European Risk Management Council

Risk Landscape Review

December 2017

- **Brexit**: why the process so painful and what can help to progress
- **Cybersecurity**: when cyber criminals become more sophisticated, what should the Board and decision-makers do in response?
- **Fintech**: it's time to get technical dividends in risk management
- **Blockchain**: when distributed ledger technology makes sense

DEAR READER,

I am delighted to present the Q4 2017 edition of the Risk Landscape Review. This time the Review is dedicated to three "hot" risk topics:

Brexit: First six months of Brexit negotiations were confusing and frustrating with some moderate progress reached just now. In his article, Sir Stewart Eldon analyses why Brexit talks are so difficult and, as an international expert in negotiation and diplomatic skills, provides his suggestion on what can be done to help the Brexit process.

Cyber security remains a prime concern for financial institutions globally. In our Q4 edition, we present two articles dedicated to cyber risk. Michael Imeson looks at a recent evolution in cyber threats and provides an overview of the cybersecurity best practice in Europe and the US. Kevin Duffey explains how CROs and the Board should be prepared to lead recovery in case of a major data breach and why a simulation of cyber-attack becomes a vital tool for training the Board and decision-makers.

Fintech continues a rapidly transformation of many areas of the financial services including risk management. In their article, Christian Pedersen and Wolfram Hedrich analyse opportunities offered by technological advancements for improving performance and building new capabilities of risk management. They propose a road map to creating an efficient digitized risk function. Claudia Marcusson in her Blackchin breakfast for CROs explains in layman's terms what blockchain is about, why blockchain does not equal Bitcoin (although both words share five letters of the alphabet) and when blockchain technology makes sense.

My huge thank you to all authors who contributed to our Q4 Risk Landscape Review.

Enjoy the reading.

Yours sincerely,

Dr Evgueni Ivantsov

Chairman of European Risk Management Council

Table of Contents

Brexit after the European Council

By Sir Stewart Eldon, KCMG OBE, former UK Permanent Representative to NATO, UK Deputy Permanent Representative to the UN and UK Ambassador to Ireland

The analysis of the BREXIT negotiations below was developed from remarks made to the Partners Dinner of the FERMA Risk Management Conference shortly before the October European Council. It has been updated to reflect developments since.

The October European Council decided the BREXIT negotiations had not made sufficient progress to move to the second stage covering the UK's future relationship with the EU. But the atmosphere had changed since Mrs May's Florence speech in September, and EU leaders did decide to begin internal discussion of the future relationship.

Leaving aside the complex substance, BREXIT is difficult because so much emotion is involved. In the UK, the debate is still largely ruled by people's hearts rather than their heads. It will be fuelled further by the Parliamentary debate on the EU (Withdrawal) Bill.

Emotion plays a role for the EU too. This is evident from e.g. M Juncker's and Mr Verhofstadt's periodic statements and from the furore and concern over leaks from various parts of the EU apparatus. Fortunately, EU leaders have recognised that public rows don't help and have moved to cool things down. But the strong EU reactions to David Davis' television interview following the December May/Juncker agreement illustrates the continuing sensitivities.

The second reason Brexit is complicated is that it needs strong leadership from all sides to navigate successfully through a highly charged situation. In the UK, it was never going to be easy to hold together either divided political parties or a self-evidently divided nation.

Leadership is complex on the EU side too. Until October the Commission negotiators could motor on behind the European Council guidelines. They were good enough to start with – and certainly set out the EU's key concerns. But since Mrs May's Florence speech and the discussion around the October European Council it was increasingly clear the guidelines needed to grow and adapt to meet the EU's purpose. The papers put to the December European Council will be important in that context and should be calibrated carefully. There will be a requirement to stake out a negotiating position. But that should not obscure the need to secure an outcome that meets the EU's broader strategic interests – and I would argue those of the UK, since, ultimately, they largely coincide.

EU leadership dynamics are inevitably complicated by national agendas. Given the history of many messy EU budget negotiations, it's not surprising the supposed lack of clarity over the financial divorce settlement featured so heavily in the run-up to the October European Council and beyond. Ireland also has its very specific issues in a BREXIT context (which of course affect both parts of the island of Ireland). And the continuing negotiations in Germany over the formation of a new coalition government add a sense of unease.

There is also a continuing feeling across European governments and business that – put at its most benign – the UK cannot be seen to do

better outside the tent than in. The rationale varies from discouraging other EU member states from leaving the Union to demonstrating clearly the benefits the EU offers to its members. Both are difficult arguments for UK Brexiteers to swallow. Certainly, at present there seems no rush for the exit door.

Thirdly, there is the big issue of uncertainty and lack of clarity. This has become – and remains - hugely important. Complaints about the lack of a clear UK position are probably the biggest issue in the public (let alone private) debate on both sides of the English Channel. On any given day, a fair proportion of the British press will be devoted to the strapline 'Business needs Clarity'. This is mirrored in Europe, though with somewhat different emphasis and motivation.

Views about Brexit among British and European business vary by company, sector and individual but the need for clarity is a fair one. Various statements by business leaders in the run-up to the May/Juncker agreement have served to concentrate minds and underline how important this is.

The December European Council will mark a significant turning point in the negotiations. How can we expect the subsequent discussions to go? And what can be done to ensure they remain on track? The answer to the first of these questions is almost certainly 'not as fast or well as one would like'. It's important not to get carried away by the ebb and flow of negotiations and over-hyped media coverage. In no negotiation will everything ever be put on the table, and lots of things will be said and done for effect. Atmospherics are now better. But the British government still has a lot to do to clarify its positions and think through its negotiating options, as does the EU.

What can be done to help the process? The key issue is to move the negotiations from a 'win/lose' mentality to 'win/win'. As the BREXIT deadline moves closer, I would expect more EU member states to share that view.

Negotiations on a transitional period and the subsequent relationship will not be easy. There is as yet little clarity about what the transition period would entail – except, in the British Government view, little immediate change! The major argument will be about the extent to which the terms of the transition might pre-empt what follows thereafter. But it is essential to prepare the ground for the even longer and harder slog of agreeing future economic and trade relationships. Here again, the major issue will be the extent of the freedom the UK has to plough its own trade and economic furrow in the future. So moving to 'win-win' now is of extreme importance. It's also important to remember that successful negotiations need durable outcomes – and that those are best achieved through fair process.

The Cyber Risks Facing Banks

By Michael Imeson, a Contributing Editor of The Banker magazine and a Senior Content Editor at Financial Times Live

Cyber attacks on banks have become more frequent and serious and are hitting the headlines with depressing regulatory. The Petya offensive that struck some of the world's largest companies, including banks, in more than 60 countries in June 2017 was just one of many recent incidents that have set alarm bells ringing at bank HQs.

The largest known cyber heist to date remains the $81m theft in 2016 from the central bank of Bangladesh's account at the Federal Reserve Bank of New York, where funds ended up in accounts in the Philippines, Sri Lanka and other parts of Asia.

"Cyber threats to banks are very real," says Rich Baich, chief information security officer (CISO) for US banking giant Wells Fargo. "Why? It's obvious. When a notorious bank robber in the 1920s was asked by a reporter why he robbed banks he replied, 'Because that's where the money is'."

But today there are many other motives as well, says Mr Baich, such as one country wanting to disrupt another's financial system for political reasons. Or for criminal gangs wanting to steal intellectual property or customer data.

Effective cyber security is therefore essential, but technology on its own is not enough. "You have to instil the right culture in the bank," says Mr Baich, who is also chairman of the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC), a public private partnership between more than 70 financial institutions and the US Treasury Department.

Ensuring the CEO and board of directors are clued up is essential. That is why two years ago Wells Fargo appointed to its board Suzanne Vautrinot, a former US Air Force major general who worked in cyber operations and for US Cyber Command.

Wieland Alge, EMEA general manager at information security provider Barracuda Networks, says bank's executive and supervisory boards tend to be too hierarchical, which inhibits their ability to understand the threats their organisations face in cyberspace. It also makes them particularly prone to CEO email fraud, also known as "business email compromise", where an imposter impersonating the CEO directs the finance department to wire large sums to a fraudster's account, usually abroad.

Sophisticated attack tools

Some of the advanced tools used by criminals are stolen from national intelligence agencies and repurposed, such as the US National Security Agency's Eternal Blue which was used by the Wannacry attackers in 2017. But simpler tools can be just as effective, such as the pdf malware used in the Bank of Bangladesh fraud. In this case the malware adulterated the targeted bank's pdf reader, thereby altering its pdf statements in order to obfuscate the traces of the fraudulent messages which had previously been sent over the SWIFT financial messaging network to request and authorise payments.

It is important to mention that SWIFT's network was not compromised. It was the bank that was compromised in the way it communicated with SWIFT.In the wake of the Bangladesh incident, SWIFT set up a Customer Security Programme. "It helps banks defend themselves," says Marc Hofmann, SWIFT's chief information security officer (CISO). "One aspect of the Programme is the customer security control framework, under which we define security controls especially for banks' payment processes and local environments, establishing a community-wide baseline for basic security."

Counter measures

What, therefore, should banks be doing to improve security? "Risk mitigation strategies need to shift from 'compliance-driven' to 'threat-driven' with the speed of detection and response aligning with the speed and sophistication of threat actors," says Brendan Goode, regional CISO for UK & Ireland, and global head of information security operations, at Deutsche Bank. "A good cyber security strategy acknowledges that not all threats can be blocked and aligns preventive and detective controls with business priorities and risk appetite."

Fannie Mae, the US government sponsored enterprise that securitises mortgages, has a security policy it characterises as Get Right, Get Small, See Big. "Get Right is a continuous improvement programme of fixing and identifying all the problems we have, so we get the fundamentals of security right," says Chris Porter, Fannie Mae's CISO. "Get Small means shrinking the attack surface, shrinking data, shrinking access management entitlements – keeping the attack surface as small as possible.

"See Big is about visibility – having visibility over your network and third parties, putting the right cyber intelligence components in place and having the ability to identify, respond to and recover from attacks quickly."

"Two things worry me," says Robert Hannigan, who was director of GCHQ, the UK intelligence agency, until April 2017 and is now a cyber security adviser to insurance company Hiscox and consultants McKinsey. "One is the rising sophistication of attacks. There are more sophisticated tools available, some of them stolen, of course, and out there on the dark web.

"The second is that the finance sector has always worked on the basis that rational people are not going to damage a system on which they rely. But that doesn't apply to North Korea and one or two other actors – they don't have a stake in the international financial system and therefore probably don't care much if they cause disproportionate damage to it."

The legal and regulatory dimension

Legislators in Europe and elsewhere have been enacting laws to require banks and others to improve security. "Cyber crime is growing scarily fast and banks are in the front line," says Sir Julian King, the European Commissioner for the Security Union. "In the UK, Netherlands and Germany there are some innovative partnerships between banks and law enforcement agencies which could serve as a model for wider public-private cooperation, which is one of the themes that we pursue in our EU cyber security review published in September 2017, which updated the 2013 EU Cyber Security Strategy."

Enhancements to the NIS (Network and Information Systems) Directive, GDPR (General Data Protection Regulation), Payment Services Directive 2, ENISA (EU Agency for Network and Information Security) and many other things feature in the review. "What we are trying to do is catch up," adds Sir Julian. "The 2013 strategy was fine, but that was four years ago. We want a package of measures looking at how to strengthen across Europe human, technical, legal and international responses to the shifting threat."

In the US, the Office of the Comptroller of the Currency (OCC) is one of several regulators responsible for ensuring banks' information security is up to scratch. It is a member of the Federal Financial Institutions Examination Council (FFIEC) and it uses the FFIEC's IT handbook and the FFIEC's Cyber Security Assessment Tool when inspecting banks. The tool, introduced in 2015, is used by examiners and institutions to help identify the risks institutions face, and their cyber security preparedness.

"Although we do not require our institutions to use it, the tool is a very good way to thoroughly review an institution's cyber security posture and the level of controls they should have, depending on their activities and what their threat landscape looks like," says Beth Dugan, deputy comptroller for operational risk at the OCC. "There was a minor update a few months ago to give more flexibility when answering questions in the tool. They may be boring and mundane, but basic internal controls are invaluable."

Regulatory fragmentation

"Policy makers around the world have been introducing measures and standards to boost cyber resilience in financial institutions, but given the substantial differences in these regulations, there is too much fragmentation," says Martin Boer, director of regulatory affairs at the Institute of International Finance. This can lead to duplication and inconsistencies for internationally active firms and it is an issue we have been working on. We welcome the fact that the G20 has asked the Financial Stability Board (FSB) to review all cyber security regulation with a view to developing recommended practices."

Jenny Menna, SVP for security intelligence, engagement and awareness at US Bank, says there also needs to be greater regulatory harmonisation in the US, at federal and state level. "We recognise the importance of securing our systems and our customers' information, but when you have a mosaic of different regulations it becomes an extremely burdensome drill rather than something that supports security. So we'd like to see harmonisation between regulators at the federal level.

Risk tolerance

Given that crime can never be eradicated, only contained, what level of cyber intrusion can a bank tolerate? The level of loss a bank can stomach boils down to its risk appetite.

"The risk appetite of each organisation is different and needs to be determined as part of its risk management processes," says Brendan Goode, Deutsche Bank's regional CISO. "Although cyber-crime can only be 'contained', banks still need to invest in controls to deter cyber criminals from targeting them."

Those with the best defences will certainly be safer and help maintain the security of the financial system. But a repelled attack will only be deflected elsewhere, to a bank that is less well protected. Hackers will keep searching for a weak link until they eventually find one.

This article is a shorter version of one that was originally published in The Banker.

Chief Risk Officers and Cyber: Reducing risk by preparing the Board to lead recovery after a major data breach

By Kevin Duffey, Managing Director of Cyber Rescue, a European membership association that specialises in helping CEOs reduce the harm from cyberattack.

Chief Risk Officers frequently report that cyber is among the top risks they face. Companies suffer reputational, revenue and regulatory damage if they fail to respond to cyber attacks appropriately. And such attacks are growing exponentially, in sophistication as well as volume. Your organisation, and your suppliers, are increasingly likely to be breached. But while most banks are well prepared to respond to major market and credit events, few have sufficient experience of the operational and commercial challenges that follow a catastrophic cyber event.

So forward-thinking CROs are helping their Boards prepare to lead business recovery on the day of a major data breach. That preparation helps executives to handle the cascade of commercial consequences that follow a breach, to make things better rather than worse. Such preparation also helps focus the senior leadership on why regulations like GDPR deserve attention, why cyber resilience is a strategic issue, and why digital threats can't be left just to the IT Department.

Sadly, some Board members find the acronyms used by IT specialists off-putting. In a few companies, this gradually isolates the IT function: they are expected to protect the business, and scenarios in which protection fails aren't properly explored. But suppliers and staff cause as many cyber vulnerabilities as in-house IT systems. And when your defences are breached, it is your CEO and your commercial executives who will be called on to lead business recovery.

So CROs must encourage a whole-business response to cyber threats. An excellent start is to run an annual cyber attack simulation for the executive leadership. In ninety minutes, every director experiences the decisions they'll be called on to make – from operations to marketing to finance to HR. Such simulations have huge value, because the reputational damage caused by a bad commercial response is often more harmful to a business than the breach itself. Rehearsing recovery also motivates directors to consider the governance, compliance, culture and defences they'd want to have in place before the next real-life attack.

The European Risk Management Council will include a short cyber attack simulation at its annual European Leadership Meeting in March 2018. Participants will be invited to consider how their risk register calculations on cyber threats will be mitigated, or aggravated, by how well their executive colleagues are prepared for the cascade of consequences that follow a breach.

Shock is often the first – and paralysing – reaction to a breach. This emotion can be heightened by several factors. Executives often learn they've been breached by an outsider, e.g. by Law Enforcement (41%) or Third Parties including customers (35%). Executives often haven't been told of previous Data Incidents. Even worse, you are weeks behind the attackers, as the average time to discover a breach is 69 days.

Executives sometimes expect help from authorities, but are not sure who to engage. There are 31 (semi-) official organisations fighting cyber threats to Financial Services in the UK, where 68% of the Institute of Directors members are unaware of who to call. Some authorities are under-resourced. The UK's Information Commissioner's Office has 30 officers handling 200,000 concerns and 1,000 cases per year. The police have said only 4% of cybercrime is dealt with appropriately.

Your chain of command will be stressed by ambiguity during a suspected breach, and opinions may fill the gap where facts are missing. Only 45% of security professionals are confident they can determine the scope of a breach. External forensics typically lasts 43 days. Yet 91% of consumers expect to be told of a breach "in 24 hours or less."

Your legal responsibilities might not be immediately clear. For example, law enforcement may ask you not to notify customers, so that the hacker won't be alerted to their investigations. Extra-territorial laws on protection of citizens from cyberattack mean you may be subject to the requirements of more countries than you operate in. Just a summary of Privacy & Breach Notification laws runs to 425 pages.

Serious decisions require money. In the UK, 52% of CEOs think they have cyber insurance, but less than 10% do. Some 81% of companies with cyber cover in USA have never claimed on it. Claims paid have been on: Crisis Services (78%), Legal Defence (8%) & Settlement (9%) Executives must decide very quickly if they will pay for a big gesture of remorse. In the USA, 53% of Breach Notifications offer Credit Monitoring. But what's the trade-off? Abnormal churn after a breach ranges from 6.2% in the Financial Services sector, to 0.1% in Public Sector.

The surge in enquiries that follow a breach can quickly turn into even more irate calls from customers who – in their moment of crisis - want to speak to your team. But after a breach, call volumes can be one hundred times higher than normal. And in addition, you must communicate with Regulators, Suppliers, Press, Staff, Police and Shareholders, and manage Social Media.

You will be criticised, even if your company clearly suffered a criminal attack. Some customers will complain that you notified "too slowly … too fast … without cause … putting us at risk of scammers." Consumers might say "Credit Monitoring doesn't help me" or "How will you make this good" or simply "I want to break my contract and leave."

Every data breach is different, so no simulation can cover every scenario. And the follow-up from a simulation is in many ways more important than the simulation itself. So if you run such an event, prepare carefully. For example, some executives feel nervous about exposing their ignorance in front of their colleagues. So it's important to emphasise that no one is being evaluated. But a simulation isn't realistic without a bit of pressure. So consider splitting your Board into two teams, to encourage friendly competition. And you must introduce time pressure, as "the golden hour" is a defining characteristic of many crises. Most importantly, ensure that the simulation leads to signed-off improvements to your business continuity plan as well as to your cyber defences.

CROs can reduce the real risk of serious harm from cyber attacks, by ensuring the leadership are ready to lead recovery from such rare but high impact events. After a breach, your executives will be under enormous pressure to establish command and control, to stand-up qualified experts, to identify uncertainties and set priorities. You can avoid the shock, paralysis and well-intentioned mistakes many

executives make, by running a well-planned simulation.

An effective simulation is a springboard for cooperation between departments, energising work on regulatory compliance, good governance, employee training and technical defences. And after the simulation, there'll be much more engagement around your cyber risk dashboard. Your IT and Security teams will be working more closely together, knowing that the commercial significance of their functions are better appreciated by colleagues. Cyber is just another business risk, and CROs are best placed to lead efforts to mitigate it.

Targeting a Technology Dividend in Risk

By Christian Pedersen, Partner and Head of APAC Finance & Risk practice at Oliver Wyman; Wolfram Hedrich, Executive Director of Marsh & McLennan Companies' Asia Pacific Risk Center, Partner at Oliver Wyman

Current headwinds including high global debt levels, low economic and productivity growth, growing anti-globalization sentiment, increasing policy uncertainty and the hike in U.S. interest rates create significant macroeconomic challenges. At the same time, emerging risks from technological advancements are exposing organizations to new risks such as data fraud and cybersecurity. Strategic risk from technology that can disrupt business models is a growing concern.

The regulatory landscape is evolving too, with a deluge of regulations introduced after the global financial crisis substantially increasing expectations of risk management and increasing the cost of risk-taking for financial institutions. Globally, regulators have increased oversight of multiple areas including stress testing, recovery and resolution planning, cyber resilience and capital estimation. Risk teams are now under pressure to anticipate and solve newer uncertainties with insufficient additional resources to do so. The only way for organizations to address this conundrum is to leverage on emerging technologies to find material gains in productivity.

While many risk managers recognize the importance of harnessing emerging technologies for identifying and mitigating both traditional and 'newer' risks, few have implemented these solutions on a wide-enough-scale to be able to claim a material change in the way they run the risk function. We believe that the long-term benefits of new data and technologies widely outweigh the initial costs of development and that it is therefore crucial for risk managers to push forth with digitizing their firms' risk functions.

Targeting a Technology Dividend

More financial services institutions are starting to seize the substantial opportunities offered by technological advancements for improving

efficiency and building new capabilities to address risk. Risk managers are deploying advanced analytics, non-traditional data, natural-language processing and process digitization. Technology gains can be realized across multiple functions and processes, only if risk teams adopt a more practical and affordable approach by focusing on three major levers.

Data— By deploying new internal and external sources of data which continue to grow at an unprecedented rate, more and more financial institutions are turning to data analytics to manage their growing knowledge base. For example, leading banks are using transactions data, social media and other sources to achieve close to real-time insights into customer-level risk. This has produced dividends in early warning signalling and problem loan management, as well as helping to lower initial underwriting costs. In our experience, social media data can provide predictive measures of enhanced default risk up to six months ahead of traditional indicators.

Analytics—Machine learning, natural language processing, self-learning algorithms and other advanced analytics have become affordable and readily available. A good illustration of using advanced analytics is improving debt collection. Traditional debt repayment collection practice involves a high volume of calls, most of them unsuccessful. Using natural-language processing and advanced analytics, a suite of predictive models can give organizations rich insights into when and how customers will respond to different forms of outreach. Collections strategies informed and enhanced by advanced analytics have lowered call volumes by over 30 percent. This has resulted in a 15-20 percent reduction in handling time, yielding savings of more than 20-30 percent.

Processes—Digitization also provides opportunities to automate and create new risk-monitoring processes for managing emerging or hidden risks. For example, to address conduct risk, financial institutions are combining machine learning and transaction data to automate conduct monitoring for mortgage underwriting. Similarly, credit-underwriting automation is quickly becoming the norm for financial services, with loan application process times falling from more than a few weeks to a few minutes. Pre-population of information by integrating customer data provides a hassle-free experience, and advanced analytics are built-in to implement quick decisions.

Horizons of Change

Maximizing the benefits accruing from a fully-digitized risk function will require a complete revamp of risk management processes, people, systems and data. In the context of digital opportunities, we see three horizons of change for risk teams:

- Traditional risk function optimization. Most financial institutions have undertaken initiatives to streamline and automate their existing risk value chain. While the source of efficiency gains comes from automation and near/offshoring, the core risk activities remain in-house. About 15-20 percent efficiency gains are typically observed in terms of costs savings and resource deployment to more value-adding tasks.
- Progressive risk foundation. Individuals need to be equipped with the right mix of capabilities to manage the newly-developed information technology infrastructure and extract insights from advanced risk-data analysis.
- Fully-digitized risk function. Ultimately, many risk processes may no longer remain owned by organizations. One popular future scenario envisaged is risk “staked in the cloud” where – subject to data protection and regulatory approvals - a fully in-house risk management function is no longer needed. Through application programming interfaces,

vendors and utilities are able to leverage technology to provide standardized solutions, risk estimates, and releases. The focus of the risk management function shifts from "scanning-the-horizon" activities to identifying new risks and managing vendors, providers and interfaces. Team sizes in any area of high human touch will diminish, leading to an estimated 60-70 percent efficiency gain.

For a typical medium-sized bank, realizing the full digitization potential is expected to translate to large cost savings along with higher levels of effectiveness, oversight and insight generation. However, the complete transformation journey will be complex with multiple interlinked elements.

Getting Started

Whilst the industry is abuzz with talk of digital ambitions, we are still not seeing as much development as we had expected, especially in Asia. The time for the risk function to embrace change and act is now. Investment in digital risk enablement is essential to remaining relevant, as the tools of tomorrow begin to become mature and accessible. There are five major steps to get started today:

1. Develop a digital risk-activity map. Understand the potential for efficiency gains across risk processes. Prioritize high-impact and quick-win areas to prove the concept. Launch a shortlist of initiatives to establish and fund the longer-term ambition.

2. Scan the competitive landscape to understand current positioning in comparison to peers. The global industry, including all players in your ecosystem, should be well understood so that you can develop transferrable insights, and anticipate where to partner and where to compete. Also, scan the FinTech world for any latest technology which can be bought or partnered with.

3. Define the digital ambition for risk to make sure it fits your vision for the future of risk management. Strategy and positioning for the future should be outlined and communicated to key stakeholders to ensure alignment. This should include all new risks such as data protection and cyber risk which may befall the risk function itself as a result of the advances.

4. Align regulatory strategy and relationship. Continuously monitor global and local regulatory changes relating to emerging technologies to understand the potential consequences. Regulators should be kept abreast of new thinking. Digital change brings material uncertainty, and regulatory bodies will need to be comfortable with your organization's response plan.

5. Establish the required talent model and implement your recruitment strategy. As automation and analytics streamline risk tasks, talent will become an important differentiator in leaner risk teams. As management teams build tomorrow's risk management function, they will need to find fewer but more broadly-skilled talent, while redeploying or reskilling staff who lose out to the machines. Future teams need to have more differentiated roles – such as data scientists and experts in data analytics – to fully embrace technological changes and improve productivity.

A digitized risk function will hence change the risk manager's role significantly:

Instead of solely measuring and setting limits on the day-to-day operational and financial risks of the firm, technology will allow risk managers to develop a wider understanding of industry innovation trends to help guide firm activities. This broader understanding of risk will help identify the many systemic and hidden risks that may arise from today's emerging and disruptive technologies.

Despite the focus on hard skills that digitization will inevitably bring, risk managers will still need to value the soft skills needed to interpret masses of data and "tell the story". Being able to simplify, contextualize, and explain the information produced by machines will be something only a human risk manager will be able to do effectively. In a digitized risk function where data processing is largely automated, communication skills will be more important than ever.

Automation will refocus skills away from "traditional" activities related to report production and compliance. Instead, risk managers will be able to become flexible and adaptable sources of analysis and advisory skills, and thus, will be able to provide more value-added services for the firm's strategy as a whole.

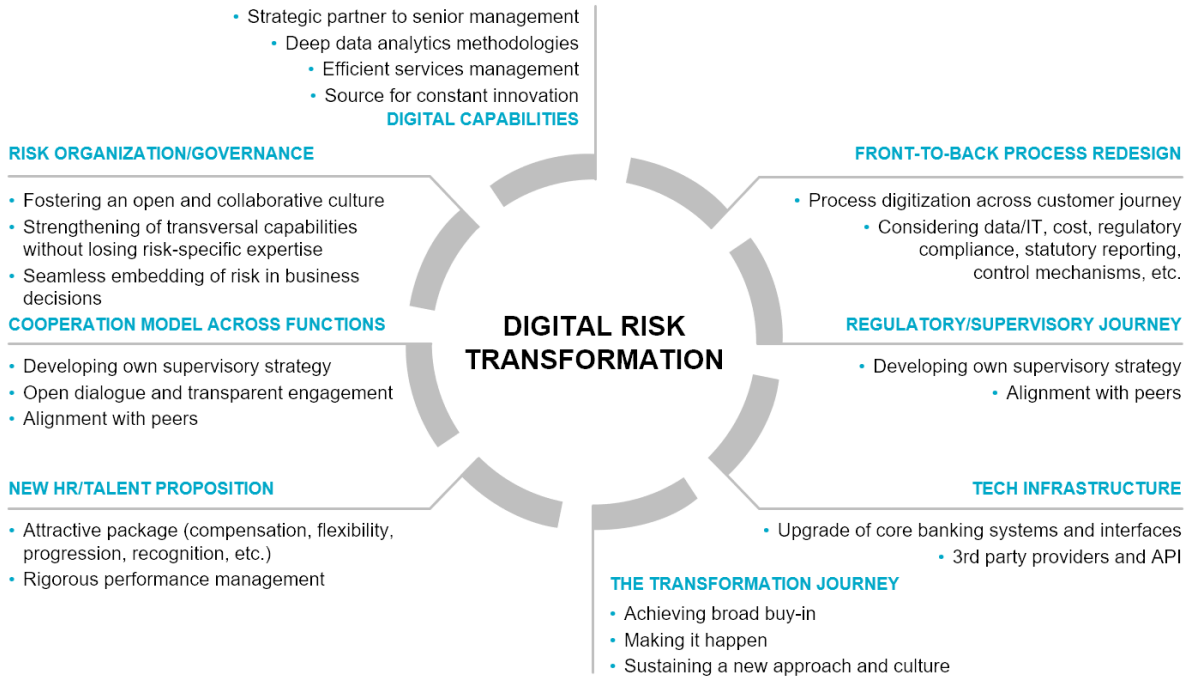
Equally crucial for this transformation will be both the ability of risk managers to educate themselves, and to expand their networks within and outside their organization. Becoming conversant in "tech-speak", attracting "new-age" talent like data scientists into the risk function, and being personally familiar with data science will be critical.

In the face of both the risks and the opportunities that new technology brings, risk managers have no choice but to redefine their operating model to reflect the evolving new reality on the ground.

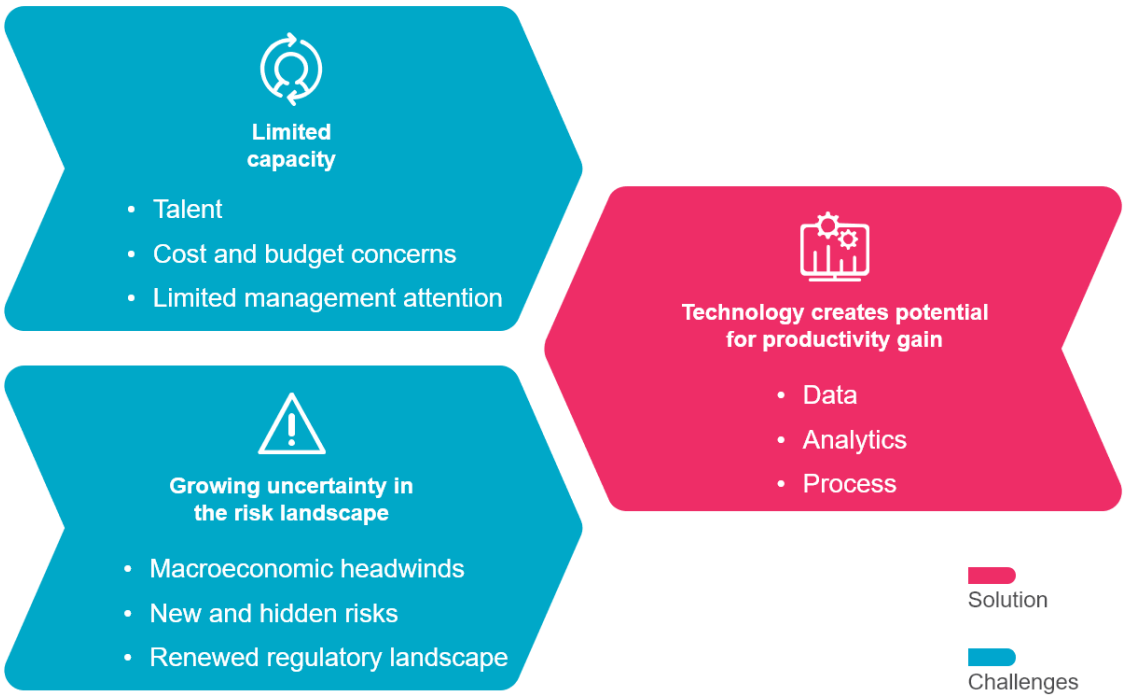
Digital transformation opens the way for risk managers to greatly increase their effectiveness and productivity. In this context, giving proper consideration to the digital transformation will definitely help risk managers add value to their respective organizations. Yet we are seeing many Asian banks' risk management functions exercise caution when it comes to changes; many Asian regulators need to get ahead of this curve to help their banking industries settle into the new world.

Parts of this article appeared on BRINK Asia.

DIGITAL RISK – NEEDS AND OPPORTUNITIES FOR TRANSFORMING RISK MANAGEMENT



SOLVING THE RISK MANAGER'S CONUNDRUM



Source: APRC analysis

Blockchain – Breakfast for CROs!

By Claudia Marcusson, Head of Risk Management and ExCo member at NN Investment Partners (formerly ING Investment Management) Singapore.

Blockchain in a nutshell

The first time I heard the term "blockchain", was a few years back at a barbeque with friends where we talked about the rapid technology developments especially here in Singapore where technology start-ups are booming. Intrigued by it, I asked questions about what it is and what it can do. My curiosity couldn't get fully satisfied over the talks and I decided to dive into it a few days later by doing some research. What struck me most was the analogy made that blockchain could be the next "big thing" and might be as revolutionary as the usage of internet up from the late 1990's.

Let me sketch a quick overview: Blockchain is often referred to as a Distributed Ledger Technology (DLT). If you talk to accountants they argue it is rather a "journal" and not a "ledger" because the sequential records of transactions are not segregated by account. Semantics aside, let's stick to the buzz term blockchain for now. Blockchain is the technology upon which bitcoin as one of the major cryptocurrencies (digital transactions without trusted intermediary) was built. Begin 2009, just after the financial crisis when trust in intermediaries shrunk, bitcoin has been developed and was the first application based on blockchain technology. Meanwhile there are >1300 different cryptocurrencies, a number growing every day and month and lots of other applications are being built using blockchain technology.

Bitcoin does not equal blockchain although both words share five letters of the alphabet. You can be sceptical about bitcoin and favourable towards blockchain. Last year when I was conducting a masterclass about blockchain for our top 200 leaders of NN Group, the bitcoin price was at US$600. This month bitcoin just hit US$17000. This steep rate hike is certainly fueled by speculation and not only the believe in growth of its underlying technology. I won't give you any investment recommendation on bitcoin, but I will explain why you should start understanding what the underlying technology is all about and why this matters to our profession.

A blockchain is a decentralized distributed ledger that records transactions and is verified by a consensus of users. It is a way for untrusted parties to reach agreement (consensus) on a common digital history or digital asset which can otherwise easily be faked and/or duplicated due to being digital. Blockchain is a data structure that solves this problem without using a trusted intermediary like a bank, clearing house or a government institution.

There are multiple blockchains and each blockchain network has different predefined rules and parameters (code standards/protocols) and different security permissions which can be used depending on the problem to be solved in the specific use case. For instance, for money transfers the tendency is to use Bitcoin protocol which has been specifically developed for remittance

purposes. It is good for transactions not demanding low latency because blocks are only created every 10 minutes. Ethereum is another blockchain network which creates blocks about every 15 seconds and has the ability to feature "smart contracts". A smart contract is a software implementation of a legal contract, basically a self-executing computable agreement being verified when its own conditions are met. You can think about financial instruments which are pre-programmed to carry out corporate actions like payments of bond coupons or dividends when certain pre-defined conditions are met. Bitcoin and Ethereum are only two examples and there are many more different blockchain networks, each having its own type of consensus mechanism, parameters for mining of the blocks, scalability, permissions and encryptions, etc.

Expect problems and eat them for breakfast

Blockchain is currently very high on the curve of the Gartner hype cycle. Therefore, motivation for corporates to develop "a blockchain solution" is similarly high. However, use cases should not be built around the technology. Instead you need to look first for the pain points in your organization and what kind of process or technology would be the best to solve it.

When blockchain technology makes sense:

- multiple parties share the same data,
- multiple parties have to update data,
- there is a requirement for verification (records need to be validated),
- intermediaries add cost and complexity,
- interactions are time sensitive (reducing latency has a business benefit),
- data records created by different participants depend on each other.

If you tick the box for at least 4 out of these 6 conditions, blockchain might be the solution. Of course, it is good to keep in mind that blockchain technology needs to solve the problem better than any alternative and it must generate a benefit greater than the cost of implementation and running it. Furthermore, it should not lead to side effects such as anticipated new risks that outweigh the generated benefits.

The general benefits are: cost reduction, efficiency and time savings, immutable transactions and real-time audit as well as enabling revenue growth e.g. attract new business through higher-quality service. Think about a mortgage or loan you can close online within 10 minutes, insurance claims which are verified within hours instead of days, settlement of securities instantly where the trade itself is the settlement which could lead to funds being so liquid that clients can invest several times per day instead of once per day or week.

Facing challenges should not be a hurdle to try!

The technology is relatively new and despite its young age it is already extremely robust and secure. Still implementations are vulnerable to hacks or bugs as we could witness the last years with successful hacks into different blockchain networks and its applications. Finding people with the right skill set and choosing the appropriate blockchain network depending on the use case, are key for success. From a risk management perspective, it is relevant to understand the technology to a certain degree to evaluate where the risks are lurking. Many corporates might be drawn back by the uncertain regulatory status in several jurisdictions, the unknown legal enforcement, the upfront investment as well as integration concerns when it comes to replacement of existing workforce and systems. In order to make the switch, companies must strategize the transition and culturally adopt it. Blockchain represents a complete shift to a decentralized network which requires the buy-in of its users and operators. Ultimately it

remains a management decision. Implementing a new technology might not be easy but that is where progress comes from. Daring to learn, doing something different in the interest of stakeholders and knowing the risks are just a few of the components. I would compare it to the internet era: for traditional businesses you do not want to be necessary the first but certainly also not the last.

Can it do your groceries?

Can you do your groceries for breakfast with blockchain? Yes, very soon it can. INS (https://ins.world) is building a decentralized grocery shopping ecosystem based on blockchain technology whereby customers can buy directly from the manufacturers. The middleman in form of retailers and wholesale companies will be cut out and according to INS it can therefore save up to 30% of costs for the consumers.

Many other applications based on blockchain technology are already in usage and more are developed every day. Blockchain has the ability to impact all industries on a global basis that rely on or utilize record keeping and require trust. In the financial industry classical examples are payment services, identity management and data verification (e.g. KYC & AML registries) and regulatory reporting.

Tomorrow Bitcoin might be at US$18000 or US$500, who knows. Do take a gamble if you can afford it. But if you consider yourself a visionary Risk Manager who likes to understand what will shape our industry in the coming years, make sure to understand the underlying technology and principles of blockchain. Happy to be your guide and sharing the knowledge on this topic, so do get in touch!

BLOCKCHAIN CHARACTERISTICS:

DECENTRALISED
shared across organisations, owned equally by all and dominated by no-one; No 3rd party or one entity can take control, reverse transactions or cease assets

DISTRIBUTED
multi-locational data structure; any user can keep own copy of the whole blockchain with all historical transaction; like a peer-to-peer network

LEDGER
like a "giant spreadsheet" shared openly on the internet (with data encryption); that can only be added to, nothing can be deleted once written; blockchains are immutable

RECORDING TRANSACTIONS
timestamped data entries ("any piece of information") identified by digital unique 'fingerprint' (hash), captured in a block and linked to each other in a chronological chain

VERIFIED
all members of the blockchain ("nodes") check that the transaction is valid and in the right order of the blockchain and pass the data to anyone else in the network who does not know yet

CONSENSUS OF USERS
consensus model, where majority of blockchain members confirm to add new data block to the ledger; each member updates own copy of blockchain by adding new block

Copyright © 2017. All Rights Reserved. Neither this publication nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without prior permission. Whilst every effort has been taken to verify the accuracy of the information presented at this publication, neither the European Risk Management Council nor its affiliates can accept any responsibility or liability for reliance by any person on this information.