Latest developments in cyber security: Managing cyber risks and the outlook for DORA

KPMG analysis shows how banks can improve and get better prepared for future crisis exercises or real incidents

3 May 2024

It is demanding times for cyber risks: geopolitical risks manifest in growing risks of cyberattacks, recent global IT incidents and a general concern due to computing powers that could eventually impair encryptions. In response to growing cyber threats, the European Central Bank (ECB) launched its first Cyber Resilience Stress Test (CRST) of banks it supervises in January 2024. Banks faced a list of 395 questions, with responses to this first phase of the test due by the end of February. In the subsequent assessment phase, the ECB gave banks just two days to answer follow-up questions. In addition, 28 institutions facing an additional IT recovery test underwent on-site quality assurance reviews (OSQAR) in March and April 2024.

These supervisory activities were expected to have finished by the end of April – the outputs of which the ECB will assess to gauge how effectively European banking is protected against cyberattacks. The results will be incorporated into banks' Supervisory Review and Evaluation Process (SREP) assessments.

What have we learned so far? KPMG analysis shows how banks can improve and get better prepared for future crisis exercises or real incidents.

Complex attack scenario, demanding test, high costs

The CSRT presented banks with several major challenges. The first was the complex CRST scenario itself, in which an unknown attacker accessed and encrypted the database of the main core banking system. This scenario was not known until a week before the start of the test, so no specific preparation or preliminary work was possible.

Another challenging task for banks was to quantify the economic impact of the attack scenario. This involved determining both direct and indirect losses, as well as assessing the impact on banks' key economic functions (such as lending, deposit taking or payments processing).

As generally expected, the CRST schedule was also very demanding. For a typical bank, answering the 395 questions and collecting evidence required hundreds of hours of work, in addition to intensive cross-departmental coordination and extensive collaboration with the third-party providers who often operate core banking systems.

Lessons learnt over recent months and areas for improvement

1. **Deviation between defined and actual recovery time**: Our market insights seem to indicate that some banks face differences between the availability requirements in the business impact analysis and the recovery times that are practically achievable. Strong dependence on service providers: The extensive use of outsourced functions requires greater cooperation with service providers and joint tests of resilience. From our perspective, many banks in Europe are at least partially reliant on service providers to operate their core business and underlying infrastructure.
2. **A lack of end-to-end testing:** Most banks test processes and systems regularly. End-to-end testing of both technical and banking processes using serious and realistic scenarios is a key driver of the ability to successfully deal with cyber-attacks.
3. **Need to improve centralized inventories of processes and assets**: Based on our insights, despite investment, some banks still lack a comprehensive centralized inventory of business processes and associated IT assets that provide quick information on impacts in the event of emergency. A multidisciplinary approach is required to determine economic impact holistically.
4. **Maturity of requirements is good – implementation needs improvement**: Our experience shows that the quality and maturity level of the resilience policies and documents, even when rated highly by the banks, can only be assessed in the context of a test.

Preparing for future tests and leveraging synergies with the Digital Operational Resilience Act (DORA)

Based on banks' experience of the CRST, we believe the following steps will be key to helping institutions to prepare for future crisis simulations by the ECB or national supervisory authorities:

- Perform end-to-end tabletop testing to explore possible scenarios and compare the quality of response and recovery against regulatory expectations and industry best practices.
- Develop scenario-based methods to determine economic impact, and to identify the most important banking systems based on a clearly documented system and process landscape.
- Clarify responsibilities along the entire process chain to help ensure smooth collaboration – define roles and responsibilities for business units, third-party vendors and key support functions.
- Manage information and communications technology (ICT) service providers with defined responsibilities and requirements during the collaboration, including their active participation in tests.

Although DORA will not be fully applicable until January 2025, the CRST provides an insight into supervisors’ likely expectations for practical implementation. Meeting the requirements of DORA will not only address some issues identified by the CRST. Experience of the CRST could also be relevant to DORA implementation projects – including DORA’s requirements for ICT risk management around response and recovery, as well as for incident reporting and communication.

The ECB will enforce necessary improvements via the SREP process, but other authorities such as the European Insurance and Occupational Pensions Authority (EIOPA) and Federal Financial Supervisory Authority (BaFin) are also planning exercises. From January 2025 onwards, DORA will provide the underlying cyber resilience framework. In our view, the steps recommended above could help banks both in implementing DORA and in preparing for future crisis exercises.