Discussion of:
Cyberattacks on Small Banks and the Impact on Local Banking Markets

Fabian Gogolin, Ivan Lim and Francesco Vallascas

Eric Vansteenberghe[a]

2022 EBA Policy Research Workshop
27 October 2022

[a]Paris School of Economics-EHESS; Banque de France-ACPR

Cyberattacks, reputation and resilience

Financial institutions exposure to cyberattacks is a concern for a supervisor
Cyberattack: unauthorized system/network access by a third party.

1. **Resilience**:
   - Malware
     - **Ransomware**: institution's files get encrypted, leading to a temporary or permanent loss of service;
   - hack financial assets
   - Denial-of-Service Attack
2. **Reputation:**
   - Malware
     - **Spyware**: confidential data is stolen.

- In Europe: Digital Operational Resilience Act (DORA):
  - Financial institution will exchange information on attacks.

Small banks might be privileged targets

- Deloitte (2020)
  - U.S. financial organizations with less than USD500 million in annual revenue spend about 11.2% of their information technology budget on cybersecurity;
  - overall banking sector average of 9.4%.
- Nationwide:
  - U.S. lenders with under USD1 billion in assets also accounted for nearly half of cybercrimes against banks from 2012 through 2017,
  - the average asset size of targeted banks declined 28% during the study period.

The smaller banks are just not going to have the time, the money, nor the people resources to respond to an attack.

Paul Ferrillo (Seyfarth Shaw LLP).

[How do you put a price on cybersecurity when] you have to explain to every single one of your customers that their account has been compromised

Megan Prendergast Millard (Guidepost Solutions).

US small banks and real effects to SMEs

- In the US, small banks play a pivotal and unique role in the access to finance for SMEs;
- Gaps in cybersecurity investments in small banks might induce depositors to shift to large (safer) rivals;
- This can have real effect for SMEs.

This paper - cyberattacks on small banks

Documents how cyberattacks on small banks
create significant challenges to retain customers.

- How depositors react to cyberattacks on small banks:
  - direct effect: growth rate of hacked banks;
  - indirect effect: reallocation to larger banks.
- Two competing effects:
  - information loss explanation, *flight-to-reputation*;
  - stability concern explanation, *flight-to-safety*.
- Asses loss of competitiveness of hacked small banks with negative consequences for small business lending.

This paper - main diff-in-diff

$$\ln\left(\text{Deposit}_{i,j,z,c,t}\right) = \alpha + \beta \text{Treated}_{i,j,c} \times \text{Post}_{c,t} + \gamma_i + \gamma_z \times t + \epsilon_{i,j,z,c,t} \quad (1)$$

with i branch, j bank, z county, c cohort, t time

Panel A	Ln(Deposits)		
	Treated	Untreated	Diff-in-diff
	(1)	(2)	(3)
Average Diff. Pre-Post	0.163**	0.371***	-0.209***
T-value	(3.734)	(18.140)	(4.490)
Panel B	Ln(Deposits)		
	(1)	(2)	(3)
Treated × Post	-0.250***	-0.241***	-0.216***
	(0.086)	(0.084)	(0.077)
Size		0.062	0.080
		(0.066)	(0.085)
ROA			3.547
			(3.547)
NPL			1.218
			(1.200)
Tier 1			-0.026
			(0.597)
Loan			-0.132
			(0.229)
Productivity			0.001
			(0.017)
Branch FE	Yes	Yes	Yes
County x Year FE	Yes	Yes	Yes
Observations	15460	15334	14382
Adjusted R^2	0.935	0.936	0.936

This paper - flight-to-safety or reputation first diff-in-diff

$$\ln\left(\text{Deposit}_{i,j,z,t}\right) = \alpha + \beta_h \text{Treated High Identity Theft Risk}_j \times \text{Post}_t + \beta_l \text{Treated Low Identity Theft Risk}_j \times \text{Post}_t + \gamma_i + \gamma_z \times t + \epsilon_{i,j,z,t}$$

with i branch, j bank, z county, t time

Panel A	Identity Theft			Digital Sophistication		
	Ln(Deposits)			Ln(Deposits)		
	(1)	(2)	(3)	(4)	(5)	(6)
Treated High × Post	-0.446***	-0.438***	-0.402***	-0.063	-0.058	-0.050
	(0.103)	(0.102)	(0.095)	(0.039)	(0.041)	(0.044)
Treated Low × Post	-0.108**	-0.104**	-0.096**	-0.521***	-0.514***	-0.481***
	(0.045)	(0.046)	(0.048)	(0.098)	(0.098)	(0.095)
Size Control	No	Yes	Yes	No	Yes	Yes
Other Bank Controls	No	No	Yes	No	No	Yes
Branch FE	Yes	Yes	Yes	Yes	Yes	Yes
County x Year FE	Yes	Yes	Yes	Yes	Yes	Yes
High-Low	-0.452***	-0.449***	-0.405**	-0.459***	-0.456***	-0.431***
Observations	15460	15334	14382	15460	15334	14382
Adjusted R^2	0.935	0.936	0.936	0.936	0.936	0.937

This paper - flight-to-safety or reputation second diff-in-diff

$$\ln\left(\text{Lending}_{j,z,t}\right) = \alpha + \beta \text{Treated}_j \times \text{Post}_t + \gamma_j + \gamma_z \times t + \epsilon_{j,z,t} \quad (2)$$

with j bank, z county, t time

	Mortgage Lending							
	Ln(Num. Loans)		Submitted LTI		Approval Rate		Approved LTI	
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Treated × Post	0.103	0.106	0.166**	0.167**	-0.019	-0.020	0.111**	0.111*
	(0.148)	(0.148)	(0.073)	(0.073)	(0.021)	(0.023)	(0.055)	(0.057)
Ln(Num. Loans)			-0.636***	-0.638***	-0.033	-0.035	-0.747***	-0.747***
			(0.105)	(0.105)	(0.023)	(0.023)	(0.056)	(0.057)
Ln(Total Loan Applied)			0.591***	0.593***	0.036	0.037	0.703***	0.703***
			(0.104)	(0.104)	(0.023)	(0.023)	(0.051)	(0.052)
Approval Rate							0.132	0.130
							(0.094)	(0.093)
Size Control	No	Yes	No	Yes	No	Yes	No	Yes
Other Bank Controls	No	Yes	No	Yes	No	Yes	No	Yes
Loan Controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Bank FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
County x Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	2033	2033	2033	2033	2033	2033	1992	1992
R^2	0.817	0.818	0.882	0.883	0.744	0.745	0.872	0.873

Questions - Cyberattacks, small banks and SMEs

- Could you document the type of attacks, how different banks are impacted?
- Do small banks face more attacks than large banks?
- or
- Are attacks more successful when targeted at small banks?

Link to the real economy

- If banks are hit by cyberattacks, so should their SMEs counterparties:
  - How do you make sure that the decrease in lending to SMEs, in time of successful cyberattacks, are not driven by the fact that SMEs are also victims of cyberattacks?
  - Can you control for SMEs' attacks?

Questions - Are cyberattacks random in practice?

$$\ln\left(\text{Deposit}_{i,j,z,c,t}\right) = \alpha + \beta \text{Treated}_{i,j,c} \times \text{Post}_{c,t} + \gamma_i + \gamma_z \times t + \epsilon_{i,j,z,c,t} \quad (3)$$

Do you assume that all banks are randomly targeted?

- You consider **exogenous** cyberattacks:
  - if each bank investment in cybersecurity is common knowledge, isn't this information used by hackers to efficiently choose their targets?
  - if there is some **targeting** by hackers, how do your results and conclusion hold/change?
- Hackers are likely to target banks based on their characteristics:
  - endogenous treatment selection:
    - indirect by bank underinvestment in cybersecurity;
    - direct by hackers.

Questions - Flight-to-safety or reputation first diff-in-diff

$$\ln\left(\text{Deposit}_{i,j,z,t}\right) = \alpha + \beta_h \text{Treated High Identity Theft Risk}_j \times \text{Post}_t + \beta_l \text{Treated Low Identity Theft Risk}_j \times \text{Post}_t + \gamma_i + \gamma_z \times t + \epsilon_{i,j,z,t}$$

with i branch, j bank, z county, t time

- What happens if you apply a triple interaction?
- How do you treat time variation in banks' investment in cybersecurity?
  - After being a victim of a cyberattack, a bank should urgently invest more in cybersecurity, do you observe this is the data? If there are some banks variation in reaction/investment post attack, do you observe an effect on the deposit growths, or is it to late for the reputation of the bank?

Question- flight-to-safety or reputation second diff-in-diff

$$\ln\left(\text{Lending}_{j,z,t}\right) = \alpha + \beta \text{Treated}_j \times \text{Post}_t + \gamma_j + \gamma_z \times t + \epsilon_{j,z,t} \tag{4}$$

with j bank, z county, t time

- How do you treat variation in banks' risk over time?
- You observe a relative increase in the Loan-to-Income ratio of submitted (and accepted) loans:
  - This is in fact an increase in the bank's portfolio risk, how do you treat this potential endogeneity?

Suggestions: exogenous shock affecting all banks

zero-day vulnerabilities

Apple warns users to install software updates to prevent hackers accessing devices

iPhone maker releases fixes to security issues that expert says could give attackers 'full access to a vulnerable device'

Apple said customers should update to the latest software to avoid risks affecting its Safari browser and Mac computers, as well as its iPhone and iPad devices © Richard Drew/AP

By **Patrick McGee** in San Francisco and **Rafe Uddin** in London AUGUST 19 2022 69

- August 2022 zero-day risk affecting Mac, iPhone and iPad;
- zero-day when no fix for a vulnerability has yet been available;
- such a vulnerability initially affect equally all firms with these device/software;
- as a fix/update become available, large banks might be faster at deploying it.

$\Longrightarrow$ do we have such examples in your data set? Do we still observe a flight-to-reputation?

Suggestions- flight-to-safety or reputation second diff-in-diff

$$\ln\left(\text{Lending}_{j,z,t}\right) = \alpha + \beta \text{Treated}_j \times \text{Post}_t + \gamma_j + \gamma_z \times t + \epsilon_{j,z,t} \tag{5}$$

with j bank, z county, t time

- Do you have inter-bank lending data?
  - After a cyberattack, there could be some reactions in the inter-bank lending market.
  - You could observe if there are some variation in bank's evaluation of attacked banks probability of default (or any other scoring method)?
  - You could look at how CCP change their margin requests.

Main take away

1. Great paper documenting the effect of cyber-attacks on small business lending via small bank vulnerabilities
   - 1.1 policy implications for banks cyber security strategies;
   - 1.2 policy implications for SME financing.
2. Channel of depositor flight-to-reputation well documented
   - this flight-to-reputation raise a concentration question (philosophical): if hackers force banks to merge, then having less diversity could increase the incentive to target large banks with sophisticated attacks, hence increasing systemic risk?