ESRB
European Systemic Risk Board
European System of Financial Supervision

Crisis Preparedness for Europe: Financial and Payments Systems Facing New Risks

Are we prepared for a systemic cyber crisis?

25/08/2025

Francesco Mazzaferro
Head of the ESRB Secretariat

No truly systemic cyber incident to date

However, near miss events in the past

- 2016: Central bank of Bangladesh's SWIFT terminal hacked in 2016 (financial theft)
- 2017: Equifax data breach (data breach/theft)
- 2018: Cosmos Bank's ATM server hacked (financial theft)
- 2018: Banco de Mexico's domestic interbank payment system incident (financial theft)
- 2023: Ransomware attack on ION Trading whose services include automated matching of trade/clearing of ETD
- 2023: Ransomware attack on ICBC FS
- 2024: Ransomware attack on securities lending platform and post-trade services provider Equilend

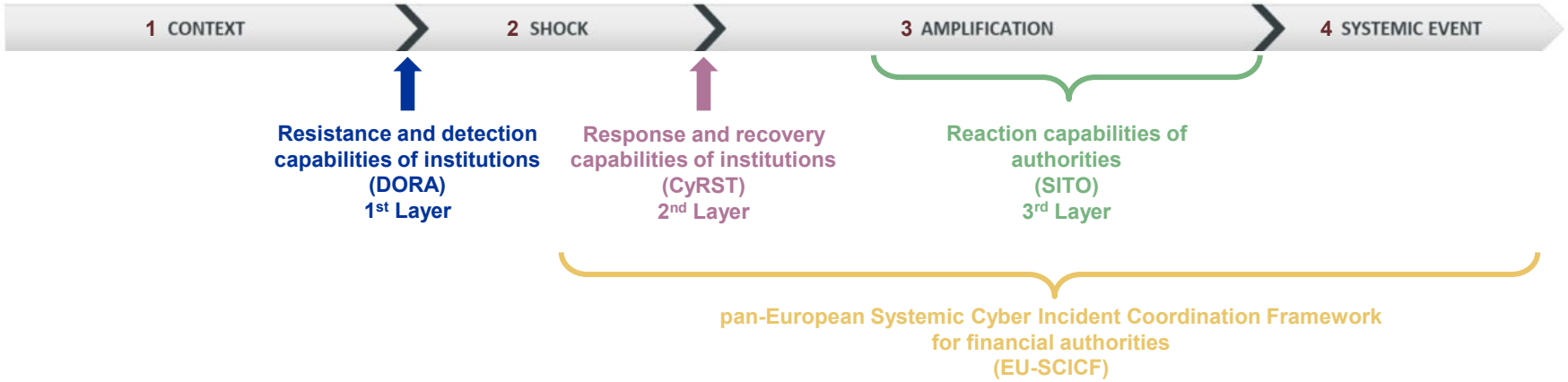
- 2024: CrowdStrike – failed upgrade, not cyber, but warning signal

Systemicness in cyber

"Systemic risk" means a risk of disruption in the financial system with the potential to have serious negative consequences for the internal market and the real economy.

- Magnitude of financial losses, uncertainty and the loss of confidence.
- Both the size and the distribution of the initial shock matter.
- Chain of propagation of contagion to other sectors and second-round effects.
- Not every cyber incident represents a threat to financial stability.
- However, there is no cyber incident, which per se, will never turn systemic.
- Compared to traditional financial and liquidity crises, the underlying shock "is a different animal".

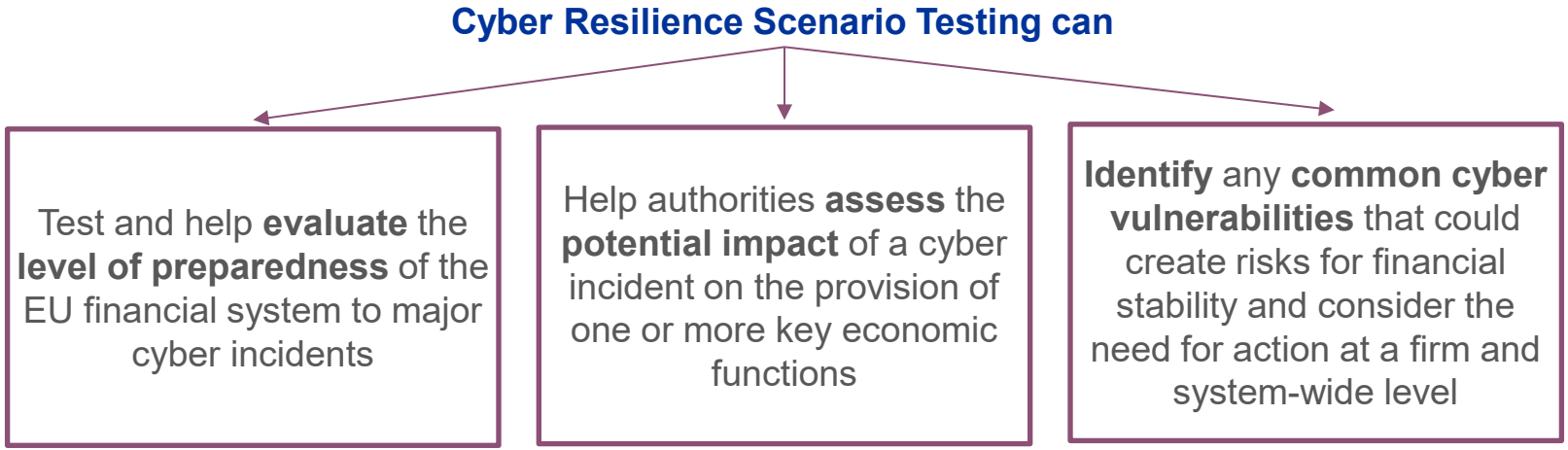
The ESRB's simplified systemic cyber model & layers of resilience



Note: See appendix for detailed model.

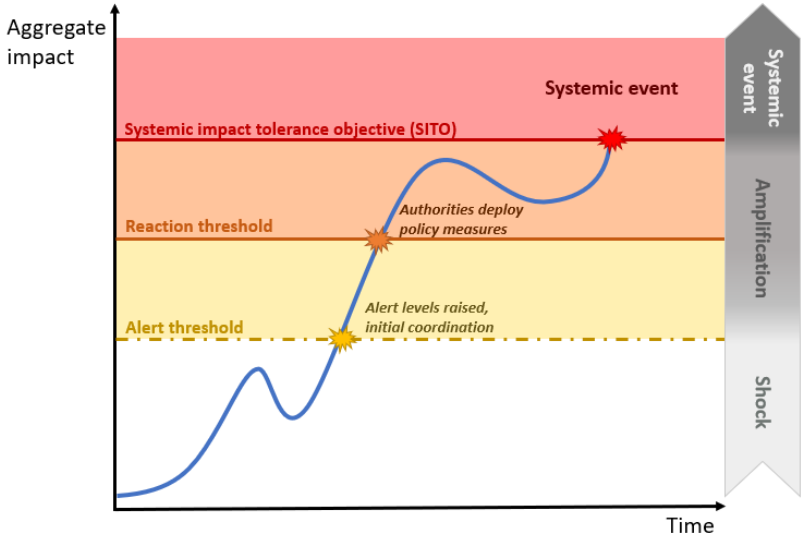
Cyber Resilience Scenario Testing (CyRST) – 2nd layer of defence

CyRST is a tool to assess the capacity of the financial system to support the continuity of key economic functions (KEF) by responding to and recovering from, in a timely and efficient manner, a severe but plausible cyber incident that causes a significant disruption and could affect financial stability.



Systemic Impact Tolerance Objectives (SITO) – 3rd layer of defence

Systemic Impact Tolerance Objectives (SITOs) define the point beyond the impact tolerance of the financial system is deemed to be exhausted.

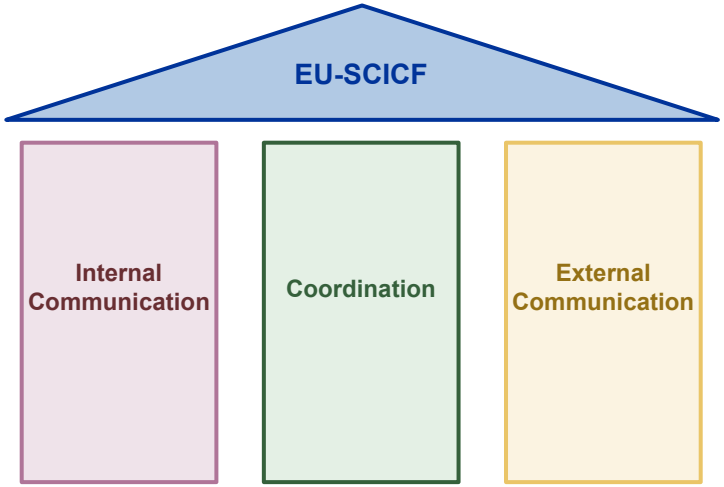


SITOs can assist authorities in several ways:

- **Assessing** when a cyber incident might pose a risk to financial stability.
- **Identifying** an 'intervention ladder' for response and recovery measures.
- **Anchoring** expectations on the maximum acceptable level of disruption to key economic functions to financial entities.

A pan-European systemic cyber incident coordination framework

The EU-SCICF builds on DORA to gradually enable an effective Union-level coordinated response in the event of a major cross-border ICT related incident or related threat.

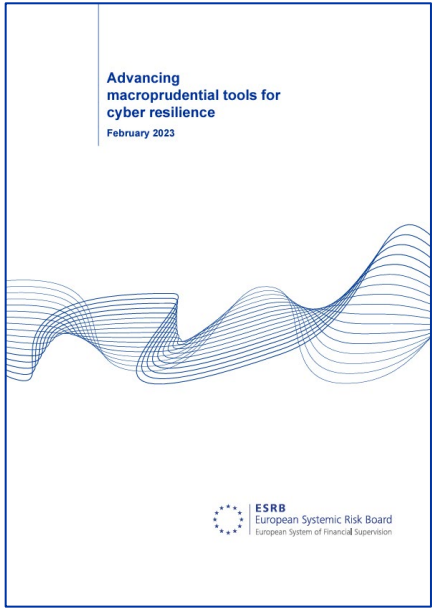


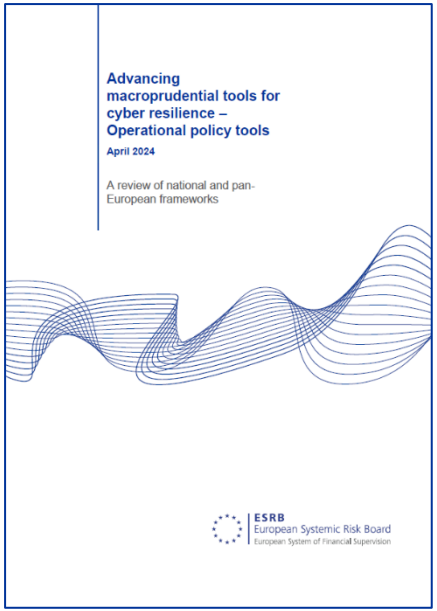
The EU-SCICF can

- **Reduce complexity** in communication and coordination between financial authorities.
- **Reduce uncertainty** by aligning authorities' actions
- **Boost confidence** in the financial system by reducing probability of a coordination failure.
- **Increase** financial authorities' **level of preparedness** to manage financial stability consequences of a systemic cyber incident.

→ Cyber equivalents of capital buffers are preparedness and resilience

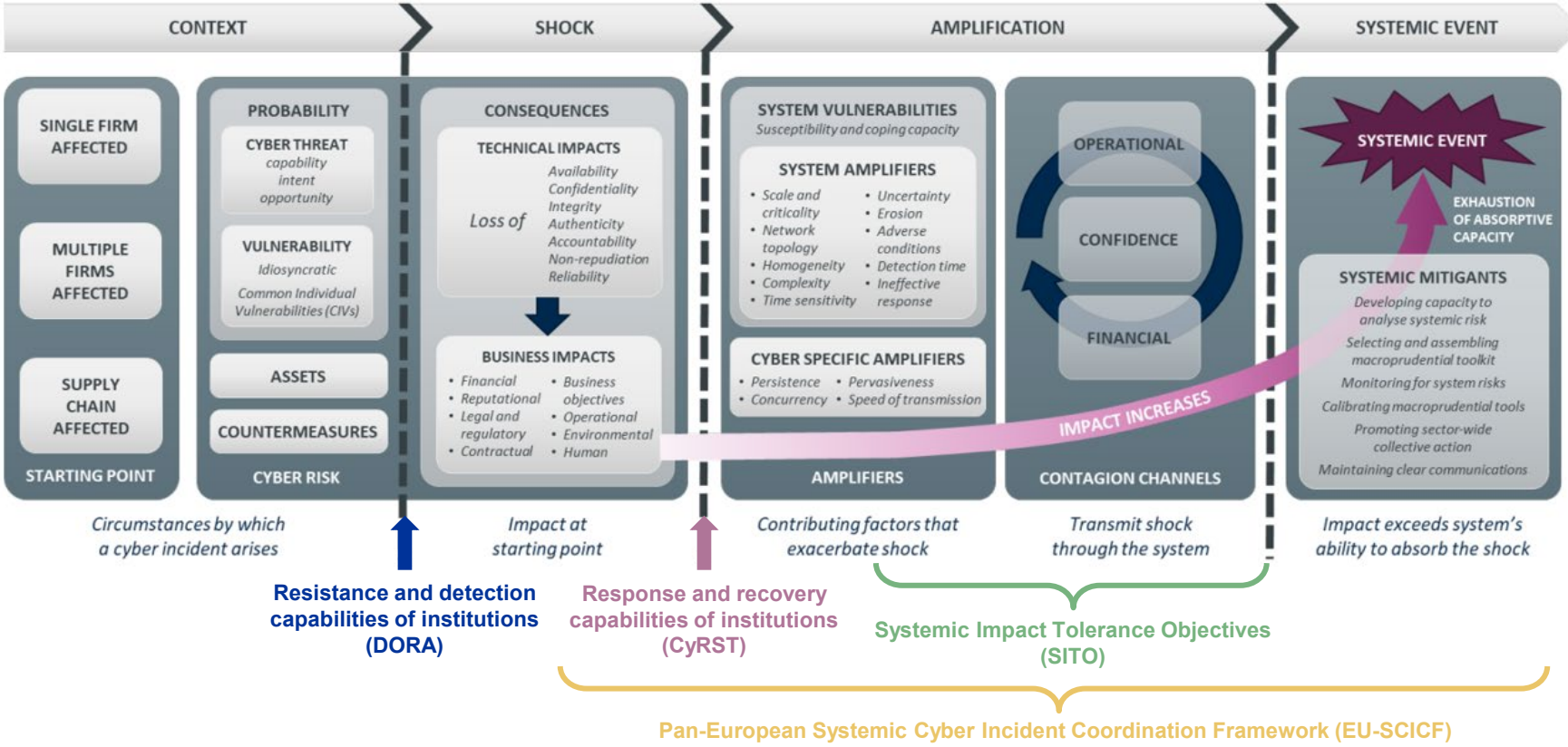
What the ESRB has been doing to advance cyber resilience





Annex

The ESRB's systemic cyber model



Source: ESRB (2020, 2022, 2024)