European Risk Management Council

Risk Landscape Review

March 2020

- Addressing payment and settlement risk
- Climate change as global financial risk
- Cyber resilience and business resilience

DEAR READER,

I am delighted to present Q1 2020 edition of the Risk Landscape Review which includes three articles. While COVID-19 pandemic dominates the agenda of risk management executives, they should not ignore other existing risks. This issue includes articles which are dedicated to three different risk types.

The article "**It's called risk management for a reason**", written by Alex Knight, EMEA Head at Baton Systems, focuses on risks related to the financial payment and settlement process. Alex discusses how to overcome the settlement challenges and build an effective settlement risk solution that can offer improved data security and resilience.

The second article that we included in the current issue is "**Climate change is a global financial risk**" prepared by Oliver Wyman. The article not only discusses an importance for financial institutions to interpret correctly this risk, but also highlights a role of risk leaders in dealing with this global challenge and opportunities that can be exploited.

Margarete McGrath, Chief Digital Officer UK and Ireland at Dell Technologies, and Michael Imeson, Senior Content Editor at Financial Times Live, consider cyber security as a vital component of business resilience. In their article "**Cyber resilience – an essential component of overall business resilience**" they explore recent changes in regulation related to cyber security. They also suggest other collective and individual actions that firms should take to strengthen their business resilience.

My huge thanks to all contributors.

Enjoy the reading, take care and stay healthy.

Yours sincerely,

Dr Evgueni Ivantsov

Chairman of European Risk Management Council

Table of Contents

It's called risk management for a reason

By Alex Knight, EMEA Head, Baton Systems

Financial markets and their participants are experiencing an extended period of unprecedented stress – volumes and volatility are sky-high, while liquidity and confidence are in short supply.

In times of extreme volatility, it is vital that markets continue to operate and function smoothly. Unfortunately, like a small hole in a dam, any weakness in systems and processes will be exposed over time – especially during these periods of increased market activity and stress. As a result, it is absolutely critical that comprehensive risk management be prioritised for firms to not only succeed but, simply, to survive.

The core areas of risk management – liquidity and funding risk; settlement risk; operational risk; and data security and resiliency – are indeed the linchpins of financial services firms. Take settlement risk and liquidity risk, which of course are highly intertwined. Following the dramatic flight to USD cash in the second half of March, central banks are announcing bold measures to ensure continued access to liquidity. Nevertheless, market participants still have an acute need to accurately monitor, plan and source funding.

At the same time, settlement processes need to be monitored and optimised, and settlement failures (actual or potential) must be flagged and acted upon in real-time. And all of this has to be managed efficiently and effectively in the context of an increasingly challenging funding and risk environment.

Settlement challenges

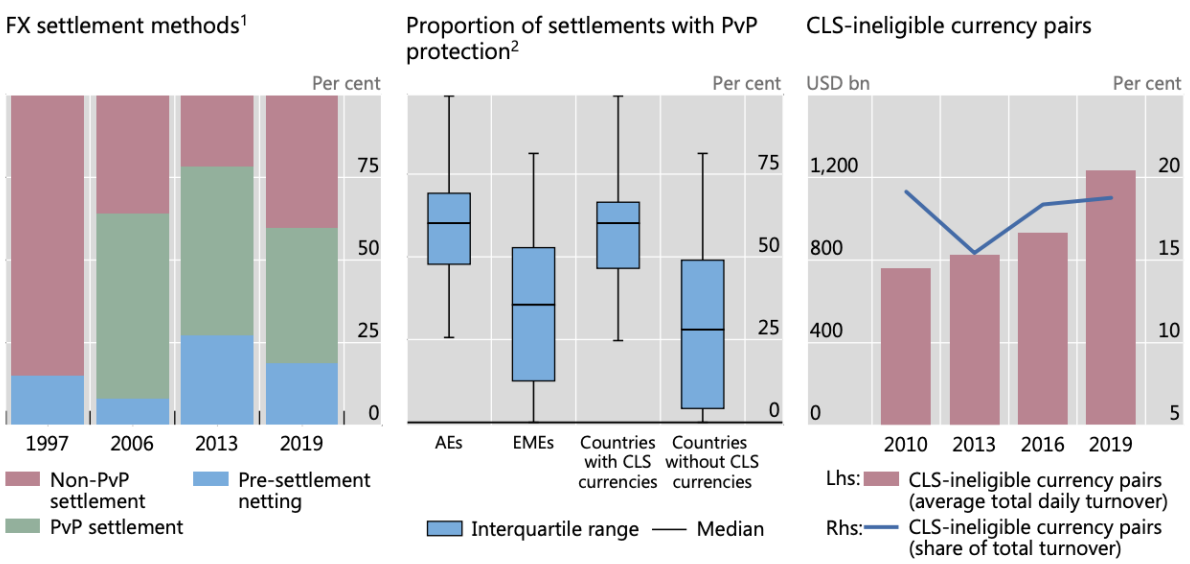
Even a slight delay in settlements and payments increases risk and cost, much less a full settlement failure. Settlement problems can arise due to a number of factors, including:

- Siloed banking systems and processes
- Inconsistent (and generally manual) workflows
- Restrictions imposed by central bank payments windows
- No established tool for the settlement of non-CLS eligible transactions
- Lack of visibility into intraday payment and funding information

Even if an institution is able to address each of these issues on its own, it faces the challenge of interoperability – requiring the settlement solutions it implements to be compatible with the wider ecosystem. Anything that causes delay or friction is costing money.

It is worth noting that while CLS has been a tremendous tool in specifically eliminating settlement risk related to FX transactions, the *BIS Quarterly Review* (December 2019) revealed that total settlement risk has actually risen since 2013, as the charts on the left and right below show.

FX settlement risk: increasing and global Graph A.1



[1] "PvP settlement" includes settlement through systems such as CLS and Hong Kong CHATS. [2] The median value is represented by a horizontal line, with 50% of the values falling in the range shown in the box. The highest and lowest values are represented by the upper and lower end points of the vertical lines.

Sources: Committee on Payment and Settlement Systems, "Progress in reducing foreign exchange settlement risk", *CPMI Papers*, no 83, May 2008; D Kos and R Levich, "Settlement risk in the global FX market: how much remains?", *SSRN*, October 2016; BIS Triennial Central Bank Survey; authors' calculations.

Source: BIS Quarterly Review (December 2019)

But how can firms with limited resources – and no appetite to enter into a multi-year implementation – solve this problem?

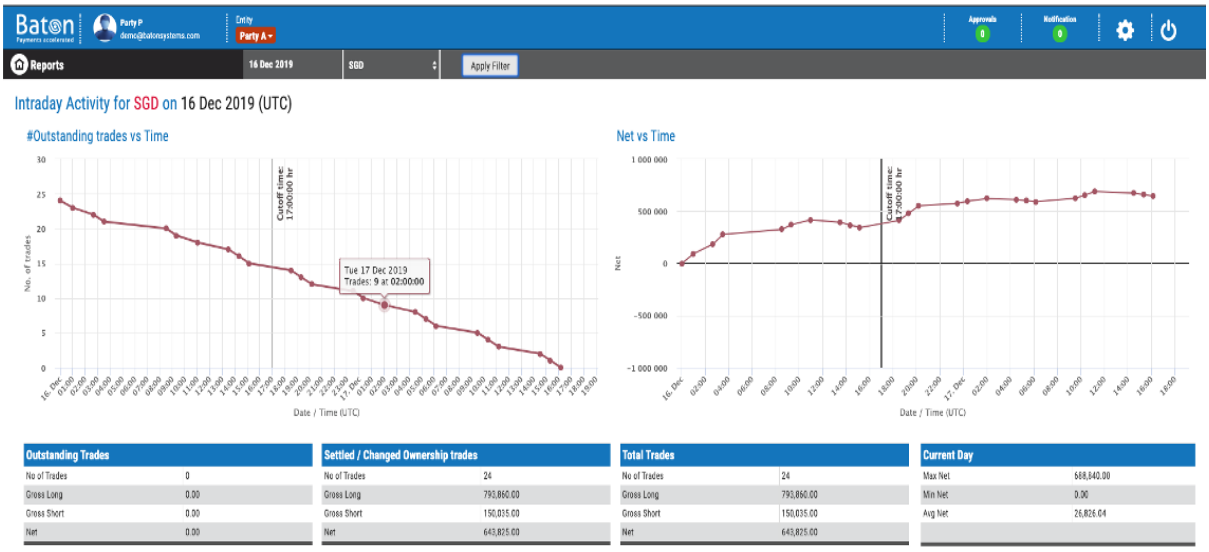
One flexible approach is to adopt the best elements of distributed ledger design and overlay these seamlessly on top of existing platforms and ledgers. These advantages include using a shared, permissioned, replicated ledger to connect counterparties' disparate ledgers, while maintaining all the transparency and security required. This can reduce settlement times from days to minutes, enabling speed, efficiency and accuracy while ensuring settlement finality, providing full visibility and confidence to all parties, and freeing up capital.

Any settlement and payments engine should also be integrated with a comprehensive view of obligations and exposures across business or product siloes, along with a global "longbox" to access a complete inventory of funding sources, and a rulebook to confirm the agreed parameters. It does not require radically re-engineering and harmonising existing processes and workflows, or changing any payment rails.

Reducing settlement risk

An effective settlement risk solution overcomes the barriers posed by legacy technology systems and offers improved data security and resilience. It facilitates visibility and optimisation of intraday funding, delivering real-time updates on settlement exposure across business siloes, with centralised

controls to throttle (where appropriate) or sequence. Distributed workflows that eliminate manual intervention significantly reduce errors. Crucially, such a solution provides an opportunity to reduce or even eliminate settlement risk – even for non-CLS transactions.



Banks' ability to monitor settlements and outstanding obligations, alongside available funding, on an intraday basis, is a prerequisite for effective management and control of settlement risk and liquidity.

While headlines around the world are understandably focused on the fallout from COVID-19 and the extreme volatility of financial markets, we shouldn't underestimate how the rather more mundane requirements of risk management will determine how well we, as a society, pull through this crisis.

Baton Systems is helping banks and other financial institutions synchronise and orchestrate the movement of financial assets, using existing payment rails. To find out more, contact alex.knight@batonsystems.com, or visit batonsystems.com.

Climate change is a global financial risk

By Oliver Wyman

Climate change poses a major risk – one that is already impacting the lives and finances of many. The latest Global Risks Report from the World Economic Forum released in January 2020, only confirms its critical importance. The impact of climate change is global, and with far reaching consequences. Events such as the bankruptcy of the Pacific Gas and Electric Company (PG&E) in January 2019, the historic water shortages in South Africa, and the recent announcement by the Indonesian government to move its capital from Jakarta, all illustrate that the impact is also directly financial.

Climate change is one of the most—if not the most—pressing challenge of our times. There are wildfires raging in the Amazon, California and Australia. Thousands of people have been displaced. Homes have been lost. Species pushed to the brink of extinction. Corporations bankrupted. Large swathes of vegetation destroyed. Sea levels continue to rise alarmingly. And this is just to name just a few consequences already experienced. There is also the imminent possibility of more wildfires, student protests and the growth of movements like 'extinction rebellion' that can stem from the direct impacts of climate change.

Climate change will put at risk around 2 percent of global financial assets by the year 2100. A worst-case scenario could see up to 10 percent of global financial assets being at risk by 2100. Such is the scale of the devastation that we should be ready for – and we need to accelerate our preparation now.

Does Climate Change merit its own category in Risk Taxonomies?

Many financial sector firms have updated their risk taxonomies in recent years to reflect the greater focus on non-financial risks such as conduct and culture, cyber and reputation. By calling them out specifically, they have sought to ensure appropriate focus and attention is given to these crucial areas which were so defining in the years running up to and after the Global Financial Crisis.

In this context, firms are asking whether Climate Change also deserves its own risk category. To this question, one view offers a purist answer and one that is more pragmatic. The purist view suggests that climate change represents a change in circumstances, such as the discovery of new technology which could render old methods obsolete. It is therefore not a risk type in itself and does not necessitate change in an organisation's risk taxonomy. Risk taxonomies are by construction exhaustive, and any losses arising from Climate Change will (or will not) arrive and be measured and managed through existing frameworks.

By contrast, the pragmatic view is considerably different. This perspective favours calling out substantial risks to ensure they are accorded appropriate attention. This is very much the perspective which drove firms to modify their non-financial risk taxonomies and, given the scale of

potential challenges arising from Climate Change, it is reasonable to ask whether the same logic applies.

The issue of course is that Climate Change is not a risk type and will affect firms across their exposures. In the context of PG&E's bankruptcy, its bankers experienced climate change as a credit risk; for PG&E's clients, including banks, it triggered operational risks. For PG&E's California-based professional investors, climate change could have been a credit, market, operational and reputational risk. This breadth of impact of climate change risk from a single event well-illustrates its wide-ranging implications.

Role of Risk Executives

The sheer scale of the potential adverse impact of climate change means, whether or not it merits changing the risk taxonomy, it must feature as a line item among the key tasks for risk executives. Risk leaders will need to be in the forefront of understanding climate change risks and alerting and educating their organizations to its potential impact. In addition, they need to ensure firms define processes to manage and mitigate its consequences. This work entails understanding and measuring an organization's portfolio exposure to climate change, including both direct financial and indirect reputational and societal components. The required expectations are well-mapped in the work of the Task-Force for Climate-related Financial Disclosures and related efforts[1].

Climate change will wipe out enormous amounts of capital, and it will possibly take years to measure its impact and recover from the associated mispricing that will be revealed. There will also be – as in the case of all category-based market mispricing events – a tipping point, which in hindsight will become the moment when valuations, insurance markets, and individual and government choices all start to shift. Potentially this tipping point will be traced back as early as 2019 and the failure of PCGE.

Opportunities from Climate Change

Although there is a plethora of challenges—financial and otherwise—resulting from climate change, efforts to address these challenges are resulting in opportunity.

For example, in the case of harnessing solar energy, both concentrated solar power and photovoltaics have registered falling prices and are already below $20 a GT of CO2 equivalent. Globally renewable power will on average be cheaper than coal-based power in 2020. Fully hybrid cars and LED lighting, meanwhile, are already negative costs in abatement terms – cheaper to run and carbon positive in comparison to other options. Electric cars such as the Tesla are carbon positive through whole-of-lifecycle. This has gone hand-in-hand with consumer preferences which

[1] E.g. https://www.oliverwyman.com/media-center/2018/may/oliver-wyman-designs-new-climate-change-methodology-with-un-and-.html

have also evolved – this is evident considering Tesla just registered back-to-back quarterly profits for the first time at the end of 2018 and is already the most valuable auto manufacturer in the world[2] .

The process of solid-state refrigeration, which involves extracting gases possessing 9,000 times the greenhouse impact of carbon, is also now a reality in certain applications. Reforestation and afforestation efforts, meanwhile, are creating sources of carbon credits for developed nations to trade with developing economies. Furthermore, there is also the process of carbon capturing, sequestration and bio-sequestration. In the latter case, a basic machine can sequester as much carbon as an acre of trees and produce bio-fuel in the process.

So while the risks are immense, climate change is also presenting a myriad of opportunities. Business and the scientific community is investing towards the common goal of a cleaner planet and productive new technologies that raise efficiency at lower impact. But the need of the hour remains to press for quicker consensus and action, because the pace of change at present is too slow, and absent radical acceleration the world in 2100 is forecast to become a hot and unpleasant place[3] .

Room for Optimism

Banks are in a strong position to allocate resources to the next generation of energy efficient alternatives. In line with the United Nations Environment Program Finance Initiative and the Task Force on Climate-Related Financial Disclosures, major banks have already committed towards reducing their overall emissions intensity portfolio. They have also introduced renewable energy financing schemes and have established financial incentives for low-emissions projects. Similar initiatives are being seen globally in the areas of green financing, and through the provision of financing to companies that is dependent on them meeting some climate- or emissions-related goals.

Technology provides room for optimism too. It is interesting to note that just the installation of LED lights and usage of effective insulation are enough to keep the world flat in terms of carbon dioxide emissions. Separately, plenty of work is going into enhancing energy efficiency, through improved battery storage solutions, and more efficient energy transmission and distribution. Happily, the facilitation of technologies such as these are on the agenda of several governments worldwide, with willingness to provide support for their adoption and implementation on the increase.

The technology to battle climate change is beginning to mainstream and it will be critical to facilitating the required pivot to a lower carbon economy. Nevertheless, the changes ahead will be seismic, and the associated costs of inaction will be astronomical. It therefore falls upon risk executives to assume the mantle of mitigating climate change risks, primarily by measuring the scale of the challenges faced and opportunities presented. What is required more than anything else is intent to understand the problem, and act on the opportunities.

[2] https://www.reuters.com/article/us-tesla-stock/tesla-overtakes-gm-as-most-valuable-us-automaker-short-sellers-burned-idUSKBN1X31NG
[3] https://www.businessinsider.com/paris-climate-change-limits-100-years-2017-6

Cyber resilience – an essential component of overall business resilience

By Margarete McGrath, Chief Digital Officer, UK and Ireland, Dell Technologies, and Michael Imeson, Senior Content Editor, Financial Times Live

In times of uncertainty and emerging risks, it is important for businesses to be strong and adaptable. Cyber risk is a growing concern for financial services firms today, and they are among the most targeted. It is no coincidence that those best equipped to deal with the cyber threat are the best equipped to manage other operational risks, as well as any political, economic or other harmful scenarios they may face.

The data breach suffered by US bank Capital One, announced last July, was just one of the latest in a series of incidents afflicting the financial sector and a vivid reminder of the scale of the problem – a hacker obtained the personal details of 106m credit card customers and applicants in the US and Canada.

Thankfully, the bank was able to respond and recover quickly, and the alleged perpetrator was arrested. The bank said it was unlikely the information had been passed on by the hacker or there were any fraud losses. However, it said it expected the incident "to generate incremental costs of approximately $100m to $150m in 2019" to cover notifying customers, credit monitoring, technology and legal costs.

From cyber security, to cyber resilience, to business resilience

Companies like Capital One are adopting a more rounded approach to managing cyber risk. A shift in emphasis is taking place, from cyber security to the broader concept of cyber resilience. An effective cyber strategy is not just about businesses improving security to prevent and detect attacks; it is also about improving cyber resilience, so they can respond to, and recover from, attacks quickly, and learn from the experience.

Cyber resilience is therefore being viewed as an essential component of overall business resilience. Executives must be able to respond to cyber incidents with as much agility and effectiveness as they do to any other shocks.

The regulatory dimension

Financial regulators are thinking along the same lines. In Switzerland, the Basel Committee on Banking Supervision regards cyber resilience as a vital aspect of operational resilience. "Actors in both the private and official sector" should approach cyber risk management "from a broader strategic and operational resilience perspective rather than restricting it to a purely technical discipline focusing on security", it says.

The Basel Committee set up an Operational Resilience Working Group in 2018, and one of its first jobs was to compare banks' cyber resilience practices around the world, which it published in Cyber resilience: Range of Practices. The group is now working on broader operational resilience principles to be published in the first half of 2020.

In Frankfurt, the European Central Bank (ECB) works with national central banks and other EU institutions – like the European Commission, and the EU's Computer Emergency Response Team – to maintain the cyber resilience of the financial system.

Christine Lagarde, the ECB's new President, in a speech in February, said the global cost of cyber-attacks in 2018 across all industries could have been as high as $654bn. She was quoting figures from the European Systemic Risk Board's forthcoming Systemic Cyber Risk report, adding that a "cyber-attack could morph into a serious financial crisis".

The ECB's banking supervision department already has a cyber-incident reporting framework under which all significant banks in the 19 eurozone countries must report serious incidents as soon as they detect them. Cyber resilience is an area "where we intend to stay at the forefront of developments", said Ms Lagarde.

In London, the Bank of England, Prudential Regulation Authority and Financial Conduct Authority last December published consultation papers and a shared policy summary on new requirements to strengthen operational resilience in the financial sector. The operational risks highlighted include, among many others, cyber, power cuts, IT system failures, severe weather, fire and epidemics. The consultation is open until 3 April.

If the UK authorities' proposals come into effect, firms and financial market infrastructures – the "plumbing in the system", namely payment systems, central counterparties (CCPs) and central securities depositories (CSDs) – will have to take four key steps:

1. Identify their critical business services that, if disrupted, could harm the firm, customers or the financial system;
2. Set limits on the maximum level of disruption each service could tolerate;
3. Identify the people, processes and technology behind the services; and
4. Take action to remain below their maximum tolerance levels.

Industry collaboration

Financial services firms are working together to hammer out solutions. Innovative partnerships are being forged between businesses to provide greater levels of security and improve cyber resilience.

For example, in the US the financial services industry has set up the Sheltered Harbor initiative to protect customer account data if a catastrophic cyber-attack or other event causes a firm's systems to fail and data to be compromised. A not-for-profit subsidiary of the Financial Services – Information Sharing and Analysis Center (FS –ISAC), Sheltered Harbor comprises asset management firms, banks, trade associations, technology providers and other organisations.

Every night, financial institutions in the initiative back up critical customer account data in a data vault using the Sheltered Harbor standard format. Each institution does the backup itself or uses a service provider. The data vault is separate from the institution's IT infrastructure, including all other backups, and the data is encrypted and unchangeable. If the institution suffers a cyber-attack or IT failure, the data is safe and, by activating a "resiliency plan", can be quickly recovered from the vault to give customers access to their funds.

What more could be done

An important part of building business resilience in any firm is to ensure that the leadership team is agile and diverse in its thinking. We recommend they take the following steps:

- Encourage different opinions and business models throughout the firm. Diversity of thought and action in a world of uncertainty creates a strong organisation. Different teams can look at products, services and operational challenges in many ways, and then come together when needed to develop synergies. Dell Technologies is a good example: it operates seven different businesses under one brand with strategic overlaps in some areas.
- Participate in war gaming scenarios covering a range of threats such as cyberattacks, economic shocks and epidemics like the Coronavirus outbreak. Crisis management exercises using real life scenarios will help build agility and fine-tune disaster recovery and business continuity plans. Chaos engineering should be used to test whether IT infrastructure and software can withstand failures, just as Netflix does with its chaos monkey.
- Identify critical data and protect it in an off-the-network vault. This is not an easy exercise and requires executive sponsorship. Typically, critical data accounts for between 10-15% of a business's overall data but most businesses struggle to define it.

Cyber resilience has become a strategic priority for boards and senior management. This is as it should be. The challenge now is for them to integrate it into an overall business resilience mindset, one that ensures their company can survive any kind of operational, commercial, economic, political or natural disaster. Only by taking such a holistic approach will the business succeed in these uncertain times.