Digital operational resilience

Thomas Plomteux

Assessing cyber and ICT risks as well as encouraging control over those risks are key priorities for the Bank in the exercise of its different missions. This article takes a look at the cyber and ICT-related threats and risks facing financial institutions in general and market infrastructures, payment institutions and electronic money institutions in particular. This is followed by a summary of the various initiatives taken by the Bank in this context. Finally, there is an overview of common observations made during on-site inspections focused on cyber and ICT risk, also with particular attention to FMIs, PIs and ELMIs.

Continuing rise in cyber and ICT threats

In 2020 and the first half of 2021, the digital operational resilience of the financial sector was tested to a considerable degree by the COVID-19 pandemic. Since March 2020, companies and institutions have largely switched to working from home, which poses unprecedented challenges and additional risks. Initially, these challenges were mainly operational, such as the need to expand IT capacity for teleworking. As the pandemic drags on, the challenges are becoming increasingly strategic in nature. For instance, institutions are being forced to set priorities between current and planned strategic projects, the current circumstances often preventing them from maintaining their pre-crisis pace and extent of change. Furthermore, while wide-scale teleworking reduces the health risk, it heightens the inherent cyber and ICT risks. Some institutions may have had to temporarily adjust their security controls in order to facilitate this remote working. Additionally, the reduced physical availability of operators can make it more difficult to resolve incidents, or the large number of company computers simultaneously connecting remotely to the institution over the internet can present challenges. Fortunately, owing to the precautions taken by the institutions, this situation has not yet led to any major operational incidents.

In any case, cyber attacks have become an everyday reality throughout the world in recent years. Attackers are also evidently refining the techniques and methods used, so that some of the attacks are becoming ever more sophisticated and powerful. The number of persistent, targeted cyber attacks is therefore likely to increase further in the future, with the financial sector logically remaining a potential target. The list of cyber attacks targeting financial institutions worldwide drawn up by the think tank Carnegie Endowment for International Peace[1] provides an up-to-date view of the cyber threats facing the sector. An additional example is the large-scale attack on SolarWinds, a global service provider of software for network, system and infrastructure management. The impact of this attack on SolarWinds customers is still being mapped today.

1 https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline.

In these circumstances, it is challenging for financial institutions and infrastructures to provide adequate protection for their IT systems, services and data against all the various attacks. As cyber threats are evolving very rapidly, it is more necessary than ever to ensure that the defence capability of financial institutions and FMIs enables them to respond flexibly to changing patterns of attack. It is vital in this regard to have solutions for collecting data on potential threats, attackers and types of attack. It is also important not only for the external perimeter of the institution's network to be properly secured and monitored, but also for the internal measures to be sufficiently fine-meshed, incorporating multiple layers of protection. For financial institutions, it is likewise useful to know the risk profile of the customer and/or counterparty when determining the risk of fraud for certain transactions. In the context of retail banking, for example, that involves the use of security mechanisms built into the mobile or online banking application. As regards correspondent banking activities, examples include the Customer Security Programme (CSP) developed by SWIFT to assist financial institutions in assessing the counterparty risk relating to their messaging traffic. The CSP also stresses the importance of frequent reconciliation of outgoing transactions, to ensure prompt detection of potentially fraudulent activities and, where necessary, to stop them before they reach their final destination.

Apart from cyber risks, the financial sector's heavy dependence on IT solutions also presents other challenges. Under pressure from innovative players and customer expectations regarding the services offered, traditional institutions are being forced to renew their sometimes outdated IT architecture in a relatively short period of time. Growing security risks, e.g. from the use of end-of-life software that is no longer supported, may also lead to such a need. However, in some cases, the complexity of these institutions' IT environment makes it a major challenge to achieve this in a responsible way. There is likewise a high risk of growing dependence on third parties for IT services and other standardised IT system components. In particular, cloud solutions are increasingly being used, and for ever more important processes. That is also among the reasons why, throughout the sector, a small number of critical service providers present an ever-increasing concentration risk for the financial industry. The need for sufficiently representative testing of developed software and recovery solutions for various extreme but plausible scenarios remains another key point of focus.

It is therefore important for financial institutions' management bodies to have the necessary expertise and information to monitor risks appropriately, and to incorporate adequate measures in their strategic planning in order to keep risks within acceptable limits. However, many institutions say they have difficulty in recruiting sufficient staff with the required skills and expertise. In addition, all the staff of those institutions must be aware of the cyber and ICT risks in order to understand how those risks can arise and be ready to respond to them as expected.

Regulatory and operational initiatives

In recent years, the Bank has made a substantial contribution to the development of a regulatory framework aimed at improving the control of cyber and ICT risks. The prudential Circular on the Bank's expectations regarding operational business continuity and security of systemically important institutions[1] remains a key reference point. The Bank is also making an active contribution to establishing a European regulatory framework for the management of cyber and ICT risks. Under the aegis of the EBA, this has led to the publication of guidelines for supervisory authorities on the assessment of the ICT risk in the SREP[2], guidelines on outsourcing[3], and guidelines on ICT and security risk management[4]. These guidelines have since all become part of the Bank's supervision and policy framework.

1 Circular NBB_2015_32 of 18 December 2015 on the additional prudential expectations regarding operational business continuity and security of systemically important financial institutions.

2 EBA Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process (SREP) (May 2017).

3 EBA Guidelines on outsourcing arrangements (February 2019).

4 EBA Guidelines on ICT and security risk management (November 2019).

In September 2020, the European Commission published a proposal for a Regulation called the Digital Operational Resilience Act (DORA). The Bank also plays an important advisory role in the Belgian delegation for discussions on draft legislation at European level, and will probably also be closely involved in complementing DORA with technical standards. More information on this subject can be found in box 13.

The approach concerning individual institutions is two-pronged. On the one hand, institutions subject to prudential supervision are required to hold capital to cover their operational risks, including cyber and ICT risks. At the same time, the operational security and robustness of the critical processes of financial institutions and FMIs are subject to close monitoring. The availability, integrity and confidentiality of IT systems and data are crucial here. In 2020, the Bank once again conducted a number of inspections to check on compliance with the regulatory framework and to verify proper management of IT systems in relation to cyber and ICT risks. In addition, the Bank monitors these risks in financial institutions and FMIs in the course of its ongoing and recurrent supervisory activities. The COVID-19 health crisis forced the Bank to review its approach to these supervisory activities. The content of the activities was adjusted to the new reality, with particular emphasis on COVID-19, while working methods were adapted to give preference where possible to remote meetings and technological resources. Finally, the Bank operationalised a framework for ethical hacking, which is discussed in the thematic article on Threat Intelligence-Based Ethical Red teaming in Belgium (TIBER-BE).

The Bank is also paying closer attention to sectoral initiatives. Prompted by the SSM, among other things, some FMIs are regularly asked to complete an IT questionnaire which provides important data for the annual SREP and also permits cross-sectoral analyses. In its role as the sectoral authority for application of the Law on the security and protection of critical infrastructures (principally systemically important banks and FMIs), the Bank also assesses the effectiveness of the control systems of critical financial infrastructures. In that context, the Bank organises and coordinates sectoral crisis simulation exercises in order to prepare the Belgian financial sector for potential operational incidents of a systemic nature, should they occur in the future. Under the Law on network and information system security (NIS), the Bank acts as the sectoral point of contact for major incidents in the financial sector.

BOX 13

Digital Operational Resilience Act

Context

On 24 September 2020, the European Commission's Directorate-General for Financial Stability, Financial Services and Capital Markets Union (DG FISMA) presented its proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector, the so-called Digital Operational Resilience Act (DORA)[1]. This piece of legislation is part of a much broader Digital Financial Strategy that sets out general lines on how Europe can support the digital transformation of finance in the coming years, while regulating and mitigating the risks arising from it.

The proposal for a Regulation on digital operational resilience is motivated by the ever-increasing dependence of the financial sector on software and digital processes, resulting in information and

1 COM/2020/595 final – https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act.

communication technology (ICT) risks posing a challenge to the operational resilience, performance and stability of the EU financial system as a whole. The Commission tabled the proposal because it believes that current legislation across Member States does not fully address the topic, nor does it provide financial supervisors with the most adequate tools to fulfil their mandates, and leaves too much room for diverging approaches across the Single Market. Last but not least, the proposal responds to the 2019 Joint Technical Advice of the European Supervisory Authorities (ESAs) that called for a more coherent approach in addressing ICT risk in finance[1].

The DORA proposal contains five distinct pillars:

- **Governance-** and **ICT-risk-management-**related key principles and requirements for financial entities, inspired by relevant international, national and industry-set standards, guidelines and recommendations. These requirements revolve around specific functions in ICT risk management (identification, protection & prevention, detection, response & recovery, learning & evolving, and communication), but also underline the importance of an adequate governance and organisational framework. Amongst others, the crucial, active role the management body has in steering the ICT risk management framework and the assignment of clear roles and responsibilities for ICT-related functions is covered by this first pillar.
- The second pillar relates to requirements for financial entities with regard to **managing** and **classifying ICT-related incidents**, and a proposal to harmonise and streamline the **reporting** of such major incidents to the competent authorities, alongside responsibilities for competent authorities in providing feedback and guidance to financial entities and in forwarding relevant details to other authorities with a legitimate interest. The ambition put forward is that financial entities should report major incidents only to one competent authority. To this end, the feasibility of a single EU hub will be studied by the ESAs, the ECB and ENISA.
- The third pillar addresses requirements for **digital operational resilience testing**, i.e. periodically testing for preparedness and identification of weaknesses, deficiencies or gaps, as well as the prompt implementation of corrective measures. While all financial entities should test their ICT systems by making use of tests ranging from vulnerability scanning to software code analysis, only those entities identified by competent authorities as significant and cyber mature will be required to conduct advanced Threat-Led Penetration Tests.
- Fourth, there are provisions that should ensure the sound management of **ICT third-party risk**. On the one hand, this objective will be achieved through the respect of **principle-based rules** applying to financial entities' monitoring of this risk, and through regulation **harmonising key elements** of the service and relationship with ICT third-party providers. On the other hand, the regulation seeks to promote convergence on supervisory approaches to ICT-third-party risk in the financial sector by **subjecting critical ICT third-party service providers to an EU oversight framework**.
- Fifth, to raise awareness on ICT risk, to minimise the propagation of risk, to support financial entities' defensive capabilities and threat detection techniques, the regulation explicitly allows financial entities to set up arrangements to **exchange** amongst themselves **cyber threat information and intelligence**.

The foreseen scope of application of DORA is a broad range of financial entity types, amongst others credit institutions, insurance and reinsurance undertakings, investment firms, payment institutions and

1 Joint Advice of the European Supervisory Authorities to the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector, JC 2019 26 (2019).

electronic money institutions. By having this broad scope, DORA seeks to harmonise approaches across the financial sector with the objective of an increased operational resilience and to ensure a safer overall financial system. A lighter regime is on the cards for microenterprises[1].

Points of focus for the National Bank of Belgium

Since the publication of the DORA proposal, experts from the National Bank have contributed to defining the Belgian position that is reflected in discussions on this proposal in the EU Council's Working Party on Financial Services, held first under the German and now the Portuguese presidency. It is to be expected that the NBB experts will also play a role in the development of the regulatory and implementation technical standards that will support the final DORA Regulation.

Overall, the NBB is very supportive of the DORA initiative and its ambition to strengthen digital operational resilience and to further harmonise ICT risk management practices and requirements in the financial sector. In some areas, there are nevertheless some issues that warrant further discussions in the Working Party so as to clarify the exact scope and impact of the Regulation. Some examples are the following:

- *Proportionality principle* – In order to avoid imposing undue burdens on smaller financial entities and smaller ICT third-party providers, the DORA proposal should be scrutinised to include some further exemptions from its provisions; and/or some DORA provisions could be modulated according to the size and/or criticality of the financial entities in scope.
- *Scope of DORA* – The rationale for including external auditors and insurance intermediaries in the scope of application of the Regulation needs to be further investigated and clarified. On the other hand, the exclusion of payment systems, card schemes and clearing and settlement systems from the scope is welcomed, since these are typically already covered by the oversight of central banks, with a well-developed and harmonised framework set up by national central banks and the ECB.
- Another element of scope that warrants further clarification is the current definition of "ICT services" and "ICT third-party providers". As both terms are defined in a very wide sense, this could lead to the unintended inclusion of several service providers that are better left out of the scope of DORA. In particular, undertakings whose core business is in the processing of payment transactions come to mind. In Belgium, such processors of payment transactions are already subject to a specific oversight regime.
- *Concurrent legislative undertakings* – While the text of the DORA Regulation is being negotiated, discussions on a revised NIS directive on the Security of Network and Information Systems (NIS 2) have also started. To avoid overlap and collusion between both undertakings, the relationship between them should be clarified and clearly delineated. While DORA is a Regulation specific to the financial sector, the renewed NIS Directive could be transposed differently across EU countries and is not limited to the financial sector but has a more transversal scope across industries.
- *Interplay between PSD2 and DORA* – With regard to major incident reporting, the interplay between the PSD2 Directive and DORA needs to be clarified. More specifically, any doubt should be removed as to the competent authority that should receive the incident reports directly from the reporting entity. With DORA being limited to the reporting of ICT incidents, further clarification should also be provided on the treatment of non-ICT related incidents as foreseen under PSD2.

1 As defined in Commission Recommendation 2003/361/EC, a microenterprise is an enterprise which employs fewer than 10 people and whose annual turnover and/or annual balance sheet total does not exceed € 2 million.

- *Recognition of well-established TIBER-EU framework* – Regarding advanced digital resilience testing, the Eurosystem already developed harmonised Threat Lead Penetration Testing standards and practices with its TIBER-EU framework. So, DORA provisions on advanced digital resilience testing could be largely based on referencing the TIBER-EU framework. Valuable characteristics of the current TIBER-EU approach could thus be maintained (e.g. the planning of tests based on constructive dialogue; mutual recognition principles) and not all competent supervisory authorities should become operationally involved in the tests, nor should they validate the correct execution or the results of the tests. Involving competent authorities when discussing the scope of a test and incorporating test results into their supervision could be beneficial.
- *Provisions on outsourcing* – Concerning ICT third-party management, wording in DORA can be clarified to explain which outsourcing rules will prevail in the event of a conflict between DORA and sector-specific rules on outsourcing. On the requirement under DORA for critical ICT third-party service providers to be established in the European Economic Area, care is needed to strike the balance between, on the one hand, the risk such dependence might involve for financial institutions (either directly or via subcontracting) and, on the other hand, the risk of then no longer having access to certain ICT services.
- *Dedicated DORA oversight regime on critical ICT third-party service providers* – In the proposed oversight regime, it is key to foresee a more important role for the national competent authority of the Member State where the critical third-party service provider is established. Also, it will be more efficient and less costly to pool resources and expertise through centralisation of the Lead Overseer role at one ESA, rather than making all three ESAs responsible. Regarding the means of enforcement of (non-binding) recommendations made to critical third-party service providers, a comply-or-explain approach and an involvement of the Lead Overseer in the follow-up process to these recommendations is preferable. This will further ensure a coordinated and consistent approach across the Union. Furthermore, competent authorities of financial entities already interacting with critical ICT third-party providers used by entities under their supervision should be able to continue exercising their (prudential or other) powers with respect to these financial entities regardless of the (non-binding) recommendations issued under the oversight framework for critical third-party providers.

The Bank will continue to monitor how the DORA Regulation is further developed and how it can contribute to the successful implementation of this legislation within its current supervisory, oversight and policy-setting mandate.

Common observations from on-site inspections

As mentioned previously, a number of FMIs, PIs and ELMIs have in recent years been subject to on-site inspections focused on cyber and ICT risks. These activities frequently resulted in similar observations. Some of these thematic findings are summarised below.

In many cases, institutions still have room for progress in establishing sufficiently detailed and concrete strategies regarding security and continuity risks. Structured strategic reflection, decision-making and monitoring at board and senior management level is crucial here, as is sufficiently clear and comprehensive reporting on these risks and their evolution under the influence of mitigating measures and projects.

Institutions often still invest insufficient time and resources in their policy frameworks, including the related technical standards and procedures. This sometimes results in them not being sufficiently up to date, consistent, clear, feasible and/or adapted to the specific organisation.

Not all institutions have an adequate and sufficiently documented framework for managing ICT risks. This deficiency often impedes the performance of credible, standardised and sufficiently detailed risk assessments and prevents proper registration and monitoring of all identified risks.

In several cases, financial institutions were found to have insufficient resources or expertise or not to operate efficiently enough to manage and/or assess security-related risks appropriately. It is essential to avoid excessive fragmentation of responsibilities, but also to maintain the so-called three-lines-of-defence model for those institutions to which this applies.

Many institutions should still organise initiatives to make their staff aware of security risks more regularly, and monitor the effectiveness of these initiatives. Such initiatives should cover a wide range of topics and address all relevant target groups (board of directors, executive committee, end users, IT administrators, developers, etc.).

Furthermore, in order to properly define and prioritise controls, it is important that these institutions map their IT architecture, IT and data assets, interdependencies and associated communication flows in sufficient detail. However, it has been found that institutions often have only a partial overview of these elements. In addition, as mentioned earlier, it is crucial that institutions proactively identify which software is nearing the end of its life cycle, and take action in good time to avoid using software that is no longer supported by the supplier.

Some institutions should further improve their outsourcing and third-party risk policy frameworks and ensure that they are effectively implemented, in order to obtain a complete overview of the outsourcing on which they are dependent and of the controls that should mitigate the associated risks. This should also ensure, among other things, that all outsourcing contracts contain the necessary clauses and that important outsourcings are regularly audited.

Another frequent issue is the management, protection and monitoring of logical access rights. Particular attention should be paid to privileged access rights. Access to highly confidential and/or critical applications and administrator accounts should be protected by strong authentication solutions.

The resources provided for implementing and maintaining basic security controls and processes such as network segmentation, encryption, automated real-time detection of IT assets, vulnerability management, secure development practices, compliance monitoring, etc., are often still inadequate.

Solutions for detecting and responding to anomalous behaviour can often be further strengthened. In particular, the coverage of IT systems and applications, the intelligence used, the analytical capabilities to correlate different sources of information, the available response plans and resources, etc. are often in need of improvement.

Institutions should test their security and continuity measures and plans more regularly and in an integrated and representative manner, taking into account various extreme but plausible scenarios.

Finally, internal audit programmes sometimes do not yet sufficiently cover security and IT continuity risks. Institutions should also ensure that the resultant findings and recommendations are addressed as soon as possible.