The need for resilience in the face of disruption: Regulatory expectations in the Digital World

INTRODUCTION

Good morning ladies and gentlemen. It is a pleasure to be here at the Financial Centre Summit and I thank Finance Dublin for inviting me to speak today[i].

We have entered a new era in the world of financial services. Technology change, as evidenced by the description of a fourth industrial revolution[ii], is more than just an enabler for conducting business in a faster, smarter, or cheaper way, for better managing costs, or for gaining better analytical insights. It is a revolution that is completely transforming the playing field for financial services firms.

Opportunities and risks abound.

The competitive landscape is changing, with new entrants, new business models, a race by incumbents to invest in developing the necessary capabilities, and in many cases the potential for a fundamental disruption in the value chain of traditional financial services firms and sectors. Moreover, it is becoming ever more evident that data, and the harnessing of it, is the new currency of this new digital age[iii].

All this brings more complexity into the system, and complexity brings risk. Financial services firms and whole sectors face the challenges of: needing a clear vision for the future in a radically changing world; having a sufficiently flexible strategy and building the necessary capabilities for thriving in it; and be able to manage the significant transition risks along the way. And throughout, financial services firms will need to ensure that they are sufficiently focused on their customers, and serving them in a sustainable way.

So today, I am going to talk about some of these opportunities and challenges. I will cover:

- the importance of understanding the role technology plays in value chains and the implications should something go wrong;
- the need to get the basics right when it comes to IT;
- the criticality of taking a data-centric view to understand key assets, and thus how to protect them; and
- the responsibilities of the senior management and boards of financial services firms to own these critical risks and to build resilience in their firms to be able to withstand, absorb, and recover from technology-related risks.

In covering the above, I will also summarise how the Central Bank is continuing to evolve its approach to regulation and supervision in the context of technological change.

The Implications of the Digitalisation of Financial Services

"Artificial intelligence and exponential increases in computing power are forcing firms to re-examine how they do business. The financial services industry is no exception. Digitalisation has already left bustling stock exchange floors in demise. High-frequency trading is increasingly shaping market dynamics. And in the future, thousands of financial analysts may be replaced with robo-advisors."[iv]

Technology developments over the last decade have, among many other things: exponentially increased the proliferation of data and the speed with which it can now be analysed and processed; customer expectations of functionality; and increased outsourcing of technology services, including cloud storage. And if the current pace of change is anything to go by, the future is a vast unknown where only those able to adapt at pace will be able to survive.

All of this new innovation is exciting and creates a myriad of opportunities. Indeed, it is arguable that there is no part of the traditional financial services value chain that cannot be done better, smarter and more effectively. In my role, I welcome the opportunities for the financial services system to better serve the needs of the economy and its customers, but I am also mindful of the risks.

As we look forward, it is important to reflect on the past to see what if any lessons we can learn. The onset of the financial crisis in 2008 has been much discussed in the last few weeks. The years leading up to the financial crisis were characterised by, *inter alia*: high levels of financial innovation; an over and incorrect reliance on implicit and explicit assumptions; the approach to regulation and supervision failing to keep pace with the growing systemic risks; and boards and senior managers not truly understanding the risks and, in many cases, the underlying activities being undertaken in their businesses. In other words, as Christine Lagarde recently stated, at the core of the last crisis "was financial innovation that vastly outpaced regulation and supervision. Financial institutions…went on a frenzy of reckless risk-taking."[v]

I will not labour the comparison that could be made with the potential risks arising from the latest wave of innovation and risk-taking in the financial system, driven by technological change. But the pace of change, together with the borderless nature of technology, does require an appropriate level of caution to be taken, through financial services firms taking risk-based approaches to strategic and business initiatives. Financial services firms need to make informed choices about where and how they are going to adapt and make sure that the associated risks are understood, considered, and measured as they make changes to their processes and business models.

Getting the basics right

Worryingly, in too many cases the foundations to support success and effectively manage the technology risks are not sufficiently robust. We have repeatedly found that too many firms are lacking in the fundamentals of IT risk management and IT security while at the same time espousing a digital strategy for the future. We find that too many firms are not aware of all the IT assets on their estate and have not undertaken adequate risk assessments to adequately understand the threats and vulnerabilities to them.

Too many firms do not fully understand all the systems and processes that support their business services and they are not aware of all the third-party relationships that support their value chain. And we have found that in many firms the board does not fully understand the IT risk profile of their firm and is not asking the questions that need to be asked in relation their risk appetite or how the IT strategy is aligned with the business strategy of the firm.

As outlined in our 2016 Guidelines on Information Technology and Cybersecurity Risks[vi], Boards and senior management across the financial services sector need to more actively engage in the oversight of technology risk. This requires having both the necessary skillset and mindset at these senior levels to understand the evolving technology landscape and make informed decisions about it. The technical changes that are sweeping through financial services need to be accompanied by governance and risk management changes.

Data as an Asset

A firm's data is, in many cases, its biggest asset. So it is vital that firms are taking a data-centric view of their business and systems to identify what data they have or need to support their core business services, and how it is classified, used and protected.

In this fourth industrial revolution, firms that can harness data effectively can expect competitive advantages. The use of artificial intelligence and machine learning can be very powerful for analysing big data to better understand how to meet customers' needs in a sustainable manner over the long term.

But this can only happen if the data is reliable and available. From our on-site inspection work over the last number of years, we have identified many weaknesses in firms' abilities to effectively understand, use and report on their data. Issues arise from a patchwork of legacy and newer systems that do not talk to each other, resulting in fragmented data that requires manual interventions and adjustments before it can be used. Firms need to have a single source of their key data if they are to rely on it for critical intelligence and decision-making. Those that manage this transition best are likely to be the firms that survive and thrive.

But along with the benefits to the business of using this data comes the responsibility to your customers and counterparties to protect it from loss or theft and to use it to get the best outcome for all stakeholders – i.e. to not to use the advantages of big data to the long term detriment of customers.

Many industry experts believe that the future of financial services will increasingly involve a battle for the customer relationship[vii] and the user-friendliness and trustworthiness of firms' digital offerings.[viii] Unfortunately, as we have seen in Ireland, trust in the financial services system is an endangered commodity. Boards and senior management need to take responsibility for safeguarding the trust in and reputation of their organisation by prioritising the security, resilience and use of their data and systems.

In the increasingly interconnected world of financial services, there are a multitude of interdependencies that all form links in a chain. Technology has deepened this chain and all parties are reliant on other members in the complex web of financial market infrastructures that underpin day-to day business.[ix] This gives rise to two key risks that are too frequently underestimated; reliance on third-parties for delivery of your business services and increased cyber risk.

Outsourcing and Third-Party Risk Management

Let me talk first about reliance on third-parties. How many of you are aware of all the systems or services that support your value chain that are outsourced to third-parties? How many of you know where all of your data is residing at this very minute? Do you know how many third parties connect to your systems or have access to your data and for what reason?

These are questions that boards need to be asking of their senior management. While it is possible to outsource a service, you cannot outsource the risk. The responsibility and accountability for ensuring security and resilience of your data and services remains firmly with the board.

A recent cross-sector survey on outsourcing conducted by the Central Bank, identified issues across the life-cycle of outsourcing arrangements and suggests that outsourcing is not being considered a core priority of many financial services firms. Some of the most critical observations from the survey, which tie in with findings from on-site inspection work, relate to poor governance and controls around the risk assessment and management of outsourcing, inadequate monitoring and reporting, failure to consider third-parties in business continuity plans and tests, and a lack of exit strategies or contingency plans should

the firm need to find a new service provider or bring the service back in house. These issues are more concerning given that a large proportion of outsourcing arrangements were reported to involve sensitive customer and business data, including to cloud service providers, and that 75% of firms outsource all or part of their information technology.[x]

With all outsourcing arrangements, boards and senior management must understand that they are placing the resilience of their firm into the hands of a third-party and while they may be able to monitor the service during normal operation, when something goes wrong, they are reliant on someone else to fix it. Some firms might seek to take comfort from the fact that they outsource to a parent or sister group company rather than a third party, but, as has been seen with a number of high-profile events, firms cannot always rely on the parent to provide uninterrupted service. Boards and senior management need to understand where their firm's systems and data sit on the group priority list should something go wrong.

Cyber Security Risk

As I am sure you are aware, October is Cyber Security Awareness Month.[xi] But cyber security and cyber resilience is not something we should focus on for just one month of the year. It requires vigilance and attention, day in, day out.

Former Cisco CEO John Chambers once said, "There are two types of companies: those that have been hacked, and those who do not yet know they have been hacked."[xii] The cyber threat is constantly evolving – the frequency, sophistication and volume of attacks is increasing. The failure to adequately protect against cyber-attacks can have far-reaching repercussions given the interconnected nature of the financial system.[xiii]

Efforts to increase security and combat attacks is also increasing and cooperation between international organisations is improving.[xiv] For example, in May the ECB published the TIBER-EU framework which sets out a programme to enable national authorities to work with financial institutions to test and improve their resilience against sophisticated cyber-attacks.[xv]

Closer to home, in 2016 the Central Bank issued the Cross Industry Guidance in respect of IT and Cybersecurity Risks[xvi], which set out our minimum expectations of firms in relation to these risks. As with the other areas I have covered already, much more needs to be done to meet these expectations. Cyber-security needs to become part of the culture of an organisation and an integral part of the organisation's risk management, crisis management, and business continuity planning.

Senior management and boards of financial services firms need to own these critical risks and build resilience in their firms to be able to endure and survive operational or technology-related shocks, be they systems failures, change processes gone wrong, or a data breach.

We have seen a lot of progress in the area of IT risk management and resilience, but there is huge amount of work still to be done. Almost three quarters of our findings from on-site inspections relate to four key areas: IT risk management, IT security, IT outsourcing, and IT continuity management. Thus, firms can expect to see a continued focus by the Central Bank on these fundamentals and on firms' resilience capabilities.

But the overall responsibility for resilience rests with the board and senior management which is why I am most concerned about the many findings in our work that relate to the failings of boards and senior management to understand and appreciate the significance of the IT and operational risks their firms face. We have seen evidence of risks and messages

being diluted as they are filtered up through the organisation such that they are so high-level once they get to senior levels that they lose their meaning or impact.

I expect boards to: understand how disruptions of key business services could impact their customers and their value chain; ensure operational and cyber resilience strategies are fit for purpose; and oversee risk tolerances and appetite metrics to track, measure and trigger a response to disruptive events. They need to ensure that their firms have the resilience to withstand future shocks, absorb the impacts of the shock and communicate effectively to stakeholders throughout, and to ultimately recover from the incident and use the learnings to further improve their future resilience.

Firms need to be better prepared for the future challenges that technology will pose to their firms' competitiveness and business models and they need to acknowledge and take ownership of the risks that go along with this changing environment.

The approach of the Central Bank

I have touched on the work of the IT inspection team in the Central Bank. Despite its relatively small size, the team has significantly enhanced the intensity and intrusiveness of our supervision of IT related risk across the financial services sector. Identified issues are required to be resolved through risk mitigation programmes and we will continue to issue thematic findings from our work to highlight areas for improvement for all firms. Where necessary we have used our powers to sanction failures and require the use of third parties to help drive improvements.

The inspection team is ably supported by and contributes to policy and regulatory development within Ireland and as part of the wider European system. We will continue to enhance and invest in our capability in this area.

Moreover, recognising the challenges and opportunities that arise from this revolution, we are continuing to enhance our data analytical capabilities, including through investment in our systems, our data collection and a restructuring of our organisation of Prudential Regulation to best utilise our resources.

Conclusion

This is a very broad topic, in which I have only really scratched the surface. I have touched on the opportunities and risks, and recognised that for the financial services system to continue to serve the needs of the economy and its customers it must continue to evolve. To evolve it must leverage the advances of the fourth industrial revolution, while at the same time acknowledging and addressing the inherent risks.

I expect boards and senior management of financial services firms to prioritise the issue of digital transformation and allocate the resources necessary to meet their customers' needs. Firms need to demonstrate their understanding of the role technology plays in value chains. While looking at the opportunities for the future, many firms also need to continue to invest to get the basics right. Significant improvements are required across the system to manage the incumbent and growing technology risks within it.

A change in mindset is needed to see data as a valuable asset and to invest in protecting that asset. Firms also need to be prepared for when things go wrong and to build resilience to be able to withstand, absorb, and recover from technology-related risks.

As the popular wisdom tells us, you do not have to be faster than the bear, just faster than the other people running away from it. One of my greatest fears in my role is the call from the firm that is not fast enough.

I thank you for your attention.

[i] With thanks to Jane Woodcock, Thomas Farrell and Tim O'Hanrahan for their assistance in drafting these remarks.

[ii] See among others Klaus Schwab, Founder and Executive Chairman, World Economic Forum (https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/)

[iii] See for example Big Data, Big Impact: New Possibilities for International Development, World Economic Forum.

[iv] See Coeure, B (2018), The future of financial market infrastructures: spearheading progress without renouncing safety. Singapore, 26 June.

[v] See Lagarde , Christine: Ten Years After Lehman – Lessons Learned and Challenges Ahead.

[vi] See Central Bank of Ireland, Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks, September 2016.

[vii] Basel Committee on Banking Supervision, Sound Practices, Implications of Fintech developments for banks and bank supervisors. February 2018.

[viii] See Hakkarainen, Pentti (2018): The Digitalisation of banking – supervisory implications, remarks at the Lisbon Research Centre on Regulation and Supervision of the Financial Sector Conference, Lisbon, 6 June 2018.

[ix] See Lautenschlager, Sabine (2018): Cyber resilience – objectives and tools. Remarks at the first meeting of the Euro Cyber Resilience Board for pan-European Financial Infrastructures, Frankfurt am Main, 9 March 2018.

[x] Outsourcing, August 2018 - Unpublished internal Central Bank report on the results of the 2017 outsourcing survey.

[xi] https://cybersecuritymonth.eu/

[xii] https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

[xiii] See Coeure, Benoit (2018): The future of financial market infrastructures: spearheading progress without renouncing safety. Remarks at the Central Bank Payments Conference, Singapore, 26 June 2018.

[xiv] Cambridge Centre for Risk Studies and Risk Management Solutions, Inc. Cyber Risk Outlook 2018,

[xv] See ECB (2018), TIBER-EU FRAMEWORK – How to implement the European framework for Threat Intelligence-based Ethical Red Teaming, May 2018.

[xvi] See Central Bank of Ireland, Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks, September 2016.