When It Rains, It Pours: Cyber Vulnerability and Financial Conditions

by

Thomas Eisenbach Anna Kovner Michael J. Lee

Discussant: Yiming Ma

Columbia Business School

June 18, 2024

Big Picture

- There has been a lof of attention on cyber risk
- And the impact of cyber risk on financial conditions

- This paper:
- Novel perspective that cyber risk does not exist in isolation
- The impact of cyber risk *interacts* with financial conditions
- $\rightarrow$ Understanding the interaction effect is crucial

This Paper

What do the systemic consequences of a cyber attack depend on?

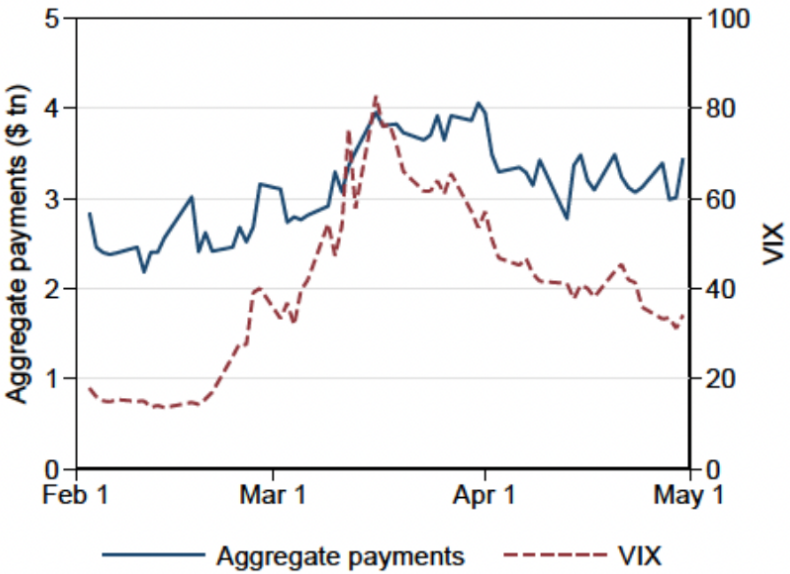
- Context: Fedwire payment system
- Cyber risk/attack: Inability to send payments
- Systemic consequences: when a given institution is exposed to a cyber attack, what is the effect on other institutions and payments lost

This Paper

The systemic consequences of a cyber attack are higher when markets are more volatile

1. Payment needs increases
2. Market concentration increases
3. Risk of coordination failure increases

VIX and Payments

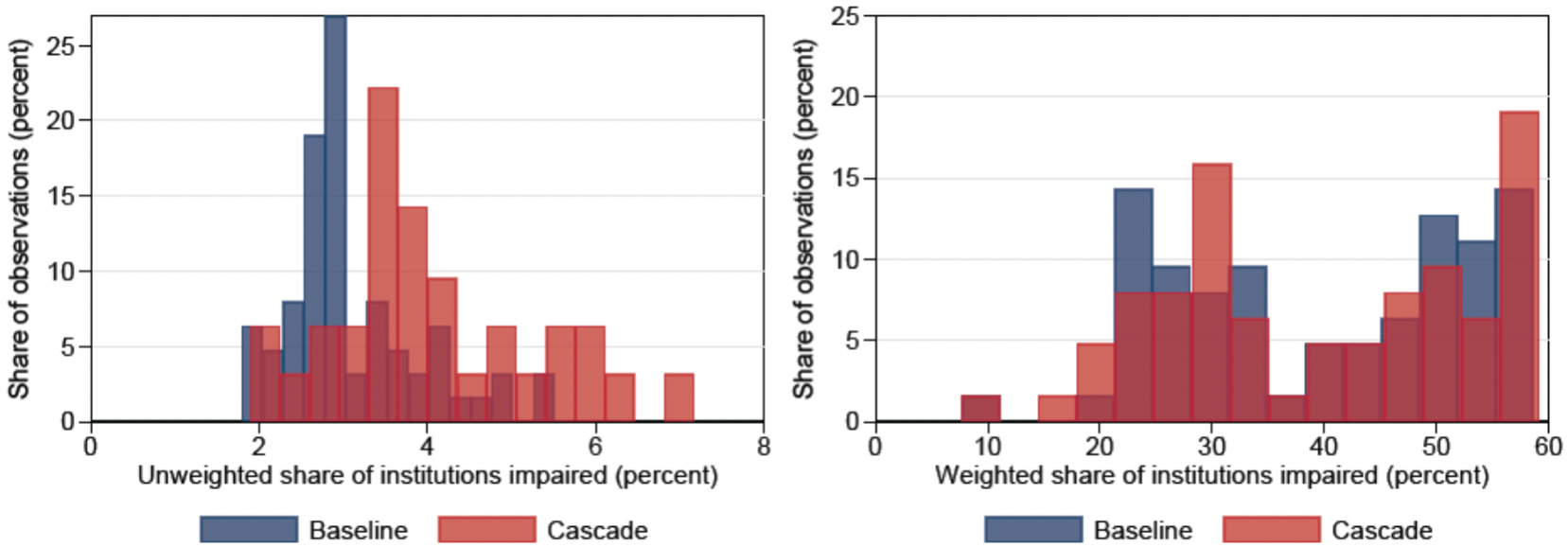


Market Concentration

Overall Comments

- Very important question
- Novel perspective on the interaction between cyber risk and financial conditions
- Plausible results
- Comments
  1. Network structure and cascades
  2. Reserve preservation versus payment facilitation
  3. Relationship between coordination failure and technology

1. Coordination Failure May Not Always Amplify Losses!



- Banks's ability to respond with delaying payments does not necessarily lead to more losses (in terms of reserve-imparied banks)
- $\sim$ coordination failure may not necessarily amplify losses
- Why? What does it depend on ?

1. Effect of Network Structure

- Consider a very simple example
  - Core $Bank_c$ gets attacked, periphery $Bank_p$ may choose to hoard
- Case A: $Bank_{p1} \rightarrow Bank_c$
  - Shock to $Bank_c$ has no effect on $Bank_{p1}$

1. Effect of Network Structure

- Consider a very simple example
  - Core $Bank_c$ gets attacked, periphery $Bank_p$ may choose to hoard
- Case A: $Bank_{p1} \rightarrow Bank_c$
  - Shock to $Bank_c$ has no effect on $Bank_{p1}$
- Case B: $Bank_c \rightarrow Bank_{p2}$
  - $Bank_{p2}$ hoarding has no effect

1. Effect of Network Structure

- Consider a very simple example
  - Core $Bank_c$ gets attacked, periphery $Bank_p$ may choose to hoard
- Case A: $Bank_{p1} \rightarrow Bank_c$
  - Shock to $Bank_c$ has no effect on $Bank_{p1}$
- Case B: $Bank_c \rightarrow Bank_{p2}$
  - $Bank_{p2}$ hoarding has no effect
- Case C: $Bank_c \rightarrow Bank_{p2} \rightarrow Bank_{p3}$
  - $Bank_{p2}$ hoarding has an effect: benefits $Bank_{p2}$ and hurts $Bank_{p3}$

1. Effect of Network Structure

- Consider a very simple example
  - Core $Bank_c$ gets attacked, periphery $Bank_p$ may choose to hoard
- Case A: $Bank_{p1} \rightarrow Bank_c$
  - Shock to $Bank_c$ has no effect on $Bank_{p1}$
- Case B: $Bank_c \rightarrow Bank_{p2}$
  - $Bank_{p2}$ hoarding has no effect
- Case C: $Bank_c \rightarrow Bank_{p2} \rightarrow Bank_{p3}$
  - $Bank_{p2}$ hoarding has an effect: benefits $Bank_{p2}$ and hurts $Bank_{p3}$
- Case D: Only gross no net payments between $Bank_c$, and $Bank_{p2}$
  - $Bank_{p2}$ hoarding helps to avoid reserve impairment
- $\rightarrow$ **Consider how the impact of coordination failure depends on the network structure, esp. for payment receivers**

2. Reserve Preservation versus Payment Facilitation

- The number of reserve-impaired banks and the amount of payments lost are both used as measures of systemic consequences
- However, these measures may go against each other
  - Case D: Only gross payments between $Bank_c$, and $Bank_{p2}$
  - $Bank_{p2}$ hoarding preserves reserves but forfeits the value of payments
- Intuitively, if a bank uses reserves to facilitate payment, it no longer has the reserve
- $\rightarrow$ **Consider the tradeoff between preserving reserves and facilitating payments in measuring the impact of cyber risk**

3. Coordination Failure and Cyber Risk

- So far: banks' inability to send payments (cyber risk) may trigger payment delays by other banks (hoarding) and their implications
- But, for a payment to be successful:
  1. Paying bank receives a payment request
  2. Paying bank chooses to pay
  3. Payment goes through (= no cyber attack)
- Even if banks know that payments will go through, they will *choose* to delay if they believe that other banks will *choose* to delay
- "Technology improvement (= no cyber risk) may not necessarily resolve the lack of trust" - Goldstein, Yang, and Zeng 24

3. Coordination Failure and Cyber Risk

- The absence of cyber risk $\neq$ the absence of coordination failure
- But, a technology that automatically and instantly enforces payment $=$ the absence of coordination failure
- It already exists: instant payment systems like Pix, UPI, FedNow
- **If the goal is to eliminate coordination failure in payments, resolving cyber risk may not be a panacea**

Conclusion

- Very important question
- Novel perspective on the interaction between cyber risk and financial conditions
- Plausible results
- Comments
  1. Network structure and cascades
  2. Reserve preservation versus payment facilitation
  3. Relationship between coordination failure and technology