OPINION: CYBERSECURITY

Exploring DORA

Reflections on the role of regulation, including the Digital Operational Resilience Act, in promoting insurers' own cyber resilience

Mirenchu del Valle Schaan

President & secretary general, Association of Spanish Insurers (UNESPA)

The assessment of an insurer's technological risk profile and its resilience to such risks has involved intensive work from corporate management for many years. The introduction of the Solvency II regulatory framework was a key milestone, obliging the industry to adopt common approaches to technological risk management within the context of requirements such as the ISO standards. The latest development has been the approval of the EU Digital Operational Resilience Act (DORA), for which Level 2 measures are currently being drafted. Complying with these new rules will require significant efforts by insurers.

Building on NIS1

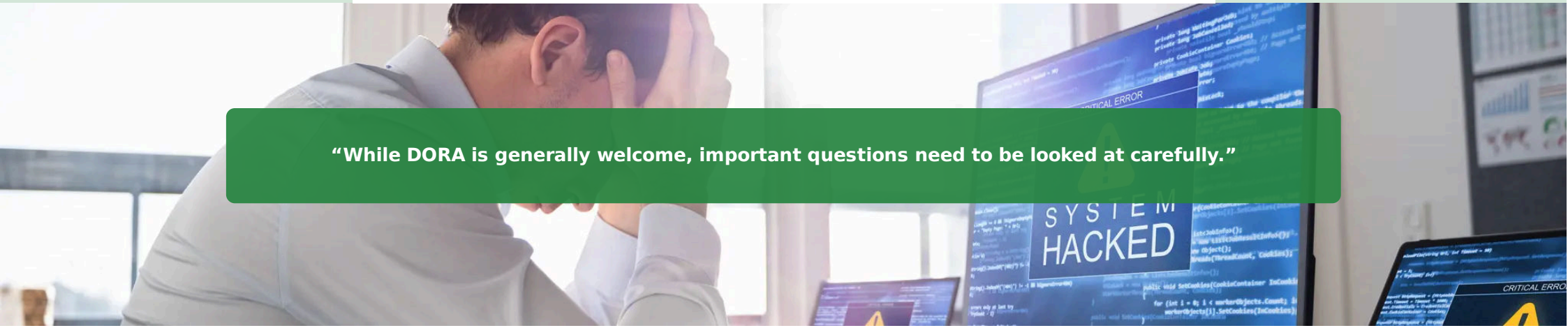
The Spanish insurance industry has welcomed DORA, as it represents a clarification of an area that previously lacked definition. The approval of an EU directive concerning measures for a high common level of security of network and information systems, generally known as the NIS1 Directive, represented an important step towards the harmonisation of technological risk management in Europe. However, this directive's objective was not to include all sectors, but rather to focus on critical infrastructure. Nor was it a regulation specifically designed for the financial industry, and the decision whether to include insurers was left to member states.

In Spain, the insurance industry was defined as a sector in NIS1, although when it came to implementing the regulation the undertakings affected by this definition were not specified. Another concern with NIS1 was that it did not provide for adequate levels of harmonisation, allowing significant room for member states to define their own prevention schemes.

DORA brings precision

Corporations needed a more precise regulation, and one that could also work as a unique reference point. This is the function that the DORA regulation fulfills. It has been provided with *lex specialis*[1] status, which is clearly stated in clause 28 of the revised NIS (known as the NIS2 Directive and published on the same day as DORA) and DORA article 2.2, among other points of reference. DORA foresees that, two years after its publication, when the financial undertakings have fully deployed its provisions, the European financial sector should be able to declare that it is addressing the problems of cybersecurity in its systems and technological assets and those of its suppliers; everything based on uniform and harmonised governing principles.

Inevitably, as DORA aims to fully encompass the management of the technological risk profile of insurance companies, a number of aspects will require discussion and evaluation, part of which will take place during the Level 2 implementation process by the European supervisory authorities (ESAs). For the insurance sector, a very important element is the fact that that the drafting of Level 2 measures will be based on the work already undertaken by the European Insurance and Occupational Pensions Authority (EIOPA) in its “Guidelines on information and communication technology security and governance”. This allows one to predict that the final implementation of DORA Level 2 will respect the efforts that organisations have already made to align themselves to a harmonised framework for the management of cybersecurity. This is the case of the Spanish industry, which has followed the guidelines since their adoption at national level in June 2021.



“While DORA is generally welcome, important questions need to be looked at carefully.”

Outstanding questions

While DORA is generally welcome, important questions need to be looked at carefully.

Firstly, there is a need to define and clarify the guiding principles in relation to supplier policy. This refers to third parties who assume critical or significant functions, especially where those suppliers' services are cloud-based. There are some important concerns in this field that are well known to Spanish insurers, since in this area DORA builds on EIOPA's "Guidelines on outsourcing to cloud services providers", which have been applied by the Spanish supervisor since July 2020.

A particular concern is that, in practice, complying with some of DORA's requirements, will be challenging. For instance, DORA states that insurers should include a series of clauses in their contracts with suppliers guaranteeing rights of inspection and auditing. Such provisions are difficult to enforce, especially with certain suppliers who already have well-established market positions; this "dominant position" is implicitly recognised by DORA itself through the definition it contains of a code of reinforced vigilance for suppliers of a systemic nature. In general, the process for certifying supplier cybersecurity where it relates to insurers, particularly in the aforementioned cases, involves grey areas that, in general, could be significantly clarified with the introduction of standard clauses.

Another important question is the rules for reporting cyber incidents. The initial DORA proposal by the Commission included deadlines for submitting three related reports (initial notification, intermediate and final) on a cyber incident, with relatively strict timeframes, particularly for the initial notification. The difficulty in defining these has resulted in DORA ultimately removing the reference to deadlines, with a request to the ESAs to define these at Level 2 — one of the key issues to be looked at at that level. On this issue, the Spanish insurance industry believes that the reporting periods should be in line with those that already exist; for example, those related to data protection authorities.

Adaptation challenge

Overall, it is clear that DORA presents an important and intensive adaptation challenge for insurers and one that, furthermore, will be practically universal; only those undertakings outside the parameters of Solvency II have also remained outside the parameters of DORA. Initially, it will be a technical challenge, obviously directly affecting the specific departments and professionals engaged in cybersecurity. But it will also test the governance of the undertaking, other departments such as communications and, indeed, the entire organisation, which will need to share a common philosophy on technological security. In short, there will be two years of exhaustive work in the insurance industry.

1. The *lex specialis* doctrine specifies that if two laws govern the same situation, the specific law overrides the general one