Regulation for cyber-resilience in the financial sector

Ludovic Van Egroo examines what the consequences for insolvency professionals are since the introduction of the new Digital Operating Resilience Act

LUDOVIC VAN EGROO
Governance Risk & Compliance Manager, Sopra Steria, Paris, France

The pandemic has generated the emergence of new vectors of cyber-threats, such as the increased use of telecommuting, the increase in remote exchanges and the digitalization of most business sectors.

The deterioration of the geopolitical context has seen an increase in "sleeping" cyberattacks of state origin, as well as a professionalization of cyber-malicious actors, as illustrated by the Atlas of Cyberattacks produced by Thales.[1]

ANSSI, the French cybersecurity agency, has identified a 37.7% increase in attacks in Europe between 2020 and 2021.[2] This increase in cyber-attacks goes hand in hand with the development of intrusion techniques and rebound attacks. The latter consists in infecting subcontractors and partners of the target companies, such as software editors and service providers. There are now entire ecosystems becoming targets.

In this context, the European institutions and Member States are continuing to secure the European market in terms of cyber-security with the adoption of a second version of the NIS Directive adopted in 2016 (Network Infrastructure System No. 2) to cover new sectors, including energy, transport, financial markets, health and digital infrastructure. The proposals aim to strengthen security requirements by imposing a risk management approach.

The NIS2 directive is strengthened by a new Act called the Digital Operational Resilience Act (DORA)[3], specifically dedicated to financial actors. This regulation presents a major evolution in the definition of financial actors, which is extended to the broadest sense to subcontractors. The DORA regulation aims to cover the cyber-risk of the entire value chain of the financial sector.

Who are the new actors concerned by this regulation? What are the changes for the actors of the financial sector? What are the consequences for insolvency professionals?

Who are Financial Sector Actors within the meaning of the DORA regulation?

Entities concerned by the Digital Operating Resilience Act:

- Credit institutions
- Payment institutions
- Electronic money institutions
- Investment firms
- Crypto asset service providers, crypto asset issuers
- Central securities depositories
- Central counterparties
- Trading platforms
- Central repositories
- Alternative investment fund managers
- Management companies
- Data communication service providers
- Insurance and reinsurance companies
- Insurance intermediaries, reinsurance intermediaries and incidental insurance intermediaries
- Institutions for occupational retirement
- Credit rating agencies
- Statutory auditors and audit firms
- Administrators of critical benchmark
- Participatory finance service providers
- Securitization repositories

AND Third party IT service providers

Regulatory developments in the sector: Towards the greater accountability of economic actors

What are the new obligations of the regulatory framework?

The regulation is based on five pillars:

- Identifying exposure to cyber-risks by ensuring that controls are functioning properly and up to date (Articles 4-14);
- Harmonising and centralising incident reporting for transmission to authorities ICT incident report (Articles 15 to 20);
- Digital Operational Resilience Tests (Articles 21 to 24);
- Management of ICT risks by Third Parties (Articles 25-39): verifying the level of sufficient controls of third parties, especially IBOs, and putting into place required monitoring measures; and
- Information and Intelligence Sharing (Article 40) Establish information sharing agreements between companies for cyber-threats, including confidentiality requirements and the need to notify the regulator.

The Digital Operating Resilience Act in practice:

In practice, this regulation will allow the companies concerned to:

- Establish a risk governance strategy, involving management, defining responsibilities and identifying stakeholders;
- Develop a risk management framework with the function of identifying preventive and corrective measures as well as disaster recovery plans and continuous improvement and crisis communication plans;
- Assess cyber-risk exposure, particularly through company risk mapping;
- Identify and map critical functions and associated risks (which also includes interdependencies with third parties, such as service providers);
- Organize cyber-risk awareness plans not only for teams in charge of governance, but also for operational teams;

- Elaborate a standardized classification of cyber-incidents;
- Subscribe, where necessary, to insurance against cyber-risks;
- Be subject to an obligation to declare major incidents (1 week) to regulatory authorities (ANSSI, CNIL, ECB); and
- Implement a third-party risk strategy and policy, in particular through:
  - Establishing a registry containing a complete view of all third-party ICT service providers (services provided and functions);
  - Reporting annually on the criticality of outsourced services, updating the tracking of changes and keeping a register for regulators; and
  - Evaluating the level of security, concentration risk, subcontracting risks (termination, exit under constraints) prior to any contracting.

One of the key success factors of compliance for organizations is the development of a transverse governance framework, including management, legal and compliance departments, information systems departments and information systems security departments.

What are the penalties?

In case of non-compliance, the DORA regulation provides for several types of sanctions:

- Administrative Penalties and Remedial Measures (Article 44);
- An injunction ordering the person or entity to cease the conduct in question and prohibiting it from being repeated;
- Temporary or permanent cessation of any practice or conduct deemed by the appropriate authority to be contrary to the provisions of this bylaw and to prevent its recurrence;
- Any measure, including monetary measures, to ensure that financial entities continue to meet their legal obligations;
- Requiring records of existing data exchanges held by a telecommunications operator where there is reasonable suspicion of a violation of this law and where such records may be material to an investigation of a violation of this law;
- Issuing communications to the public, including public statements, indicating the identity of the individual or entity and the nature of the violation; and
- Criminal sanctions left to the discretion of the Member States (Article 46).

To carry out their missions, the regulatory authorities will be able to:

- Access and receive or make copies of any document or data;
- Conduct on-site inspections or investigations; and
- Impose corrective measures.

DORA: The challenges for insolvency professionals

Insolvency professionals are particularly affected by this regulation, as the companies concerned are no longer just major players in the financial sector. Financial start-ups and SMEs are also affected by these obligations, as are subcontractors.

First issue: Identify the criticality of activities within companies:

The insolvency practitioner will need to consider these cyber-resilience requirements to the extent that the defaulting business is engaged in activities that define it as a financial actor. The insolvency practitioner will need to verify the company's cybersecurity compliance. As such, insolvency practitioner will be able to request documents attesting to the good governance of cyber-risks, including the documents mentioned above, if needed. These documents can be added to the file as a guarantee of the compliance of the financial activity.

In order to carry out his/her mission, the insolvency professional may rely on the expertise of a consulting firm to conduct a compliance audit of the DORA regulation. In the event that the company is not in compliance, it is up to the insolvency practitioner to request that the company be brought into compliance with the identified discrepancy.

Second Issue: Taking cyber-factors into account in the due diligence of third parties

The second issue concerns the control of cyber-risk with the company's service providers. The insolvency practitioner will be responsible for verifying that the service providers do not pose a risk to the business, beforehand, by identifying the critical services, then by checking the security devices implemented.

The difficulty here lies in the ability to defend the cyber-security requirements of the business in a difficult context for the latter, where faced with third parties critical for its activity, but very often in an already degraded relationship. It is in this difficult context intersecting legal, financial and also security issues exogenous to the company that the practitioner will be able to employ his/her skills before the court of jurisdiction.

Conclusion

Facing systemic risks that cyber-risk represents for the economies of the Member States, the European Union continues to secure its digital borders by involving economic players.

The European regulation responds to the need to harmonize the response measures, but also the resilience capacity of financial players in order to avoid the scenario of serial bankruptcy of the economic fabric, faced with a risk of continuous change in order to guarantee the security of the common market and the interests of European consumers.

As illustrated by the measures defined in the regulations, cyber risk is a cross-functional risk, both within companies and in terms of law.

Of note, however: law is one of the first preventive measures to secure cyberspace. ■

Facing systemic risks that cyber-risk represents for the economies of the Member States, the European Union continues to secure its digital borders by involving economic players.

Footnotes:

1 Thales, Atlas des Cyberattaquants (2022), available at: www.thalesgroup.com/fr/monde/securite/press_release/thales-presente-son-atlas-des-cyberattaquants-2022.

2 ANSSI, Une année 2021 marquée par la professionnalisation des acteurs malveillants, available at: www.ssi.gouv.fr/actualite/une-annee-2021-marquee-par-la-professionnalisation-des-acteurs-malveillants/

3 Proposal for a Regulation 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 and (EU) No 909/2014 of 24 September 2020 which will be adopted this year in accordance with the ordinary legislative procedure.