Maple Financial Group – Technology Risk Identification Case

Author: Lois Tullo

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 my 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.

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.

I - Cloud

Maple Finance is currently looking to shift from managing their own data centre to a cloud environment. Identification of the risks is an important step in the decision-making process.

i. Characteristics of Cloud Computing

Cloud computing is the dynamic provisioning of computing capabilities (hardware, software or services) provided by a third party via the network.

1. Self-service on-demand – A cloud user can access the desired computing resources without the intervention of the provider
2. Broad network access – Cloud services supplied by the provider are available thanks to the use of protocols supporting the use of heterogeneous client platforms such as destop computers, mobile computers, and mobile phones.
3. Polling resources – The Cloud provider uses a multi-tenant model to support queries from multiple and different clients at the same time.

4. Rapid elasticity – It is the ability to meet the needs of customers by reducing or extending the supply of resources
5. Paid per use – the customer pays only what is really needed.

ii. Types of Cloud Computing

1. Infrastructure-as-a-Service (IaaS) – Access to a virtual computer park that includes the set of servers, routers, firewalls, processors and others. The customer is permitted to choose the configuration of these components according to their needs. The customer manages their infrastructure themselves such as network traffic, physical security, and investigations.
2. Platform-as-a-Service (PaaS) – The customer uses a virtual platform via the web. The customers developers deploy their own applications and services without downloading their own applications and services. However, they are forced to use the tools provided by the supplier. This requires a good identity management of strong privileges, especially for users administering the software platform.
3. Software-as-a-Service (SaaS) – The end user needs only a simple web access to use the application. The consumer does not have to worry about making updates, adding security codes and ensuring the availability of service. The supplier is responsible for almost all aspects of security. However, transparency is limited, so the consumer loses control over their resources.

iii. Cloud Models of Deployment

1. Public – can be used by the public via the internet, the disadvantage being a weakness of security.
2. Private – Reserved for the exclusive use of a single organization. The weakness is that this does not allow the reduction of operational costs.
3. Community Cloud – provisioned to be used by organizations having a specific community purpose (mission). It can be managed by any of these organizations or a 3rd party.
4. Hybrid – Comprise of 2 of (private, public or community, or internal and external), this allows the flexibility to move between platforms, however, it does increase the possibility of reaching the private cloud from the public cloud by hackers.

iv. Types of Cloud Hosting

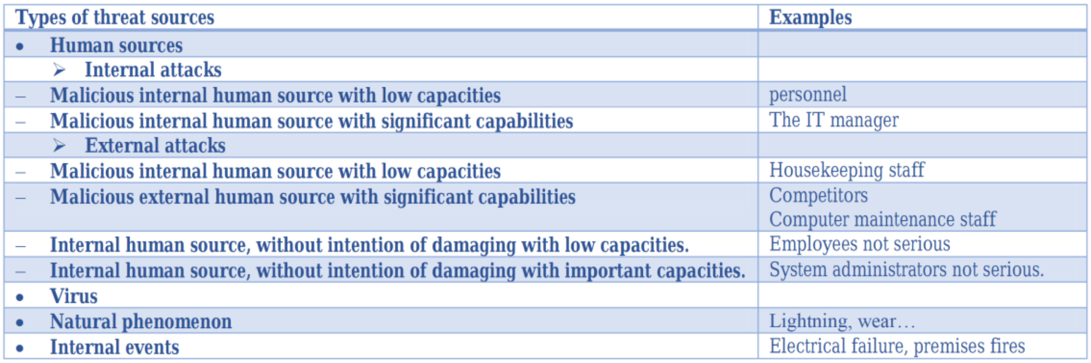
1. External – via the internet
2. Internal

v. Essential Elements to Protect

1. Access Objects – is a tool that allows access to applications and uses (computers, tablets, smartphones, ect.), using browsers to consume Cloud services (Chrome, Firefox, IE, Opera, or Safari).

2. IT Infrastructure – virtual machines, virtual servers, applications, platforms, infrastructures, databases, etc.
3. Consumer resources – personal data, critical data, applications, etc.
4. The networks – the channel between access objects and servers or applications is a very attractive attack target for hackers.

vi. Threat Sources



Types of threat sources	Examples
• Human sources	
➢ Internal attacks	
– Malicious internal human source with low capacities	personnel
– Malicious internal human source with significant capabilities	The IT manager
➢ External attacks	
– Malicious internal human source with low capacities	Housekeeping staff
– Malicious external human source with significant capabilities	Competitors Computer maintenance staff
– Internal human source, without intention of damaging with low capacities.	Employees not serious
– Internal human source, without intention of damaging with important capacities.	System administrators not serious.
• Virus	
• Natural phenomenon	Lightning, wear…
• Internal events	Electrical failure, premises fires

vii. Security Constraints and Requirements of a Cloud environment

1. Availability: This is the property of timely accessibility of an essential element, by authorized users.
2. Integrity: This is the property of accuracy and exhaustiveness of an essential element
3. Confidentiality: This is the property of an essential element of being known only by authorized users
4. Audibility: It is the property of an essential element, allowing to recover, with sufficient confidence, the circumstances in which this element evolves

viii. What are the benefits/risks of using the cloud?

1. Benefits
   a. Cost cutting
   b. Guaranteed accessibility
   c. Flexibility
   d. Automatic updates

2. Risks - Outsourcing data to a cloud computing provider creates a risk to the **integrity of the information system** due to;
   a. Dependency of the supplier, potential unavailability of the infrastructure
   b. Technical risks – deficiencies in interfaces and APIs.
   c. Loss of data, modification of data, non-recovery of data, loss of control of data, and loss of control of destruction of data.
   d. Lack of data and communications encryption,
   e. Vulnerabilities that result in account theft and unauthorized access (Usurpation of Identity)
   f. Legal risk - Potential inconsistencies between jurisdictions may lead to compromised confidentiality of data as authorities of the country may have access rights to the data.

g. Risks related to the choices of the Service Provider – data maybe used for purposes other than the customers (sale of data); management of the Cloud by incompetent or malicious people; non-compliance with security requirements (difficult to audit due to lack of traceability of data access, difficulty in ensuring SLA clauses are respected).
h. Risk of Break in service – moving to another service provider is very difficult due to lack of portability of data or solutions. Cessation of service maybe due to late payment of invoices, failed internet connection, or service decision to close the service or end of contract.

II - 5G

Maple Finance is currently evaluating the shift of their customer applications to the 5G network, risk identification is an important input into this decision process.

i. 5G Overview

5G promises to transform "dumb pipes" into a massively scalable, high-speed and low-latency service delivery platform, enabling diverse applications such as autonomous cars, smart grids, industrialized robotics, and more.[1] Industrial IoT connections will increase from 17.7 billion in 2020 to 36.8 billion in 2025[2]

5G network architecture is significantly different from the architectures of any previous generation network, where new network technologies are proposed both for the access and core network infrastructures, new actors (stakeholders) arise, and novel business models are made possible.

The biggest difference between 4G and 5G design requirements is the diversity of use-cases that 5G networks must support as compared to 4G networks that were primarily designed for the single use-case of delivering high speed mobile broadband.

5G is the new generation of radio systems and network architecture delivering extreme broadband and ultra robust, low latency connectivity and massive networking for the Internet of Things to enable the programmable world, which will transform our individual lives, economy and society.

ii. Use Cases

1. Massive broadband that delivers gigabytes of bandwidth on demand
2. Critical machine-type communication that allows for the immediate, synchronous eye-hand feedback that enables remote control over robots
3. Massive machine-type communication that connects billions of sensors and machines

A key design principle for 5G networks is flexibility, to cater to unknown use-cases of the future. And related to flexibility is another key design principle of 'reliability'. With the flexible

[1] https://www.allot.com/nfv-5g-architecture/
[2] https://www.juniperresearch.com/press/industrial-iot-iiot-connections-smart-factories

integration of different technology components, we will see a step away from best effort mobile broadband towards truly reliable communication. Reliability is not only about equipment up-time, it also relates to the perception of infinite capacity and coverage that future mobile networks need to deliver anytime anywhere. Furthermore, reliability is becoming more critical as we start to rely on mobile communications for control and safety.

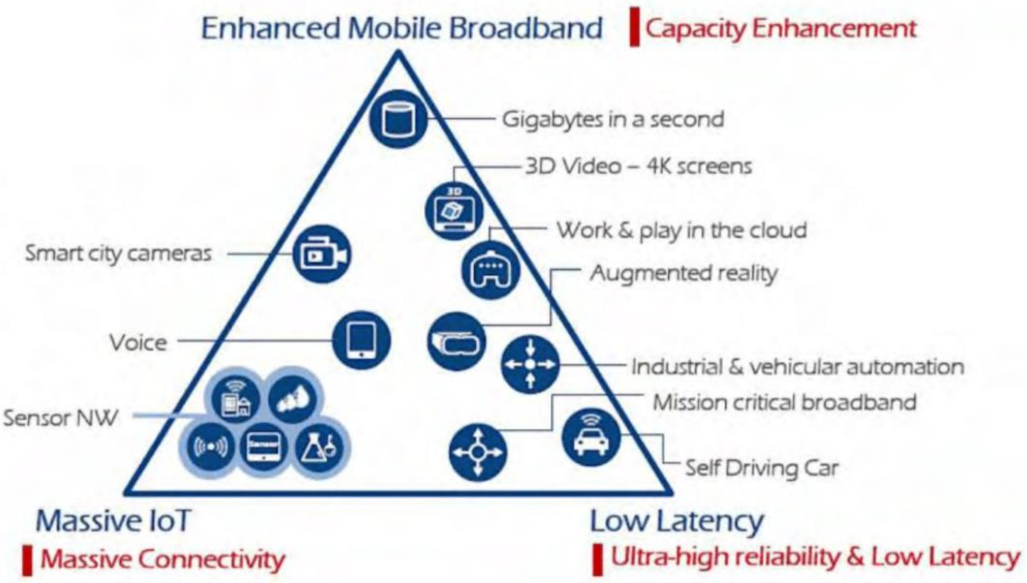
iii. Attack Surface

The attack surface in 5G is much bigger because of massive number of connected devices, the virtualization techniques, the support for open networks, etc. We foresee that 5G systems design and deployment will raise numerous security challenges and resulting risks, like:

1. related to network virtualization (specific mobile and multi-tenant VNFs, sensitive data isolation etc.);
2. risks induced by wireless network topology: multi-RAT, HetNets, multi-hop, D2D, unlicensed spectrum as alternative access…;
3. new services (plain "old" communication services, utilities, mission-critical applications, M2M/IOT/sensors, V2X…) will co-exist and thus will necessitate devising particular end-to-end 5G security architecture allying optimization and complexity of the system.

iv. Risk Assessment

Therefore, the Risk assessment for 5G must be carefully studied and defined by examining the current methodologies and coming with a comprehensive model that will best adapt to the new network architecture, stakeholders, and business models. Our approach is to perform a risk assessment and mitigation evaluation related to multi-stakeholder 5G system and Network Function Virtualization (NFV), comprising new risks, and modifying existing ones[3]



[3] http://5gensure.eu/sites/default/files/5G-ENSURE_D2.6_Risk%20assessment%20mitigation%20and%20requirements%20%28final%29_0.pdf

v. Security questions

Securing 'things' as opposed to human-owned devices is a complicated process. But it can be understood in terms of answering six key questions:

1. What is the device's identity?
2. How can the device authenticate itself?
3. Does on-device data need to be encrypted?
4. Does over-the-air data need to be encrypted?
5. How will trust be managed on the device?
6. How can vendors validate software/firmware updates?[4]

III – AI

Maple Finance is currently using AI in their insurance and banking divisions.

The insurance unit is using Natural Language Processing to improve decision-making by analyzing large volumes of text and identify 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, Maple Finance 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. Maple is planning to expand the use of AI for all loan applications.

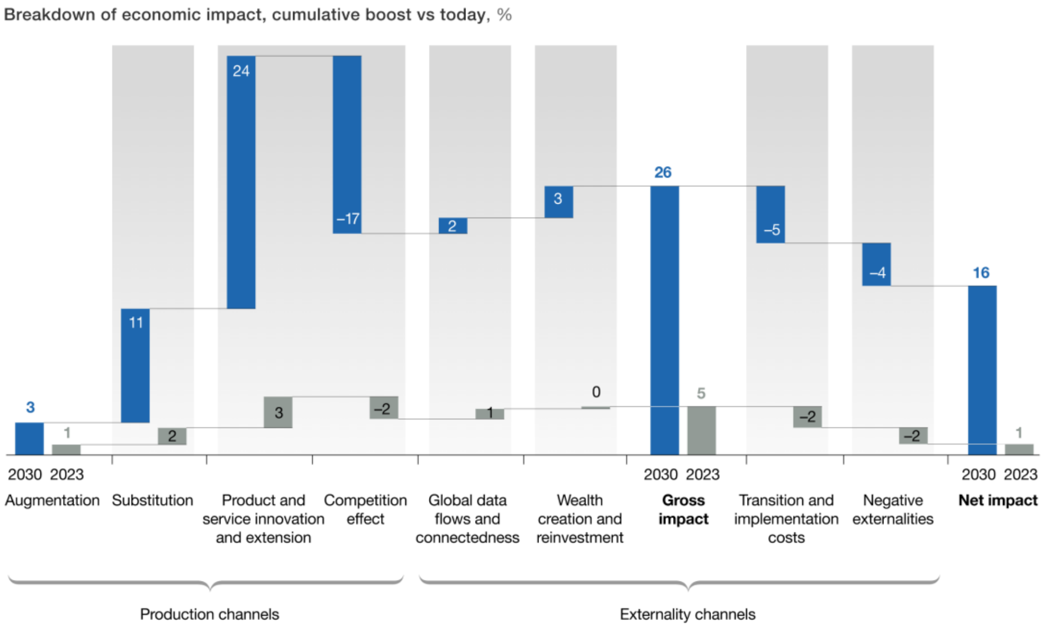
i. AI Overview

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.[5]

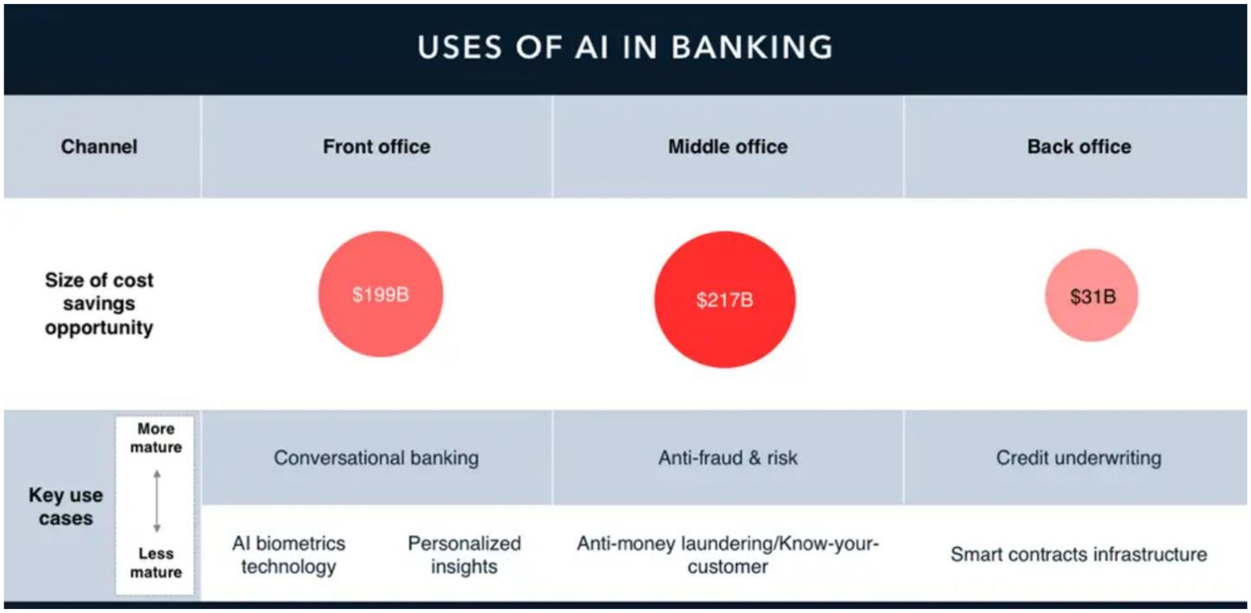
[4] https://www.thalesgroup.com/en/worldwide-digital-identity-and-security/iot/magazine/why-5g-creating-perfect-conditions-industrial?utm_source=acoustic&utm_medium=email&utm_campaign=DIS-Newsletter-2021-December%20remainder&spMailingID=26068951&spUserID=MTU1NjE3MTczNTU1S0&spJobID=2121554202&spReportId=MjEyMTU1NDIwMgS2

[5] https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-ai-frontier-modeling-the-impact-of-ai-on-the-world-economy


Breakdown of economic impact, cumulative boost vs today, %

ii. Uses of AI[6]

The management team at Maple Finance 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**[7] - 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.

[6] https://www.businessinsider.com/ai-in-banking-report

[77] https://www.ibm.com/ca-fr/topics/computer-vision

2. **natural language processing** - giving computers the ability to understand text and spoken words in much the same way human beings can.[8]
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.[9]
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.

[8] https://www.ibm.com/cloud/learn/natural-language-processing
[9] https://en.wikipedia.org/wiki/Virtual_assistant

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 Risk[10]

1. data difficulties,
2. technology troubles, and
3. security snags
4. algorithms and
5. human–machine interactions

[10] https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/confronting-the-risks-of-artificial-intelligence

vi. Unintended Consequences of AI[11]

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		

[11] https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/confronting-the-risks-of-artificial-intelligence

IV – Quantum Computing

Maple Finance is currently evaluating the application of quantum computing to run neural networks for their algorithmic risk modeling, as well as the potential cyber security threats that quantum computers may pose to the organization. A risk identification is an important input into this review process.

i. How does Quantum Computing Work?

Quantum computers perform calculations based on the probability of an object's state before it is measured - instead of just 1s or 0s - which means they have the potential to process exponentially more data compared to classical computers.

In quantum computing, operations instead use the quantum state of an object to produce what's known as a qubit. These states are the undefined properties of an object before they've been detected, such as the spin of an electron or the polarisation of a photon.

Rather than having a clear position, unmeasured quantum states occur in a mixed 'superposition', not unlike a coin spinning through the air before it lands in your hand.

These superpositions can be entangled with those of other objects, meaning their final outcomes will be mathematically related even if we don't know yet what they are.

The complex mathematics behind these unsettled states of entangled 'spinning coins' can be plugged into special algorithms to make short work of problems that would take a classical computer a long time to work out... if they could ever calculate them at all.

Such algorithms would be useful in solving complex mathematical problems, producing hard-to-break security codes, or predicting multiple particle interactions in chemical reactions.[12]

ii. Quantum Risk

Quantum Risk exists because of the business dependency we have on data from our co-dependent supply chains to dependent ecosystems. Quantum is a term from physics that describes particles' properties, "quantum" will help frame new risk characteristics. [13].

iii. Primary characteristics of quantum particles' behaviour are:

- the uncertainty principle,
- composite systems and
- entanglement.

iv. Examples of characteristics for Quantum risk are:

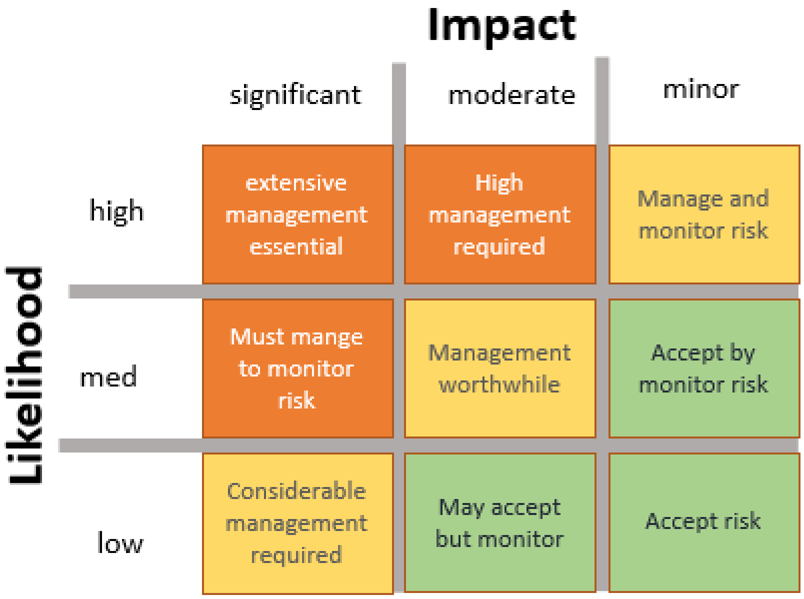
- When you observe the same risk twice, it might not be there, and it will look different.
- The same risk can be in many places simultaneously, but it is only one risk.
- Your risk and my risk directly affect each other across our data ecosystem; they are coupled but may not be directly connected.

[12] https://www.sciencealert.com/quantum-computers

[13] https://opengovernance.net/quantum-risk-a-wicked-problem-that-emerges-at-the-boundaries-of-our-data-dependency-2dc36dfb21fb

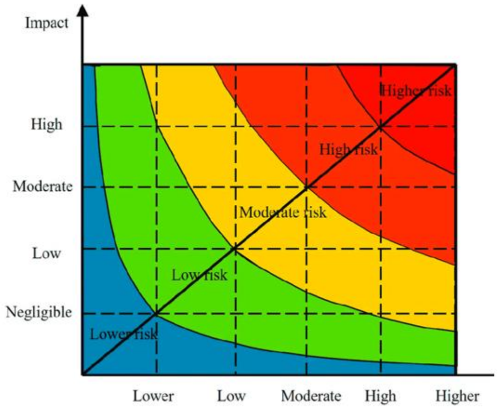
v. Impact of data quality

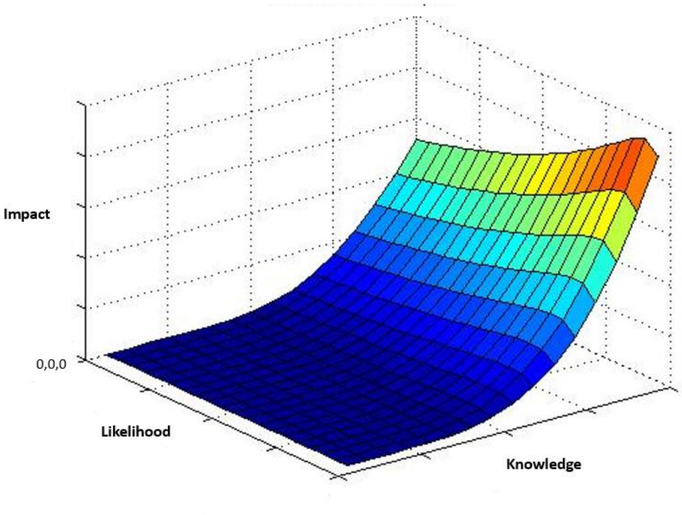
The output of Quantum computing relies on the quality of the data. If there is a deficit in knowledge because of poor data, it translates into an increased risk hidden because of poor data at any point in the matrix. Poor data (knowledge) can mean that either the impact (consequence) will be more severe, or the likelihood (probability) is more likely. In part, we can overcome poor data problems by recognising that it always exists, but it easily hides the rather current issues of pandemics and systemic risk. However, if the quality of knowledge is based on erroneous data (data without rights and attestation), we have no truth to the likelihood and impact.



		Impact		
		significant	moderate	minor
Likelihood	high	extensive management essential	High management required	Manage and monitor risk
	med	Must mange to monitor risk	Management worthwhile	Accept by monitor risk
	low	Considerable management required	May accept but monitor	Accept risk

Some sophisticated models and maths help qualify and understand the nature of risk depending on its nature and size. However, the list of risks that any one company faces is defined, specified and has been thought about over a long period.





vi. The Growing Universe of Risk

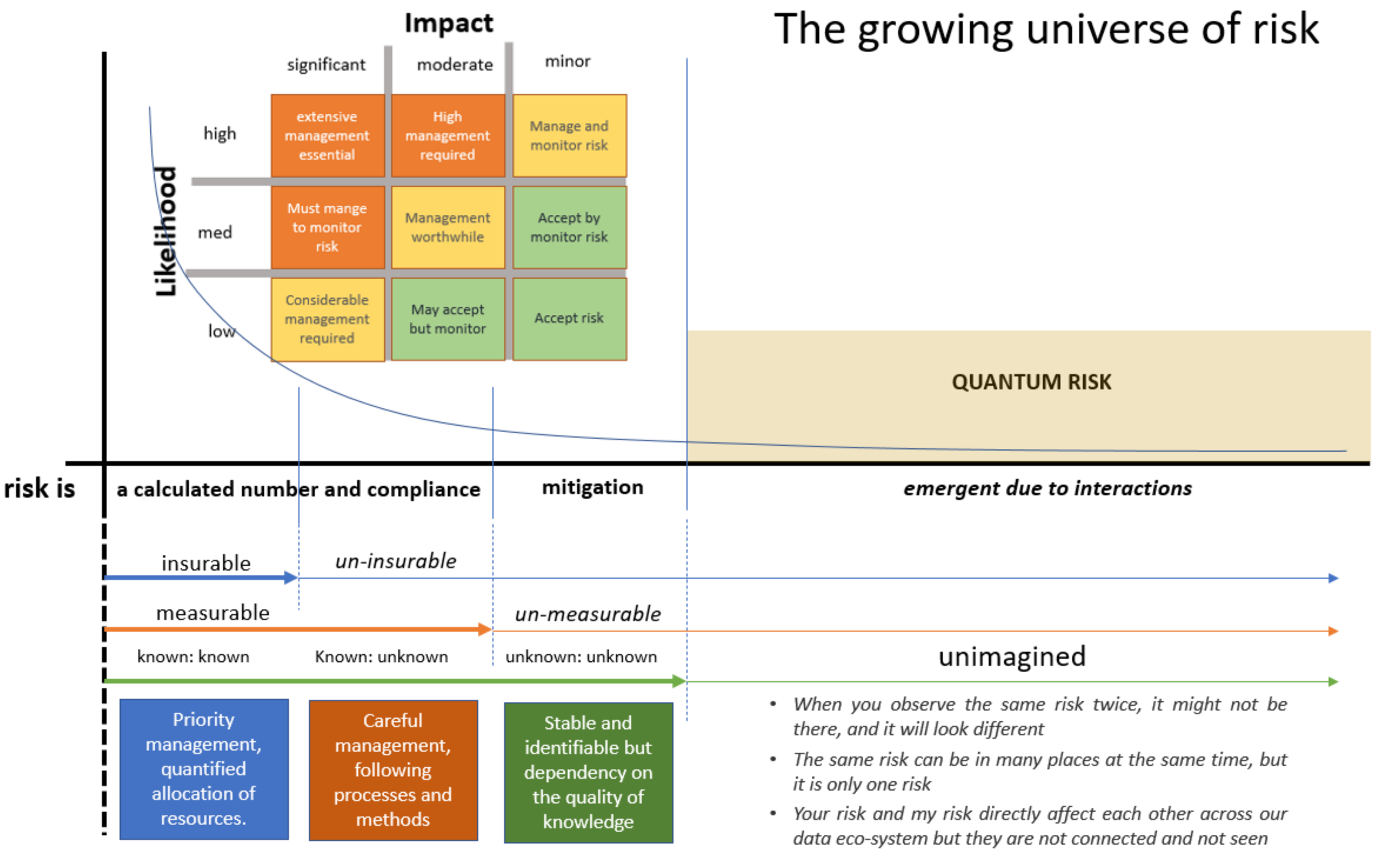
Quantum Risk arises, at the boundaries, in the long-tail of the universe of risk.

The Growing Universe of Risk illustrates the management of

1. insurable, measurable known:known (identified and shared) risk and
2. the un-insurable, measurable (impact, likelihood, knowledge) and known:unknown risk mainly because the determined likelihood of occurrence and impact is moderate is illustrated.
3. un-measurable unknown:unknown risk.

In mitigation, we accept that the data quality (knowledge) is poor, but the impact is low, as is the likelihood.

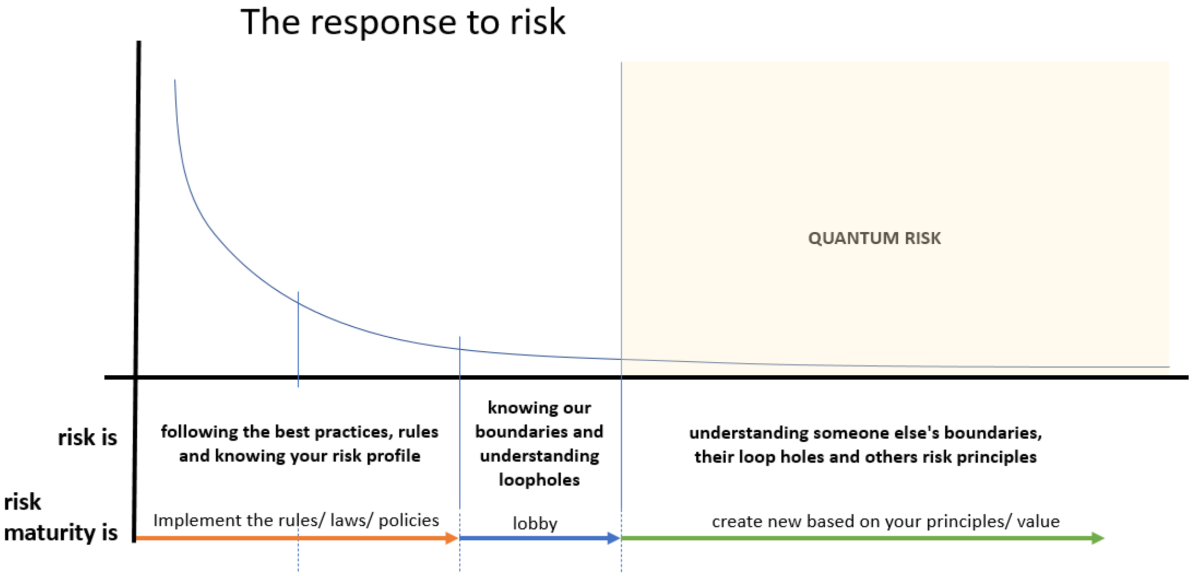
The Growing Universe of Risk


The growing universe of risk
Impact
Likelihood
QUANTUM RISK
risk is
a calculated number and compliance
mitigation
emergent due to interactions
insurable
un-insurable
measurable
un-measurable
known: known
Known: unknown
unknown: unknown
unimagined
Priority management, quantified allocation of resources.
Careful management, following processes and methods
Stable and identifiable but dependency on the quality of knowledge

	significant	moderate	minor
high	extensive management essential	High management required	Manage and monitor risk
med	Must mange to monitor risk	Management worthwhile	Accept by monitor risk
low	Considerable management required	May accept but monitor	Accept risk

- *When you observe the same risk twice, it might not be there, and it will look different*
- *The same risk can be in many places at the same time, but it is only one risk*
- *Your risk and my risk directly affect each other across our data eco-system but they are not connected and not seen*

Technology including Quantum risk is the next step out; it is emergent at the boundaries of (inter)-dependencies created as we need to create sustainable ecosystems where we share data. We are increasingly reliant on data from indirectly related players to our ecosystem, and we have no power or control. We have no rights to data and no clue on attestation. Quantum risk is not in our current risk model, or existing risk frameworks and maybe unimagined to us. The RIC discussed our response to Quantum risk in the context of The Response to Risk – Figure 2. MFG is currently at the beginning of the risk continuum when it comes to quantum risk, rule/laws/and policy based.


The response to risk
QUANTUM RISK
risk is
following the best practices, rules and knowing your risk profile
knowing our boundaries and understanding loopholes
understanding someone else's boundaries, their loop holes and others risk principles
risk maturity is
Implement the rules/ laws/ policies
lobby
create new based on your principles/ value

Quantum computers could break cryptography in a manner that adversely affects the financial system. NIST is currently working on post-quantum cryptography. Intelligence agencies and standardisation bodies including GCHQ (UK), NSA (USA) and NIST advocate a mitigation against quantum threat is to use post-quantum cryptography which simply relies on mathematical problems that are not affected by Shor's algorithm. NIST is on the verge of announcing the post-quantum algorithm that will protect date, identities, and devises over the next decade.[14]

[14] https://www.risk.net/risk-management/7911576/quantum-computing-kryptonite-for-bitcoin-and-cyber-security