


# *Enterprise Risk Management 2019: The New Wave of Risks*

Canadian  
Institute of  
Actuaries



Institut  
canadien  
des actuaires

[cia-ica.ca](http://cia-ica.ca)



As actuaries, we are in the business of risk and uncertainty – we estimate it, model it, analyze it, and assess it. Depending on our appetite, we either accept the risk, manage it, mitigate it, or try to eliminate it altogether. Doing nothing is generally not an option.

The universe of risks is unlimited. Changes in products, processes, and the environment, as well as in the global, regulatory, and digital landscape, give rise to new risks and potential opportunities.

This collection of articles on enterprise risk management (ERM) from the Canadian Institute of Actuaries (CIA) highlights new and emerging hot topics taking centre stage in today's world of risk management. The articles are written by subject matter experts, both actuaries and non-actuaries, giving us their own professional opinions and experiences.

Topics include: ERM maturity, climate change, ERM for pension plans, cannabis legalization, algorithm risk, cyber risk, and risk culture. Risk practitioners should evaluate how to respond and adapt to these new risks, which may impact business models, resources, processes, and systems for their companies. Organizations may need to elevate their ERM capabilities in light of them.

The CIA's Enterprise Risk Management Practice Committee (ERMPC) would like to acknowledge the authors who have provided us with these thought-provoking articles. In addition, this publication could not have been possible without the efforts from our committed volunteers and the staff at the CIA Head Office.



# Contents

- 4** Legalization of cannabis and the effects on the life insurance industry in Canada
- 8** Algorithms gone wild
- 11** Climate change and Canada's property and casualty insurance industry
- 14** "Are we there yet?" Advancing your organization's ERM capability to the next level of maturity
- 18** How ERM creates value in a pension plan
- 21** Cyber: financial and insurance threat landscape
- 24** Building a strong risk culture
- 28** Sources

---

# Legalization of cannabis and the effects on the life insurance industry in Canada

---

**LLOYD MILANI, FCIA, FSA, MAAA**

---

*EVP and CRO, North America Life and Health,  
Munich Re*

Well, October 17, 2018, came and went, and it seems like the world, or at least the small part we Canadians occupy, hasn't fallen apart yet. The only thing I noticed one cold day in January, as I wandered through the PATH in Toronto, was the pungent smell of burnt grass wafting in from the outdoors. It was during the lunch hour, after all.

Seriously though, should we be concerned about the legalization of cannabis in Canada? Is smoking cannabis any different than consuming alcohol? Is the insurance industry ready for the multitude of potential policyholders about to acknowledge on their insurance applications that they enjoy the occasional puff? What are the long-term effects on mortality as a result of smoking cannabis? How are we, as actuaries, going to assess this new risk?

### Understanding what cannabis is

Cannabis (a.k.a. marijuana) is a plant that can grow in varied climates and produces a psychoactive chemical called tetrahydrocannabinol (THC). This chemical is found within the flower buds of the plant. The bud itself can be smoked or the active ingredient can be extracted as an oil. Both can also be used in food or drink as an "edible". THC, once in your blood system, acts on certain brain cell receptors, and provides euphoria and a sense of relaxation. Other common effects (NIDA 2018), which may vary dramatically among different people, include heightened sensory perception, laughter, altered perception of time, and increased appetite (but I don't think I needed to explain that to anyone!).

### Cannabis use in Canada

According to a recent study by Statistics Canada, cannabis use has not increased since its legalization (Statistics Canada 2019a). One reason could be that the legalization is fairly recent and it will take time before we see its impact. Another

reason is that the legal supply and distribution of cannabis is still limited. It will be interesting to see how these stats compare a year or two from now.

Table 1 shows cannabis use in 2018 by quarter in Canada. The results are based on self-reported use. Although not

---

Just like any substance we use or eat, in order to gain a certain level of satisfaction you may need to consume more each time, and use can lead to abuse.

---

explicitly stated in the documentation, one needs to consider that these results have an element of under-reporting. The table shows cannabis use by province, gender, and age groups.

### Is there going to be a large increase in the use of cannabis now that it is legal?

My own view is there will not be a large increase in usage. Those who have never used it may try it once because they are curious. However, the likelihood that these people will use cannabis on a consistent basis in the future will probably be low. Figure 1 shows the percentage of the Canadian population using cannabis from 1960 to 2015. As you will notice, there was an increasing trend in cannabis use starting in 2010. This was primarily driven by the age 25–44 cohort (see Figure 2). The increasing trend occurred well before cannabis became legal.

### Can recreational cannabis use lead to addiction?

Just like any substance we use or eat, in order to gain a certain level of satisfaction you may need to consume more each time, and use can lead to abuse. Alcohol, nicotine, cannabis, caffeine, and even sugar can be addictive.

According to the National Institute on Drug Abuse, it would seem that cannabis can be psychologically addictive but not physically addictive (Canadian Public Health Association 2018). Cannabis withdrawal symptoms can include moodiness, sleeplessness, decreased appetite, and anxiety ... sounds like me without

my morning coffee. In addition, quitting the drug may cause various forms of physical discomfort such as abdominal pain, tremors, sweating, fever, chills, and headache that can last up to two weeks.

### Impact of the legalization of cannabis use on the insurance industry

#### Do cannabis users exhibit the same mortality as non-smokers?

According to a few studies, cannabis smoking does not lead to higher mortality relative to a non-smoker.

In one study, Cannabis Smoking and Lung Cancer Risk (Zhang et al. 2015), cannabis users within a group of lung cancer cases were compared with cannabis users within a control group. The results showed only a weak relationship between cannabis use and lung cancer.

The second study, Associations between Cannabis Use and Physical Health Problems in Early Midlife (Meier et al. 2016), involved a cohort of just over 1,000 individuals born in New Zealand in 1972 and 1973 who were tracked from birth to age 38. The study measured the change in certain health indicators between the ages of 18 and 38. Other

than poor periodontal health among cannabis smokers, there were no negative impacts on other health indicators such as lung function, systemic inflammation, and metabolic health.

Given this information, it seems that a non-smoker and a cannabis smoker are expected to have the same mortality outcome. I was just as surprised when our medical director tried to explain this to a group of actuaries ... though I would like to see a few more pieces of evidence to support this fact before I'll be fully convinced.

### **What are the long-term effects of cannabis use and how will it impact mortality improvement and overall health status?**

One could argue that some of these effects may already be built into our experience data, either within the

Figure 1, from 1970 to 2010, the percentage usage of cannabis remained fairly stable, hovering between 10 per cent and 14 per cent, with the exception for the period around 1992.

### **Will the easy access to cannabis lead to an increase in accidental death or injury?**

One of the biggest concerns I keep hearing is the dangers of people driving "high". Studies (Aydelotte et al. 2017; Tefft et al. 2016) were performed on the number of driving deaths as a result of cannabis use shortly after the drug was legalized in the states of Colorado and Washington. The first study, conducted one year after legalization, showed a bump in fatalities. However, a follow-up study a few years later showed no significant change compared to pre-legalization.

they parallel a typical mortality study we would conduct within our companies. Another question is whether the prevalence will increase. Just because cannabis is now legal, will more people use it?

For example, if we assume that an additional 15 per cent of the population use cannabis on a repeated basis, and their mortality is equivalent to that of a smoker and there was no correlation to tobacco use, it would require an additional 25 per cent load to non-smoker life insurance premium rates. This would include in-force business as well.

To answer these questions properly, we need to start analyzing the data we are already collecting, so that more refined mortality studies can be performed. We also need to develop key leading indicators on the business we accept to determine if any action is required during the underwriting assessment phase or if changes are needed to mortality assumptions. As risk management practitioners, we can start by tracking whether we see an increase in cannabis use via the information provided on insurance applications and cross-reference this information with publicly available data on cannabis use.

---

To answer these questions properly, we need to start analyzing the data we are already collecting, so that more refined mortality studies can be performed. We also need to develop key leading indicators on the business we accept to determine if any action is required during the underwriting assessment phase or if changes are needed to mortality assumptions.

---

general population or within a company's own book of business. Although the insurance industry has been accepting healthy "occasional" cannabis smokers as non-smokers only in recent years, there may be some undeclared use within the insured population. The two studies referred to above would lead you to conclude that if there was an impact it would be small. Finally, referring back to

### **What are some of the risks that we need to address in the life insurance industry?**

The biggest risk we face is trying to deal with the unknowns or the soft data. We need to question the data on usage and how reliable it can be. Despite the studies on cannabis use and mortality, due to the level of subjectivity I don't think

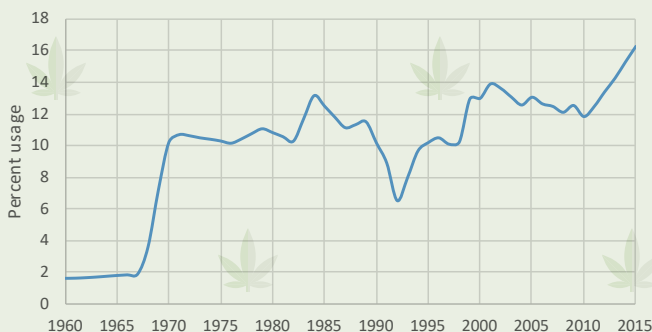
Other possible indicators may be changes to causes of deaths and frequency, including asking for additional information at time of claim, such as alcohol use, cannabis use, and exercise. As we move towards an age of digitalization, I wonder whether predictive analytics and machine learning can be used to help us get ahead of the curve in analyzing the risk of cannabis use, instead of being stuck in the "weed"s.

**Table 1: Cannabis use in Canada (% of population)**

	2018 Q1	2018 Q2	2018 Q3	2018 Q4
<b>Canada</b>	<b>14.0</b>	<b>15.6</b>	<b>15.2</b>	<b>15.4</b>
Newfoundland and Labrador	16.4	18.1	16.1	19.2
Prince Edward Island	14.1	19.2	15.0	17.9
Nova Scotia	20.0	21.0	23.0	21.6
New Brunswick	14.3	17.3	13.8	18.9
Québec	10.4	10.6	10.1	13.6
Ontario	13.5	17.8	15.1	15.4
Manitoba	16.6	15.1	18.9	15.1
Saskatchewan	15.1	9.9	15.7	16.5
Alberta	16.6	15.6	17.0	16.2
British Columbia	17.1	17.3	20.0	15.3
<b>By gender</b>				
Male	15.8	19.1	17.5	19.4
Female	12.2	12.2	12.5	11.3
<b>By age group</b>				
15–24 years	23.2	32.7	27.0	27.4
25–34 years	26.1	26.9	24.5	23.2
35–44 years	15.9	14.9	16.5	17.5
45–54 years	8.2	10.6	12.0	12.8
55–64 years	9.4	10.0	9.9	10.4
65 years and over	4.0	3.4	4.9	5.2

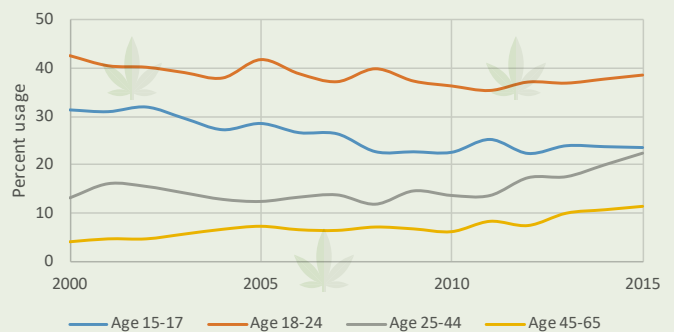
Source: Statistics Canada 2019b.

**Figure 1: Cannabis usage (% of population) 1960–2015**



Source: Statistics Canada 2018.

**Figure 2: Cannabis usage (% of population) 2000–2015 by age group**



Source: Statistics Canada 2018.

---

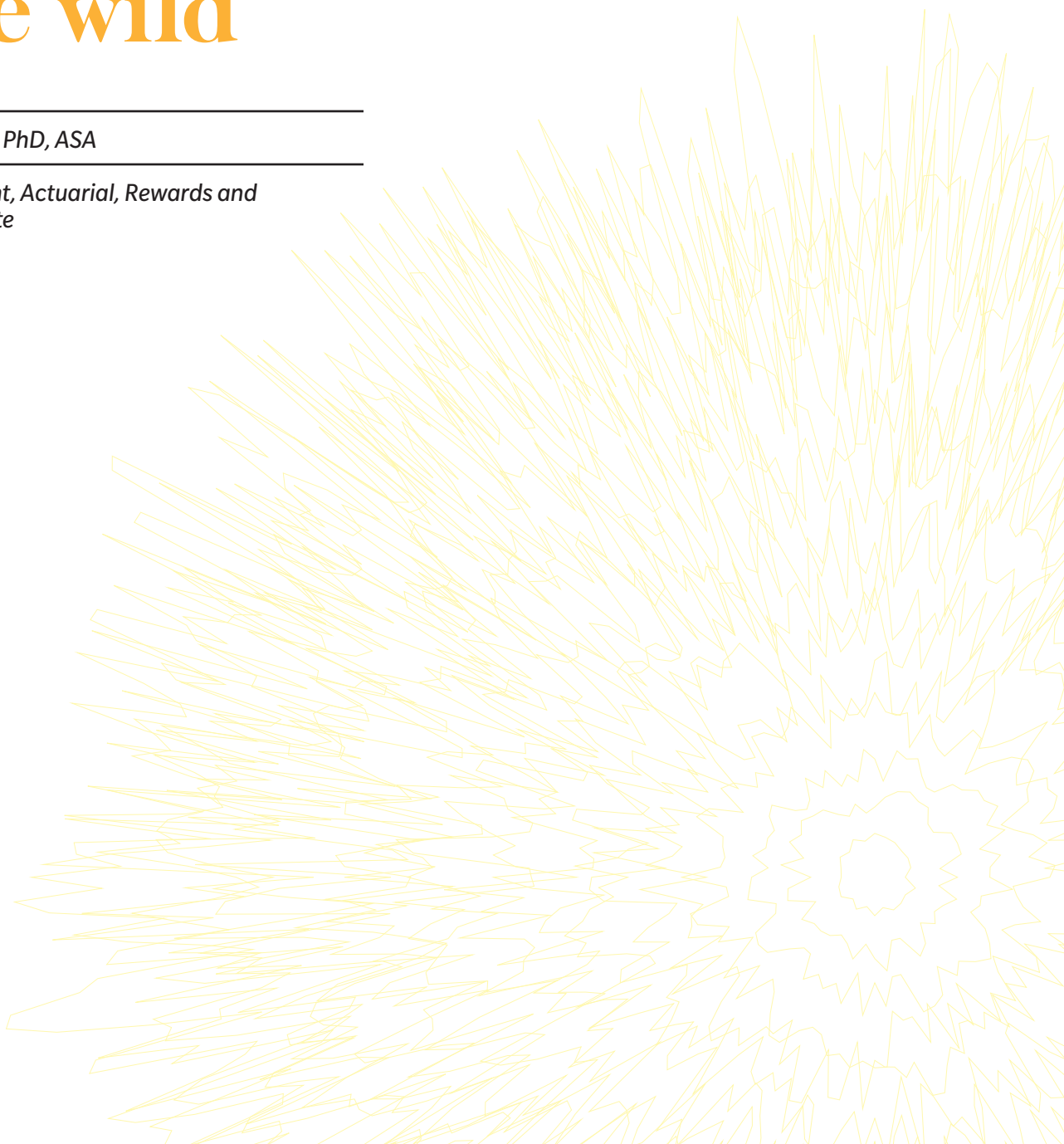
# Algorithms gone wild

---

**SAISAI ZHANG, PhD, ASA**

---

*Senior Consultant, Actuarial, Rewards and  
Analytics, Deloitte*





## Why should we care about algorithmic risk?

Algorithms are becoming increasingly ubiquitous in our day-to-day living. With the rise of advanced data analytics, faster processing power, and growing cognitive computing capabilities, the meaning of the term “algorithm” has gone through a transformative shift, from being rules-based computer programs to intelligent agents informing, or even making, decisions in ways similar to the human brain.

These decisions often give rise to social or societal consequences, ranging from targeted advertising and product and credit offers to hiring, automated driv-

Characteristics Augmentation System (a set of sensors and algorithms) of the Boeing 737 Max aircraft was suspected to be the culprit of two plane crashes in 2018 and 2019, killing a total of 346 people onboard the flights.

### So why does algorithmic risk exist?

Algorithmic risks can arise from each stage in the automated or semi-automated decision-making process: from data input to algorithm design and output decisions. As we move away from rules-based to machine-learning solutions, algorithms begin to break free of strictly coded protocols, and assimilate new “rules” based on data.

The implication is that these algorithms are, at best, only as good as the data feeding into them, which are at the risk of being incomplete or extraneous,

algorithms is vulnerable to a variety of risks such as flawed modelling/calibration techniques, logic, or assumptions. But more importantly, a unique set of risks arise from their opacity (i.e., their “black box” nature). Such opacity comes in three distinct forms (Burrell 2016):

- The first is intentional corporate secrecy – if companies adopt proprietary solutions, the inner workings of its algorithms are considered to be its trade secrets and would not be visible to the users.
- The second is technical illiteracy – an algorithm may be completely open-source but remains a “black box” since reading and writing code (well) is a specialized skill set possessed only by the minority.
- The third resides in the characteristics of the algorithms together with the scale required for meaningful applications – this form of opacity goes beyond technical illiteracy, as a technician may be able to comprehend the code but unable to understand how the routines operate in action or give rise to conclusions in a realistic production environment, due to their high degree of complexity, high dimensionality, and the intricacy of inter-linkages among numerous subroutines.

## For example, research found that in 2015 Google’s algorithms were much more likely to show advertisements of highly paid jobs to male job seekers than female

ing, and personalized medicine. We are entering a time when algorithms rule, which is why the aftermath of “algorithms gone wild” can lead to astronomical financial and reputational losses.

In the past decade, high-profile algorithm failures have already made international headlines. The 2010 Flash Crash, caused by algorithmic trading, triggered a 9 per cent drop in the Dow Jones Industrial Average within minutes. In the initial lead-up to Hurricane Irma in 2017, the yield management algorithms of Delta Airlines raised fares to an unethical extent as an automated response to a demand shock in the state of crisis. Most recently, the Maneuvering

or contain societal biases that require human intervention to counterbalance the negative impacts on the outcomes.

For example, research found that in 2015 Google’s algorithms were much more likely to show advertisements of highly paid jobs to male job seekers than female, implying that gender was a “consideration” that drove its decision-making outcomes. Although gender may very well be a valid predictor according to data, the outcome of exacerbating the gender pay gap would be inconsistent with the company’s mission and values.

Similar to classical statistical modeling, the design of machine learning

The key takeaway is that companies should strive to understand why opacity exists, and situate it in the context where algorithms are deployed, rather than taking opacity as an inherent trait. Targeted risk management strategies, such as algorithm audit or validation, can be devised to effectively mitigate potential losses.

The decision outputs of algorithms are vulnerable to the risk of being misinterpreted or misused – such risks are especially prominent when opacity is high. Opacity also leads to a multitude of risks arising from ethical dilemmas, where algorithms are deployed on making socially consequential decisions

that cannot be easily explained to the affected individuals.

For example, breast cancer prediction algorithms may improve the predictive power of susceptibility from a mathematical point of view, but medical specialists may not be able to pinpoint why such indications of propensity exist, putting the patient in the position of making serious life choices in the dark.

Cyber security is also a growing concern in this modern age of connectivity. Companies should also be aware of IT security risks, as their susceptibility to being hacked can negatively affect their data, algorithms, and output, which would forcibly push them to arrive at flawed outcomes.

### What can we do to prevent algorithms from producing negative consequences?

It is important to understand that with the buzz surrounding InsurTech, it can only mean that we are starting to see and hear more about algorithms being leveraged and integrated as part of modern insurance solutions.

There is no question that algorithms are the future for driving efficiency and value. As insurance companies continue to look into algorithmic use cases in areas such as pricing, driver performance analysis, claim processing, fraud detection, and consumer sentiment analysis, there are several pressing questions that need to be considered:

- Are companies aware of the presence of algorithmic risks?
- How do companies develop policies and cultivate a corporate culture that ensures algorithmic risks are understood across its functions?
- What does an effective algorithmic risk management framework look like?
- What are the ethical considerations surrounding automated decision

making, including data collection and privacy concerns?

- Who are the right talents in the era of algorithms?
- What are the new skill sets actuaries need to acquire?
- How do we retain full control over the technologies that are impacting our lives and making the decisions for us?

Regulators are picking up their pace by introducing reactive legislative measures to regulate algorithmic decision making. The European Union's General Data Protection Regulation (GDPR) (EU 2016), which took effect in 2018, poses restrictions on algorithms that make decisions based on user-level inputs, stressing an individual's "right to explanation" when subjected to an algorithmic decision that significantly affects them. Most importantly, it explicitly states that an individual shall have the right not to be subject to a decision based "solely" on automated processing, including profiling.

set of standards for establishing sound risk management, and for ensuring that ethical considerations are at the forefront of algorithm design and deployment.

Auditing firms have been quick to extend their services to include algorithm audit and assurance services. They play a vital role in the overall ecosystem of algorithmic risk management, as ultimately algorithm audit requires a multitude of interdisciplinary expertise, including computer science, statistical learning, ethics, legal, professional skepticism, and communication. Auditing firms will need to evolve their auditing standards and guidelines to capture algorithmic risk, and develop the means to measure the appropriateness of algorithm designs and decision-making processes. Challenges, such as rapid technological advancement in algorithm designs, regulatory movements, consumer sentiment, data privacy, and cyber security concerns, need to be considered and closely monitored to ensure success.

---

## Auditing firms will need to evolve their auditing standards and guidelines to capture algorithmic risk

---

The 2016 Digital Republic Act of France imposes stricter rules than the GDPR on the public sector by extending such a right to include decisions merely "supported" by algorithmic processing. More recently, in 2019 US lawmakers are recognizing the increasing impact of algorithms on individuals and are pushing for algorithms to be tested for biases before production (US Congress 2019).

Nonetheless, regulations on algorithmic decision making are largely at an early stage, focusing primarily on transparency (i.e., opening the "black box") in order to promote accountability. While transparency lays the groundwork for assessing fairness and probity, there still lacks a clear

The future of algorithms is already here and the various stakeholders in our Canadian ecosystem need to play their part in order to become better educated on its potential risks, and demand that algorithms be safely deployed for commercial use and scrutinized with the lens of public security.

---

# Climate change and Canada's property and casualty insurance industry

---

**PAUL KOVACS**

---

*Executive Director, Institute for Catastrophic Loss  
Reduction, Western University*



Insurance companies have adapted to the remarkable increase in catastrophic (cat) claims over the past decade. Nevertheless, changes in the climate will introduce significant new risks and opportunities for property and casualty (P&C) insurance companies over the next 10 years and beyond. This includes underwriting, claims, operational, investment, reputational, and regulatory risks and opportunities.

Insurance is the business of managing risk. P&C insurance includes the risk of loss and damage due to catastrophic events like flood, wildfire, severe wind, hail, lightning, winter storms, and other severe weather hazards.

Governments have been pursuing two policy files that include addressing catastrophic risk: climate change and disaster management. A third policy file – financial stability – is opening as a result of the failure to achieve the international policy goals set out for climate change and disaster management.

The policy discussion on climate change was formally launched at the Earth Summit in 1992. The goal – first established 27 years ago and clarified in the 2015 Paris Agreement – is to reduce global greenhouse gas emissions to stabilize the global average temperature. However, global emissions continue to increase, not fall, and the temperature is rising, not stabilizing.

In 1989, Canada and most other countries established the International Decade for Natural Disaster Reduction. In three subsequent international agreements the policy goal over the past 30 years has been to reduce the direct damage resulting from disasters. However, disaster damage increased alarmingly, and the underlying driving factors warn that losses will increase further.

Early in 2019, the World Economic Forum identified the increasing risk of damage from severe weather and failure

to achieve the mitigation and adaptation goals of climate change as the two leading global risks over the next 10 years.

Mark Carney, Governor of the Bank of England and past Chair of the Financial Stability Forum, warned that failure to adequately address climate change risks is an emerging threat to the stability

and larger emitters introduces uncertainty and presents opportunities for insurers, lenders, and investors.

Massive investments are needed to support the transition to a low-carbon society. This includes construction of energy-efficient homes and buildings, supporting the transition to electric and

---

**Massive investments are needed to support the transition to a low-carbon society. This includes construction of energy-efficient homes and buildings, supporting the transition to electric and hybrid vehicles, and the development of carbon-capture and carbon-storage technology.**

---

of the financial system. He addressed three critical trends that present risk and opportunity for insurance companies, banks, and investors:

- the rising risk of physical damage
- increased climate-related litigation
- investment risk related to the transition to a low-carbon future

Over the past 40 years, cat claims paid by Canada's insurers have doubled every five to 10 years. Large increases in physical damage have also been evident in most other countries. Moreover, a number of factors threaten further increases in the years ahead, including growth in structures located in areas at risk, aging infrastructure, and expectation of increased frequency and severity of extreme weather events as a result of climate change.

Climate-related litigation also increased over this period. In particular, there has been a surge in legal challenges in the United States over the past 10 years addressing an expanding range of issues. Litigation targeting governments

hybrid vehicles, and the development of carbon-capture and carbon-storage technology. The transition will be



driven by changes in technology, shifting consumer expectations, and government regulations/taxes. The transition presents significant opportunities and risks, including investment risk for insurance companies.

The insurance industry in Canada has adapted to the increase in cat claims. In particular, the industry reported a modest overall underwriting profit in 15 of the



past 16 years despite the remarkable increase in cat claims paid. This included Canada's most costly flood (Calgary 2013), hurricane (Juan 2013), hailstorm (Airdrie 2014), wildfire (Fort McMurray 2016), tornado (Ottawa 2018), and severe wind event (Ontario 2018). Moreover, the industry expressed its willingness to expand coverage, at a fair premium, to address uninsured or underinsured hazards. This included the introduction of residential flood coverage (2015).

Through 2030 and beyond, severe weather and climate change are expected to introduce significant risks and opportunities for Canada's insur-



ance industry. These will include underwriting, claims, operational, investment, reputational, and regulatory risks and opportunities.

First and foremost, the rising risk of physical damage presents insurance companies with an opportunity for growth. This is accompanied by the need to ensure rate adequacy and appropriate reinsurance cover. Rate regulation disrupts insurer efforts to ensure rate adequacy in the United States, but this interference is not found in the Canadian property markets.

Many factors are expected to contribute to rising damage claims, including aging infrastructure increasingly unable to cope with severe weather events; changes in consumer behaviour, like conversion of basements to living areas;

and more frequent intense weather hazards. These concerns will be offset for homes and businesses that invest in climate-resilient construction of new buildings and renovation to existing buildings. Much effort will be required to ensure that insurance pricing appropriately reflects the risk of loss.

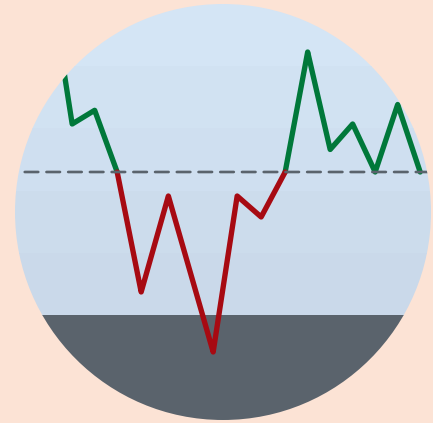
Rising cat claims present increased opportunities and risk for claims management. Cat claims represent a growing share of property damage. Cat events are concentrated across time and geography; several events can come over a short period of time, and there can be an increased risk of total loss claims. Cat claims management will continue to evolve, including development of cat response teams and use of specialized external support.

Insurers need to manage operational risk resulting from more extreme events. Employees may experience personal losses that disrupt their capacity to work, insurance facilities may lose power, and buildings may be damaged. Current business continuity plans may be insufficient for the anticipated future risks.

The transition to a low-carbon economy will introduce investment risk and opportunity for insurers, lenders, and investors. Significant funds are needed to help businesses and homeowners invest in climate resilience measures. Governments seek partners to invest in infrastructure renewal, including projects that will reduce the risk of severe weather damage. However, investors may be subject to regulatory and technological climate risks, with the threat of sudden shifts in asset values and stranded assets.

Climate change introduces reputational risk for companies, including insurance firms, that are not actively managing their environmental impact.

Failure to address climate change is introducing regulatory risk and opportunity



for insurance companies. The Task Force on Climate-related Financial Disclosures is developing international disclosure guidance for insurance companies and seven other industry groups. The Office of the Superintendent of Financial Institutions, the Autorité des marchés financiers, and the Canadian Council of Insurance Regulators are reviewing their supervision of climate risks. In 2019, the Expert Panel on Sustainable finance will report to the federal minister of Finance, and the Bank of Canada launched a climate research program. Concern about financial stability is a foundation of this new regulatory interest in lending, insurance, and investment practices.

Insurance companies in Canada successfully adapted to the increase in cat claims over the past 20 years and will be challenged again by the risks and opportunities introduced over the next 10 years and beyond.

---

# “Are we there yet?” Advancing your organization’s ERM capability to the next level of maturity

---

**DANIELLE HARRISON, FCIA**

---

*Former Chief Risk Officer, The Co-operators Group*



**E**RM within insurance companies is at a critical stage of evolution. The chief risk officer (CRO) role is still finding its place within organizations, and risk professionals have emerged from diverse backgrounds. Attention and effort have focused on responding to the regulatory requirements, which can take some time to address.

You’ve got the following checked off your list:

- ✓ Appointed a qualified and independent CRO or head of the ERM function.
- ✓ Mandated board and management risk committees.
- ✓ Implemented a “three lines of defence” operating model or appropriately robust structure.
- ✓ Approved ERM frameworks and policies that comprehensively outline the vision and expectations for ERM, as well as how risks are governed.
- ✓ Developed a common risk taxonomy and an inventory of key risks and controls.
- ✓ Articulated risk appetite with succinctly defined statements.
- ✓ Selected key risk indicators (“KRIs”) that underpin your risk appetite with defined limits and early-warning triggers, and regularly monitor actual risk profile relative to your risk appetite.
- ✓ Assessed and quantified the most material risks facing the organization and performed stress tests to determine capital requirements.

It can take many years to bring an organization’s ERM program up to speed with the regulatory requirements and expectations. It is no easy feat to get to this point.

### **You’re all done now ... right?**

While taking a regulatory tick-the-box approach is a strong start, it is also the end for many organizations in the maturity of their ERM capability. Upon closer examination, perhaps those boxes aren’t covered off as well as you first thought.

Complacency is dangerous. You can oscillate around the checklist indefinitely. It is not a once-and-done exercise. What worked for you in the past may not be what is needed now. Constant change will keep you busy to ensure that the boxes you’ve checked continue to remain

But ultimately the purpose of ERM is to protect the organization from inadvertently taking on risks that it never intended to, and to direct attention to opportunities to strategically assume more risk or to engage in risk arbitrage. Checking the boxes is necessary, but it is not enough.

## **Your ERM frameworks, policies, and reporting may be developed, but are you truly living them in action?**

checked. We operate in a dynamic environment where risks, strategies, the organization, and the competitive landscape are endlessly evolving. Emerging risks posed by cyber, analytics and artificial intelligence advancements, marijuana legalization, shifting population demographics, and climate change are all topical examples of issues that impact the design of our ERM programs and the prioritization of our risk mitigation effort. Regulators also release additional ERM expectations, which expand our checklist.

Regulatory guidelines that were intended to help organizations gain ground with their ERM programs and provide senior management and board members with role clarity have become, in many cases, the *raison d’être* for the CRO role and dedicated risk professionals within insurance companies.

### **Where do you go from here?**

It can be difficult to change gears and progress to the next level. How can we support this shift? To truly entrench ERM as a strategic enabler of the business, the hard work must begin. ERM capability can successfully advance in maturity when you actively deploy your “regulatory” toolbox and integrate it into your organizational culture. Two powerful levers to achieve this are embedment and constructive challenge.

#### **1. From earmarked to embedded (awareness, ownership, decision making)**

ERM is most effective when it permeates an organization’s culture so that every employee recognizes that they have a role to play when it comes to the

## **Who knows that your enterprise senior management risk committee exists and what its mandate is?**

Given how much work it takes to develop these items in your ERM program, it can feel like having them is enough ... but it’s not. The regulatory requirements are a good start since they provide people with the tools needed to do their jobs better.

management of risk. Risk is not something that is managed only by ERM professionals, senior management, the CRO, or the board. There are a few questions you can explore to objectively assess your current state of embedment.

**Your ERM frameworks, policies, and reporting may be developed, but are you truly living them in action?**

They need to be communicated, understood, followed, and accurately portray how the most material risks are managed. In other words, they must be more than words on paper. To really put your governance into practice, the principles and processes you've defined to manage risks must be put into play when making decisions.

**Can you think of a situation where you would have expected an employee to raise or act on a risk concern, but they didn't?**

Even the best constructed policy guidance and risk monitoring won't address every circumstance. Risk situations will arise that weren't contemplated, and an organization whose employees have embraced a strong risk aware and ownership culture will look beyond the letter of the law to the spirit of the law to ensure that the proper escalation occurs, and the right risk-informed decisions are made. Your employees will fill in the gaps and appropriately map to the circumstance.

**Who knows that your enterprise senior management risk committee exists and what its mandate is?**

All of your employees must understand how and when to escalate issues to that committee; it should not be a committee just for the CRO or for the ERM team to bring forward issues. The typical distinction between items that are risk relevant and items that are not is rooted in the regulatory checklist. Often strategic management issues are reserved for a separate C-suite discussion and not tabled at the enterprise senior

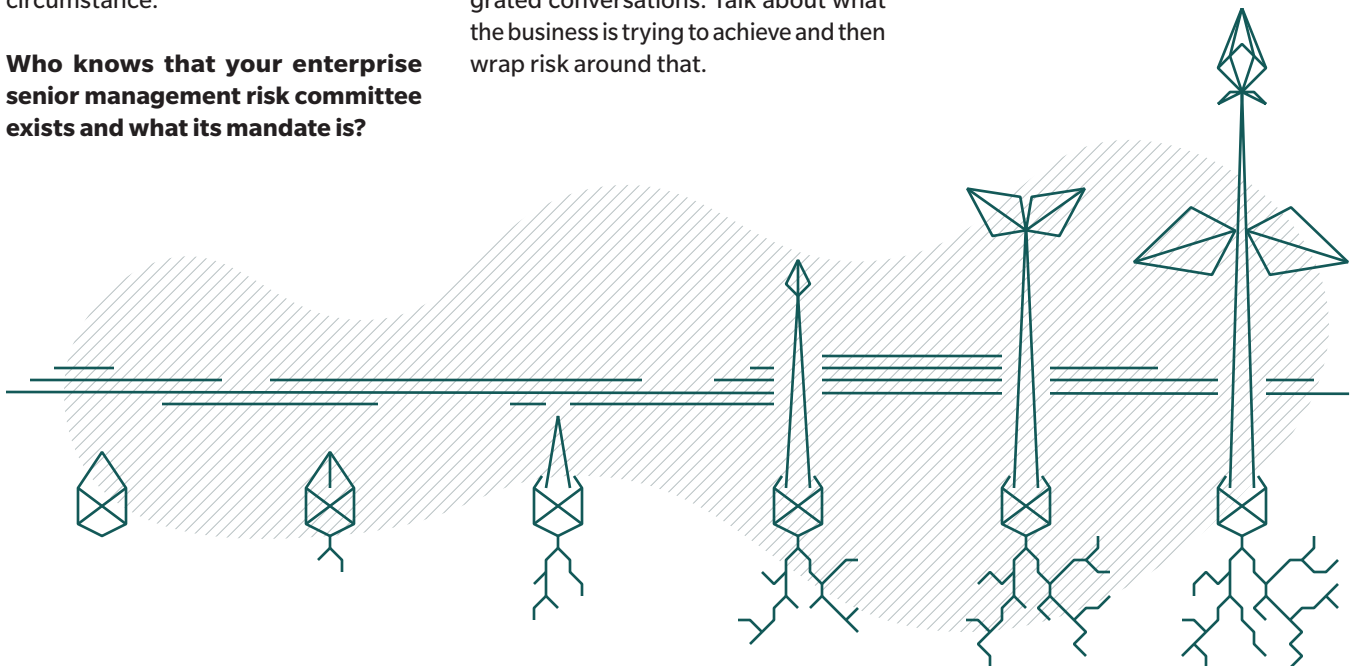
**2. From facilitation to constructive challenge (trust, safety, credibility)**

Identifying, assessing, mitigating, measuring, and monitoring risks on an aggregate basis requires a tremendous amount of knowledge about the organization and the industry in which it operates. It is not surprising that many ERM professionals take on the role of facilitator, drawing on the specialized knowledge

**Can you think of a situation where you would have expected an employee to raise or act on a risk concern, but they didn't?**

management risk committee. Separate enterprise senior management risk committees make the artificial distinction between risk and strategy necessary. Seamlessly blend the grey areas so that risk becomes a natural part of everything that you do. Incorporate risk directly within the already recognized enterprise authority structure. Where those do not exist, then it makes sense to create a new venue to start those integrated conversations. Talk about what the business is trying to achieve and then wrap risk around that.

that exists within many roles and assembling the collective wisdom. This is a very important exercise for an organization to undertake and an equally important skill set for an ERM professional to hone. But there is more that can be gained beyond collecting the input from our experts and moving on. ERM professionals are in the privileged position of observing activities across the enterprise and they operate with independence. By looking





across the organization, they can identify inconsistencies and spot cross-functional opportunities. As a second line of defence oversight function, they are not accountable for the operational decisions of the business, but they can influence

ensure that everything has been considered and that there are no blind spots or “sacred cows” that are off the table for deliberation. This is their role and it can come with battle scars. A knowledge and/or power imbalance within

risks are and the practical constraints that exist to mitigate them; they have the knowledge and insight to meaningfully challenge the views that are presented. Likewise, many valued business leaders have worked within an ERM function at some point during their careers. They have an appreciation for the difficulty of influencing when you do not own and have a well-exercised “challenge” muscle that shapes healthy decisions.

---

## The ERM team should be a training ground for top talent as they rotate throughout the organization and fortify its culture

---

those decisions. How do you enable this independent enterprise perspective to be brought to the table and effectively influence decisions? There are some key actions you can take to allow constructive challenge to flourish.

Position your ERM leaders as strategic advisors on the business, not as tattletales. Challenge for the sake of challenge is not constructive, nor does it build trusting relationships. ERM leaders and business leaders must actively communicate with one another and examine all sides of an issue to develop alternative solutions. ERM tools can provide an unbiased yardstick to anchor those discussions. A mutually agreeable resolution may not be achievable, but this exercise, if done correctly, will result in a more robust consideration of the options, thereby strengthening the resolve in the ultimate decision that is made. If leaders trust that they will be engaged fairly, then there should be no fear of threat when there is disagreement.

Constructive challenge is a critical competency that is enabled by the safety that comes from independence and stature, and the credibility that comes with education and experience. ERM leaders need to speak up, especially when those in the business feel that they cannot. They have a platform to shine a spotlight on different perspectives to

any discussion venue can intimidate and prevent the expression of constructive challenge. And an organizational culture that shies away from productive conflict can label ERM leaders as antagonistic. Our tendency for conformity can literally change what we see (Clearfield et al. 2018). Organizations must lessen “the pain of independence” to cultivate diverse viewpoints.

“If you can articulate what desirable, healthy, productive tensions look like, you can prevent people from interpreting diversity of thought as a dysfunctional dynamic,” advises Liane Davey in her recently published book, *The Good Fight* (Davey 2019). “With heightened awareness and a shared language, your team will start to realize that much of what they have been interpreting as interpersonal friction has actually been perfectly healthy role-based tension.” Differences of opinion are inconvenient and make us work harder. But creating an environment where those opinions are explored up front can prevent devastating missteps.

The ERM team should be a training ground for top talent as they rotate throughout the organization and fortify its culture. Many valued ERM leaders have worked directly in different areas of the business. Their experience provides them with an understanding of what the

### What does a mature ERM capability look like?

My vision for enterprise risk management includes evolving beyond a well-maintained regulatory checklist to full deployment of these ERM tools through embedment and constructive challenge. Only then can organizations address what really matters – ensuring that they make risk-informed decisions in order to increase the success of reliable outcomes.

Insurance companies are attempting to manage at an ever-increasing rate of change, seeking efficiency in their operations while simultaneously strengthening financial and operational resilience. Embedded strategy-risk dialogue and comprehensive decision-making fortified with diverse perspectives, are hallmarks of a mature ERM capability and lend themselves well to these common efficiency and resilience goals. We are a workforce that is learning to embrace the “fail fast” philosophy; application of our ERM capability will lessen the likelihood that our initiatives will fail straight out of the gate with disastrous consequences.

We look to many areas to enhance our strategic advantage, from customer experience to digital and analytics. I encourage the senior management and boards of our organizations to also elevate their ERM capability as a strategic differentiator.

---

# How ERM creates value in a pension plan

---

**LEEANNE K. BARNES**

---

*Director, Enterprise and Operational Risk Management, Strategy and Risk, Ontario Teachers' Pension Plan*

For a multi-employer pension plan such as the Ontario Teachers' Pension Plan (Ontario Teachers'), the mission is to deliver retirement benefits to its members for life. Pension plans such as Ontario Teachers' understand that there is risk inherent in all activities – from the investment portfolio and member services to governance, strategic, and operational decisions made. To deal with the array of risks that face pension plans, boards and management teams have introduced ERM programs. Further, they recognize that a strong culture and robust approach to risk management are fundamental to the objective to deliver on the pension promise to members.

This means that ERM at a pension plan moves beyond the traditional five pillars of identifying, assessing, mitigating and managing, measuring and monitoring, and reporting risk. When the value of ERM is recognized and championed by the board and management, it cascades through the organization and embeds risk consciousness into the culture. ERM evolves into a strategic enabler by providing meaningful insights to leadership to support decision making on organizational priorities and effective allocation of resources for long-term sustainability while balancing risk and reward trade-offs.

Several pension plans established an ERM program after the global financial crisis of 2008. Since then many have matured from a baseline program

with a goal to grow into a strategically focused function where existing internal and external assumptions are challenged, risk information is effectively communicated, and focus areas are highlighted. An ERM framework provides a consistent and straightforward approach to articulate risk appetite and risk across broad categories and can leverage a governance structure with escalation protocols to discuss how to manage existing, new, and emerging risks.

There are three key enablers that Ontario Teachers' believes are important to support ERM maturity:

- Strong support for ERM from the board and executive team based on the value it provides to the organization. The value is in focusing attention on risk areas that trigger in-depth, rigorous discussions on how to achieve objectives.
- Partnership model with the business based on trust and transparency. Engagement with senior leaders across the organization supported by executive team risk owners and risk partners is essential for key insights to be surfaced.
- Continual evolution of the risk methodology, where industry best practices are leveraged and adjusted to meet the needs of a specific pension plan, as one size does not fit all.

For example, at Ontario Teachers', climate change and cyber security were identified as two important risks for management to address now in order to avoid significant negative impacts in the future. The former might affect the sustainability of our investment returns over the long term while the latter is a potential threat to our systems and data.

Identifying these risks is a good first step, but value is not realized until the approaches to mitigate these risks are adjusted. Ontario Teachers' has enhanced investment processes to systematically consider the potential impacts of environmental, social, and governance factors, including those related to climate change, by engaging with portfolio companies and external investment managers to obtain information to better understand how they assess, manage, and disclose climate risk exposures. We advocate for clear, stable policies and regulations that foster an orderly transition to a low-carbon economy, and support the recommendations from the Task Force on Climate-related Financial Disclosures, issued in 2017 by the Financial Stability Board to promote climate-related financial disclosures that are consistent, comparable, reliable, and efficient, and provide decision-useful information to lenders, insurers, and investors.

With cyber security we employ a comprehensive program to help protect the organization against data breaches and other incidents. The program ensures that appropriate controls are in place to protect our corporate information and that these controls are regularly assessed. Our incident response plans are regularly tested and practised, so that the plan is as ready as possible to manage and recover from cyber security or business continuity incidents, should they occur.

As multi-employer pension plans continue on their ERM journey they should be mindful to avoid complacency with their current programs, no matter how mature. There is always room for evolution and improvement. For instance, further advancements may be around building capabilities to better understand the interconnectedness of risks. This would provide important insights on key themes and trends that could impact sustainability.

Another area of focus could be to broaden ERM engagement to stakeholders at all levels of the organization

and externally, through various channels. This may lead to capturing fresh perspectives on risks and opportunities to enhance strategic discussions. By reinforcing the importance of day-to-day risk management and front-line decision making, ERM may also have a positive effect on the culture of the organization. Since enterprise risks are aligned with enterprise planning, ERM communication can be leveraged to raise awareness of the connections between team-level work and bigger-picture organizational objectives.

Multi-employer pension plans are expected to be in business for generations to come and define corporate objectives to deliver on their missions. An ERM program can add value by keeping management focused on significant current and potential risks and opportunities that may have the most impact on these organizational objectives. This will also lead to

better safeguarding of the pension plan's reputation while supporting the business to focus on innovative growth strategies to continue delivering retirement benefits to members for life.

*This article has been written based on lessons learned by Ontario Teachers' Pension Plan ERM professionals, and is not intended to speak on behalf of other pension plans.*



---

# Cyber: financial and insurance threat landscape

---

**JESSE JORDAN**

---

*Principal Consultant, FireEye Mandiant*

Cyber security attacks continue to evolve. Organizations of all sizes being targeted by a variety of threat actors using a wide range of tactics and techniques. Extortion incidents are on the rise and attacks against cloud services have increased due to organizations moving more workloads to the cloud as part of their broader IT strategies.

Although cyber security attacks against all industries are noted, financial institutions continue to make up the majority. Of the incidents that the Mandiant consulting division at FireEye (a cyber-

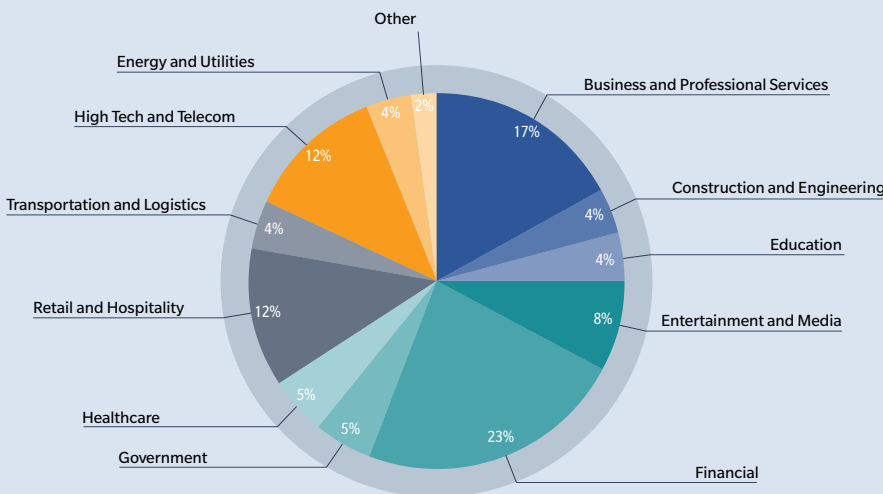
of vulnerabilities in high-value assets, can be used by threat actors to derive where potential weaknesses exist. State-sponsored threat actors can also inform a nation’s commercial interests by obtaining economic intelligence from business negotiations with foreign entities.

In 2018, North Korea, Russia, China, and Iran were responsible for the greatest number of cyber espionage attacks worldwide. We have seen enhanced sophistication of attacks from North Korean actors targeting financial institutions through the exploitation of

malicious code into collaborative software resources, in some cases via malicious insiders, or where devices with malware pre-installed were shipped to clients. If the supply chain breach is deep enough, state-sponsored threat actors essentially go unnoticed.

Supply chain attacks are seen by threat actors as an effective way of bypassing years of investment into perimeter-based defences made by organizations with mature cyber defence capabilities. Over the past few years, Mandiant has identified a substantial increase in these types of attacks.

**Figure 1: FireEye Mandiant M-Trends Report 2019 – industries investigated**



Source: FireEye Mandiant 2019. Reproduced with permission.

security firm) responded to in 2018, 23 per cent were from the financial services industry.

### Financial and insurance threat landscape

State-sponsored threat actors continue to pose a high risk to the financial and insurance industries, both of which have access to a range of sensitive information on their clients. Specific to insurance, brokers examine potential risks associated with their clients as part of the underwriting process. The information gathered, which includes comprehensive profiles

previously unreported vulnerabilities (zero-day vulnerabilities), targeted phishing attacks against CEOs and chief financial officers, and financially motivated supply chain attacks. Supply chain attacks can occur when threat actors successfully infiltrate an organization through a third-party supplier or service provider through shared code or infrastructure via trusted distribution methods. These attacks are particularly effective, as a single compromise along the supply chain can compromise a vast number of victims. Mandiant has noted recent examples where threat actors were able to embed

The rise of financially motivated supply chain attacks by state-sponsored threat actors can partially be attributed to increased sanctions against some of the referenced nation states, where the need to obtain funds using any means is considered necessary. For example, in operations across the globe, North Korean threat actors have attempted to steal over US\$1.1 billion from financial companies by abusing bank-to-bank transfers over the previous two years.

Cyber criminals also continue to target companies in the financial and insurance space by leveraging social engineering and phishing attacks to deliver ransomware with the aim of extorting organizations for financial gain. Cyber criminals use similar methods to steal sensitive information from both insurers and their respective clients, holding this information with the threat of public disclosure should the organization not meet certain financial demands. Cyber criminals will also leverage client/underwriting relationships to gather sensitive information and subsequently sell this on underground markets for identity theft, extortion, and fraud.

Mandiant predicts that cyber crime, especially cyber fraud, will continue to increase in 2019. Attacks against financial websites where virtual “skimmers” are used to steal personal information,

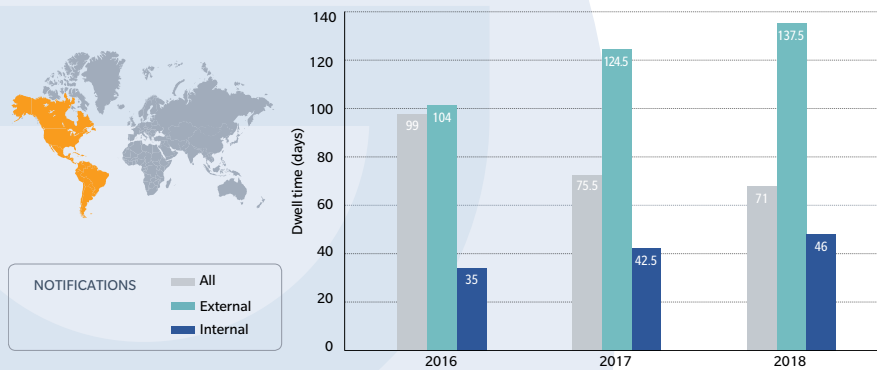
payment card numbers, and credit card CVV codes will continue to rise. In 2018, financial threat actors used advanced techniques to reverse-engineer account registration processes against online portals to gain access to accounts, transfer funds, order cheques, and modify transaction destinations.

later (see Figure 2). Much of the decrease can be attributed to organizations working to continually improve their ability to detect threats early – either through creating internal-threat-hunting capabilities or developing enhanced network, endpoint, and cloud detection and response capabilities.

software are detected through established processes.

Organizations must also ensure a consistent and systematic framework and methodology for detecting cyber security incidents, along with a defined process for analysis, prioritization, containment, and response.

**Figure 2: FireEye Mandiant M-Trends Report 2019 – Americas median dwell time**



Source: FireEye Mandiant 2019. Reproduced with permission.

Hacktivists, although posing a relatively low risk to the finance and insurance sector, continue to cause disruption in the form of ideologically motivated attacks where the goal is often to cause reputational damage to an organization that results in loss of business, either by exposing sensitive client information, stealing proprietary information, or attempting to cause business downtime by performing denial-of-service attacks against customer-facing websites or other critical systems.

### Early detection and response are key

Organizations in the Americas are getting better at detecting threats to their environments early. The median dwell time, which is the amount of time threat actors have remained on victim networks from first evidence of compromise through to detection of the breach, decreased from 99 days in 2016 to 71 days two years

In addition, ensuring security involvement within ERM practices with a clearly defined risk strategy as it relates to cyber threats is important. Organizations should adopt a structured and measured view of security risks and provide clear strategies for mitigation and remediation.

Detailed processes around quantification, ranking, ownership, tracking, and mitigation should be developed to ensure a consistent and comprehensive approach is followed. Centralized risk management solutions can be implemented to assist with standardized tracking of cyber security risks and associated processes.

When tracking risk, factor in suppliers that could expose the organization if breached, and associated controls such as managing a reduced supplier base and imposing strict vendor controls and attestation requirements, while also ensuring that unauthorized changes to

Table-top exercises to test response effectiveness combined with regular “red-team” assessments to test the organization’s detection and response capabilities can be used to further streamline and enhance capabilities. Internal and external penetration testing are also an effective way to detect vulnerabilities and configuration issues that threat actors use to exploit environments to gain further access.

Training staff on how to spot and report a phishing email, especially those that ask the user to take a particular action, is also an important factor in preventing threat actors from gaining initial access into the environment. Regular phishing simulations are a proven way to test awareness messaging and overall program effectiveness.

Security breaches are inevitable, but with strong security governance practices, along with a defined approach to incident handling combined with preventive measures, organizations can lessen their overall impact.

# Building a strong risk culture

---

**MIKE STRAMAGLIA, FCIA, FSA, CERA, ICD.D**

---

*Executive in Residence, Global Risk Institute*





Even the most casual observer will notice that newspaper headlines continue to be fuelled by a steady stream of corporate scandals, malfeasance, and other assorted conduct and risk management “missteps”. While no industry, sector, or region appears to be immune to these incidents, the financial services sector seems to have gained a particularly prominent profile in this regard (e.g., rogue trading, misleading sales practices, Ponzi investment schemes, dubious accounting practices, market/benchmark manipulation, and, of course, the late-2000s financial crisis).

Not surprisingly, these events inevitably generate considerable post-mortem analysis and commentary, as regulators, boards, management, and other key stakeholders strive to understand the root causes, and how these insights might help in preventing similar debacles from occurring.

A commonly recurring theme in much of the ensuing narrative and analysis is that these events are often directly attributable to some form of material “failure of (risk) culture.”

The obvious question this revelation raises for risk managers is “What organizational practices or conditions undermine the establishment of an effective risk culture, and hence our ability to avoid significant losses?” or, equivalently, but framed in more constructive terms, “What organizational practices/conditions help to foster a strong risk culture, and thereby increase our confidence of successfully achieving organizational objectives?”

The process of informing a response to these questions needs to begin with a clear definition of what constitutes a “strong risk culture”:

- “Consistently” applies across multiple dimensions, including over time (not just periodically, or only during certain parts of the economic/

## A strong risk culture can be attributed to an organization that consistently takes the right risks in the right way.

business cycle, etc.), across the entire organization (all business units/entities/divisions, the corporate office, etc.) and up/down the management hierarchy (from the front lines all the way up to the boardroom with risk management expectations also explicitly extended to all third-party suppliers/intermediaries, etc.).

- The “right risks” means only actively taking those risks that are aligned with the organization’s established risk appetite and risk-taking capacity and skill, are actually required to advance the organization’s strategy, mission, and objectives, risks for which the organization is adequately compensated, etc. Also note that this definition acknowledges that organizations need to actively “take” and manage risks in order to achieve their objectives. Strong risk cultures are not characterized by a persistent and uniform bias towards continual risk avoidance.
- The “right way” implies risk-taking follows robust risk assessment/measurement processes, is subject to proportionate ongoing risk oversight and control, the manner of risk-taking is aligned with organizational values, etc.

With this working definition in mind, it is possible to identify key management practices and conditions that can often play a critical role in shaping an organization’s risk culture. These include the organization’s risk appetite articulation and alignment, ability to envision low incidence/high severity risks, reward and recognition systems, leadership practices, continuous learning discipline and ability to foster constructive challenge. In order to illustrate how the above definition of a “strong risk

culture” might help to shape management practices in these key areas, the first three of these are explored in more detail below. Each example is accompanied by a short description, and questions that risk managers should consider in evaluating whether the current state of this practice/condition in their organization serves to foster either a strong or weak risk culture.

### Aligning and articulating risk appetite

Risk appetite alignment is a fundamental determinant of what constitutes the “right risks.” It is therefore impossible to have a strong risk culture without the requisite level of organization-wide understanding and consensus regarding the entity’s risk appetite. Risk appetite also provides shared context for facilitating the type of constructive challenge that is also essential for building a strong risk culture, illustrating the interconnectivity that is often inherent in these critical risk culture shaping practices/conditions.

- Is the risk appetite aligned with the organization’s strategy/mission/objectives, or does attainment of these goals actually require higher/lower levels of risk appetite than is actually being provided for?
- How effective are the associated communications, training programs, etc., in ensuring that all internal and external stakeholders understand the risk appetite at a level commensurate with their risk management activities?
- How effectively is the risk appetite embedded into routine risk management decisions (e.g., does the business case approval process require

a demonstration of how well the proposed initiative aligns with the organization's risk appetite)?

- Does the risk appetite articulation sufficiently support navigating unusual, emerging, or non-contemplated risks by providing context around the organization's underlying risk-taking core principles and philosophy?

### Organizational ability to envision low-incidence/high-severity events

Organizations characterized by weak risk cultures often seem to have a systemic myopia, or at least a fundamental lack of imagination, around low-incident/high-severity events ("That could never happen here..."). This may be attributed to various factors, including the inability to recognize and mitigate the type of cognitive biases that can often lead to a material understatement of the underlying probabilities for extreme tail risk events. For example, by definition, the probability of having observed, say, a 1:200 event may be inherently remote relative to the organization's applicable shared history. However, risk appetites are often calibrated to very low, so heretofore unobserved, frequencies. Organizations therefore need to overcome the natural tendency to unduly rely on apparently benign past experience when formulating these risk assessments.

- Has the organization taken explicit steps to ensure that it does not succumb to small sample size or recency biases in making its risk assessments around low-incidence/high-severity risk events?
- Does the organization routinely apply reverse stress-testing techniques (or what is sometimes referred to as "pre-mortems") to help table discussions/assessments of extreme risk scenarios that might not otherwise occur?
- Do the organization's risk identification and assessment processes

extend beyond just the direct risk impacts to appropriately capture interconnectivity and multiple-generation ("domino") effects?

- Does the organization routinely challenge parts of the business that might appear to be running particularly well, as opposed to just focusing on the underperforming lines?

### Reward and recognition systems

Not surprisingly, poorly designed reward and recognition systems are often cited as the key driver of misdirected management behaviour. An incentive system's ability to influence risk-taking behaviour (in this context, taking the "right risks" in the "right way"), and therefore shape risk culture, is well documented. Unintended consequences in risk-taking behaviour can often be traced to some form of structural outcome bias, where incentive systems focus exclusively on what results are achieved, without due consideration of how these results are achieved.

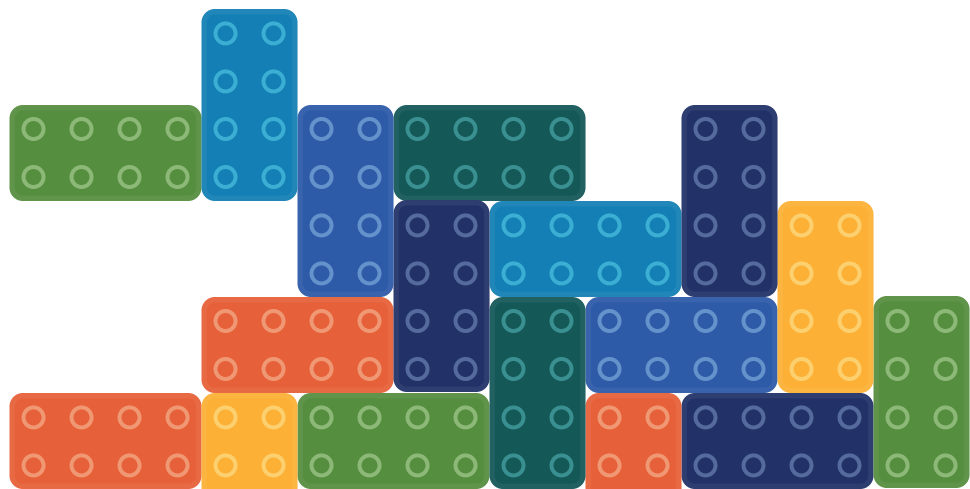
- Are performance targets embedded within incentive programs reasonably attainable by operating within the prescribed risk appetite, and with ethical business practices?
- Are key performance measures appropriately risk adjusted?
- To what extent are risk management objectives explicitly reflected in annual performance management objectives?
- Do incentive programs explicitly incorporate protocols for applying discretion whenever required in

order to appropriately reflect risk-based outcomes? Do key incentive programs include appropriate levels of deferrals, claw-back provisions, etc., in order to similarly advance this objective?

- Is the chief risk officer (CRO) engaged in a review of the design of the incentive compensation programs, and the pro forma results achieved, in order to independently assess alignment with risk appetite? Does the CRO formally report on this assessment to the board (or a designated compensation committee)?
- To what extent do key human resources decisions (hiring, promoting, terminations, etc.) explicitly incorporate assessments of an individual's demonstrated values and overall risk management behaviours?

By similarly applying this article's working definition of a strong risk culture as a guide, risk managers can develop a comprehensive functional catalogue of the management practices required to cultivate the three risk culture principles illustrated above, as well as for other key risk culture drivers, such as the organization's leadership practices, continuous learning discipline, and ability to actively foster constructive challenge.

The resulting inventory can be used to help assess the organization's current state of alignment with these core risk culture principles, and thereby direct efforts to establish the key management practices required to consistently take the right risks in the right way, leading to increased confidence for achieving organizational objectives.



---

## **This publication was created by the CIA's Enterprise Risk Management Practice Committee (ERMPC)**

### **Members:**

Mario Robitaille (Chair)  
Joel Cornberg  
Claude Désilets  
Maja Dos Santos  
Pierre Lepage  
Frédéric Matte  
Karim Nanji  
Phil Rivard  
Anandhi Sarvananthan

The Canadian Institute of Actuaries (CIA) is the national, bilingual organization and voice of the actuarial profession in Canada. Our members are dedicated to providing actuarial services and advice of the highest quality. The Institute holds the duty of the profession to the public above the needs of the profession and its members.

Actuaries are risk management experts. They use mathematics, statistics, and probability to help ensure the financial security of Canadians. Traditional actuarial practice areas include insurance (both life and property/casualty), investments, pensions, actuarial evidence, and enterprise risk management.

**Our thanks to the authors who contributed articles to this publication.**

*Opinions expressed are those of the authors.*



# Sources

- Aydelotte JD, Brown LH, Luftman KM, Mardock AL, Teixeira PGR, Coopwood B, and Brown CVR. 2017. "Crash fatality rates after recreational marijuana legalization in Washington and Colorado." *American Journal of Public Health*. 107(8):1329–1331. <https://www.ncbi.nlm.nih.gov/pubmed/28640679>
- Burrell J. 2016. "How the machine "thinks": Understanding opacity in machine learning algorithms." *Big Data & Society* 3(1). <https://doi.org/10.1177/2053951715622512>
- Canadian Public Health Association. 2018. <https://cpha.ca/sites/default/files/uploads/resources/cannabis/evidence-brief-addictive-e.pdf>
- Clearfield C and Tilcsik A. 2018. *MELTDOWN: Why Our Systems Fail and What We Can Do About It*. Toronto: Allen Lane.
- [EU] European Union, Parliament and Council. 2016. General Data Protection Regulation. *Official Journal of the European Union*, L 119/1. May 4. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC>
- Davey L. 2019. *The Good Fight: Use Productive Conflict to Get Your Team and Organization Back on Track*. Vancouver: Page Two Books.
- [Mandiant] FireEye Mandiant Services. 2019. *M-Trends 2019: FireEye Mandiant Services [Special Report]*. Milpitas: FireEye. <https://content.fireeye.com/m-trends>
- Meier MH, Caspi A, Cerdá M, Hancox RJ, Harrington H, Houts R, Poulton R, Ramrakha S, Thomson WM, and Moffitt TE. 2016. "Associations between cannabis use and physical health problems in early midlife: A longitudinal comparison of persistent cannabis vs tobacco users." *JAMA Psychiatry* 73(7):731–740. doi:10.1001/jamapsychiatry.2016.0637
- [NIDA] National Institute on Drug Abuse. 2018. "What is marijuana?" [www.drugabuse.gov/publications/drugfacts/marijuana](http://www.drugabuse.gov/publications/drugfacts/marijuana) [Accessed May 2019]
- Statistics Canada. 2019a. *Cannabis Stats Hub*. [www150.statcan.gc.ca/n1/pub/13-610-x/cannabis-eng.htm](http://www150.statcan.gc.ca/n1/pub/13-610-x/cannabis-eng.htm) [Accessed May 2019]
- Statistics Canada. 2019b. *Prevalence of cannabis use in the past three months, self-reported*. 13-10-0383-01. [www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=1310038301](http://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=1310038301) [Accessed May 2019]
- Statistics Canada. 2018. *Constructing Historical Cannabis Consumption Volume Estimates for Canada, 1960 to 2015*. 11-633-X2018015. [www150.statcan.gc.ca/n1/en/catalogue/11-633-X2018015](http://www150.statcan.gc.ca/n1/en/catalogue/11-633-X2018015)
- Tefft B, Arnold L, and Grabowski JG. 2016. *Prevalence of marijuana involvement in fatal crashes: Washington 2010–2014*. Washington: AAA Foundation for Traffic Safety. <https://aaafoundation.org/wp-content/uploads/2017/12/PrevalenceOfMarijuanaInvolvement.pdf>
- US Congress. 2019. *Algorithmic Accountability Act*. [www.wyden.senate.gov/imo/media/doc/Algorithmic%20Accountability%20Act%20of%202019%20Bill%20Text.pdf](http://www.wyden.senate.gov/imo/media/doc/Algorithmic%20Accountability%20Act%20of%202019%20Bill%20Text.pdf)
- Zhang LR, Morgenstern H, Greenland S, Chang SC, Lazarus P, Teare MD, Woll PJ, Orlow I, Cox B, Cannabis and Respiratory Disease Research Group of New Zealand, Brhane Y, Liu G, and Hung RJ. 2015. "Cannabis smoking and lung cancer risk: Pooled analysis in the International Lung Cancer Consortium." *Int J Cancer* 136(4):894–903. <https://www.ncbi.nlm.nih.gov/pubmed/24947688>



Canadian  
Institute of  
Actuaries



Institut  
canadien  
des actuaires

[cia-ica.ca](http://cia-ica.ca)