Operational Resilience in Financial Services Conference

London, 27/09/2018

Regulatory Framework for Mitigating Key Resilience Risks

Slavka Eley, Head of Unit - Banking markets, Innovation and Products, European Banking Authority

Introduction: Where are we coming from?

With the increased digitalisation of financial services, financial institutions becoming more intertwined and dependent on computer networks and third party service providers, an insufficient level of protection against cyber incidents and a failure of critical IT infrastructure could lead to major damages in individual financial institutions and have potential spillover effect on the whole financial system. This explains why ICT related risks, and in particular cybersecurity, are high on the agenda of policymakers, regulators and supervisors of the financial sector.

The European Banking Authority (EBA), as an EU agency with an objective of ensuring the integrity, transparency, efficiency and orderly functioning of financial markets, must monitor market developments, prevent regulatory arbitrage, ensure supervisory convergence and effective and consistent regulation – as well as enhance consumer protection. Our activities build on supervisory experience and expertise at national level

in each EU country, and are linked with the overall EU policies on cybersecurity as part of the Digital Single Market strategy.

Today I would like to cover the following three areas

- Digitalisations trends in financial services and related risks;
- Operational resilience as a new challenge and the EBA's response;
- Mitigation of resilience risks in outsourcing and use of third party service providers.

Digitalisation trends in financial services

When we speak of trends, we very often refer to the innovative technological trends in finance. This is due to the rapid evolution of innovations in finance such as the use of cloud, biometric authentication, artificial intelligence, machine learning, big data and the like. Their increased use in the market has been supported and encouraged by the shift in users' behaviour, where customers are demanding quicker and easier digital access to financial products and services.

Furthermore, the push towards digital channels in finance is also down to the growing number of FinTech providers joining the market and delivering digital products and services quickly to heed to customer demand for fast, accessible, digital banking and payments. This also encourages incumbents to adapt their business models in order to remain competitive.

More open systems, outsourcing and third party services

In recent discussions with institutions on this topic we found that incumbents are putting a lot of faith in FinTech, telling us that FinTech has enabled new products and services and that cooperation with FinTech companies will be a key driver for business growth. All of them[1] expect FinTech to increase revenues, while 97% hope it will help to expand their customer base. For incumbents, who are often weighed down by legacy systems and a complex IT infrastructure, one of the most frequently used methods for innovative solutions is through outsourcing providers or third party providers. Outsourcing is a way to get relatively early access to new technologies and allows institutions a number of other benefits too, for example:

- Access to economies of scale (more efficient resource utilisation, 'state-of-the art systems');

[1] Respondents the semi-annual EBA Risk Assessment questionnaire (November 2017) were 37 European banks.

- Cost effectiveness (in cloud you have 'pay as you use' models turning large up-front fixed costs into variable costs);
- Cost-savings (expertise personnel, infrastructure development and maintenance)
- Flexibility and scalability (on-demand infrastructure, scaling up and down as needed)

The benefits above can lead to business agility and the enabling of innovation, which ease the deployment of new services, and reducing the "time to market".

Another method used increasingly is open banking, where open Application Programming Interfaces (APIs) – which enable third party developers build and connect applications and services around the financial institution - are perceived as an opportunity to bring more tailored products to customers and offer new propositions. Open banking allows banks to share customer data with third-party companies or apps securely and in real time. In our discussions with institutions2, it has emerged that open banking has the potential to change the dynamics of the sector, with potentially greater interconnection between different actors, including entities falling outside the regulatory perimeter, and as a result potentially greater disintermediation.

The EBA has specific mandates in PSD2 implementation, which encourages APIs and this work is only the first step into open banking.

More sophisticated attacks

What comes with the digital territory and the new technological architecture is the increased number of entry points for attacks which impact the security and therefore the viability of an institution. Cyber risk is one of the key risks threatening data integrity and business continuity in today's interconnected financial system. It is a multi-faceted challenge for financial institutions as attacks from skilled intruders trying to gain unauthorised access to critical systems and data are rising. The EBA's 2017 risk assessment report, which surveys the largest EU banks, noted that cyber risk, data security and outsourcing ranked the three highest operational risks in banks.

Cyber incidents put institutions at risk of potential operational, legal and reputational risks, including business interruptions, data and software loss, fraud, breach of privacy, or network failures, which can result in financial losses. On top of the direct costs related to cyber incidents such as the cost of forensic investigation, there are also a number of indirect costs including negative effects on brand name and customer relationships.

[2] **EBA r**eport on impact on business models from FinTech

Additionally, with the use of outsourcing and third party service providers, supply chain risk is an amplified reality. The cloud, besides its wide range of benefits, is an attractive environment for attackers. In 2018 we have seen various sophisticated techniques and tools exploited against cloud storage services. In the past year alone, 51% of organisations worldwide have experienced cloud-based attacks, including FedEx, Intel, and Honda3.

Note that we talk of sophisticated attacks but we should also be cognisant of the human risk. A survey published at the start of this year[4] pointed out some fundamental lack of controls with 88% of employees being unaware of their organisation's IT security policies. Furthermore several cloud-based attacks, mainly those involving data exfiltration and information disclosure, derived from poor security practices, credentials left available on public source code repositories or the use of weak passwords are just some examples of how threat actors gained access and control over unprotected resources hosted in the cloud.

These attacks can adversely impact the confidentiality, integrity, and availability of an institution's critical business operations.

Operational resilience as new area of regulatory and supervisory focus

What are the regulators and supervisor doing to mitigate and oversee these challenges?

Traditionally IT security risks including cyber, have mainly been seen as an IT issue within institutions, while from a supervisory perspective, supervisors would look at IT risk as an element within operational risk and evaluate the appropriate controls and coverage by capital. However, the focus from both the institution and the supervisor is adapting recognising that the mitigation of cyber threats and IT security risks can only be achieved through the readiness of the institution as a whole. A high and growing reliance of banking operations on IT platforms, digitalised product channels for banking services, outsourcing to third-party providers of IT-related tasks and functions, and communication networks makes banks vulnerable to much wider range of operational risks.

What I am referring to is the operational resilience of an institution. This is the key term that brings us here together today.

Operational resilience is multi-dimensional, ensuring that institutions robustly plan for the inevitable disruptive operational events. Good operational resilience involves good governance, adequacy and expertise of resources, business continuity planning,

[3] RedLock - 2018 from Checkpoint Cyber attack trends – mid year report 2018

[4] Kaspersky lab report – Jan 2018

information security including cyber-security management, and third party provider management in particular on security. Operational resilience is necessary for the individual institution and also for the system as a whole.

Before moving to the more detailed overview of the regulatory framework in the EU, I would like to mention initiatives of other EU and global bodies contributing to the regulatory and supervisory work related to cyber and operational resilience. In this respect, the G7 Cyber Expert Group work, the BCBS work on Operational Resilience, the FSB Cyber Lexicon, and the ECB TIBER-EU - the first European framework for controlled cyber hacking to test resilience of financial market entities are all particularly relevant.

The EBA's response: regulatory and supervisory framework

In line with its mandate to ensure effective and consistent prudential regulation and supervision across the European financial sector, the EBA has undertaken several initiatives to adjust the regulatory framework and promote consistent supervisory practices, both for payment and for financial institutions including in the field of cybersecurity.

While some pieces of our work are still in the pipeline, the regulatory and supervisory framework related to operational resilience is built around the following three areas:

- Regulation: strengthening governance and risk management arrangements
- Supervision: common framework for supervisory assessment and knowledge sharing
- Resilience testing: sound and proportionate resilience testing

In the area of regulation, we published the EBA Guidelines on Internal Governance at the start of 2018, specifying internal governance arrangement including risk management, business continuity management and outsourcing. Around the same time, we also completed the EBA Recommendations on Outsourcing to Cloud Service Providers as a very specific response to uncertainty in cloud adoption.

In the area of payment services, the EBA published guidelines on security measures on operational and security risks, guidelines for the notification of major operational and security incidents, and guidelines on fraud reporting requirements.

These guidelines are now being accompanied or replaced by two important policy products: Guidelines on Outsourcing Arrangements (currently on consultation) and Guidelines on ICT and security management, including expectations on resilience testing. These two sets of guidelines will be applicable to all regulated institutions under the remit of the EBA and aim to provide a comprehensive set of provisions to strengthen governance and security arrangements.

Supervision plays an equally important role in evaluating the resilience of individual institutions and the financial system. As a practical contribution to this process, the EBA published guidelines in 2017 for supervisors on the assessment of ICT risk as part of the Supervisory review and evaluation process and organised number of workshops and training events supporting knowledge sharing.

As an extension of the supervisory activities, the third component of operational resilience is the resilience testing. At country level, the UK and the Netherlands have established their own respective exercises. The European Central Bank (ECB) this year published its European framework for Threat Intelligence-based Ethical (TIBER-EU), aimed at testing and improving the entities' resilience against sophisticated cyber attacks in the EU. The European Commission's FinTech Action Plan has mandated the three European Supervisory Authorities (i.e. the EBA, ESMA and EIOPA) to evaluate the need for a coherent threat testing framework at EU level for significant market entities.

There are a number of different models and approaches for cyber threat testing, ranging from supervisory-Led and regulatory-Approved frameworks to private cyber resilience testing services.This is the area that we are currently working on, considering different options for resilience testing and proportionality in its application.

Mitigation of resilience risks in outsourcing and use of third party service providers

Let me now move to the last part related to the promotion of operational resilience by outlining the regulatory development for outsourcing to cloud. As part of our monitoring of innovation and engagement with supervisors, we identified a high interest from regulated entities on cloud adoption and a related uncertainty regarding the supervisory expectations for outsourcing to cloud services, which does not fit into a model of an IT services provider offering bespoke IT solution. The EBA responded to the high level of uncertainty, which had been identified as a barrier to cloud adoption, by developing specific guidance on outsourcing to cloud.

As banks continue to use cloud computing with its multiple benefits we must also consider the risks that such an innovative technology carries. The specific risks depend on the type of *service model* used (i.e. its components such as servers, network and software) as well as the *deployment model* (i.e. whether it is public, private or hybrid cloud). However, we can generally group the risks into three main categories:

- Firstly, *data management, protection and data location.* Banks operate under strict rules in the EU for data protection and security. However,

cloud service providers may slice and store data across multiple locations worldwide. These locations are not always disclosed, or the cloud service provider in these jurisdictions, might apply lower standards leading to security breaches and issues;

- Secondly, *dependency on external providers for regulated services,* which can lead to concentration risks not only from the point of view of individual institutions, but also at industry level where large suppliers of cloud services can become a single point of failure when many institutions rely on them;
- And thirdly, *effective oversight and supervision.* A bank as a regulated entity is expected to have sufficient oversight over its IT infrastructure. If there are multiple layers in a cloud supply chain, this makes it difficult to properly identify and monitor this risk.

The EBA Recommendations on outsourcing to cloud service providers set out the supervisory expectations for the use of cloud and focus on a number of points specific to cloud outsourcing namely:

- *Adequate security of data and systems* – i.e. ensuring an adequate level of protection of data confidentiality, as well as integrity and traceability of data and systems.

- *Guaranteed supervisory access and audit rights* – Banks are expected to contractually ensure an unrestricted right to access and audit for auditors and supervisors. This includes physical and virtual access to the data and systems in the cloud.

- *Consideration of location of data* – the institution must ensure that the data security and availability is not compromised by legal risks or compliance issues related to data storage location.

All these provisions aim to support the safety and resilience of institutions using cloud services while recognising the innovative nature of cloud technology. These Recommendations also served as a basis for preparing the new Guidelines on outsourcing arrangements.

The new outsourcing Guidelines, whose consultation period ended on 24 September, are addressed to Credit institutions, Payment institutions, e-money and investment firms and also set out requirements to competent authorities. Outsourcing is defined as an arrangement of any form between a regulated institution and a service provider for provision of a service or an activity that would otherwise be undertaken by the institution

itself. The guidelines differentiate requirements for the outsourcing of critical or important operational functions and other operational functions, with less strict requirements.

Broadly speaking, these guidelines elaborate a process for

- identifying material and important outsourcing;
- carrying out due diligence and risk assessment – with a focus on operational and reputational risk;
- specifying data and system security requirements and access, information and audit rights , sub outsourcing and termination rights.

Regulated institutions are expected to have robust governance arrangements and retain an appropriate internal organisation to oversee and manage the relationship with service providers. Outsourced operational functions remain subject to the institution's internal audit, and audit and access rights should be sufficiently ensured by contractual arrangements. Furthermore, the regulated institution should also ensure that service providers comply with appropriate security and data protection standards and should oversee the outsourced functions. Finally, institutions are expected to have clearly defined exit strategies for critical or important functions.

While recognising that regulated institutions can benefit from outsourcing and achieve cost efficient solutions, they remain responsible for ensuring compliance with the regulatory framework of the services provided.

This is a practical contribution into supporting resilience of regulated institutions, which benefit from the use of outsourcing.

Conclusion

In conclusion, operational resilience, in the context of cyber, is on the regulatory agenda in the EU and globally. There are limits to what can be achieved by regulation in this area. While significant burden on cyber resilience lays on the shoulders of institutions themselves, a combined effort by institutions and supervisors, including cyber threat testing and information sharing, can contribute to the mitigation of resilience risks. Regulators' coordinated approached to resilience and interaction with market participants at national, European or global level is essential for the technological innovation and tackling related resilience threats with timely and appropriate regulatory and supervisory responses. The EBA's particular role here includes ensuring these coordinated approaches across the EU single market.

Thank you very much for your attention.