Financial institutions are expected to embrace technological changes. A lot of attention is directed to evolution in financial services and the competition to existing institutions from financial technology participants. The so-called FinTech companies are presented as competitors to existing actors.

To improve banks’ profitability, Andrea Enria, Chair of the Supervisory Board of the ECB, said recently, “Banks need to focus on areas where they can improve, namely increasing cost efficiency, investing in technologies and designing and implementing better strategies.” However, the increased exposure of financial services to technology and the deep interconnectivity of systems have attracted attention to risks linked to the use of technology. Within IT Risk, cyber risk is often perceived as a technological risk emanating from external threats. Those external threats are often grouped under cyber security attacks. Many instances have been reported in 2019 alone. From cyber-attacks on ATMs, to data thefts or fraudulent transfer requests, cyber criminals show an impressive inventiveness.

Occurrences of events that have been classified as cyber risk over the past few years include both external and internal events. In fact, some of the most important disruptions were not external attacks. Many banks experienced IT issues in the past two years that were visible externally but not initiated by external attacks. In 2018 TSB was hit by a severe incident that originated from a routine maintenance that kept millions of bank customers from accessing their accounts for several weeks. In late October 2019, following investigation into the TSB issue, the United Kingdom Parliament published a statement on IT failures (actually, ICT to include Communication) in the Financial Services Sector. Some of the main points were:

- While considering that completely uninterrupted access to banking services is not achievable and that some IT failures are inevitable, the current level of financial services IT failures was unacceptable, especially when customers are expected to use digital services for day-to-day banking activities.
- Regulators were expected to act through two main directions: 1) Ensuring that the Senior Management Regime would also apply to IT failures, and to 2) Consider extension of the Senior Management Regime to Financial Market Infrastructure firms.

---

2 / List of cyber incidents: https://www.carnegieendowment.org/specialprojects/protectingfinancialstability/timeline
managing IT risk

A quick review of traditional bank responses to risks shows that their options are limited. Accepting risks linked to technology is clearly not acceptable given recent events, nor is trying to avoid the use of technology, as it cannot be avoided anymore. The developing market of cyber insurance does have some potential but, with current data available, insurance contracts are clearly limited in the exposure that can potentially be transferred. So, attention needs to be given to mitigation.

All these considerations are important, but attention is shifting to a more complete view of operational resilience. The 2018 discussion paper issued jointly by the Bank of England, FCA and PRA was aimed to promote dialogue and improve resilience.

The Bank of England has defined Operational Resilience as “the ability of firms and the financial system as a whole to absorb and adapt to shocks, rather than contribute to them.”

The discussion paper points to the fact that operational resilience needs to encompass all elements of operations (as does Gartner in its glossary). ICT systems are one obvious element, but so are people involved in the delivery of the process, any supplier involved (e.g. Data and services), premises, responses to abnormal operating conditions, and all dependencies with other processes. Dependencies must be identified to ensure that the full scope is covered. Painful experiences have shown firms and their clients that a missing link in a chain can render a partial recovery useless, if the process cannot be executed.

setting resilience priorities

The increasing complexity of processes and systems often results in too many processes and systems in a firm being classified with the highest priority for recovery. This makes recovery of every element extremely difficult in the appointed timeframe. In a constrained environment, choices must be made to ensure that some business processes are restored fully rather than trying to restore too many and risk having some processes interrupted for lack of one critical link. These choices must be documented to ensure that priorities are clear in case of a crisis. The resilient organisation must be defined to ensure that selected priorities can be executed and that all possible issues are identified.

With responsibilities expected up to Board level, attention to operational resilience is likely to increase for financial firms and market infrastructure.


5 / Definition: https://www.bankofengland.co.uk/financial-stability/financial-sector-continuity

Pierre-Yves Maurois has a strong risk management background. He has more than 20 years of consulting experience covering banks, asset management and insurance in Europe. He has seen widely different implementation of risk management structure in particular in the light of different crises and regulatory changes. His experience ranges from transactions activities and portfolio management to structural issues on data management, organization, and risk culture.

Pierre-Yves participated in the creation of the PRMIA Paris chapter in 2002 where he is still co-regional director. He is also co-chairing the Global Council of Regional Director and is a former Global Board Member.