Digital operational and cyber-resilience

Introduction

The Chair stated that the speed of the digital transformation of financial institutions is unprecedented providing many opportunities but also greater ICT (information and communication technology) and cyber risks. This includes malicious attacks against financial institutions and their customers, which are on the rise, as well as a growing exposure of financial institutions to operational resilience risks due to the complexity of their ICT systems and their increasing reliance on tech third parties such as cloud service providers (CSPs).

The Digital Operational Resilience Act (DORA) is part of the wider EU digital finance package and aims to implement uniform requirements across the EU financial sector relating to digital operational resilience. DORA entered into force in January 2023 and will be applicable to financial firms from early 2025. Besides DORA, the reviewed Network and Information System directive, NIS2, which aims to strengthen and harmonise cybersecurity laws across the EU, is due to enter into force by the end of 2024. The enhancement of cyber and operational resilience is also a priority at the global level with guidance and principles recently published by CPMI-IOSCO and the BCBS and on-going work at FSB level on achieving greater convergence on cyber incident reporting and the management of third-party risk.

1. Evolution of ICT and cyber-risks in the financial sector with increased digitalisation

An industry representative stated that there are three main areas of ICT and cyber-risk: geopolitical risks, technological risks and the risks posed by new market entrants. Concerning geopolitical risks, nation-state actors are becoming more prevalent. These threat actors are well funded, well-coordinated and persistent, which means that they probably represent the largest threat for the financial sector. Secondly, while technological change is providing many opportunities in terms of efficiency and enhanced customer service in the financial sector with the implementation of new technologies such as cloud services, artificial intelligence (AI) and blockchain, security measures need to keep pace with these changes, otherwise new vulnerabilities will emerge. Thirdly, the tech firms that have entered the financial services sector, providing financial products, supporting the supply chain or both also create new vulnerabilities. Public and private sector participants need to continue to find ways to identify and quantify these risks and develop strategies to address them.

Adversaries are always looking to take advantage of new technological developments and sophisticating their approaches, the industry speaker emphasized. Statistics show that adversaries can begin to permeate through networks within 84 minutes of an initial breach, which mandates very rapid reaction. Figures also show the magnitude of breaches. There has been a 112% increase in advertisements selling user credentials recently and 71% of initial detections are malware-free, since once adversaries have access to systems, they use user credentials and their own tools and techniques to further permeate the network and no longer need malware. There has also been a 50% increase in interactive, hands-on keyboard attacks. The increased sophistication and intelligence of threat actors demonstrates the vital importance of regulations such as DORA, which aims to ensure consistency across the EU in the fight against cyber-risk.

A regulator agreed that while ICT provides many benefits, transforming the operations of financial entities, it also increases their exposure to new threats and risks. Financial entities have been outsourcing activities to third-party ICT providers (TPP) for some time and are already facing significant cyber-resilience challenges. These trends are due to accelerate with stronger digitalisation and changes in the business models of financial entities. Previously, banks created idiosyncratic information from their day-to-day businesses that was used for risk management or to grant credit. All this happened in-house. Now they are relying on external providers for many activities and some of these providers have become critical to the provision of their services, so it is essential to ensure that resilience is preserved in this context. DORA is an ambitious and welcome European response in this context.

A second regulator agreed that digitisation introduces new risks and changes the profile of existing risks in the sector. Operational risks in financial services are increasing in terms of complexity, volume and speed. When thinking about improvements in risk management and resilience outcomes, digitisation is also helping to reduce human error in both front office and back office functions. Repeat processing and legacy systems have also improved thanks to technology, reducing risks and increasing resilience. Cloud services in particular are helping to improve resilience relative to traditional on-premise systems, with better firewall technology and back-up or failover arrangements that help to improve continuity of service from an individual firm and system-wide perspective. However, the increasing use of technology is also introducing new vulnerabilities. There are vulnerabilities drawn from concentration, with a relatively small number of providers such as CSPs providing firms with core and critical ICT services. Where services cannot be substituted at speed, vulnerabilities become more acute.

A second industry representative stated that the different players operating in the financial sector have a responsibility to make the entire ecosystem more resilient and secure in a rapidly changing landscape. The financial services industry is one of the most advanced industries in terms of cybersecurity, resilience and privacy and on-going collaboration between financial institutions and ICT providers is helping to sustain this position. CSPs contribute to this objective by providing the possibility of a more seamless and secure continuity of service. CSPs are constantly fending off cyber-attacks using sophisticated tools. Their clients benefit from their learning curve in terms of cybersecurity and resilience and also from the opportunities offered by the cloud computing environment to integrate new technologies such as AI in a more effective way. This is however a journey of continuous improvement where there is no end destination of total safety. It is imperative for financial institutions to have comprehensive ICT risk management mechanisms in place, including identification, protection, prevention and detection tools. CSPs and other ICT providers are supporting them in this regard by providing a broad set of build-in cyber-resilience capabilities. They are also investing massively in enhancing their cybersecurity toolkit, contributing to ensuring stability throughout the ecosystem[1]. This is important because the threat landscape is always evolving. In the future, AI and built-in tools, coupled with quantum computing and post-quantum cryptography (PQC) capabilities, will move the security of the industry and the ecosystem to a new level. ICT providers look forward to supporting partners in the ecosystem as they embrace these new technologies. Digital operational resilience testing such as penetration testing is a further area on which CSPs are working to ensure business continuity for financial institutions.

2. Implementation of the EU DORA framework

2.1 Main objectives of DORA

An official stated that DORA is a timely, well-designed and ambitious text that includes some unique features. One is that it is completely cross-sectoral, making no distinction between banks, insurers, securities firms, asset managers and payment firms and applying to firms of all sizes and levels of complexity. Implementation will still be a challenge, but the legislation's approach in terms of proportionality should help. DORA is also unique in that it asks European supervisors – the national competent authorities (NCAs) from all member states and EU level supervisors, including the ESAs, ECB, ENISA, SRB and ESRB - to jointly implement the legislation in a completely integrated way. The ESAs Joint Committee has thus established a dedicated sub-committee to work on the implementation of DORA and support the establishment of the Level 2 standards and required policy tools.

DORA addresses three main issues, the official explained. The first is firms' risk and threat management. Secondly, incident identification and reporting both of major and smaller incidents, as the latter incidents can also have significant implications. Thirdly, the oversight of critical third-party service providers (CTPPs). This oversight concept is completely new in that it concerns third party ICT providers that are not regulated or supervised at present. Designated CTPPs are now so important for the resilience of the financial sector that they should be brought into the scope, with a system of audit and engagement allowing oversight to be conducted in a cost-effective, proportionate and reasonable way.

The Chair noted that the scope of DORA is ambitious and cross-sectoral and asked if some sectors are better equipped than others in terms of cyber-resilience. The official stated that there is healthy divergence, with each financial sector having strong points to draw from. This is an opportunity to learn from existing best practices and to define a more integrated pan-European way forward.

A regulator emphasized that the DORA response regarding CTPPs is about oversight rather than supervision. It aims to ensure that financial entities remain in control so that the system is able to continue operating. The oversight of CTPPs will be jointly handled by the three ESAs (European Supervisory Authorities): EIOPA, ESMA and the EBA, with a lead overseer designated for each CTPP.

A second regulator noted that firms and supervisors must manage risk both at the individual firm and system-wide levels. Financial firms and TPPs such as CSPs collaborate with a shared responsibility model, which introduces a dual set of responsibilities shared between them. Currently, there is legislation going through the UK Parliament concerning CTPPs that will introduce a framework mandating supervisors to identify, oversee and influence them. Financial firms will also be required to implement playbooks introducing minimum resilience standards and recognising in particular the possible effect of multiple firm failures or disruptions. Supervisors will also be provided with a stress testing toolkit including scenarios for the testing of material services. Sector-wide exercises are also needed with the participation of CTPPs that provide services for a wide range of institutions. This will also contribute to enhancing the cyber resilience capabilities of the public authorities.

An industry representative stated that the EU supervisory authorities should also ensure that DORA is closely aligned with NIS2. Harmonising reporting timelines, cyber incident criteria and cyber incident thresholds with existing standards is needed in particular. This will enhance legal certainty, establish clarity and trust in the ecosystem and allow cyber-resilience measures to be adapted and applied sustainably. However, cyber-resilience measures will continue to evolve. It is important

1. Microsoft for example has been investing more than $1 billion in cybersecurity measures every year over the last few years and has quadrupled that amount in 2023. The aim is to reach a total of $20 billion of investment in cybersecurity by 2026.

to ensure that regulatory changes are flexible, principle-based and harmonised so that all players operating in the financial ecosystem are able to apply them and contribute to the resilience, security and continuity of the overall financial sector.

A second industry representative stated that resilience is mostly about building capabilities. The aim is to assess, test and identify weaknesses and then implement capabilities likely to build sufficient resilience to operational stress events. Secondly, when thinking about concentration risks, it is important to focus on the risks from this concentration rather than the concentration of providers itself. Concentration exists in many parts of the financial market providing economies of scale or improved liquidity and is not a problem per se. What is needed is considering the possible risks associated with this concentration and proposing specific risk mitigation actions.

2.2 The DORA implementation approach and challenges

An official illustrated the challenges associated with the implementation of DORA, which needs to be completed within 20 months. A joint committee has been established by the ESAs to take the work forward in an integrated way, and progress is being made quickly. There are three core operating principles. The first is momentum. This work has to be completed quickly. The second is pragmatism. Rather than pursuing perfection, the work needs to be completed in such a way that a first basis is in place 20 months from now, on which iteration and a lessons learning process will continue. The third principle is quality. The implementation work on DORA will be carried out on the basis of three consultations. There will be a first consultation starting by the beginning of June 2023 in response to the Commission's request for advice from the ESAs on the concepts and criteria to use in identifying CTPPs. Secondly, there will be a consultation starting in late June, with a focus on aspects such as risk management and registers of incidents. There will then be a further consultation starting towards the end of this year on remaining issues relating to the implementation of DORA.

A regulator stated that regarding the implementation of the oversight framework for CTPPs, the ESAs are in the process of building an oversight model on which feedback will be sought from the financial industry and third-party providers in the coming months. The approach proposed will follow four main principles. The first principle is to build on the available experience at the European level and at the NCAs, which will be working together in an integrated way in the context of the DORA implementation sub-committee. The second principle is that the oversight scope should be broad enough, covering both contractual arrangements and system aspects. The third principle is to leverage the experience in terms of prudential and conduct supervision to identify weaknesses and areas of focus. In future, an oversight forum will allow all information to be brought together in order to make decisions. The final principle is the importance of proportionality. Using those four principles, the aim is to build an oversight system that will be organised in three main blocks. One is about identifying criticality regarding TPPs. A first exercise has been run to collect data from financial entities in order to conduct a criticality assessment. A discussion paper will be issued in May including first indications about criteria to use. This criticality assessment will also lead to the appointment of a lead overseer for each CTPP identified from one of the three sectors. Secondly, the resources from the three ESAs will be brought together to work in an integrated manner on the onsite and offsite oversight of CTPPs and the planning of activities and actions. There will be a need for coordinating across sectors and EU member states to ensure consistency of the oversight, the identification of best practices and also the possibility for agreements with third countries on cooperation arrangements. The final area will involve issuing recommendations to CTPPs and following-up their implementation, making sure that CTPPs take into account the needs of the three main financial sector in their processes and activities.

A second regulator stated that DORA and the stronger harmonisation of the supervision of ICT and cyber threats in the EU that is aimed for is an ambitious and important step towards ensuring the resilience of the EU financial system. DORA is however more an evolution rather than a revolution. There are already many regulations supporting adequate levels of information management, information security and business continuity. DORA provides a more specific set of tools for tackling ICT and cyber risks, but it is important to be able to use these new tools efficiently. Supervisors already authorise and monitor the outsourcing of activities to ICT TPPs, but DORA will increase the level of oversight, notably with the new role of lead overseer for CTPPs. Conceptually, this approach is similar to the joint supervisory teams (JSTs) of the ECB in charge of supervising significant banks under the single supervisory mechanism (SSM). There will also be stronger cooperation on AML issues with the forthcoming implementation of the AML Authority (AMLA). There are still pending questions about how the lead overseers of CTPPs will work in practice and how this approach will differ from the JSTs. The availability of sufficient ICT and cyber-security skills within supervisory authorities is another challenge, as there is already a scarcity of these profiles in the market.

The proportionality of DORA is a further important point to consider, the regulator emphasized. The principle of proportionality is clearly stated in the Level 1 text and should also be clearly established in the Level 2 RTSs in order to facilitate the implementation of the DORA requirements across the financial sector and the EU member states in a coherent way.

The Chair agreed that with a stronger role of the authorities in the ICT and cyber-resilience space, it is important to ensure that they have the adequate skills and resources to conduct this mission. Coordination is also crucial among the different stakeholders concerned in the EU in order to make the financial system more resilient in terms of operational risks, as well as international cooperation and ensuring that the global perspective is taken into account.

3. Policy approach to digital operational resilience at the international level

A regulator stated that a global regulatory response is important to ensure a sufficient level of digital operational resilience, as global financial institutions are relying on TPPs able to operate on a cross-border and global scale. Financial firms are centralising technology and operations for efficiency purposes, potentially creating new critical points of failure. It is important for the supervisory community to continue learning, sharing and iterating its policy approach to these developments. The consultation due to be published by the FSB by summer 2023 on third party risks and outsourcing will be an important element in this perspective.

There is a great deal of commonality between the UK and EU in the thinking around digital operational resilience, the regulator observed, although the UK has picked up on a few additional points around operational incidents in particular. Since it is inevitable that operational failure will happen at some point, firms are asked to set impact tolerances that will not lead to financial disruption at a systemic level. Firms need to be able to continue their business services within their impact tolerances, even after an extreme but plausible stress scenario. This requires that firms analyse their end-to-end risks and identify the critical business services that may have wider repercussions for the financial system and on which they need to share information with the authorities.

An industry representative stated that work is underway in the US on improving the cybersecurity framework and providing additional guidance in this area. In March 2023, the SEC proposed a broad suite of cybersecurity rules including policies and procedures to address cybersecurity risk, written incident response programs, public disclosure requirements with new types of SEC filings, and an extension of the Systems Compliance and Integrity (SCI) regulation to large broker-dealers and other types of firms under an expanded Rule 10 (Cybersecurity Risk Management Rule).

A second industry representative stated that international collaboration is important in this area to ensure that jurisdictions adopt a consistent and principles-based approach when introducing new regulatory measures, and also that there is sufficient coherence between existing legislative measures and those still in development and that new legislative measures are sufficiently proportionate.