



# Brief recap of the paper

#### **Research question**

How does a multiday cyberattack on a shared technology service provider (TSP) impact the banking sector ?

#### Approach and methods

Compile a confidential dataset to quantify the impact of operational disruptions on banks including in particular on payments and liquidity.

#### **Key findings**

The attack resulted in the TSP going offline, which disrupted customers ability to send payments to the bank.

Banks and the TSP managed to reduce the impact of the disruptions including for other banks by relying on alternative payment methods in line with their business continuity plans. This included sending payments outside normal business hours.

Nevertheless, other banks experienced a material shortfall of liquidity, causing them to borrow, including from the Federal Reserve, or tap their reserves.



## Overall assessment

## Main strengths

- Unique paper which considers in detail the wider impact of an actual cyber event.
- Well written, well motivated and clearly relevant in terms of understanding contagion channels and hence what private and public sector stakeholders one should consider when look at the operational risk aspects related to cyber attacks on third parties.
- From a digital transformation perspective this is highly relevant.
- Clear results the paper includes many nice and convincing Charts.

### Scope for further work

- Draw clearer links to and implications for (existing) theoretical work?
- Consider the differences and similarities in terms of impact between TSP cyber attacks/breakdowns vs general infrastructure breakdowns banks "home-made" incidents?
- Compare with similar cases from other jurisdictions ...

PRESENTATION TITLE



# Implications for banks and wider financial sector

- Important to maintain inhouse hygiene and controls vis-à-vis third-party providers and partners
- Need consider the role of different TSPs
  - Payment services
  - Clearing and settlement
  - Cloud storage services incl. computing power
  - > IT security
  - General infrastructure
- Business continuity & recovery capacity matters
- Know your digital eco-system internal and external
- Client reliance on TSPs also important aspect
- Understand the potential liquidity implications of cyber attacks
- Financial market implications directly and indirectly



## Implications for central banks, regulators and supervisors

- Business continuity & recovery capacity matters
- Perimeter ...
  - .. large digital service providers are potential sources of systemic risk and should be regulated/supervised/monitored – but by whom?
  - Concentration risk matters for TSPs when it comes to financial stability
  - Need to collect information on the network structure similar lesson as seen during the 2008 financial crisis
- We should collect better information on the network structure similar lesson as seen during the 2008 financial crisis
- Cyber attack and operational risk stress tests are likely needed
- Should supervisors and central banks conduct "wargames" in collaboration with cyber-authorities/intelligence agencies?

PRESENTATION TITLE

