5. Specific thematic article: Digital operational resilience

Thomas Plomteux, Nikolaï Boeckx and Samuel Goret

Assessing cyber and ICT risks and encouraging control over those risks are key priorities for the Bank in performing its various missions. This article covers the cyber and ICT-related threats and risks faced by financial institutions in general, and those confronting 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. 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

Since March 2020, the COVID-19 pandemic has tested the financial sector's digital operational resilience to a considerable degree. Institutions have largely switched to working from home, which posed unprecedented challenges and additional risks. Initially, these challenges were mainly operational, such as the need to expand IT capacity for teleworking. However, as the pandemic dragged on, the challenges became increasingly strategic in nature. For instance, institutions were forced to set priorities between ongoing and planned strategic projects, circumstances often preventing them from maintaining the pace and extent of the changes planned before the crisis. Furthermore, while large-scale teleworking reduces the health risk, it amplifies the inherent cyber and ICT risks. Some institutions may have had to temporarily adjust their security controls in order to facilitate this teleworking. Additionally, the reduced on-site availability of operators can make it more difficult to resolve incidents. Furthermore, the large number of company devices simultaneously connecting remotely to the institution over the internet can present additional challenges. Fortunately, owing to the precautions taken by the institutions, this situation has not yet led to any major operational incidents.

More recently, the geopolitical crisis related to the war in Ukraine has had an impact on the cyber threat landscape, leading to increased vigilance on the part of the Bank and the Belgian financial sector as a whole. So far, also in this context, no major incidents have occurred in the Belgian financial sector.

In any case, cyber-attacks have become an everyday reality throughout the world in recent years. Malicious actors are also evidently refining the techniques and methods they use, with the result that some attacks are becoming ever more sophisticated and powerful. The number of persistent and targeted cyber-attacks is therefore likely to increase further in the future, with the financial sector understandably remaining a potential high value 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. In 2021, for example, reported cyber-attacks resulted in the theft of sensitive data, systems disruption and the initiation of fraudulent transactions. This often involved the use of so-called (crypto) malware, distributed denial-of-service (DDoS) attacks, the abuse of credulous employees or the exploitation of other vulnerabilities in the institutions' infrastructure and processes, including their supply chain. In recent years, it has indeed become clear that compromising third-party providers or exploiting vulnerabilities in their products permits the launch of large-scale attacks that may affect multiple companies, public authorities, and financial institutions simultaneously.

In this context, it is challenging for financial institutions and infrastructures to provide adequate protection for their IT systems, services and data against such a variety of attack types. As cyber threats are evolving very rapidly, it is more necessary than ever to ensure that the defence capabilities (including prevention, protection, detection and response) of institutions and FMIs enable them to adapt flexibly to changing patterns of attack. It is vital in this regard to have solutions that assist in collecting, analysing and managing intelligence on potential threats, attackers and types of attack. It is not only crucial that the external perimeter of the institution's network be properly secured and monitored, but also that the internal measures be sufficiently granular, incorporating multiple layers of protection. For financial institutions, it is also relevant to know the risk profile of the customer and/or counterparty when determining the fraud potential of certain transactions. In the context of retail banking, for example, this involves the use of security mechanisms built into mobile and online banking applications. 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, whenever necessary, to stop them before they reach the ultimate beneficiary.

Apart from cyber risks, the financial sector's heavy dependence on IT solutions also presents other challenges. Under pressure from innovative players and increased customer expectations regarding the services offered, traditional institutions are forced to renew their sometimes 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, in some cases the IT environment of these institutions is so complex that responsible modernisation presents a major challenge. 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 an ever-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. 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 other words, in order to monitor the risks and keep them within acceptable limits, it is important for the management bodies of financial players to have the necessary information and expertise, and to incorporate adequate counter-measures in their strategic planning. However, many institutions state that they have difficulty in recruiting sufficient staff with the required cyber/ICT expert skills. In addition, all the staff of those institutions must have a basic understanding and awareness of cyber and ICT risks, understand how those risks can arise, and be ready to respond to them adequately.

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

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 resulted in 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 all become part of the Bank's supervision and policy framework. For FMIs, the ECB's oversight expectations regarding cyber resilience are the benchmark[5]. Last but not least, there are also important developments at a global level: in March 2021, the Basel Committee on Banking Supervision published new principles for strengthening the operational resilience of banks, including a specific focus on ICT and cyber security[6].

In September 2020, the European Commission published a proposal for a Regulation called the Digital Operational Resilience Act (DORA). This proposal aims to mitigate the risks associated with the digital transformation of the financial industry by imposing strict, common rules on ICT governance and risk management, ICT incident reporting and information sharing, security testing and ICT third party risk. These rules would apply to a wide range of financial institutions, and to critical IT third-party service providers, for example cloud service providers, who would be subject to a form of EU oversight. More information on this topic can be found in box 9.

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 9

Digital Operational Resilience Act

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 act is part of a much broader Digital Financial Strategy that sets out general ways in which Europe can support the digital transformation of finance in the coming years, while regulating and mitigating the risks arising from it.

1 COM/2020/595 final (24/09/2020):
- https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act

The proposal for a regulation on digital operational resilience is motivated by the financial sector's ever-increasing dependency on digital assets and processes, resulting in information & communication technology (ICT) risks posing a challenge for the operational resilience, performance and stability of the EU financial system as a whole. The Commission made 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. 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 standards, guidelines and recommendations. These requirements centre on 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. Aspects covered by the first pillar include the management body's crucial and active role in steering the ICT risk management framework, and the assignment of clear roles and responsibilities for ICT-related functions.
- 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, as well as 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 proposed aim is for financial entities to have to report major incidents to a single competent authority. To this end, the ESAs, the ECB and ENISA are to study the feasibility of a single EU hub.
- The third pillar addresses requirements for **digital operational resilience testing**, i.e. periodically assessing cyber resilience and identifying 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 tools 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 by adherence to **principle-based rules** applicable to financial entities' monitoring of this risk and by regulation that **harmonises key elements** of the service and relationships 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**.
- The fifth and final pillar raises awareness of ICT risk and related aspects such as: minimising the propagation of risk, supporting financial entities' defensive capabilities and threat detection techniques, and explicitly allowing financial entities to set up **cyber threat information and intelligence exchange** arrangements amongst themselves.

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).

The intention is that DORA should apply to a broad range of financial entity types, such as 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 increasing operational resilience and ensuring a safer and more stable financial system overall.

DORA is expected to be a so-called "*lex specialis*" with respect to the Network and Information Security (NIS) directive, which is currently also being revised and renegotiated[1]. This means that the requirements under DORA regarding security and incident notification, for example, are in principle more far-reaching than those under the NIS directive, and that compliance with the DORA provisions is sufficient in the case of institutions to which DORA applies.

In 2020 and 2021 experts at the Bank helped to define the Belgian position in the discussions on DORA organised under the umbrella of the Council of the European Union. These discussions resulted in the adoption of a position by the Council in November 2021[2]. The European Parliament likewise adopted a position in December 2021[3]. In the meanwhile, the Council, the European Parliament and the European Commission have entered into trialogue negotiations.

Overall, the Bank 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. The Bank will continue to monitor how DORA develops further, and examine how to contribute to its successful implementation within the Banks' current supervisory, oversight and policy-setting mandate. We expect that the NBB experts will also play a role in drawing up the regulatory and implementation technical standards that will support the final DORA regulation.

1 This new initiative is also known as "NIS 2":
- COM(2020)823 final (16 December 2020):
  - o https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Cybersecurity-review-of-EU-rules-on-the-security-of-network-and-information-systems_en
- European Parliament position (18 October 2021):
  - o https://www.europarl.europa.eu/news/en/press-room/20211022IPR15610/cybersecurity-meps-strengthen-eu-wide-requirements-against-threats
  - o https://www.europarl.europa.eu/doceo/document/A-9-2021-0313_EN.html
- Council position (3 December 2021):
  - o https://www.consilium.europa.eu/en/press/press-releases/2021/12/03/strengthening-eu-wide-cybersecurity-and-resilience-council-agrees-its-position/

2 DORA: Council position (24 November 2021):
- https://www.consilium.europa.eu/en/press/press-releases/2021/11/24/digital-finance-package-council-reaches-agreement-on-mica-and-dora/

3 DORA: European Parliament position (1 December 2021):
- https://www.europarl.europa.eu/news/en/press-room/20211129IPR18302/protecing-the-eu-s-financial-system-from-cyber-attacks-and-ict-disruptions
- https://www.europarl.europa.eu/doceo/document/A-9-2021-0341_EN.html

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, in 2021 the Bank conducted a number of

inspections to check compliance with the regulatory framework and to verify the proper management of IT systems in relation to cyber and ICT risks. In addition, the Bank monitors these risks in financial institutions and FMIs during its ongoing and recurrent supervisory activities. The COVID-19 health crisis compelled the Bank to revise its approach to these supervisory activities. The content of the activities was adjusted to the new reality, with particular emphasis on COVID-19 related impact, while the ways of working were adapted to give preference to remote activities where possible. Inspired by the approach for credit institutions under the SREP, some FMIs, PIs and ELMIs are now requested to complete IT risk questionnaires on a regular basis. This provides important data for the prioritisation of supervisory work and also permits cross-sectoral analyses.

In 2018, the Bank set up a framework for ethical hacking, namely TIBER-BE (Threat Intelligence Based Ethical Red Teaming Belgium). This programme is the Belgian implementation of a methodology developed by the Eurosystem, which aims to increase 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 guardian of financial stability. In 2020, an updated version of the TIBER-BE framework was published on the Bank's website, further fine-tuning the methodology based on experience from tests already completed. The sector appears to be convinced of the applied methodology and of the added value of these specific tests. Meanwhile, the TIBER-BE team is also successfully conducting cross-border testing, in close and good cooperation with other EU countries that have implemented the TIBER framework, as well as with the United Kingdom, which has a similar framework, namely CBEST. The TIBER-BE programme is now coming to the end of a first cycle of tests, and the experience gained is being actively incorporated in the framework in preparation for a second cycle that will start soon.

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 likewise organises and coordinates sectoral crisis simulation exercises in order to prepare the Belgian financial sector for potential operational incidents of a systemic nature. 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.

Common observations from on-site inspections

As mentioned previously, in recent years a number of FMIs, PIs and ELMIs have been subject to on-site inspections focusing 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 still need to organise more regular initiatives to make their staff aware of security risks, and should 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. In addition, as mentioned earlier, it is crucial that institutions proactively identify any software 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 depend, including so-called intra-group arrangements, and of the controls designed to 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 insufficient.
- 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.