RISK APPETITE
Michael Stramaglia, Executive in Residence

Case Study: Risk Appetite Frameworks - Canadian Family Assurance Group

Key Learning Objectives

- To establish familiarity with the types of core principles that might underpin a financial institution's risk appetite framework
- To gain insights into how these core principles can be applied in practice
- To explore the role of the risk appetite framework to help navigate through potential risk/reward trade-offs and establish a clear "tone from the top" for disciplined risk taking behaviour

Background

Canadian Family Assurance Group ("Canadian Family") is a publicly listed (TSX: CFA) Canadian insurance group. It has two primary Business Units – the Retail BU and the Commercial BU. The Retail BU offers a wide range of simplified issue retail insurance products (primarily life, home, auto and travel insurance) to "self-directed" Canadian consumers, with a particular focus on serving the needs of families in the broad middle market. It distributes its products through various direct response channels (i.e. no intermediaries) that include internet sales and inbound/outbound telemarketing, supported by industry leading web-based insurance needs analysis tools, an integrated marketing strategy (print media, off-prime time television advertising and sophisticated web-based positioning) and the use of leading-edge simplified issue underwriting techniques. The Commercial BU is focused on serving the commercial property and casualty insurance needs of Canadian entrepreneurs and small businesses, with a particular focus on the commercial real estate, tech and professional services sectors. These products are distributed through a national network of independent insurance brokers. While Canadian Family is licensed in all provinces, it only recently expanded into Western Canada, which currently only accounts for 10% of its total revenue.

Canadian Family's success in developing these capabilities has been supported by its long-standing tradition of continuous innovation, data driven decision making and high levels of organizational agility in pursuing emerging opportunities.

While Canadian Family enjoys a long history of overall underwriting profitability, over the last three years ROEs have been in the range of 8-10%, somewhat below its stated long-term objective of 13-15% (a level it had historically been able to achieve in the period before the financial crisis). The recently tabled draft Business Plan shows projected profitability largely in line with current ranges, with relatively modest core income and revenue growth (low single digits). The Board has expressed its dissatisfaction with the draft Plan and has challenged management to *"go back and find some creative ways to bring profitability more in line with our long-term objectives".*

Canada Family's capital and surplus position is strong, and its regulatory capital ratio stands at 340% (3.4 times minimum regulatory requirements), which exceeds its long term "target" level of 235%. The ROE "drag" associate with the current "excess" surplus position accounts for approximately half of the prevailing ROE shortfall.

Canadian Family's stock has traditionally been favoured by income-oriented investors, primarily due to its reliable dividend performance. There are currently seven equity analysts rating the stock, with the following ratings distribution: 2 "sell", 4 "hold", 1 "buy". The two "sell" ratings are relatively recent developments and appear to be based on the recent period of sector underperformance and increasing concerns about future growth prospects.

Canadian Family's articulated corporate vision, mission and values are as follows:

- *Vision:* To be the most trusted provider of insurance solutions to Canadian families and small businesses.
- *Mission:* To help our customers establish control and peace of mind regarding life's inherent uncertainties.
- *Corporate Values:*
  - Innovation
  - Customer Solution Focus Integrity
  - Agility
  - Data driven decision making.

Scenario

A national reinsurance broker recently approached Canadian Family with an opportunity to participate (as part of a reinsurance syndicate) in providing catastrophic loss coverage for certain pools of commercial property insurance risks in Western Canada (i.e. covering aggregate commercial property damage losses above very high deductibles, up to a specified policy limit. The high deductible structure means that any potential claims would only arise as a result of a significant natural catastrophe). The supply of this type of capacity has contracted considerably over the last few years and the current hard market conditions therefore now appear to provide an opportunity to achieve pricing margins significantly in excess of traditional market levels. The broker has indicated a high degree of confidence in being able to place a bid yielding pro-forma ROE's in the mid-20% range. This indicative return has been validated by external actuarial advisors, who Canadian Family retained to assist in the assessment of this opportunity.

While acknowledging that this opportunity may be *"little off of our core strategy"*, both the CEO and head of the Commercial BU support advancing this bid based on the attractive indicative returns, its ability to quickly deploy excess capital and bolster top line growth, and it being a *"great diversification play"*. The CRO has indicated that based on the analysis provided by the reinsurance broker and the retained actuarial advisors, she could *"get comfortable"* with this risk, provided that the transaction is maintained within a prescribed limit and monitored closely. The New Initiatives Policy requires that any capital allocations to new business or underwriting ventures need to be presented to the Risk Committee of the Board for review and approval, hence the reason it is being table on today's agenda.

You are a member of the board Risk Committee being asked to consider this proposed transaction. This discussion has already exceeded the allotted time, with many strong views being expressed both for and against this proposal. Feeling that the Committee is struggling to reach a clear consensus, the Chair pronounced *"This is an interesting opportunity, and we've heard a number of good points being expressed on both sides, but we seem to be spinning our wheels. I don't feel that we've organized our thoughts sufficiently yet to take this to a vote. You will recall that we recently spent a lot of time and effort developing our Risk Appetite Principles, and I know we were all pretty happy with the results. It seems to me that this type of situation is precisely why we need to have a good articulation of our risk appetite. I'd therefore like to suggest that we organize our discussion around those core principles and then take this to a vote once we have the benefit of that holistic perspective in front of us".*

RISK ACTION
Michael Stramaglia, Executive in Residence

Business Case Study: Traduro S.L.

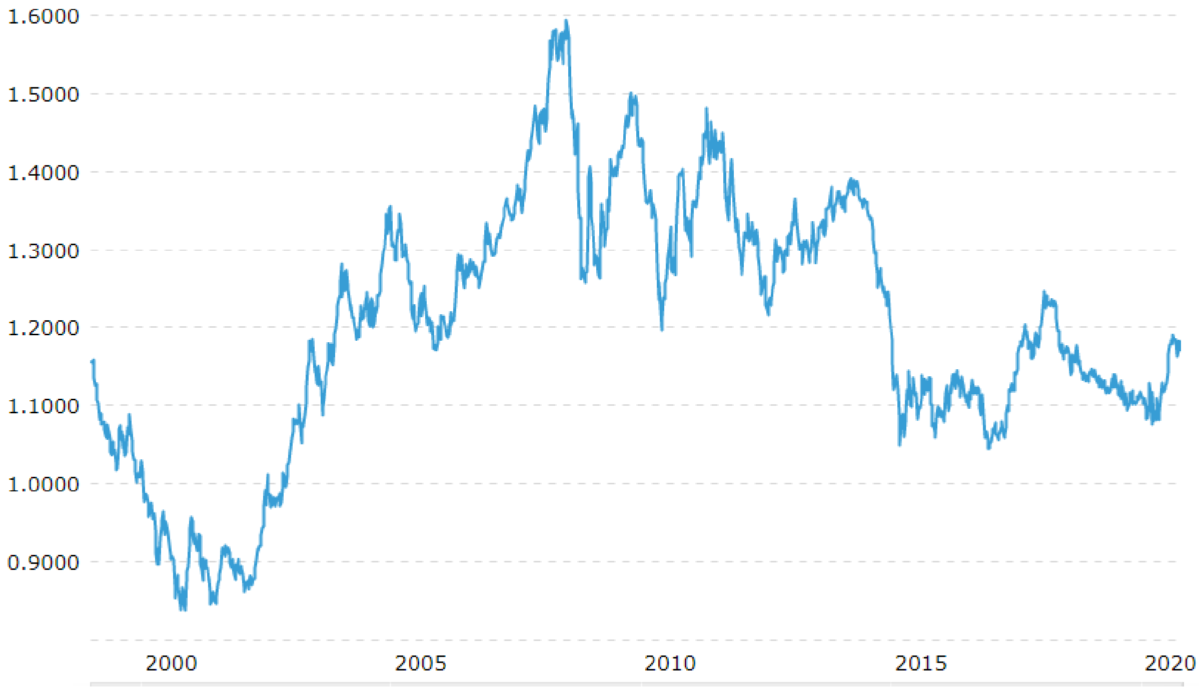
Traduro S.L. ("Traduro") is a publicly listed Spanish manufacturer of construction and large agricultural equipment. Since its original founding in 1978 until the early 2010s, it focused exclusively on the Spanish market. However, in 2014 it began to pursue a very aggressive international marketing strategy, with a particular focus on the North American market, which has been met with considerable success. As a result, over 60% of its sales are now outside of its home market, primarily in the U.S.

Table 1 - Global Sales Distribution (millions Euro)

Market	2014	2015	2016	2017	2018	2019
Spain	289	334	379	425	453	566
Other EU	56	78	121	145	162	188
Mexico	-	38	67	92	130	167
U.S.	68	241	393	569	787	994
Canada	-	-	27	57	88	113
Total	413	691	987	1,288	1,620	2,028

This growth has prompted the need for a significant expansion in Traduro's existing production facilities, which are currently located in the Catalonia Region of Spain.
With the increasing proportion of revenues coming from North America, Traduro net earnings (which are reported in its local currency, the Euro) have become increasingly impacted by changes in foreign exchange rates, particularly relative to the US$.

Chart 1 – Euro/US$ Exchange Rates 2000-2020



http://www.macrotrends.net/2548/euro-dollar-exchange-rate-historical-chart

The significant volatility in exchange rates over the last few years, coupled with the increasing growth of global revenues, have made net earnings much more volatile and difficult to predict. This has begun to impact Traduro's dividend policy and debt service coverage levels, since all of Traduro's financing to date has been raised in the local market on a Euro-denominated basis. This issue has been getting a lot of coverage in recent analysts' reports and has been a key theme in discussions with potential investment bankers as management begins to make the rounds in securing the additional financing required to support its planned production expansion project.

Management has undertaken various reviews in the past aimed at exploring the possibility of hedging its currency exposure, but has resisted doing so to date. This position is largely based on their expectation that global financial markets will be characterized by a long term secular trend of US$ strengthening against virtually all other major global currencies, particularly the Euro.

RISK IDENTIFICATION
Lois Tullo, Executive in Residence

Maple Financial Group – Risk Identification Case Study - AI

Maple Financial Group (MFG) is a large Canadian Financial Institution with operations in retail, commercial, and investment banking as well as insurance, wealth, and pension fund management. MFG has operations in Canada, the USA, Latin America, the EU, and Asia.
At the next Board meeting you, the CRO, will be giving a presentation on technology risk identification. You are reviewing a summary of your notes from the meeting with the Risk Identification Committee (RIC). The RIC was assembled from MFG's leaders in business, IT, security, and risk management to evaluate the greatest risks.

The board is interested in how the company's existing risks of credit, market, operational, and nonfinancial risk might be exacerbated by new technology, and the new risks that the technology itself could create. The Risk Identification process is in place to guard against the disregard or unawareness of certain risks that may result in inappropriate decision-making processes and inadequate risk management practices that may negatively influence MFG's performance. The board is also looking for recommendations to prioritize these risks and to develop scenarios around the potential impacts of these risks, which will be the foundation for building a resiliency strategy for the next board meeting. The board is also interested in the risk/reward of adopting/not adopting new AI opportunities within MFG.

There is a lawyer on the board that is familiar with the “Hand formula,” which has been widely influential in shaping negligence standards. According to the formula, risk is defined as the probability of the harmful event occurring multiplied by the loss the event could generate. Liability ensues any time the burden of preventing an incident is less than the harm the incident could cause. The board is also taking into consideration the significance standard of anti-discrimination laws, which govern decision making in credit, housing, employment, and other contexts.

AI

MFG is currently using AI in their insurance and banking divisions. The board is also interested in new opportunities and threats that MFG might face with the coming adoption of AI.

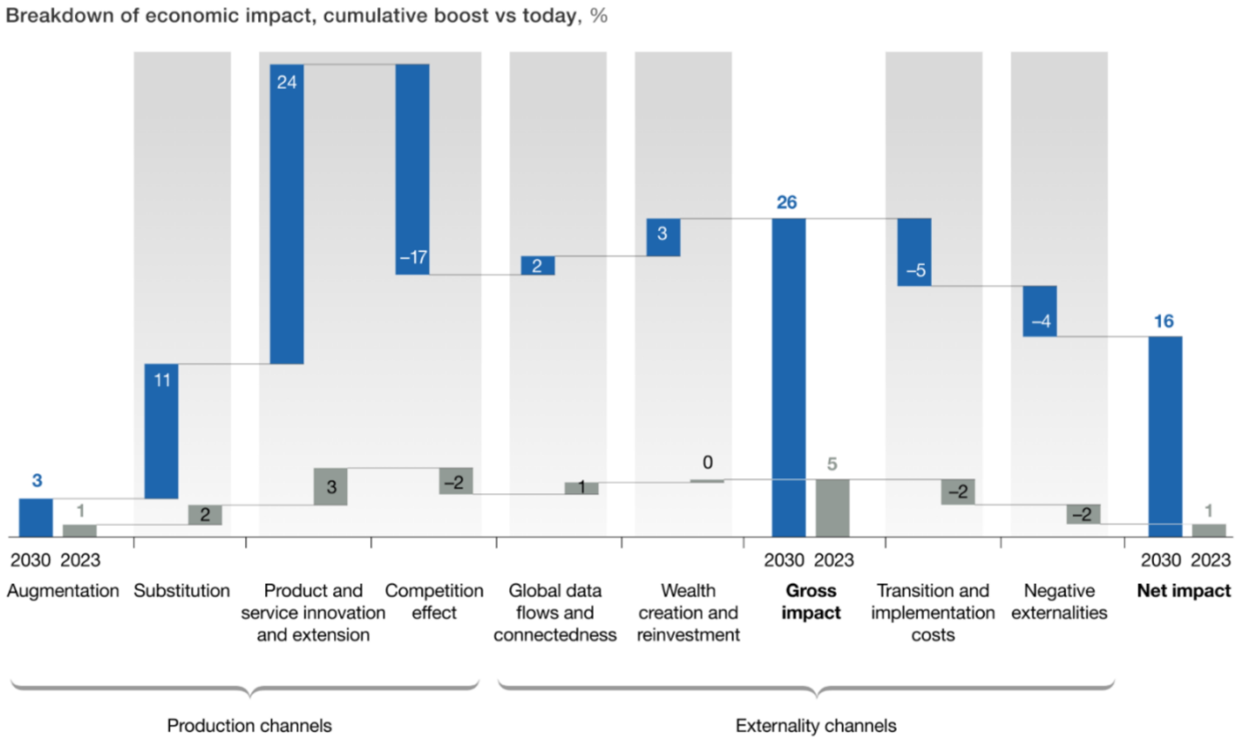
The insurance unit is using Natural Language Processing to improve decision-making by analyzing large volumes of text and identifying key considerations affecting specific claims and actions. They are looking to expand the use of AI in the claim evaluation process to include: an ongoing AI-powered dialogue through bracelets, sensors, etc. leading to a more comprehensive understanding of the insured. By collecting and analyzing additional data, MFG will be able to analyze the habits of their policyholders and offer highly customized products, adapted in real-time to the needs and expectations of their clients.

The banking unit is piloting AI to enhance their traditional credit scoring model based upon payment history. AI including mobile phone activity, social media usage is being used to assess the credit worthiness and improve the profitability of loans, particularly for "thin" credit file applications more accurately. MFG is planning to expand the use of AI for all loan applications.

Several of MFG's employees and customers have also inquired about incorporating ChatGPT into their work assignments, as well as some worrying comments about potential liability around copyright infringement, defamation and data privacy.

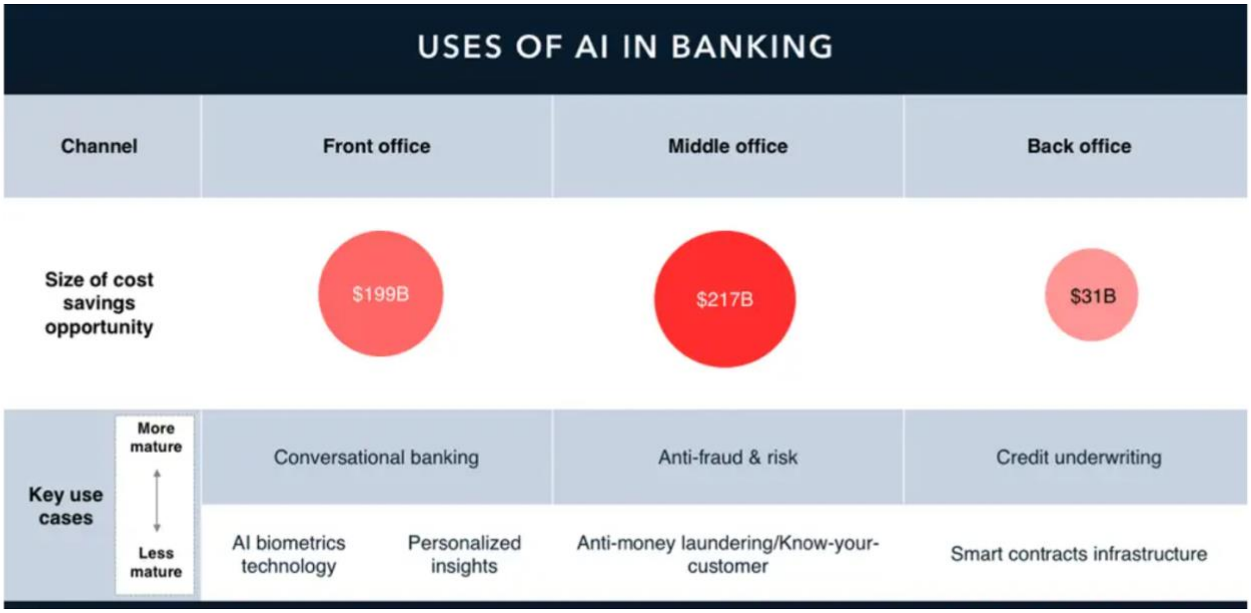
i. AI Overview

AI has the potential to deliver additional global economic activity of around $13 trillion by 2030. Economic impact has been simulated to have seven channel or impacting factors. AI might widen gaps between countries, reinforcing the current digital divide. Countries might need different strategies and responses as AI-adoption rates vary.
Leaders of AI adoption (mostly in developed countries) could increase their lead over developing countries. Leading AI countries could capture an additional 20 to 25 percent in net economic benefits, compared with today, while developing countries might capture only about 5 to 15 percent. China has had a country AI strategy since 2017.



ii. Uses of AI

The management team at MFG is considering several uses of AI.



USES OF AI IN BANKING

Channel		Front office		Middle office	Back office
Size of cost savings opportunity		$199B		$217B	$31B
Key use cases	More mature	Conversational banking		Anti-fraud & risk	Credit underwriting
	Less mature	AI biometrics technology	Personalized insights	Anti-money laundering/Know-your-customer	Smart contracts infrastructure

iii. Categories of Artificial Intelligence

1. **Computer Vision** - is a field of artificial intelligence (AI) that enables computers and systems to derive meaningful information from digital images, videos, and other visual inputs, and to take action or make recommendations based on this information.
2. **Natural Language Processing** - giving computers the ability to understand text and spoken words in much the same way human beings can.
3. **Virtual Assistants** or intelligent personal assistant (IPA) is a software agent that can perform tasks or services for an individual based on commands or questions.
4. **Robotic Process Automation** (RPA), software that mimics rules-based digital tasks performed by humans, is being applied in banking to eliminate much of the time-intensive and error-prone work involved in entering customer data from contracts, forms and other sources.
5. **Advanced Machine Learning** – provides systems the ability to automatically learn and improve from experience without being explicitly programmed. Machine learning focuses on the development of computer programs that can access data and use it to learn for themselves.
   a. **Supervised machine learning algorithms** can apply what has been learned in the past to new data using labeled examples to predict future events. Starting from the analysis of a known training dataset, the learning algorithm produces an inferred function to make predictions about the output values. The system is able to provide targets for any new

input after sufficient training. The learning algorithm can also compare its output with the correct, intended output and find errors in order to modify the model accordingly.

b. **Unsupervised machine learning algorithms** are used when the information used to train is neither classified nor labeled. Unsupervised learning studies how systems can infer a function to describe a hidden structure from unlabeled data. The system doesn't figure out the right output, but it explores the data and can draw inferences from datasets to describe hidden structures from unlabeled data.

c. **Semi-supervised machine learning algorithms** fall somewhere in between supervised and unsupervised learning, since they use both labeled and unlabeled data for training – typically a small amount of labeled data and a large amount of unlabeled data. The systems that use this method are able to considerably improve learning accuracy. Usually, semi-supervised learning is chosen when the acquired labeled data requires skilled and relevant resources in order to train it / learn from it. Otherwise, acquiring unlabeled data generally doesn't require additional resources.

d. **Reinforcement machine learning algorithms** is a learning method that interacts with its environment by producing actions and discovers errors or rewards. Trial and error search and delayed reward are the most relevant characteristics of reinforcement learning. This method allows machines and software agents to automatically determine the ideal behavior within a specific context in order to maximize its performance. Simple reward feedback is required for the agent to learn which action is best; this is known as the reinforcement signal.

iv. AI Risks

1. Late adopters might find it difficult to generate impact from AI, because front-runners have already captured AI opportunities and late adopters lag in developing capabilities and attracting talent.
2. Knock-on effects:
   - privacy violations,
   - discrimination,
   - accidents, and
   - manipulation of political systems
3. Consequences of AI risks
   - loss of human life, if an AI medical algorithm goes wrong,
   - compromise of national security, if an adversary feeds disinformation to a military AI system
   - reputational damage and revenue losses to regulatory backlash,
   - criminal investigation, and
   - diminished public trust.

v. **Pain Points that can give rise to AI Risks:** data difficulties, technology troubles, security snags, algorithms, and human–machine interactions.

vi. Unintended Consequences of AI

Individual	Organizations	Society
Physical safety • Autonomous-vehicle malfunctions leads to injury or death • Overreliance on inadequate equipment predictive-maintenance decisions leads to worker injury • Machine-learning models misdiagnose medical conditions	**Financial Performance** • Trading algorithms unable to correctly adapt to new circumstances (eg, similar to a flash crash) lead to sudden financial losses • Organization makes adverse pricing decisions that materially misgauge consumer price elasticity, leading to poor production decisions	**National security** • Actors with malicious intent coopt AI-enabled products (e.g., weaponry, drones, cybertools) and use for illegal activity • Data breaches of sensitive data expose key military vulnerabilities / technical secrets
Privacy and reputation • Private data used without consumers' consent • Personally identifiable information (PII) data are not securely stored, resulting in data breach and downstream individual implications	**Nonfinancial Performance** • Hiring and promotion use complex algorithms that unintentionally lead to nondiverse workforce or unintended behavior • Suboptimal estimates of funds and resources required during different natural disasters/ emergencies resulting in inadequate preparation	**Economic stability** • Automated trading algorithms increase volatility in financial markets • Algorithms create instability in currency markets, resulting in decreased trade • Black-box financial instruments lead to unintended systematic risk
Digital safety • Distortion of individual data/information leads to digital libel or defamation	**Legal and compliance** • Unintended discrimination embedded into lending decisions results in litigation • Disclosure of protected consumer healthcare data	**Political stability** • Manipulation of national institutional processes (e.g. elections, appointments) through misrepresentation of information and false messaging
Financial Health • Poor financial recommendations result in mismanagement or consumer or employee funds • Machine-driven, sophisticated phishing steal and exploits financial information	**Reputational Integrity** • Lack of clarity regarding consumer data-privacy setting causes social backlash • Advertising algorithm utilizing invasive PII (or other personal information) causes public to view company as intrusive/dishonest	**Infrastructure integrity** • Risk concentration materially affects societal infrastructure as more processes and decisions become interconnected (e.g. disabling power, water supplies, communications). • Intelligent systems lead to overuse/misuse of infrastructure, GPS routes cars through side streets, causing unprecedented traffic in residential areas)
Equity and fair treatment • Underwriting model inadvertently discriminates based on race, rejecting minority customers from acquiring mortgages • Lending algorithm takes into account social-media connections, giving better rates to people who have perceived "higher quality" networks and penalizing those who don't		

EMERGING RISK: POLYCRISIS
Lois Tullo, Executive in Residence

Polycrisis: What is brewing on the horizon?

A Polycrisis is a situation where multiple crises intertwine, their causes and processes inextricably bound together to create compounded effects, according to the Institute of Development Studies.

Setting the Stage for a Polycrisis:

- In 2020, Covid shuts the world down, reported Covid deaths top 6.5 million, resulting in cross-border closures, supply chain disruption, food scarcity and rising nationalism.
- In 2022, Russia invaded Ukraine, war continues, nuclear stations compromised, global geopolitical divide over support for the war, Russia removed from SWIFT, Nord Stream pipeline shutdown due to sabotage, releases 500,000 tons of methane gas, equal to a few days of the emissions from the entire fossil fuel industry, oil prices peak and ebb, and peak, cyber hack increase; Crimea causeway bombed, Russian retaliation through increase bombing of Kiev capital, US strengthens Ukraine’s position through pledging ‘advanced air defense systems’.
- Israel/Gaza war – In 2023, Hamas attacked Israel, leading to Israel’s attack on Gaza. This has led to instability in the Middle East that has spread to include the Red Sea where there are Security Threats, diverting shipping around South Africa, and increasing shipping costs and insurance.
- China/Taiwan insecurity; global dependence on CHIP manufacturing for 90% of complex CHIPs.
- Environmental Crisis – 2023 was the hottest year on record, CO2 levels are at the highest they have ever been; Australia and the US experiencing some of the most devastating bushfire seasons ever recorded, locusts swarming across parts of Africa, the Middle East and Asia, decimating crops, and a heatwave in Antarctica that saw temperatures rise above 20C for the first time. Scientists are constantly warning that the planet has crossed a series of tipping points that could have catastrophic consequences, such as advancing permafrost melt in Arctic regions, the Greenland ice sheet melting at an unprecedented rate, accelerating sixth mass extinction, and increasing deforestation in the Amazon rainforest.
- Global sovereign debt reaches unprecedented levels, $97 Trillion USD, a 40% increase from 2019.
- In 2022, inflation climbs to levels not seen since early 1980s;
- Increasing pressure on low-income individuals in the form of food and shelter prices, in-direct side effects have been linked to the highest level of drug overdoses in Canada in 2023, and spending of over $49 billion in healthcare costs, lost productivity costs, criminal justice costs or other direct costs.

- Since 2022, Central Banks raised interest rates on average by 300 bsp, putting strain on credit agreements.
- Technology Crisis - Cyber Security attacks, and breaches in 2023 reach 8.2 billion records; cyber attacks using AI examples include: manipulation of autonomous vehicles, tampering with critical infrastructure, increasing data breaches, disruption of financial systems, and spread of misinformation which could shift the trust foundation of the internet.

Example of the Tipping Point of a Polycrisis

In the UK, the Queen Elizabeth attends the Duke's funeral alone, Prime Minister Boris resigns over Covid parties, new party leader and Prime Minister Truss announces £45 billion in unfunded tax cuts. On Monday morning, as the pound was sliding sharply and interest rates surged, the UK's new prime minister Liz Truss decided to stick with her core instinct: do nothing. There were periods on Monday and Tuesday when there were no buyers for long-dated gilts. By Wednesday, as the extreme volatility in the gilts market left some pension funds facing a liquidity crisis, the Bank of England launched a £65bn emergency intervention. The gilts declines by over 100bsp, The Central Bank and the IMF chastised the Prime Minister's decision.

UK pension schemes were dumping stocks and bonds to raise cash and seeking bailouts from their corporate backers as the crisis in the industry continues to rage a week after the government's "mini" Budget. Most of the UK's 5,200 defined benefit schemes use derivatives to hedge against moves in interest rates and inflation, which require cash collateral to be added depending on market moves. The sharp fall in the price of 30-year government bonds, triggered by the previous week's tax cut announcement, led to unprecedented margin calls, or demands for more cash. To raise the funds, pension funds sold assets — including government bonds, or gilts — causing prices to fall further. By Wednesday, The Bank of England stepped in to buy gilts on October 5, 2022, stabilising the market, but the pension funds are continuing to sell assets to meet cash calls.

Some managers of the so-called liability-driven investing strategies are demanding more cash to fund the same derivatives position in a dash for safety. Many are worried about what would happen after the central bank's burst of bond-buying, which is due to end on October 14. Many are worried that as the clock ticks down to the end of the BoE committed intervention that we could see a replay of events and are determined to try to make sure that the chaos that ensued at the beginning of this week is not repeated.

Ask: Preparing for a Polycrisis in 2024

- Reflect on the risks and trends that you think may be most impactful to your organization over the next year, and some of the unprecedented events that are brewing on the horizon and may trigger a Polycrisis, destabilizing society and markets.
- Discuss your organizations readiness and approach to preparing for a potential Polycrisis. Consider the underlying assumptions of organizations strategies, continually scan the horizon for unprecedented change, prioritization of identified risks and trends, identify the interrelationship of risks and trends, and run scenario analysis and stress test their portfolios, to illuminate potential dangers to their portfolios, and influence future strategy setting.

EMERGING RISK: CYBER RISK
Tony Peccia, Executive in Residence

Cyber Risk Case Studies

Three mini scenarios will be analyzed to explore the associated cyber risk, mitigation, resilience, and governance strategies.

Background:
Globank Financial is a prominent banking institution with a vast network of retail banking services, online banking, and financial transactions processing systems. It prides itself with its cutting-edge cybersecurity measures and its robust IT infrastructure that supports millions of customers worldwide.

Questions for each scenario

1. What are the key risks in the cyber threat scenario?
2. What are other manifestations or realizations of the same type of risk?
3. What resiliency needs to be in place?
4. What are the main controls available to mitigate these risks?

Scenario 1: Sophisticated Phishing Attack on Globank Financial
The security team at Globank detects an unusual increase in customer complaints regarding unauthorized transactions and account lockouts. The investigation reveals a coordinated phishing campaign where attackers sent emails and messages mimicking Globank's communication style, directing customers and employees to fake login pages designed to harvest credentials.

Consequences:

- Reputational Damage: The phishing attack damages Globank's reputation, leading to decreased customer trust and potential loss of business.
- Financial Impact: The bank incurs significant costs associated with incident response, customer compensation, and investment in enhanced security measures.
- Regulatory Compliance and Legal Challenges: Globank faces scrutiny from regulators for potential lapses in data protection, possibly resulting in fines and legal challenges from affected customers.
- Strategic Security Enhancements: In response to the attack, Globank strengthens its cybersecurity posture, investing in advanced email filtering technologies, endpoint protection solutions, and continuous employee training on cybersecurity best practices.

Scenario 2: Insider Threat Leading to Data Integrity Breach at Globank Financial
An internal audit at Globank uncovers irregularities in loan approval processes and discrepancies in financial reports. Further investigation reveals that a long-serving employee in the loan department, motivated by personal financial gain, manipulated loan application data and approval processes to approve loans for unqualified friends and family members. Additionally, the employee altered financial reports to cover up the fraudulent activities.

Consequences:

- Reputational Damage: News of the insider fraud damages Globank's reputation, undermining customer and investor confidence in the bank's ability to manage internal risks.
- Financial Loss: The fraudulent activities lead to financial losses through bad loans and the cost of legal actions, investigations, and increased security measures.
- Regulatory Scrutiny: The incident attracts increased scrutiny from financial regulators, resulting in fines and mandates for stricter internal controls and audit processes.
- Cultural Shift: Globank recognizes the need for a cultural shift towards a more security-conscious mindset among its employees, fostering an environment where security is everyone's responsibility.
- Strategic Security Enhancements: The incident leads Globank to reevaluate its approach to insider threats, investing in advanced behavior analysis tools and insider threat detection programs to prevent future breaches.

Scenario 3: Ransomware Attack on Globank Financial

On a seemingly routine Thursday morning, Globank's IT department receives multiple reports from employees unable to access their workstations. Simultaneously, customers start reporting issues with logging into their online banking accounts. The IT department discovers ransomware has infiltrated their network, encrypting critical data across servers and workstations, leaving a ransom note demanding payment in cryptocurrency for the decryption key.

Consequences:

- Reputation Damage: Globank's reputation suffers significantly, with a loss of customer trust and confidence that takes years to rebuild.
- Financial Loss: The immediate financial impact includes the ransom payment (if made), loss of business, and the cost of incident response and recovery. Long-term financial impacts include potential regulatory fines and legal actions from affected customers.
- Cybersecurity Overhaul: Globank undertakes a comprehensive review and overhaul of its cybersecurity posture, investing in advanced threat detection and response capabilities, employee training on phishing and malware, and enhanced data encryption and backup strategies.