Cybersecurity and Financial Stability

Ryan Riordan

Queen's & LMU

∃ >

- Analyzes how cyberattacks can trigger bank runs and impact financial stability
- Examines bank's trade-off between protection (investing in cybersecurity) and resilience (ability to withstand attacks)
- Provides framework for regulators to promote socially optimal cybersecurity investment by banks

- Three periods: t = 0, 1, 2
- Bank raises deposits and invests in risky project and cybersecurity at t = 0
- Uncertainty about project's success and bank's ability to find/patch vulnerabilities
- Depositors choose to roll over or withdraw funds at t = 1 based on public signal
- Payoffs realized at t = 2

• Private vs. Social Incentives for Cybersecurity Investment

- Banks underinvest in cybersecurity relative to socially optimal level
- Do not internalize full social costs of distress and negative spillovers

• Protection vs. Resilience Trade-off

- Banks face trade-off between protection (investing in cybersecurity)
- And resilience (ability to withstand successful attacks)
- Optimal strategy depends on rollover risk and fragility

• Common IT Platforms and Public Good Nature

- With shared IT systems, cybersecurity has public good characteristics
- Misaligned incentives for individual banks to invest optimally
- Necessitates mapping dependencies and setting common standards

- Bank underinvests in cybersecurity due to not internalizing social costs of distress
- Socially optimal cybersecurity depends on threat severity and bank fragility
- When rollover risk is low, bank failure is due to deadweight losses from attack
- When rollover risk is high, inefficient runs can occur after an attack

- Builds on literature analyzing cyber risk and financial stability
 - Duffie and Younger (2019), Eisenbach et al. (2022), Goh et al. (2020)
 - Examines how cyberattacks can trigger inefficient bank runs
- Relates to economics of information security literature
 - Gordon and Loeb (2002), Grossklags et al. (2008), Gatzert and Schubert (2022)
 - Analyzes firms' investment in cybersecurity vs. self-insurance
- Draws from literature on network security and contagion
 - Goyal and Vigier (2014), Dziubinski and Goyal (2013), Bier et al. (2007)
 - Accounts for common IT platforms and interconnections
- Contributes to policy literature on cyber regulation
 - Kashyap and Wetherilt (2019), Adelmann et al. (2020), Fell et al. (2022)
 - Provides analytical framework to evaluate policy tools

- Operational resilience standards to ensure adequate cybersecurity investment
- Red team (simulated attacks) testing to identify vulnerabilities and promote information sharing
- Subsidies to enhance banks' cyber capabilities, funded by lump-sum taxes
- Negligence rules with penalties for inadequate cybersecurity practices

- Knightian uncertainty about vulnerabilities does not change core insights
- Lender of last resort support reduces rollover risk but does not address underinvestment
- Common IT platforms across banks necessitate mapping infrastructure and setting standards
- Regulation of critical technology vendors to ensure minimum cybersecurity standards

- Simplified binary outcome of cyberattack (successful or unsuccessful)
 - Real attacks can have varying degrees of impact and persistence
 - Model does not capture nuances of different attack types
- Static model with fixed deposit base and project scale
 - Does not account for dynamic adjustments by banks
 - Depositors may re-optimize based on observed cybersecurity levels

- Assumption of perfect competition in banking sector
 - Lack of market power may understate private incentives
 - Oligopolistic banks may over-invest in cybersecurity for strategic reasons
- Regulatory interventions treated independently
 - In practice, multiple policies implemented simultaneously
 - Potential interactions and unintended consequences not explored
- Limited empirical validation and calibration
 - Model insights depend critically on parameter values
 - Lack of data on cybersecurity investments, costs, and impacts

- Extend model to account for imperfect information and signaling
- Incorporate richer set of attack types and dynamic adjustments
- Analyze strategic interactions in imperfectly competitive banking
- Study interactions between different regulatory policies
- Empirically estimate key parameters using cybersecurity data
- Apply model to quantify systemic cyber risk using simulations

- Provides analytical framework linking cyberattacks, bank runs, and financial stability
- Highlights importance of regulatory interventions to correct market failures
- Insights robust to extensions like Knightian uncertainty and common IT platforms
- Lays foundation for future research on systemic cyber risk and policy design