5. Specific thematic article: 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 covers some of the cyber- and ICT-related threats and risks faced by financial institutions in general, as well as by financial market infrastructures, payment institutions and electronic money institutions in particular. This description is followed by a summary of the various initiatives, taken by the Bank in this context, both on the regulatory and supervisory side. Finally, there is an overview of common observations made during on-site inspections focused on cyber and ICT risk, again paying particular attention to FMIs, PIs and ELMIs.

Continuing rise in cyber and ICT threats

2022 was still marked to some extent by the after-effects of the COVID-19 pandemic. However, the associated challenges, such as mass working from home, more limited physical presence of operators, specific attack patterns, etc. were mostly adequately dealt with in the financial sector. The solutions found are now often part of the "new normal".

In February 2022, the geopolitical conflict in Eastern Europe took an important turn with Russia's invasion of Ukraine. Given the broad and explicit Western support for Ukraine and the European sanctions against Russia, it suddenly became much more likely that European countries, and in particular Belgium given the presence of several international institutions, would become the target of cyber attacks committed by either groups linked to nation states, or so-called "hacktivists". Scenarios in which the attackers unintentionally cause collateral damage should also not be ruled out, as well as attacks on non-financial critical infrastructures (telecom, energy, etc.), which could have a substantial impact on the financial sector. The Bank and the entire financial services industry have been in a heightened state of preparedness since the escalation of the conflict. Fortunately, thanks to various precautionary measures, this concrete threat did not lead to any major operational incidents during the reporting year.

In any case, cyber attacks have evolved worldwide into an everyday reality in recent years. Malicious actors are further honing their techniques and methods, resulting in some of the attacks becoming increasingly sophisticated, powerful and/or enabling large-scale campaigns. The number of persistent and targeted cyber attacks is therefore expected to rise further in the future, with the financial sector most probably remaining a potential high-value target. Cyber attacks may result in the theft of sensitive data, system disruption, initiation of fraudulent transactions, etc. This often involves the use of ransomware, distributed denial-of-service (DDoS) attacks, abuse of credulous employees or exploiting other vulnerabilities in the infrastructure and processes of institutions, including their supply chain. See box 1 for a detailed and more technical description of recent developments in cyber threats.

Apart from cyber risks, the financial sector's heavy dependence on IT solutions also throws up other challenges. Under pressure from innovative players and higher customer expectations regarding services offered, traditional institutions are forced to renew their at times outdated IT architecture in a relatively short timeframe. Growing security concerns, triggered for example by the use of "end-of-life" software that the vendor no longer supports, only add to this sense of urgency. However, the complexity of these institutions' IT environments makes their responsible modernisation a major challenge in some cases. 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 a growing number of critical processes. That is also one of the reasons why, across the sector, a small number of critical service providers present an ever-increasing concentration risk for the financial industry. In recent years, it has also become very clear what impact geopolitical tensions can have on certain supply chains. The need for sufficiently representative testing of developed software and recovery solutions for various extreme but plausible scenarios remains another key point of attention.

In order to monitor and keep the risks within appetite, it is important for financial institutions' management bodies to acquire the necessary information and intelligence (on external threats and the institution's operational resilience), to have appropriate expertise available, and to incorporate adequate countermeasures in the strategic planning. But quite a few institutions admit they have difficulty in recruiting sufficient staff with the required cyber/ICT expert skills.

Regulatory and legislative developments

In recent years, the Bank has made a substantial contribution to the development of a regulatory framework to improve 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 has also made an active contribution to establishing a European regulatory framework for the management of cyber and ICT risks. Under the aegis of the EBA, this resulted in the publication of a set 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 all become part of the Bank's supervision and policy framework. For payment systems and market infrastructures, the ECB's oversight expectations regarding cyber resilience are providing guidance[5]. Last but not least, there have also been important developments at global level: in March 2021, the Basel Committee on Banking Supervision published new principles for strengthening the operational resilience of banks, including specific focus on ICT and cyber security[6].

On 17 January 2023, the Digital Operational Resilience Act (DORA) entered into force. This EU regulation aims to mitigate the risks associated with the digital transformation of the financial industry by imposing strict and common rules on ICT governance and risk management, ICT incident reporting and information-sharing, security testing and ICT third-party risk. These rules will apply to a wide range of financial institutions, as well as critical ICT third-party service providers, for example cloud service providers, that will be subject to a form of EU oversight. During negotiations on the draft texts at European level, the Bank played an important advisory role in the Belgian delegation. In the meantime, NBB experts are intensively involved in the development of technical standards that will further underpin the DORA Regulation. More information on this topic can be found in box 12.

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).
5 ECB Cyber resilience oversight expectations (December 2018).
6 BCBS Principles for Operational Resilience (March 2021).

BOX 12

Digital Operational Resilience Act

On 17 January 2023, the EU Digital Operational Resilience Act (DORA) entered into force[1] after more than two years of negotiations. Its provisions will apply as of 17 January 2025. The initiative came from the European Commission's Directorate-General for Financial Stability, Financial Services and Capital Markets Union (DG FISMA) in response to the 2019 joint technical advice from the European Supervisory Authorities (ESAs) that called for a more coherent approach in addressing ICT risk in finance[2] and as part of a much broader Digital Financial Strategy setting out broad guidelines on how the European Union intends to support the digital transformation of finance in the coming years, while regulating and mitigating the risks arising from it.

The DORA Regulation is motivated by the ever-increasing dependency of the financial sector on digital assets and processes, resulting in information and 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 on the grounds that current legislation across Member States does not fully address the topic in a detailed and comprehensive way, does not provide financial supervisors with the most adequate tools to fulfil their mandates, and leaves too much room for diverging approaches across the Single Market.

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 other things, the crucial and active role the management body has been in steering the ICT risk management framework. 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, besides 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 goal is for financial entities to have to 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. In the same spirit, the incident reporting obligations under PSD2 will be fully integrated into this new incident reporting framework.
- The third pillar addresses requirements for **digital operational resilience testing**, i.e. periodically assessing cyber resilience 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

1 Regulation (EU) 2022/2554 of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No. 1060/2009, (EU) No. 648/2012, (EU) No. 600/2014, (EU) No. 909/2014 and (EU) 2016/1011 (14 December 2022)

2 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).

making use of tests ranging from vulnerability scanning to software code analysis, only those entities identified by competent authorities as significant would be required to conduct advanced threat-led penetration tests.

- Fourth, the proposal contains provisions to 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 that harmonises 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 a Union oversight framework**.
- The last and fifth pillar raises awareness around ICT risk and related aspects such as: minimising the propagation of risk, supporting financial entities' defensive capabilities and threat detection techniques, explicitly allowing financial entities to set up **cyber threat information and intelligence exchange** arrangements amongst themselves.

A broad range of financial entity types falls under the scope of DORA, including central securities depositories, credit institutions, insurance and reinsurance undertakings, investment firms, payment institutions and 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 and more stable overall financial system. Operators of payment systems and entities involved in payment processing remain out of its scope for the time being.

DORA is to be considered *lex specialis* with respect to the EU Directive on measures for a high common level of cyber security across the EU (also referred to as the NIS 2 Directive)[1]. This means that the requirements under DORA regarding for example ICT risk management and ICT-related incident reporting are in principle more far-reaching than those under the NIS 2 Directive and that institutions in the personal scope of the Regulation only have to comply with the DORA provisions, unless the national transposition of NIS 2 would explicitly extend the scope or provisions of the NIS 2 Directive (and therefore deviate from the minimum harmonisation principle).

The EU legislators have further specified that, given the strong interlinkages between the digital resilience and the physical resilience of financial entities, the obligations laid down in Chapters III and IV of the Directive on the resilience of critical entities (CER)[2] should not apply to financial entities falling within the scope of DORA. Here too, the national transposition of CER could still extend the scope or provisions of the CER Directive.

Overall, the National Bank of Belgium is very supportive of the DORA initiative, its ambition to strengthen digital operational resilience and to further harmonise ICT risk management practices and requirements in the financial sector. It is fully committed to a successful implementation of DORA and is actively contributing to the establishment of level-2 texts that will support the final DORA Regulation.

1 Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (14 December 2022).

2 Directive (EU) 2022/2557 of the European Parliament and of the Council on the resilience of critical entities and repealing Council Directive 2008/114/EC (14 December 2022).

Finally, in early 2022, the European Systemic Risk Board published recommendations for the establishment of a pan-European framework for coordinating cyber incidents of a systemic nature. The Bank is also closely involved in the elaboration of these recommendations.

Supervisory activities

The traditional supervisory 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 the IT systems and data are crucial here. As in recent years, the Bank conducted a number of inspections in 2022 to check compliance with the regulatory framework and to verify the proper management of IT systems in relation to cyber and ICT risks (see also next section).

In addition, the Bank monitors these risks in financial institutions and FMIs during its ongoing and recurrent supervisory activities. In March 2022, in response to the heightened cyber threat posed by the Russian invasion of Ukraine, the Bank decided to raise awareness among the institutions under its supervision on the cyber threat posed by this crisis and to urge them to improve their operational preparedness. In addition, a selection of significant institutions was requested to complete a short survey. The answers to this survey were further supplemented during follow-up sessions with the respondents. After a thorough analysis of the various responses, the Bank can conclude that the sector was generally well aware of the heightened threat level and that it responded appropriately.

The Bank is also taking other sector-wide initiatives. Inspired by the approach for credit institutions under the SREP, some FMIs, payment institutions and electronic money institutions are requested to respond to IT risk questionnaires on a regular basis. This provides important data for the prioritisation of supervisory work and also permits cross-sectoral analyses. One novelty this year was that a selection of financial institutions was asked to provide a list of the arrangements they have with ICT third-party service providers. This exercise was part of an initiative of the European Supervisory Authorities (ESAs), which in this way tried to obtain a first view of the third parties that could in the future be designated as critical service providers under the DORA Regulation.

In 2018, the Bank set up a framework for ethical hacking, namely TIBER-BE (Threat-Intelligence- Based Ethical Red Teaming Belgium). This program is the Belgian implementation of a methodology developed by the Eurosystem, which aims at increasing the cyber resilience of individual FMIs and financial institutions through sophisticated tests, as well as to gain important insights into the cybersecurity of the Belgian financial sector as a whole. The Bank encourages these exercises in its role as catalyst for financial stability. More information on this TIBER-BE implementation can be found in the thematic article 8 on TIBER-BE.

In its role as the sectoral authority for 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 infrastructure. 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.

The Bank also takes part in various international working groups and forums to gain a better understanding of the risks that could become systemic for the financial sector and to study mitigating measures. Other initiatives aim to promote the exchange of information between institutions, supervisors, central banks, etc.

Common observations from on-site inspections

As mentioned previously, a number of FMIs, PIs and ELMIs were subject in recent years to on-site inspections focused on cyber and ICT risks. These activities frequently resulted in similar observations. Below is an overview of some of these thematic findings:

- In many cases, institutions still need to make 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 comprehensive reporting on these risks and their evolution associated with the implementation of mitigating measures and related 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, treatment, monitoring and reporting of all identified risks.
- In a number of cases, institutions were found to have insufficient resources or expertise, or not to operate efficiently enough to manage and 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 more regularly organise initiatives to make their staff aware of security risks and monitor the effectiveness of these initiatives. These 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 infrastructure 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. And, as mentioned earlier, it is crucial that institutions proactively identify which software is nearing the end of its life cycle and take timely measures 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, including so-called intra-group arrangements, 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 sufficiently monitored and regularly audited.
- Another recurring topic 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 (i.e. multi-factor) 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. often remain 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 plans more regularly and do this 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 resulting findings and recommendations are addressed as soon as possible.