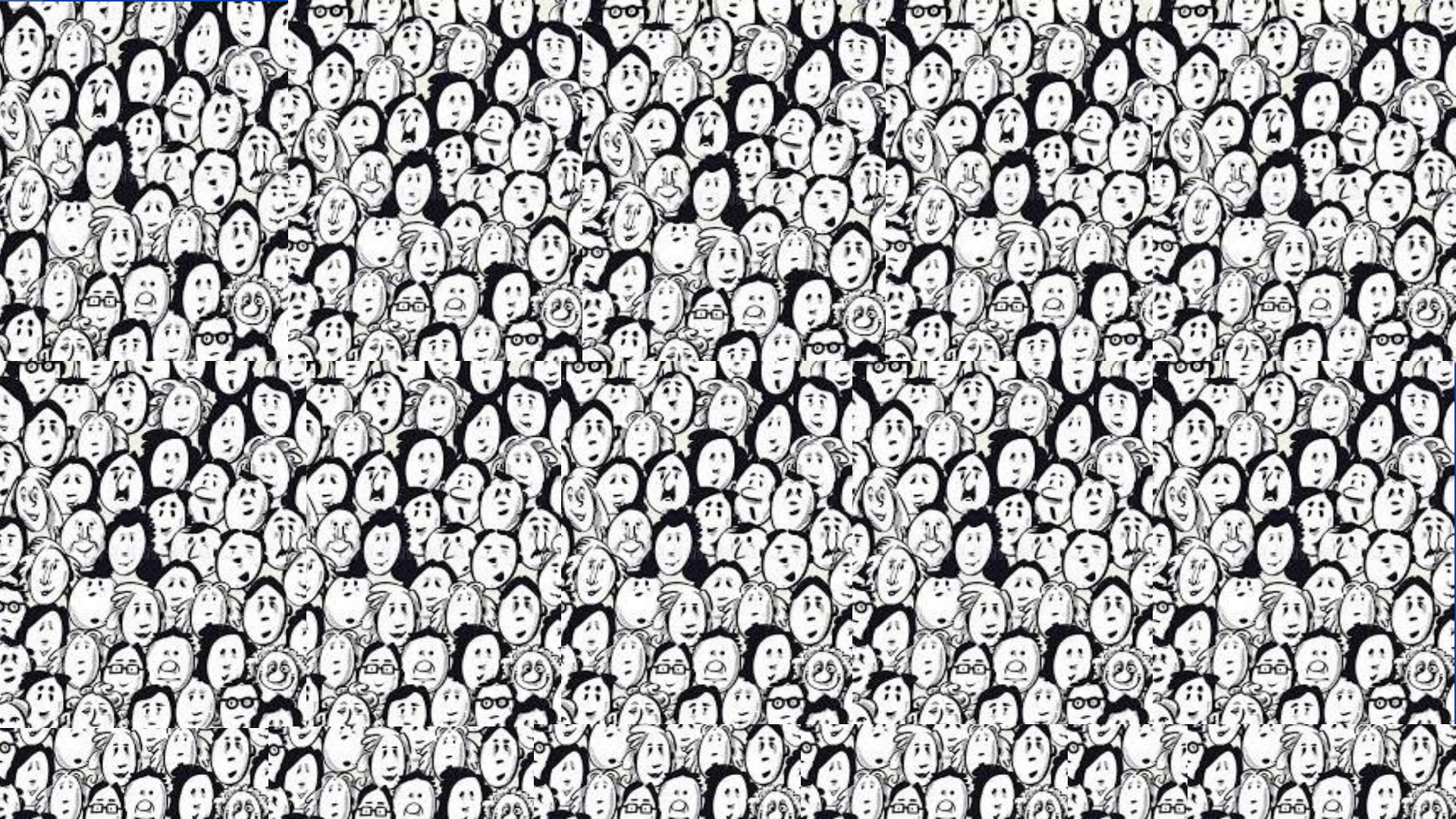
⇒ **Real time**



**Proximity**



What's the future  
of client  
communication?



What's the future  
of client  
communication?

Personalized support.

Google

amazon



 Microsoft



# Machine learning

Artificial intelligence  
technology that allows systems to  
**learn and improve**  
through experience.

# A new concept of virtual assistance

**Technology serving people:**  
reshaping the client experience





Language **recognition**



Machine **learning**



Emotion **detection**



Intention **detection**



I just got married

I'm changing jobs

I'm having a baby!

How can I reach  
my retirement goal?

Do I have  
anything pending?

I got a promotion

I'm buying a house

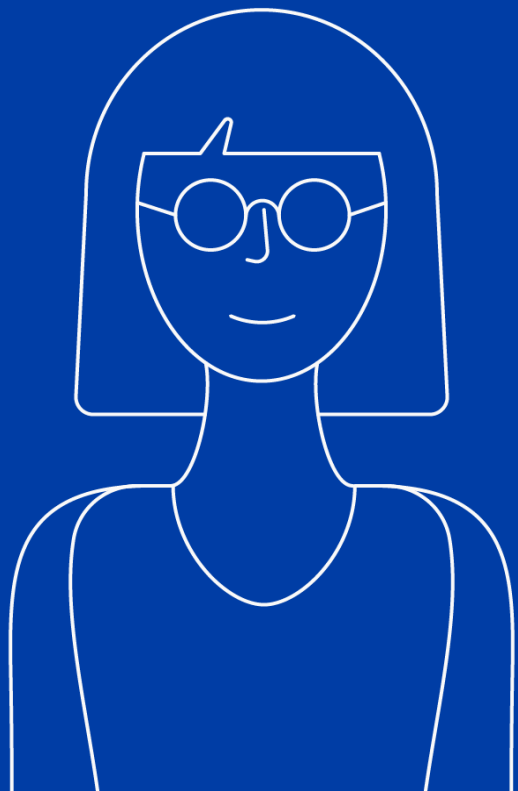
# 73% of Canadians

would like to be able  
to complete tasks by

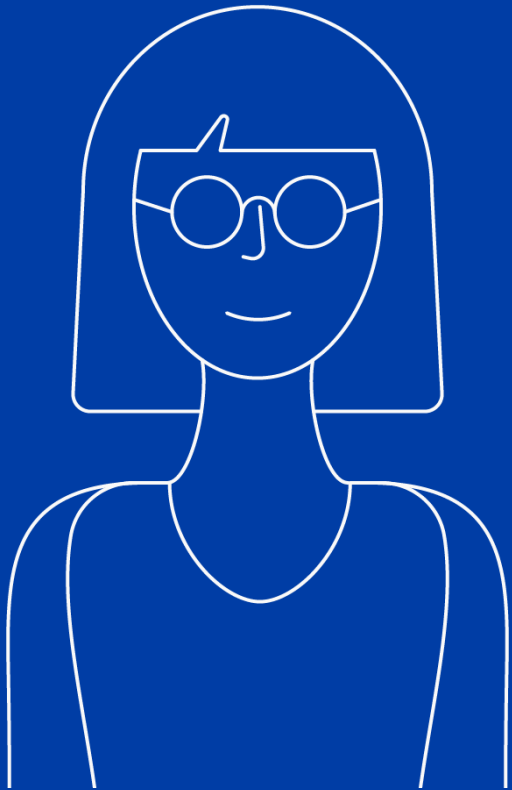
# speaking to a virtual assistant

Google





**70%** of smartphone  
owners  
are interested  
in getting things done  
**by speaking instead  
of typing or touching.**

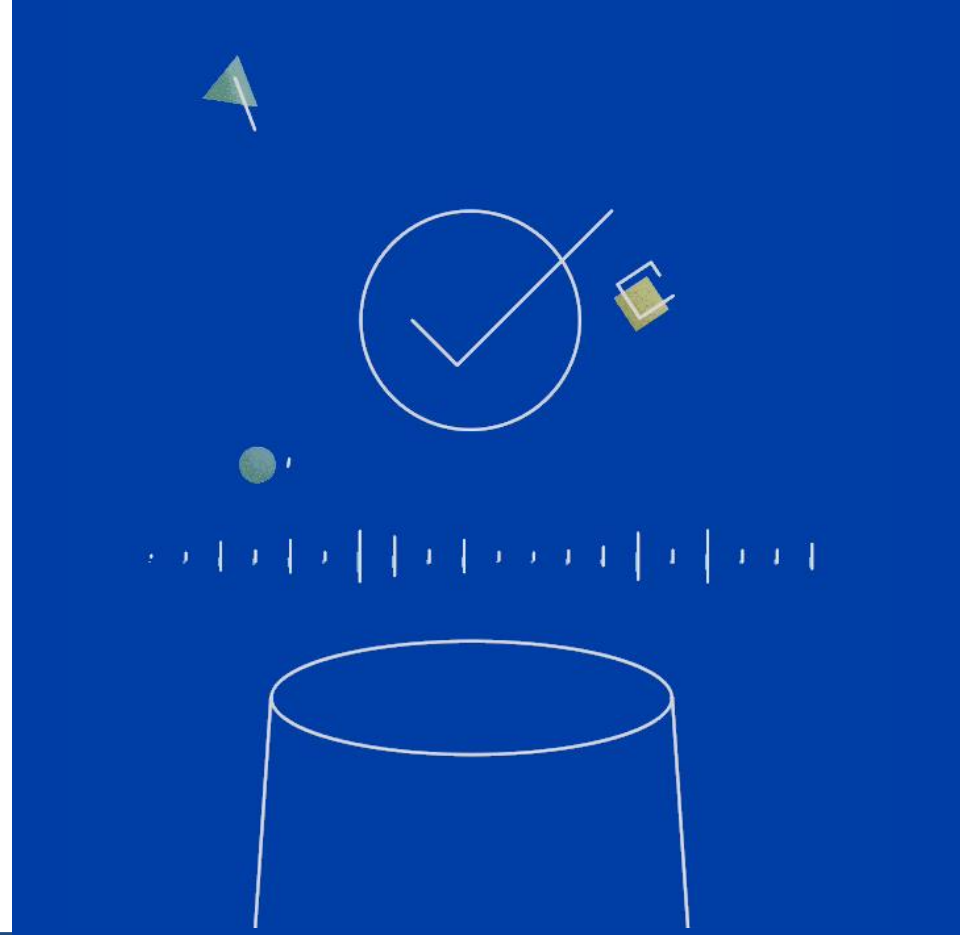


By 2020, **algorithms**  
will positively **alter**  
**the behaviour**  
of billions of global workers.

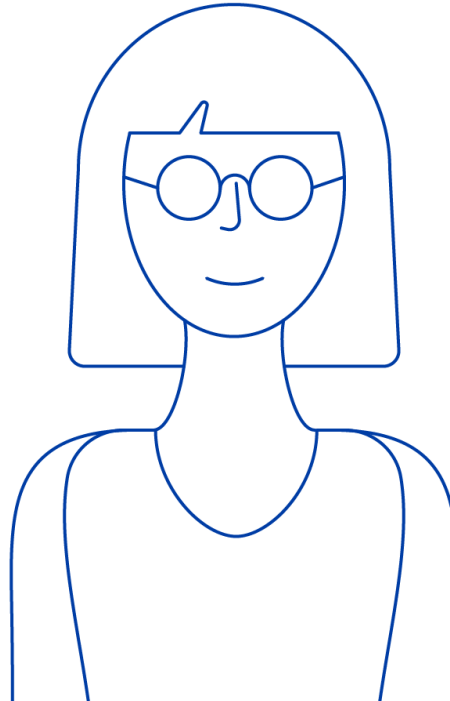
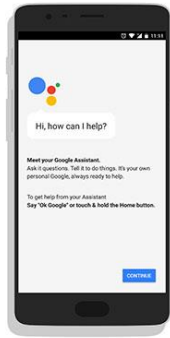
Gartner

By 2020,  
**30%** of web browsing  
sessions will be done  
**without a screen.**

Gartner



# Using technology to be more human



# Facing new cybersecurity threats

Jean-François Allard  
Partner, Cybersecurity Services  
KPMG Canada



# Agenda:

1. Evolution of cybercrime
2. Board of Director expectations

# Definition

## What is cybercrime?

- According to the GRC, there are two types:

### The technology is the target

- Hacking for criminal purposes
- Malware
- Distributed denial of service (DDoS)
- Ransomware

### The technology is the tool

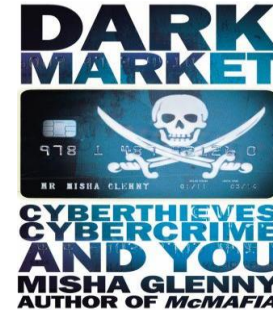
- Fraud and theft
- Identity theft
- Intellectual property violation
- Money laundering
- Drug trafficking
- Trafficking
- Cyberbullying

# Background

## Why is there an increase in cyberattacks?

– There are five key reasons:

- 1 Digitalization of the economy
- 2 Significant dependence on critical IT infrastructures
- 3 Increased ability and ease of young people with technologies
- 4 Appearance in 2010 of a communication protocol called "TOR" and anonymous exchanges on the Internet
- 5 Appearance of dark market



# The threat



Petty criminals / Reasons: financial earnings



Hackers / Reasons: political support

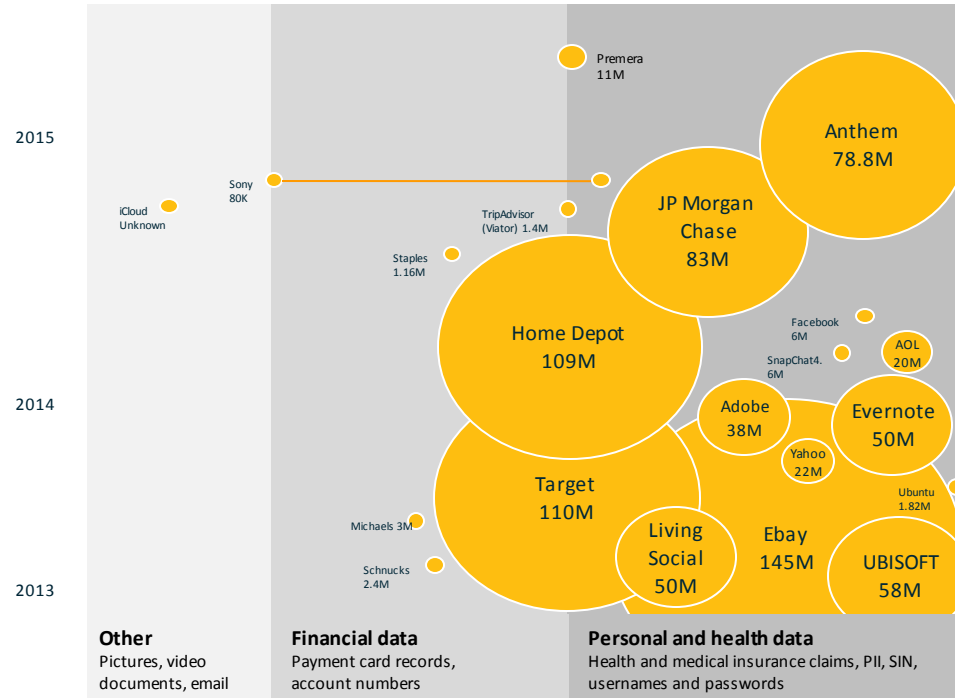


Organized crime / Reasons: financial earnings



States / Reasons: political agenda

# Top cyber-incidents



## Top data breaches 2013 – Present

Number of breached records per recognized company by data type (>1M records)

References:


<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/p-asswords-more-valuable-than-credit-card-data/>

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

# How much is worth your identity?

- USD value of stolen data on the dark market



**Login**

Username  
Password  
Login

Username / Passwords  
**\$5.60**



DEBIT CARD

1-514845 012301234567  
01/15-12/15 3456789101112

Debit Card (#)  
**\$9.55**



Health Record / SSN  
**\$47.62**




Loyalty Rewards

Loyalty Rewards  
**\$.50 for 50k points**



Social Media  
**\$.05 - \$8.00**



CreditCard

1234 5678 1234 5678  
CARDHOLDER NAME CreditCard

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/](http://www.theregister.co.uk/2015/11/05/hilton_honor_cards_breached/)

# Why do organizations get it wrong?



## Security strategy:

- The security function operates independently of the business. The security function is non-collaborative and makes security appear as a dark art. No clearly defined and agreed RACI.



## Security fundamentals:

- Failing to ensure security fundamentals are in place creates a weak foundation. Security is additive, so new challenges must be combined to existing challenges.

Not properly identifying sensitive information and requirements to protect it, and not notifying in the event of a breach, is still quite common.



## Threat intelligence:

- Not keeping up-to-date with the latest cybersecurity threats and evolving their security approach around them.

A lack of relevant threat intelligence means that you don't have the ability to make informed decisions.



## Global compliance:

- Not considering global security compliance and regulation, even if you don't operate globally.

Non-compliance with security compliance requirements can lead to significant financial penalties, including fines, potentially 5% of global revenues, or even custodial sentences. Being reactive to security compliance requirements is always a mistake.



# Why do organizations get it wrong?



## Third-party due diligence:

- Many successful cyberattacks occur through compromising the security of a third-party supplier.

A contract with the supplier to prevent/disclose breaches is no longer enough.



## Only considering prevention:

- The world has changed and prevention of security incidents is no longer enough.

Detection of security incidents and the appropriate reaction to security incidents are also key.



## Failing to react correctly:

- Reacting incorrectly after a breach can significantly increase the severity of the breach and brand damage.

It can also increase the likelihood of fines, as well as making you seem like a softer target, and make further breaches more likely.



## Security seen as tick-box exercise:

- Basic security will at best thwart the basic attacker.

Many organizations that have been breached, used to approach security as a checklist they needed to complete, rather than linking good security to the specific risks and threats of the business. Be secure by design.

# Board of Director expectations

## The role of the Board is critical to effective cybersecurity:

- Obtain and agree with answers to the three fundamental questions regarding cybersecurity:
  - Where are we?
  - Where do we want to be (your defensible position)?
  - How do we get there?
- This shouldn't be a debate about cybersecurity, but a business-led discussion about protecting corporate value.
- Understand the value of your various data sets, and whether appropriate resources are devoted to classifying and securing the most critical assets.
- Ensure cybersecurity is a regular topic and break it into three item categories: Information, Action and Decision.
- Ensure you get the right management information and metrics on the status of security on a regular basis.
- Request regular cyber-incident reports to monitor cyberattacks and trends.
- Ensure all board members are aware that they are one of the biggest risks.
- Be an active participant in your company's cyber-incident response plan.
- Conduct periodic cyber-risk assessments and consider the need for an independent risk assessment – use it to identify where to invest.
- Finally, if a cyber-risk is raised to you, either mitigate it or accept it; **do not ignore it.**



# Questions



The Next 150  
**FORTIFYING**  
RETIREMENT FOR THE FUTURE

2018 ACPM  
**NATIONAL**  
CONFERENCE



**Québec City, QC**  
**Fairmont Le Château Frontenac**  
**SEPTEMBER 11-13, 2018**

[www.acpm.com](http://www.acpm.com)

DIAMOND SPONSOR >



Life • Health • Retirement