Cybersecurity and financial stability^a

Kartik Anand¹ Chanelle Duley² Prasanna Gai²

¹Deutsche Bundesbank ²University of Auckland

^aThis paper represents the authors' personal opinions and does not necessarily reflect the views of the Deutsche Bundesbank or the Eurosystem.

Cyberattacks can disrupt banks' operations

 Nov 2023: Ransomware group Lockbit gained access to ICBC by exploiting a vulnerability in the remote desktop software Citrix (commonly used by banks)



- The attack impaired several systems, including those used to clear US Treasury trades and repo transactions, and facilitated the theft of confidential data
- Further disruptions were prevented after an undisclosed ransom was paid

- Some policymakers advocate stress-tests to assess banks' resilience in the event of cyberattacks (ESRB, 2022)
 - The ECB has (just) conducted a cyber stress test to assess how supervised banks will respond and recover from a cyberattack (ECB, 2024)
- Others endorse treat-based "red team testing" to find and eliminate vulnerabilities in banks' IT systems to boost protection against cyber violation (G7, 2018)

- Some policymakers advocate stress-tests to assess banks' resilience in the event of cyberattacks (ESRB, 2022)
 - The ECB has (just) conducted a cyber stress test to assess how supervised banks will respond and recover from a cyberattack (ECB, 2024)
- Others endorse treat-based "red team testing" to find and eliminate vulnerabilities in banks' IT systems to boost protection against cyber violation (G7, 2018)
- Our paper: Model of cyber attacks, banks, and investment in cybersecurity
 - Investment in cybersecurity is subject to a novel trade-off increasing protection against a cyberattack versus remaining resilient in the face of an attack
 - Under-investment or over-investment in cybersecurity and the optimal policy response depends on bank fragility and sophistication of the attacker

Model

- Single good economy extending over three dates, t = 0, 1, 2
- Risk-neutral bank issues a unit of demandable debt to risk-neutral investors
 - ► Face value of debt denoted F; independent of the withdrawal date
- Software and other IT solutions used to manage operations and balance sheet
 - Focus on 'in house' solutions, i.e., abstract from a third-party vendor

- Single good economy extending over three dates, t = 0, 1, 2
- Risk-neutral bank issues a unit of demandable debt to risk-neutral investors
 - ▶ Face value of debt denoted F; independent of the withdrawal date
- Software and other IT solutions used to manage operations and balance sheet
 - ▶ Focus on 'in house' solutions, i.e., abstract from a third-party vendor
- But, these solutions have vulnerabilities unknown to the bank
- A risk-neutral attacker seeks to find/exploit vulnerabilities for personal gain
 - Key difference from 'traditional' bank risks

- Single good economy extending over three dates, t = 0, 1, 2
- Risk-neutral bank issues a unit of demandable debt to risk-neutral investors
 - ▶ Face value of debt denoted F; independent of the withdrawal date
- \blacksquare Software and other IT solutions used to manage operations and balance sheet
 - ▶ Focus on 'in house' solutions, i.e., abstract from a third-party vendor
- But, these solutions have vulnerabilities unknown to the bank
- \blacksquare A risk-neutral attacker seeks to find/exploit vulnerabilities for personal gain
 - Key difference from 'traditional' bank risks
- Key idea: cyber risks are known unknowns (Rumsfeld, 2002)



- The bank invests S in cybersecurity
 - ▶ For example, banks pay security experts to hack systems or offer 'bug bounties'
- Remainder, $I \equiv 1 S$, invested in liquid assets yielding RI > I at t = 2
- Attacker invests A to find/exploit vulnerabilities at marginal cost c > 0
 - Banks have first-mover advantage in the contest (Dixit, 1987)
- Finally, debt is priced competitively given investors' outside option r > 1
 - In the event of the bank failing, assume zero-recovery for investors



At t = 1, attacker identifies a vulnerability and launches a **cyber attack** with probability



- \blacksquare Fraction α of the bank's assets are impaired following the cyber attack
 - ▶ The shock is a uniformly distributed random variable with support [0,1]
- Attacker obtains prize V > 0
- If $\ell \in [0,1]$ of debt is withdrawn, the bank fails due to **illiquidity** whenever

$$(1-\alpha)RI - \ell F < 0$$

Illiquidity threshold:

$$\alpha^{\prime L}(\ell) \equiv 1 - \frac{\ell F}{RI}$$

Rollover decisions delegated to fund managers (Rochet and Vives, 2004)

- \blacktriangleright Fund managers' conservatism $\gamma \! \leq \! 1 \rightarrow$ measure of rollover risk
- \blacktriangleright Larger $\gamma \rightarrow$ greater incentives to withdraw

Fund manager k receives a noisy private signal

$$x_k = \alpha + \varepsilon_k$$

where ε_k is a noise term that is independent of the shock and i.i.d across fund managers according to a continuous distribution *H* with support $[-\varepsilon,\varepsilon]$

- At t = 2, the impairments are resolved
- \blacksquare Bank is subject to deadweight losses $\delta\,\alpha,$ where $\delta<1,$
 - e.g., ransomware payments or loss of of banks' proprietary trading information
- The bank fails at t = 2 due to **insolvency** whenever

 $(1-\delta\alpha) \textit{RI} - \ell\textit{F} < (1-\ell)\textit{F}$

Insolvency threshold:

$$\alpha^{IN} \equiv \frac{1}{\delta} \left(1 - \frac{F}{RI} \right)$$



Analysis



· · · · · Insolvency threshold (α^{IN})

Fraction of Early Withdrawals (ℓ)

 $\cdots \cdots \qquad \text{Insolvency threshold} (\alpha^{IN}) \quad \cdots \quad \cdots \quad \text{Illiquidity threshold} (\alpha^{IL})$



Fraction of Early Withdrawals (ℓ)



······ Insolvency threshold (α^{IN}) ····· Illiquidity threshold (α^{IL})

Fraction of Early Withdrawals (ℓ)

Attacker chooses attack intensity to maximize the expected prize minus costs

$$A^*(S) \equiv \max_A \left(\frac{A}{A+S}\right) V - c A$$

The bank succeeds in finding and mitigating the vulnerability first with probability

$$p(S) \equiv p(A^*(S), S)$$

where p' > 0, $p'(0) = \infty$ and p'' < 0

Bank chooses $S^*(F)$ to maximise expected equity value, π



Bank chooses $S^*(F)$ to maximise expected equity value, π



Bank chooses $S^*(F)$ to maximise expected equity value, π



Trade-off

- Investing more in cybersecurity improves protection, i.e., chances of finding/patching vulnerabilities before the attacker
- But, it reduces investment in profitable assets
- And, conditional on the attacker successfully exploiting the vulnerability the bank is less resilient and susceptible to failing



Contribution to cybersecurity (S)

Comparative statics

Normative implications

• A planner chooses $S^{P}(F)$ to maximises bank profits minus social cost of default

$$W \equiv \pi(S) - \lambda \left(1 - p(S)\right) \left(1 - \alpha^*(\gamma, S)\right)$$

- Face value of debt, $F^*(S)$, determined by investors' participation constraint
- Let S^P denote the equilibrium choice intersection between $S^P(F)$ and $F^*(S)$
- We compare S^{**} with S^P as a function of the attacker's marginal effort cost, c
 Interpret c as a measure of the attacker's sophistication

- $\label{eq:gamma} \ensuremath{\,\bullet\)} \ensuremath{\,\circ\)} \gamma < \widehat{\gamma} \to \mbox{ conditional likelihood of failing following an attack is low }$
- $c < \hat{c} \rightarrow$ bank is the *underdog*, i.e., greater social benefit from increasing resilience

Bank over-invests, $S^P < S^{**}$

• $c \ge \hat{c} \rightarrow$ bank is the *top-dog*, i.e., larger social benefit from increasing protection

Bank under-invests, $S^P \ge S^{**}$



Attacker's cost of effort $\left(c\right)$



Attacker's cost of effort (c)

- $\gamma > \hat{\gamma} \rightarrow \text{conditional likelihood of}$ failing following an attack is high
- Social benefit of greater protection is larger
- Opportunity cost to the planner from investing in cybersecurity is smaller

Bank under-invests, $S^P > S^{**}$



- We develop a model to study cybersecurity and financial stability
- Cybersecurity investments are subject to a novel protection-vs-resilience trade-off
- \blacksquare Laissez faire outcome is constrained inefficient \rightarrow role for regulation/supervision of cybersecurity

- We develop a model to study cybersecurity and financial stability
- Cybersecurity investments are subject to a novel protection-vs-resilience trade-off
- \blacksquare Laissez faire outcome is constrained inefficient \rightarrow role for regulation/supervision of cybersecurity
- Extend the model to consider multiple banks
 - Common IT infrastructure provided by a third-party vendor correlate risks; Cybersecurity is a best-shot public good

 underinvestment is exacerbated
 - Analysis robust to introducing Knightian uncertainty to pricing of debt

- We develop a model to study cybersecurity and financial stability
- Cybersecurity investments are subject to a novel protection-vs-resilience trade-off
- \blacksquare Laissez faire outcome is constrained inefficient \rightarrow role for regulation/supervision of cybersecurity
- Extend the model to consider multiple banks
 - ► Common IT infrastructure provided by a third-party vendor correlate risks; Cybersecurity is a **best-shot public good** → underinvestment is exacerbated
 - Analysis robust to introducing Knightian uncertainty to pricing of debt

Thank you!

	<i>S</i> **	Comments
Attacker sophistication (c)	\uparrow	More likely cyber attacker will fail \rightarrow greater incentives to win contest
Deadweight loss (δ)	\uparrow	Higher benefits from mitigating impairment shock \rightarrow shore up protection
Rollover risk (γ)	¢	Bank more likely to fail following successful attack \rightarrow shore up protection

➡ return