NEW RISKS ON THE BLOCK

EMERGING RISKS SHAKING UP THE INDUSTRY

RiskMinds 365

RISKMINDS

Ed Stapley
Editor-in-Chief, RiskMinds International

Ana-Luiza Olanescu
Editor-in-Chief, RiskMinds Insurance, Asia & Americas

Charlie Burgess
Digital Content Editor

Georgia Hood & Josef Lanjri
Business Development Managers

CONTRIBUTORS

Dan Oprescu
Managing Director of Risk Surveillance and Analytics, Financial Institutions Commission of British Columbia

Periklis Thivaios
Researcher

Norman Marks
Retired CRO and CCO and thought leader in internal audit, risk management and governance

Guy Verhofstadt
Brexit Negotiator for the European Parliament & Former Belgian Prime Minister

Gerard Lyons
Leading U.K. economist

Cosimo Pacciani
CRO, European Stability Mechanism

INTRODUCTION

The nature of risk is evolving.

Some indicators are starting to suggest that economically the world is more stable than it has been since the onset of the global financial crisis. And while we may be far from a world without any financial worries, there now seems to be an increasing focus among senior risk managers on non-financial and emerging risks.

These emerging risks are different depending on who you ask, but they can range from cyber and conduct, to climate change and AI.

In this second RiskMinds365 eMagazine of 2018, we welcome experts in several key areas, to discuss their thoughts on the new risks and shed some light on the best practice to keep one step ahead.

We hope you enjoy it.

The RiskMinds365 team

CONTENTS

CAPTURING AND MODELLING EMERGING RISKS

Dan Oprescu

If you google “emerging risks” or “new risks” you will not find a Wikipedia entry, yet. Nevertheless, emerging risks are what keeps CEOs and CROs awake at night.

What defines emerging risks? Emerging risks can be new and unforeseen or future risks and/or the evolution of previously known risks that are difficult to quantify but likely have an important impact on society and industry, including the (re) insurance industry. One of the main problems to quantify emerging risks is that little historical data exists which allow for estimating potential losses and costs based on past experience. Common for all emerging risks is a lack of understanding of the threat they pose to firms and (re)insurers in today’s global and interconnected economy.

Amongst others, emerging risks include cyber risk, climate change, natural catastrophes, fiscal crises epidemics, resistance to antibiotics, cryptocurrency, water crises, and political and social instability. We will focus on cyber risk and natural catastrophes. These risks threaten firms with increased property damage and liability vulnerability. They could potentially lead to large secondary costs through disruption of supply chains and power networks. In addition, they have the potential of contagion and to affect many (re)insurers.

Risk.net presented IT disruption and data compromise among the industry’s top 10 operational risks in March 2018. Firms face the challenge of rapidly developing computer technologies and thus the rapid evolution of cyber risks. Potential liabilities could result from cyber-attacks, general failures of technology, threats to data security, cloud computing, and social media. Cyber-attacks could result in large recovery costs and reputational damage. Cyber risk is omnipresent, as every entity that relies on information technology and handles confidential information can be a target.

Another emerging risk is that of natural catastrophes that have been perceived to increase in severity. Fire hazard has been seen to increase due to climate change, resulting in less precipitation and hotter temperatures in the summer. British Columbia and Alberta saw record losses due to wildfires in 2017. A change in demographics leads to greater losses if wildfires occur as potentially more houses get burnt and infrastructure gets destroyed.

> “Each emerging risk will one day probably be treated like credit risk and be considered an ‘old and familiar risk’ that can be managed.”

In general, firms manage all forms of risk through a combination of policies and procedures aimed at preventing and mitigating each risk. This approach also applies to dealing with emerging risks. Insurance, however, is not an alternative to solid risk management. It is most effective in providing protection against residual risks that persist and resist additional proactive efforts. This approach will ultimately lead to finding appropriate insurance policies for emerging risks. Nevertheless, policy pricing and modelling assumptions are a major challenge for (re)insurers as there is lack of historical data. Understanding future claim levels and trends is essential to ensure adequate cover is offered and that premiums are priced at the right level. In order to cap potential losses, insurers set low limits and various exclusions in insuring emerging risks. As emerging risks, like cyber risks, change their patterns quickly, policies might not be up to date and leave firms with protection gaps.

Each emerging risk will one day probably be treated like credit risk, and be considered an “old and familiar risk” that can be managed, i.e. quantified and mitigated. One differentiator, however, is the potentially systemic nature of emerging risks. A cyber-attack most likely does not only target one firm but a cascade of firms doing business with the firm under attack. There is a substantial potential for contagion.

Regulators with a macroprudential mandate are carefully monitoring emerging risks, as they need to be alert with possible systemic consequences these risks could cause to the stability of a financial system that they protect. This includes assessing each emerging risk on its complete chain of consequences, including systemic impacts.

WHAT WILL BE THE IMPACT OF GLOBAL RISK IN 2018?

The World Economic Forum recently released their Global Risks Report 2018, highlighting the top concerns facing the world's population. As the pace of change accelerates and risk interconnections deepen, it is more critical than ever for risk managers to accurately identify and plan for risks which will impact their business.

The report notes that 2017 was a year of "widespread uncertainty, instability and fragility... and the latest results of our annual Global Risks Perception Survey suggests respondents are pessimistic about the year ahead."

Extreme weather events and natural disasters feature as the two most likely risk factors facing the planet this year, followed swiftly by cyber attacks and data fraud and theft. Couple this with the fact that these environmental events are also ranked as some of the most impactful and a feeling of pessimism among the respondents seems reasonable.

Many in the financial industry, and particularly within insurance, may be asking themselves what can be done to mitigate these high-stake risks, especially when so many can seem unpredictable.

Zurich Insurance's Chief Global Risk Officer, Alison Martin, took to Twitter to answer questions about the report, and how the insurance industry is stepping up.

CLIMATE CHANGE AND ITS REPERCUSSIONS

Environmental risks have been growing in prominence over the last decade, and seem to be coming to a head now, after a year filled with weather catastrophes across the globe. These risks aren't just confined to weather events though; the report highlights pressing hazards from water crises, accelerating biodiversity loss, and air, soil and water pollution.

So it isn't surprising that most questions sent in to #RiskChat were about climate change and its potential impacts over the upcoming year.

One key takeaway from Martin was that while "we're more likely to miss than hit the Paris Agreement targets," it isn't too late to make a difference. Making the shift to low-carbon energy and developing long-term solutions were key points to start managing the risks, with a particular focus coming from Martin on making responsible investments and moving away from thermal coal.

Insurance companies certainly have a vested interest in seeing the global risk of climate change being managed more effectively. As more disasters hit, homes, vehicles, travel plans and lives are impacted and more claims may need to be paid out than ever before.

WHEN RISK TURNS DIGITAL

It seems like cyber risk is on everyone's minds these days, and there's a fair reason for it. Cyber-attacks were perceived as the sixth most impactful risk, and the fourth most likely after climate change factors. Following this, massive data fraud and theft are causing concern, and even "adverse consequences of technological advances" are giving respondents pause for thought.

According to the report, cyber breaches recorded by businesses have doubled in the last five years, and in 2016 alone 357 million new malware variants were released. What were once considered large scale cyber-attacks are now becoming common place, so what can businesses do to be better prepared?

It was advised that "preparation is clearly key", and for businesses to understand their risk exposure. Indeed, this is reiterated time and again by CROs across the board, as they plan and test against cyber-threats for their own business.

THE FORGOTTEN RISKS?

With such existential risks to contend with, it can be hard to find time to focus on the (perceived) smaller and less likely risks of day-to-day. Interestingly, the report found many economical risks falling into lesser concern territory for their respondents, with unmanageable inflation, illicit trade, deflation and failure of financial mechanism or institution all being considered low likelihood-low impact.

This shift in perception will surprise no-one working in risk who has been a part of discussion on the rising emergence of non-financial risks, and how big data and AI can provide better analysis to make sense of the previously unpredictable.

Other risks failing to raise a big profile in the reports include:

- Failure of urban planning
- Failure of regional or global governance
- Unemployment and;
- Adverse consequences of technological advances

Low profile or not, risk managers, and especially those working within the insurance industry, will need to juggle a lot of urgent and important risks this year. Prioritising these will be increasingly difficult, and ensuring customer satisfaction and remaining profitable will add to the challenge.

ONE OBJECTIVE, BUT MULTIPLE RISKS

Norman Marks

One of the problems with 'traditional' risk management, which relies heavily on the periodic review of a list of risks (a risk register or what COSO calls a risk profile), is that it considers one risk at a time.

But there will usually be more than one risk that might affect the achievement of any objective. (I find it difficult to think of any objective where there is a single source of risk.)

So how do you consider the aggregate effect of these risks? How do you know whether the level of risk to your objective is acceptable?

The level of risk for each individual source of risk may be within what you call acceptable (based on risk appetite or criteria).

But the level of risk to an objective could be unacceptable when you consider all the sources of risk.

For example, if you have the objective of opening a new office and delivering additional revenue, many things might happen to affect its achievement, such as:

- Delays in the ability to open the office such as obtaining electrical supply, final inspection approvals, and so on
- Issues hiring local personnel to staff key functions
- Challenges connecting the new office to enterprise systems, such as security issues, a new language, and additional privacy regulations
- Changes in the local economy
- Adverse coverage in the local press
- Supply and logistics issues
- Turnover among key contacts at the companies you have targeted for sales

HOW DO YOU AGGREGATE THESE DIFFERENT SOURCES OF RISK?

Some organisations and consultants are wedded to the idea that the level of risk can be quantified and calculated as the magnitude of a potential effect (or consequence) multiplied by its likelihood. There are several problems with that, including:

1. There is almost always a range of possible consequences, each with its own likelihood, not a single point.
2. That range could include both positive and negative consequences. For example, the risk of a change in the value of a foreign currency (compared to your own) can be positive or negative.
3. It is difficult, if not impossible, to put a value on some sources of risk – such as employee safety.

But, let's assume we can get past those and we have five sources of risk. For each, the potential (adverse in each case) effect is assessed at $100,000 and the likelihood is 10%. So, the simple calculation gives us $10,000 for each. Do we simply calculate the aggregate level of risk at $50,000?

No. Let me explain with a hypothetical.

You are standing on the side of the street.

There is a 10% chance of rain; a 10% chance of being mugged (it's a bad area); a 10% chance of meeting your mother-in-law; a 10% chance of being hit by water thrown up by a passing car; and a 10% chance of a bird using you for target practice.

Is there a 10% chance of every single one of them happening? Even if there is a 10% chance of each happening within a year, will they all hit on the same day?

No.

Unless there is a single event or situation – a common point

of failure (something that triggers more than one effect) – the likelihood of them all occurring is the product of their likelihoods:

10% * 10% * 10% * 10% * 10% = 0.001%

Coming back to the five sources of risk, each of which is assessed at a 10% likelihood of $100,000, unless there is a single and common triggering event or situation, the likelihood of a $500,000 effect is inconsequential: 0.001%.

But can we ignore the fact that there are multiple potential sources of risk to a single objective?

Not at all.

Would you live in an area prone to earthquakes? I do.

Would you live in an area where there is a relatively high level of burglary? I do.

Would you live in an area that is likely to flood?

Would you live in an area where the level of noise is high?

You might choose to live where just one of these applies. But would you live where all of them apply, and probably others as well?

Common (and business) sense tells us that when there are more sources of risk, even if each one individually is acceptable, you are less willing to take a risk.

In the example, while there is a 10% chance of a specific one hitting, there is a 50% chance that at least one of the five (we don't know which) will hit and a 10% chance that two or more (we don't know which two) will hit.

Maybe some of you more mathematically included readers will correct the above and/or explain how to aggregate sources of risk that don't even get measured the same way (such as compliance risk, employee safety risk, reputation risk, and so on).

I have faith in the human power of common sense.

SUMMARY

1. Understand that a single objective, project, or plan has multiple sources of risk.
2. Understand the level of each and whether it is acceptable – and why.
3. Consider whether there is a common point of failure.
4. Carefully consider whether, with all the information about what might happen, it makes business sense to take the risk.

MANAGING THE RISKS OF BLOCKCHAIN

Periklis Thivaios

"Good judgement is the result of experience and experience the result of bad judgement "

- Mark Twain

The potential benefits of blockchain are widely discussed and advertised. Yet, because there is no return without risk, this article will provide an analytical framework for evaluating the risks inherent in the use of blockchain in financial services institutions.

We put forward two simple, yet significant, propositions.

1. Make sure that business problems are your main driver and technology is the supporting tool, rather than the other way around.

2. Thoroughly analyse and understand the associated risks upfront to minimise the costs and potential downsides of implementation. The ultimate decision is not a question of finding the perfect solution, but rather one where the benefits outweigh the drawbacks.

In this article, we assume a basic understanding of Distributed Ledger Technologies (DLT) which incorporate the sequencing of blocks (blockchains). We will, therefore, not delve deeply into describing what a DLT is and how it works. However, and to reduce confusion, we would like to make clear that blockchain and cryptocurrencies (such as Bitcoin) are not the same thing. Bitcoin is based on a distributed ledger technology, but one can have a blockchain that does not involve any cryptocurrencies at all. In other words, Bitcoin is not blockchain, just like email is not the internet.

ANALYSING THE RISKS

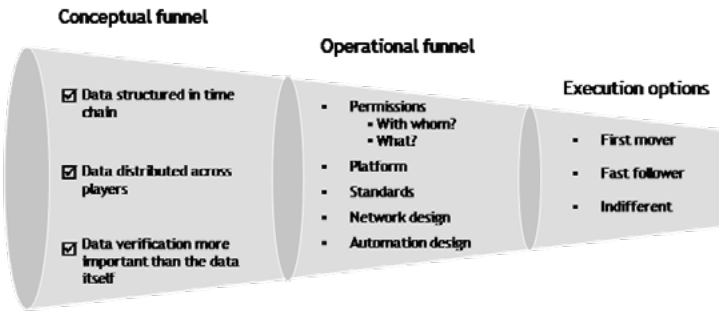
Based on the aforementioned points, we will provide a framework for analysing blockchain related risks, focusing on pre-implementation, implementation and post-implementation.

PRE-IMPLEMENTATION RISKS

Blockchain is often portrayed as the silver bullet for more problems than it is designed to solve. Therefore, the first step in pre-implementation risk analysis is to understand the cases where blockchain could be the right solution to our problem.

Practically, blockchain has the potential to address several problems, but there are also applications where blockchain is either not effective, or a rather inefficient solution. The following decision funnel can provide the analytical structure for evaluating the applicability of blockchain as a solution to the business problems we are trying to solve.

At the conceptual level, three elements stand out:



http://bankoxt.com/59140/blockchain-right-solution/
Figure 1: The blockchain decision funnel

1. Blockchain timestamps data in a sequential chain

Does the problem you are looking to solve require that the data is primarily structured in a time chain? In other words, is the sequencing of activities the most important dimension of what you are trying to capture?

2. The blockchain is about the proof of the data, not necessarily the data itself

Blockchains are designed (and therefore are most efficient) to hold a record of activity. In other words, blockchain architectures should not be understood as databases holding information, but rather as a cryptographically secured proof of the information itself.

3. The proof of the data is distributed across a network of participants

Blockchain applications are founded on the sharing of data, and therefore the deployment of such technologies needs to be chosen for business problems where sharing is a benefit more than it is a risk.

Once the conceptual criteria have been satisfied, the next step is to evaluate the benefits and risks of different operational designs. These are the following:

PERMISSIONS AND SHARING.

Generally speaking, blockchains can be public, permissioned or private.

- ***Public*** (or unrestricted) blockchains are potentially accessible by everyone. They constitute the better understood 'version' of blockchain, due to the awareness surrounding Bitcoin, a prime example of a public blockchain.

- ***Permissioned*** blockchains are restricted to a number of approved participants. In other words, even though they are not open to everyone, they can be made available to the members of a specific group of participants. The R3 consortium is a good example.

- ***Private*** blockchains are used by a single party. They constitute the most extreme version of permissioned blockchains. As we have already discussed, their usefulness is –theoretically at least– limited.

PLATFORM.

Related to the discussion above is the choice of platform. The table on the right, by Philipp Sandner of the Frankfurt School Blockchain Centre provides an excellent summary between the three most commonly referenced blockchain architectures.

Characteristic	Ethereum	Hyperledger Fabric	R3 Corda
Description of platform	Generic blockchain platform	Modular blockchain platform	Specialised distributed ledger platform for financial industry
Governance	Ethereum developers	Linux foundation	R3
Mode of operation	Permissionless, public or private	Permissioned, private	Permissioned, private
Consensus	▪ Mining based on proof-of-work (PoW) ▪ Ledger level	▪ Broad understanding of consensus that allows multiple approaches ▪ Transaction level	▪ Specific understanding of consensus (i.e. notary nodes) ▪ Transaction level
Smart contracts	Smart contract code	Smart contract code	Smart contract code
Currency	▪ Ether ▪ Tokens via smart contract	▪ None ▪ Currency and tokens via chaincode	▪ None

STANDARDS AND INTEGRATION/ INTEROPERABILITY.

Given the early stages of blockchain development, it is only natural that there are no concrete blockchain standards (something like a Blockchain ISO). While the standards are being developed (often by a trial and error approach) within each platform, the interoperability between platforms is extremely limited, if non existent.

NETWORK DESIGN.

Regardless of the platform, the network design needs careful attention. Are all the nodes equal or can some of them carry greater significance than others? Are forks (competing versions of the ledger) permissible? And so on. Each design decision comes with its own promised benefits and associated risks (known and unknown).

AUTOMATION DESIGN.

Last but not least, DLTs are equipped with a powerful automation technology known as smart contracts. Smart contracts represent a condition-based, self executable layer of code sitting on a blockchain infrastructure. The potential benefits are numerous, but so are the risks. Automated actions can be risky and the ability of humans to intervene should be considered as a mitigating factor.

Read the full article including the implementation risks involved >>

TURBULENCE AHEAD: GEOPOLITICAL RISKS OF TODAY AND TOMORROW

RiskMinds365

The political climate across the world is constantly shifting, and with new parties coming into power, new laws and bills being signed into action and Brexit on the horizon, financial institutions need to be more tuned in than ever.

Here, Guy Verfofstadt, Brexit Negotiator for the European Parliament & Former Belgian Prime Minister; Gerard Lyons, former Chief Economist at Standard Chartered bank and now Strategist at Net Wealth Investments; and Cosimo Paccaini, Chief Risk Officer at European Stability Mechanism answer some of the most pressing questions regarding the current geopolitical situation and how it impacts risk management.

GUY VERHOFSTADT | Brexit Negotiator for the European Parliament & Former Belgian Prime Minister

GERARD LYONS | Former Chief Economist at Standard Chartered bank; now Strategist at Net Wealth Investments

COSIMO PACCAINI | Chief Risk Officer at European Stability Mechanism

WHAT DOES GOOD RISK CULTURE ACTUALLY LOOK LIKE?

Whilst the scope and discussion around risk culture has grown at a rapid rate in the last decade or so, there has been an explosion on the topic of good conduct and good culture in the last couple of years. Leaving many asking the question: what does good risk culture actually look like?

To get to the bottom of this, it's crucial to understand what risk culture means. Risk culture, or conduct risk as it is interchangeably known as, can be hard to define, but what it generally boils down to is people risk. Everyone in the business, from the CEO to the receptionist on the front desk, has a part to play in their company's risk culture.

Bad conduct risk management rarely makes the headlines – in fact, it can be hard to even pinpoint where and when things start to slip. Rachel Conran, Chief Underwriting Officer at SCOR Group has the job of underwriting company conduct risk and explained what she looks for when assessing the risk culture. "I look at the causes that lead to that conduct," she began. "For instance, cultural cohesion. If the c-suite is an island, an inner circle of people, or there isn't diversity and people that will challenge the board, that can ring alarm bells. What happens at the board level trickles down; the board set the cultural acceptance of a corporation."

The few times a scandal makes it to the headlines, they are catastrophic. Cases like Nick Leeson's insider trading, which ended in the collapse of Baring's Bank, is perhaps the biggest example of irreversible repercussions from mis-managed conduct risk for a financial institution. Yet over the last 22 years, there have been several other financial scandals. It seems we still have plenty to learn.

Most (if not all) senior managers now agree that conduct risk needs to be treated with the same respect and rigor as credit risk, and while it may seem like an immature category of risk – the discipline should be the same.

THE MYTHS SURROUNDING GOOD CULTURE

As senior managers have grappled with the need to overhaul their company culture, they have increasingly come up with a number of crutches to help them, many of which don't work.

Rafael Gomes, Senior Manager at Accenture, describes four "myths" being touted around developing a good risk culture:

Myth 1 - If you hire good people, good behaviours will follow (when in fact individual behaviours are based on a culture)

Myth 2 - It's all down to apples and the barrel is sound (many of the miss-selling practices were an issue of the business model such as the overreliance on sophisticated maths)

Myth 3 - Incentives are essential for promoting the right behaviours (it's the non-financial incentives, particularly among high earners, that must complement this)

Myth 4 - Conduct and culture are all trading floor issues (when in fact this belongs across every level)

HOW TO SUPPORT GOOD CONDUCT RISK

Good culture depends on how an institution, and the people within it, interpret the rules it has been given, and the support they receive in doing this. There are perhaps two approaches, one that follows the letter of the law and uses it as a tick box exercise for compliance, and one that implements the spirit of the law. Gomes continues, "if you follow it in spirit you can set out more sustainable behaviours and that can be a strategic differentiator. That begins to breakdown the game of cat and mouse between regulators and industry."

The key to building the framework of a good culture, particularly where customers are concerned, is to identify key touchpoints; whether that's the marketing message, the decisions made within a business unit, or the employee selling the product. Customers won't be the only benefactors of this approach; proactive behaviour from banks will ward off regulatory action.

And, whilst using data and KPIs is great for keeping an eye on progress, it can be detrimental to use too many. Indeed, excessive targets and incentives on an individual level can lead to indiscriminate behaviour, and some underwriters also consider how people are remunerated, which can show how acceptable it is within the organisation to spend corporate money. Gomes adds that, "KPIs are just data. For them to be useful and to get buy in and to be used sustainably that data needs to be moderated by qualitative judgement."

"The key to seeing what good culture looks like in your own organisation," he concluded, "is to get the right information to the right people and empowering them to make better decisions."

JOIN THE CONVERSATION
#RISKMINDS