WHAT DORA MEANS FOR MAINFRAME TEAMS IN AND AROUND EMEA

Over the past month, I have had the opportunity to discuss the European Union's Digital Operational Resilience Act (DORA) with the mainframe teams of 14 of the largest financial institutions in EMEA and the UK. Here are my key takeaways from those conversations:

There is general agreement that for mainframe teams, the DORA requirements are different than previous regulatory guidelines:

- Penalties that include one percent of annual revenues and criminal liability are getting the attention of executives and board members
- As DORA calls out "all critical infrastructure," the spotlight is shining on mainframe infrastructure like never before
- DORA requires an independent penetration test/security assessment of all critical infrastructure. Only some mainframe teams are heeding that advice.
- The biggest change in requirements when comparing DORA to other regulations is the ability to prove that your financial institution can recover from a cyberattack—which is much different than a disaster recovery.
- At least half of the financial institutions have already been engaged in European Central Bank (ECB) stress tests to evaluate their organizational ability to recover from a cyberattack.
- There is considerable concern over the "interpretation" of the technical/business/resilience requirements for DORA, even after the January final report was published.

- Most financial institutions are already in the process of implementing immutable backup solutions for their mainframe environments—a key step toward cyberattack resilience.
- For those organizations implementing immutable backups, nearly all recognize the challenge of determining which immutable backup is appropriate to use for their recovery.
- Many financial institutions recognize that recovering from an immutable backup poses a critical issue around data loss, potentially losing hours of financial transactions.
- Most financial institutions have created DORA-specific working groups to guide their IT teams on appropriate measures to take, but even those teams have difficulties translating regulation requirements into IT guidelines.

Bottom line: DORA presents new challenges for mainframe teams, not only because the cyberattack scenario is new, but because the ECB is actively engaging with financial institutions that do business in Europe to prove that they comply with the new objectives.

Learn more about how DORA guidelines help achieve operational resilience in the podcast, "Mainframe Operational Resilience: DORA and Beyond."