ESRB
European Systemic Risk Board
European System of Financial Supervision

Systemic Cyber Risk

What makes a cyber incident systemic?

30/10/2024

Francesco Mazzaferro
Head of the ESRB Secretariat

No truly systemic cyber incidents to date

However, near miss events in the past

- 2016: CB 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**

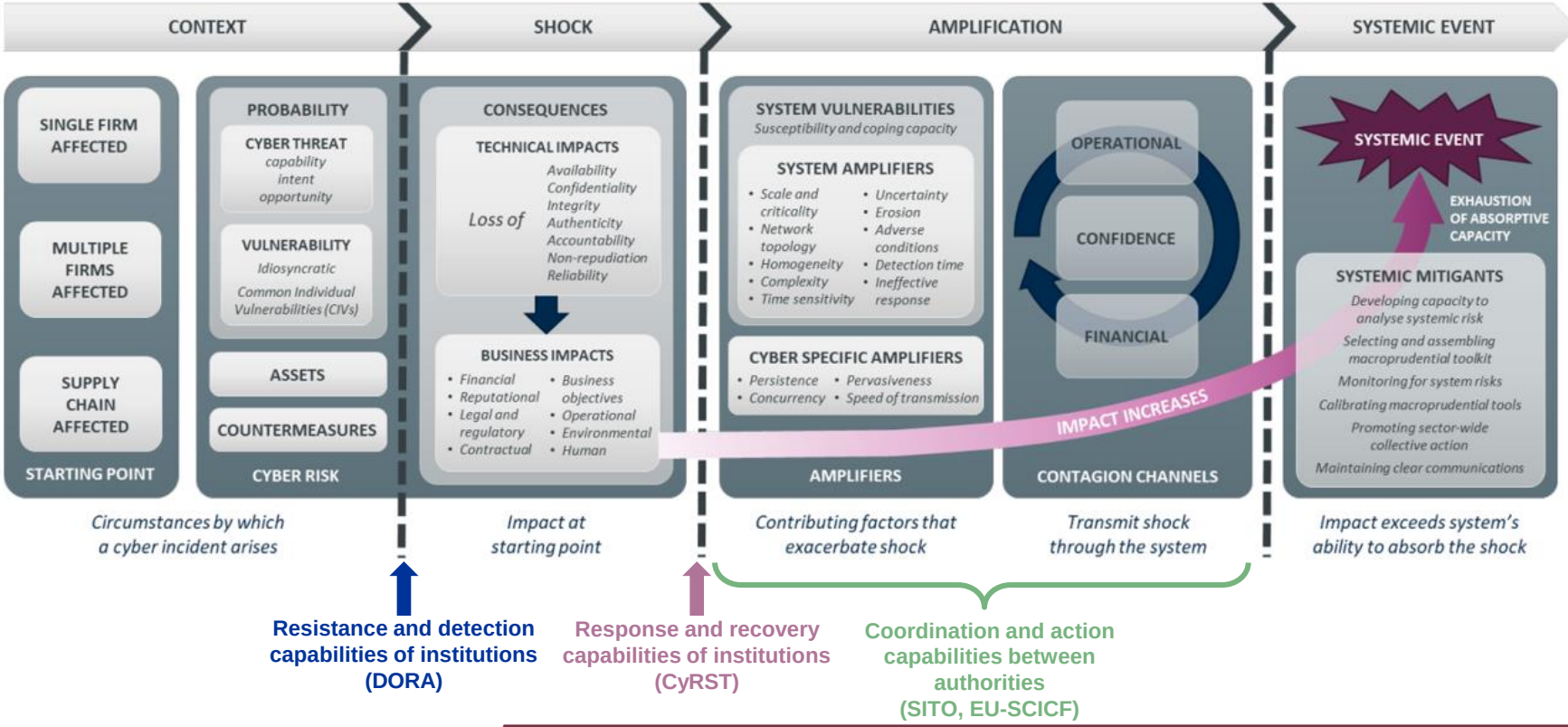
- 2024: CrowdStrike failed upgrade – not cyber, but warning signal

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 the 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.

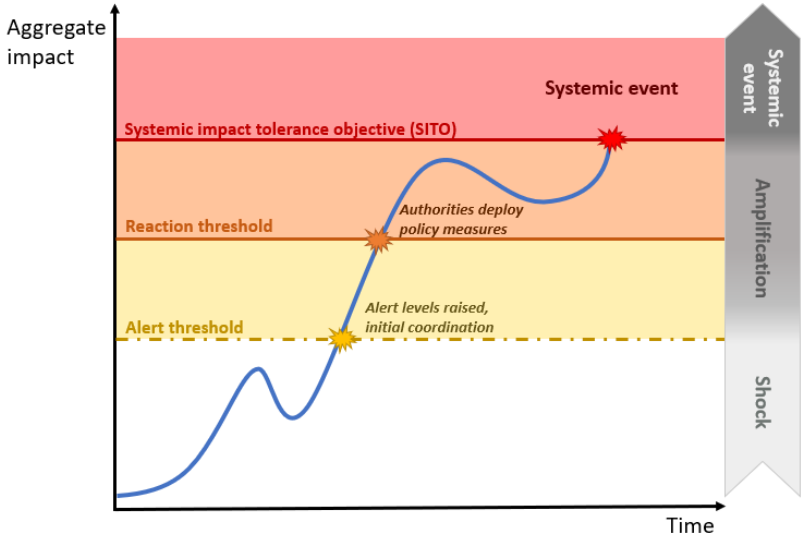
Systemic cyber risk model



Source: ESRB (2020, 2022, 2024)

Systemic Impact Tolerance Objectives (SITO)

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.
- As a yardstick against which authorities would assess their own response and recovery capabilities.
- Identifying an ‘intervention ladder’ for response and recovery measures.
- Anchoring expectation on the maximum acceptable level of disruption to key economic functions to financial entities.