EBF_045995

3 February 2023

EBF key considerations following the publication of the Cyber Resilience Act (CRA) proposal

Following the publication by the European Commission of the proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements, i.e. the Cyber Resilience Act (CRA), the European Banking Federation (EBF) hereby presents some key considerations of the European banking sector on the published text, in addition to the views on the CRA that the EBF shared with the EC during the consultation period.[1]

The EBF acknowledges that **rules on digital products would contribute to achieving higher cybersecurity levels** throughout the entire supply chain. Users of such products, both consumers and business -including banks- would **benefit from minimum requirements that would apply to vendors** of those products.

However, the EBF is of the view that the **financial sector should be excluded from the scope** of the CRA proposal, as the recently adopted DORA Regulation provides an extensive cybersecurity and digital operational resilience framework for banks which is equivalent -if not more detailed and comprehensive- to the one introduced by the CRA. It is therefore crucial that **DORA should function as *lex specialis* to the CRA** and this should be explicitly mentioned in the proposal's text, in order to avoid confusion, duplications and overlaps in the rules and requirements on the EU level.

➢ DORA includes cybersecurity requirements that extensively cover the financial sector and should be considered as *lex specialis* vis-à-vis the CRA

The core element of the banks' relationship with their customers is trust, and when it comes to the provision of digital services, trust is inextricably connected with cybersecurity and resilience. Banks have for decades applied a risk-based approach for all phases of life cycle management. Vulnerability management is a core activity in ensuring detect and response measures for banks. Testing of products and services, as well as testing of continuity plans to ensure business towards bank customers constitute basic risk management activities.

The recently adopted Digital Operational Resilience Act (DORA) [2] sets requirements on risk management activities, as well as specific requirements for the areas of incident management and reporting, testing and third-party management which are all equivalent to requirements in the CRA or even more specific. This is particularly true with regard to incident reporting. DORA already includes reporting requirements, making an important step towards incident reporting harmonization on the need of which the sector has been advocating for years[3]. **Any additional requirements for banks to report under the CRA will jeopardize the effort towards harmonizing the cyber incident reporting landscape on the EU level, and should be avoided**.

[1] EBF views on the EC initiative to propose a Cyber Resilience Act (EBF_045752)

[2] 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

[3] See EBF position on Cyber incident reporting

DORA makes no distinction of systems, applications or infrastructure for internal use or for customers, exactly because such a distinction cannot be made in practice. It should be stressed that DORA does not only regulate how banks manage ICT risks in their internal functioning. Recitals 6, 11 and 26 in DORA mention consumer protection aspects in different ways, demonstrating that the secure and resilient internal functioning of financial firms is not the sole objective of DORA. The set-up needs to be extremely secure to ensure that the bank does not expose data or their internal environment. Otherwise, the bank's entire existence could be jeopardised, as a bank that doesn't keep customers' data and transactions safe would not survive in the market. Therefore, any claims that DORA does not require banks to develop and operate secure digital services to its customers and that this instead should be regulated through the CRA seem unfounded.

Moreover, software and services on the internet provided by banks are not being placed on the market for consumers to buy, but they are rather typically provided to existing customers as part of a service offering. Such products could often, if not always, be classified as "thin clients" with a Graphic User Interface (GUI) that does not contain any business logic. Through the GUI -implemented through a web interface or an app interface- the bank customer is able to use the digital services of the bank. **The "digital products" banks provide to customers are not stand-alone systems, placed separately on the market, but rather a means of performing financial services**. In other words, they are an interface to the bank and as such they are entirely governed under the bank's own ICT risk management framework as prescribed by DORA. Subjecting such products to the CRA would thus not result in any uplift to the management of the cybersecurity risk associated with the product, and would instead bring unnecessary and confusing duplication.

DORA has been welcomed by the financial sector due to the fact that it represents a consolidated regulation for the entire sector, replacing equivalent requirements emanating from different pieces of existing EU legislation. **Subjecting banks to the CRA provisions on top of DORA would entail duplications and overlaps in rules, the avoidance of which was the very rationale of the introduction of DORA.** This would mean taking a large step back in terms of harmonizing cybersecurity requirements in the sector, before the new DORA framework even becomes applicable. It is worth noting that fragmented regulations result not only in costs, but in governance complexity that makes it more difficult to manage risk.

Moreover, as certain types of firms are more or less indirectly excluded based on other regulations that are deemed to be *lex specialis* to the CRA, it is clear that banks belong to the same category as do providers of medical devices for human use, civil aviation safety and motor vehicles, considering that banks too are already obliged to provide secure services to ensure the protection of customers' data.

A firm that is developing products under the scope of the Regulation on Medical Devices Regulation (MDR)[4] could also in theory be developing digital products in a totally different industry sector and be subject to the CRA there. From a brief review of the MDR -being *lex specialis* to the CRA- in order to assess this Regulation's level of detail of the security requirements, while the MDR is an extensive piece of legislation (175 pages with 123 Articles and 17 Annexes), its stipulations on software security requirements are only briefly

[4] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC

mentioned on a very high level in a few instances[5]. Should this level of detail of security requirements be sufficient for including a *lex specialis* provision for medical devices in the CRA, it would be expected that this should also be the case for DORA, an extensive and comprehensive legislative framework dedicated exclusively to cybersecurity and resilience in the banking sector. **Therefore the EBF suggests that DORA be included and explicitly mentioned as *lex specialis* legislation in the CRA proposal**.

In the CRA Explanatory memorandum the following is stated:

"1. *Context of the proposal, Reasons for and objectives of the proposal:*

(…) There are numerous examples of noteworthy cyberattacks resulting from suboptimal product security, such as the WannaCry ransomware worm, which exploited a Windows vulnerability that affected 200 000 computers across 150 countries in 2017 and caused a damage amounting to billions of USD; the Kaseya VSA supply chain attack, which used Kaseya's network administration software to attack over 1000 companies and forcing a supermarket chain to close all its 500 shops across Sweden; or the many incidents in which banking applications are hacked to steal money from unsuspecting consumers.(…)"

For the EBF the background to the claim that "banking applications are hacked to steal money from unsuspecting consumers" is not clear, as this is certainly not the case in practice. In the European banking market and in the vast majority of successful attacks, it is the customer, not the banking application, that is targeted by the fraudsters, luring the customer into giving up credentials or authorising payments to fraudsters etc. (i.e. by making use of social engineering practices). This is fundamentally different from a technical breach of a banking application that would allow an attacker to extract funds from a customer account. It is also the case that the CRA's requirements would not address the risk of fraud, for which there is an extensive amount of law enforcement and sector-led activity ongoing to tackle.

[5] Annex I, Chapter II:
17.2 For devices that incorporate software or for software that are devices in themselves, the software shall be developed and manufactured in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security, verification and validation.
17.3. Software referred to in this Section that is intended to be used in combination with mobile computing platforms shall be designed and manufactured taking into account the specific features of the mobile platform (e.g. size and contrast ratio of the screen) and the external factors related to their use (varying environment as regards level of light or noise).
17.4. Manufacturers shall set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended."

About EBF

The European Banking Federation is the voice of the European banking sector, bringing together national banking associations from across Europe. The federation is committed to a thriving European economy that is underpinned by a stable, secure, and inclusive financial ecosystem, and to a flourishing society where financing is available to fund the dreams of citizens, businesses and innovators everywhere.

www.ebf.eu @EBFeu

For more information contact:

Alexandra Maniati
Senior Director, Innovation & Cybersecurity
a.maniati@ebf.eu
+32 478 90 13 01

Dimos Karalis
Policy Adviser, Cybersecurity & Innovation
d.karalis@ebf.eu
+32 485 52 39 16