Cybersecurity and financial stability

Kartik Anand\textsuperscript{1}  Chanelle Duley\textsuperscript{2}  Prasanna Gai\textsuperscript{2,3}
AFA PhD Student Poster Session
7-9 January 2022

\textsuperscript{1}Deutsche Bundesbank  \textsuperscript{2}University of Auckland
\textsuperscript{3}Financial Markets Authority of New Zealand

\textsuperscript{a}This paper represents the authors’ personal opinions and does not necessarily reflect the views of the Deutsche Bundesbank or the Financial Markets Authority of New Zealand.
Two observations

- Digital transformations of banks gathering pace..

The Sum of Bank IT Spending Across North America, Europe, Asia-Pacific, and Latin America Will Grow to US$309 billion by 2022

<table>
<thead>
<tr>
<th>Year</th>
<th>NA</th>
<th>EU</th>
<th>APAC</th>
<th>LATAM</th>
<th>CAGR</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019</td>
<td>$105</td>
<td>$77</td>
<td>$67</td>
<td>$21</td>
<td>1.8%</td>
</tr>
<tr>
<td>2020</td>
<td>$110</td>
<td>$81</td>
<td>$72</td>
<td>$21</td>
<td>3.8%</td>
</tr>
<tr>
<td>2021</td>
<td>$115</td>
<td>$85</td>
<td>$75</td>
<td>$22</td>
<td>4.8%</td>
</tr>
<tr>
<td>2022</td>
<td>$120</td>
<td>$89</td>
<td>$78</td>
<td>$22</td>
<td>4.6%</td>
</tr>
</tbody>
</table>
Two observations

- Digital transformations of banks gathering pace..

- ... but so too are cyber attacks on financial institutions
- **Kashyap and Wetherilt (2019)** emphasise the role of shared services (e.g., digital platform) in creating common vulnerabilities that amplify cyber shocks.

- **Duffie and Younger (2019)** argue that cyber attacks can morph into wholesale bank runs.

- **Eisenbach et al (2021)** estimate there to be negative spillovers in wholesale funding markets following a cyber attack on a large U.S. based bank.
Our research agenda

- Kashyap and Wetherilt (2019) emphasise the role of shared services (e.g., digital platform) in creating common vulnerabilities that amplify cyber shocks.

- Duffie and Younger (2019) argue that cyber attacks can morph into wholesale bank runs.

- Eisenbach et al (2021) estimate there to be negative spillovers in wholesale funding markets following a cyber attack on a large U.S. based bank.

- **Our paper**: theoretical model of cybersecurity and financial stability.

- Key message
  
  - Cybersecurity is a **public good** = \( \begin{cases} 
  \text{Free riding problem} & \downarrow \\
  \text{Rollover risk} & \uparrow 
  \end{cases} \)
Banks own safe legacy assets funded by equity and debt (subject to runs)

IT infrastructure (software / hardware) required to manage assets
  ▶ Outsourced to a ‘platform’ that serves multiple banks
  ▶ But, the platform has a vulnerability that can be exploited using malicious code to cause outages (e.g., Stuxnet exploited vulnerabilities in industrial control systems)
  ▶ Attackers must deploy their code in banks’ systems that interface with the platform

Banks have initial endowments and choose how much to invest in
  ▶ Cybersecurity (public good) → monitor and repel unauthorised intrusions
  ▶ Operational resilience (private good) → backup systems to mitigate outages
The ‘cyber’ ingredients

- Cybersecurity is a **weakest-link public-good** (Varian, 2004)
  - Platform correlates cyber risks (Lipp et al., 2018, Canella et al., 2019).
  - Draw on Cornes (1993) in modelling cybersecurity as a “weaker-link” public good – positive externalities, and higher marginal product for lower investment levels.
The ‘cyber’ ingredients

- Cybersecurity is a **weakest-link public-good** (Varian, 2004)
  - Platform correlates cyber risks (Lipp et al., 2018, Canella et al., 2019).
  - Draw on Cornes (1993) in modelling cybersecurity as a “weaker-link” public good – positive externalities, and higher marginal product for lower investment levels

- Three elements of cyber attacks
  - **Attack intensity** is uncertain → ‘attribution problem’ (Hayden, 2011)
  - Cause **outages** that temporarily suspended operations (Cloudflare, 2021)
  - Generate **long-lasting damages** for victims (Lewis et al., 2020)
The ‘cyber’ ingredients

- Cybersecurity is a **weakest-link public-good** (Varian, 2004)
  - Platform correlates cyber risks (Lipp et al., 2018, Canella et al., 2019).
  - Draw on Cornes (1993) in modelling cybersecurity as a “weaker-link” public good – positive externalities, and higher marginal product for lower investment levels

- Three elements of cyber attacks
  - **Attack intensity** is uncertain → ‘attribution problem’ (Hayden, 2011)
  - Cause **outages** that temporarily suspended operations (Cloudflare, 2021)
  - Generate **long-lasting damages** for victims (Lewis et al., 2020)

- Disruptions mitigated through investments in **operational resilience** (e.g., data vaults, resilience planning), which is a **private good**
  - Sheltered Harbor is a certification for banks that implement robust safeguards
Related Literature


Model
Safe investment Return R > 1; Face value of debt F > 0
Investment decisions ($t = 0$)

- $\chi = \left(S_i S_j\right)^{1/2}$
- Platform
- Bank $i$'s investment in cybersecurity
- Bank $j$'s investment in cybersecurity
- Digital services required
- Bank $i$'s investment in operational resilience
- Bank $j$'s investment in operational resilience

Safe investment, Return $R > 1$; Face value of debt $F > 0$
Investment decisions \((t = 0)\)

\[ I = D + E \]

Bank i’s investment in cybersecurity

\( D = 1 - E \)

\( E > 0 \)

Bank i’s investment in operational resilience

Safe investment Return \(R > 1\); Face value of debt \(F > 0\)

Digital services required

\( \chi = (S_iS_j)^{1/2} \)

Digital services required

Bank j’s investment in cybersecurity

Bank j’s investment in operational resilience

i: endowment \(W_i\)

j: endowment \(W_j\)
Cyber attack and disruption to the platform \((t = 1)\)

If \(\ell_b \in (0, 1)\) of debt is withdrawn, bank b fails due to illiquidity whenever

\[
R \left( 1 - \alpha (1 - h(O_b)) \right) - \ell_b FD < 0
\]
Rollover decisions

- Attack intensity: $\lambda \in [0, \bar{\lambda}]$

- Outage shock: $\alpha \in [0, 1]$

- Rollover decisions delegated to fund managers (Rochet and Vives, 2004)
  - Fund managers' ‘conservatism’, $\gamma \leq 1 \rightarrow$ measure of rollover risk
  - Larger $\gamma \rightarrow$ greater incentives to withdraw

- Fund manager $k$ (bank $b$) receives a noisy private signal
  $$x_{bk} = \alpha + \varepsilon_k,$$
  with $\varepsilon_k \in [-\varepsilon, \varepsilon]$; withdraw decision based on the signal
Bank b fails due to insolvency whenever
\[
R \left( 1 - \alpha \delta \left( 1 - h(O_b) \right) \right) - \ell_b FD < (1 - \ell_b) FD
\]
Equilibrium
Symmetric pure strategy PBE

- Focus on threshold strategies
  - Fund manager $k$ rolls over debt with bank $b$ whenever $x_{bk} < x_b^*$

- Equilibrium consists of
  - At $t = 1$: given choices $(O_b^*, S_b^*)$ the threshold strategy $x_b^*$ maximises fund managers expected payoff and the bank fails whenever $\alpha > \alpha_b^*$ following a successful cyber attack
  - At $t = 0$: given $(x_b^*, \alpha_b^*)$, bank $b$ chooses $(O_b^*, S_b^*)$ to maximise expected equity value given the budget constraints, and the choices of the other bank
- **Illiquidity** threshold: $\alpha_b^{IL}(\ell_b) \equiv \frac{R - \ell_b FD}{R(1 - h(O_b))}$

- **Insolvency** threshold: $\alpha_b^{IN} \equiv \frac{R - FD}{R\delta(1 - h(O_b))}$
- **Illiquidity** threshold: \( \alpha^{IL}_b(\ell_b) \equiv \frac{R - \ell_b FD}{R(1 - h(O_b))} \)
- **Insolvency** threshold: \( \alpha^{IN}_b \equiv \frac{R - FD}{R \delta (1 - h(O_b))} \)
- **Illiquidity** threshold: $\alpha_b^{IL}(\ell_b) \equiv \frac{R - \ell_b FD}{R(1 - h(O_b))}$

- **Insolvency** threshold: $\alpha_b^{IN} \equiv \frac{R - FD}{R \delta (1 - h(O_b))}$
- **Illiquidity** threshold: \( \alpha_b^{IL}(\ell_b) \equiv \frac{R-\ell_b FD}{R(1-h(O_b))} \)

- **Insolvency** threshold: \( \alpha_b^{IN} \equiv \frac{R-FD}{R\delta(1-h(O_b))} \)
There exist a unique failure threshold:

\[ \alpha_b^* = \begin{cases} 
\alpha_b^{IN} & \text{if } \gamma < \hat{\gamma} \\
\alpha_b^{IL}(\gamma) & \text{if } \gamma \geq \hat{\gamma}
\end{cases} \]

- Funding conditions matter: illiquidity risk arises only when \( \gamma \) is large
- Greater investment in cybersecurity increases fragility
Bank $b$ chooses its investments in cybersecurity and operational resilience

- Maximise expected equity value, $\pi_b$
- Taking as given the investment by other banks, $\tilde{S}_{-b}$

\[
\max_{O_b, S_b} \pi_b \equiv \begin{cases} 
\text{Probability cyber attack fails} & \text{Equity value} \\
\text{Probability cyber attack successful} & \text{Equity value depending on outage}
\end{cases} \\
= \text{Prob}(\lambda \leq \chi(S_b, \tilde{S}_{-b})) \times [R - FD] + \text{Prob}(\lambda > \chi(S_b, \tilde{S}_{-b})) \times \int_0^{\alpha^*_b(O_b)} EV_2(\alpha, O_b) d\alpha
\]

where $EV_2(\alpha, O_b) = R(1 - \alpha \delta(1 - h(O_b))) - FD$, and $O_b + S_b = W_b$
Optimal investment choices

- Bank $b$ chooses its investments in cybersecurity and operational resilience
  - Maximise expected equity value, $\pi_b$
  - Taking as given the the investment by other banks, $\tilde{S}_{-b}$

$$\max_{O_b, S_b} \pi_b \equiv \begin{cases} \text{Probability cyber attack fails} & \text{Equity value} \\ \text{Prob} \left( \lambda \leq \chi(S_b, \tilde{S}_{-b}) \right) \times [R - FD] \\ \text{Probability cyber attack successful} & \text{Equity value depending on outage} \\ \text{Prob} \left( \lambda > \chi(S_b, \tilde{S}_{-b}) \right) \times \int_0^{\alpha^*_b(O_b)} EV_2(\alpha, O_b) d\alpha \end{cases}$$

where $EV_2(\alpha, O_b) = R(1 - \alpha \delta(1 - h(O_b))) - FD$, and $O_b + S_b = W_b$

- Trade-off
  - Investing more in cybersecurity reduces the incidents of successful cyber attacks and thereby the likelihood of earning higher returns
  - But, conditional on the cyber attack being successful the bank is more fragile and susceptible to failing the more it invests in cybersecurity
Benchmark 1: No free-riding problem and no rollover risk

- Planner accounts for how each banks’ decisions influence other banks

- When $\gamma < \hat{\gamma}$, failure driven by insolvency: failure threshold $\alpha_b^{IN}$

- **Samuelson Condition**

  $$\sum_{b=1}^{N} \left( \frac{(R - FD) - \int_{0}^{\alpha_b^{IN}} EV_2(\alpha, O_b) d\alpha}{(\tilde{\lambda} - \chi) \int_{0}^{\alpha_j^{IN}} \left( \frac{\partial EV_2}{\partial O_j} \right) d\alpha} \right) \equiv \frac{\partial \pi_b}{\partial \chi} = \frac{1}{\frac{\partial \chi}{\partial S_j}} = \frac{\partial \pi_j}{\partial O_j}$$

- Free-riding leads to under-provision of cybersecurity
Benchmark 2: No free-riding problem but with rollover risk

- When $\gamma \geq \hat{\gamma}$ → failure driven by illiquidity; failure threshold $\alpha_{IL}^{U}(\gamma)$

- **Samuelson Condition**

\[
\sum_{b=1}^{N} \frac{(\bar{\lambda} - \chi)}{\left(\bar{\lambda} - \chi\right)} \left[ EV_2(\alpha_{IL}^{U}(\gamma)) \frac{\partial \alpha_{IL}^{U}(\gamma)}{\partial O_j} + \int_{0}^{\alpha_{IL}^{U}(\gamma)} \left( \frac{\partial EV_2}{\partial O_j} \right) d\alpha \right] \equiv \frac{\partial \pi_b}{\partial \chi} \left( R - FD \right) - \int_{0}^{\alpha_{IL}^{U}(\gamma)} \frac{\partial \pi_b}{\partial \chi} d\alpha = \frac{1}{\partial \chi / \partial S_j}.
\]

- Two effects of rollover risk on marginal rate of substitution
  1. MB from an extra unit of cybersecurity is higher ($\alpha_{IL}^{U}(\gamma) < \alpha_{IN}^{U}$)
  2. MB from higher operational resilience is also higher (since run is ‘inefficient’)

- First effect dominates → over-provision of cybersecurity (relative to Benchmark 1)
Laissez-faire outcome

- Assume $\gamma \geq \hat{\gamma} \rightarrow$ failure driven by illiquidity

**Proposition**

Bank $b$’s investments, $(S^*_b, O^*_b)$, given beliefs $(\hat{S}^e_{-b}, \hat{O}^e_{-b})$, solves:

$$\frac{\partial \pi_b}{\partial \chi} = \frac{1}{\frac{\partial \chi}{\partial S_b}} \cdot \frac{\partial \pi_b}{\partial O_b}.$$

*Cybersecurity investment is increasing in the endowment, $\partial S^*_b / \partial W_b > 0$, iff $W_b \leq \hat{W}$.*

- Two countervailing effects from an increase in $W_b$
  1. Mechanical increase in $O_b$ (for given $S_b$) $\rightarrow$ reduces MRS
  2. Diminishing returns from investing in operational resilience $\rightarrow$ increases MRS

- Second effect dominates when $W_b \leq \hat{W}$

- But, what are the consequences on the system level?
Proposition

There exist two Nash equilibria: all banks, \( b = 1, \ldots, N \)
(i) invest nothing in cybersecurity, \( S^*_b = 0 \), and \( O^*_b = W_b \) in operational resilience;
(ii) invest \( S^*_b \in (0, W_b) \) in cybersecurity and \( O^*_b = W_b - S^*_b \) in operational resilience.

Proposition

Suppose \( W_1 < \bar{W} < W_2 \). Following a mean-preserving spread increase in banks’ endowments, equilibrium cybersecurity, \( \chi^* = (S^*_1 \times S^*_2)^{1/2} \), is reduced.
Normative implications
Normative implications

- Compare laissez faire outcome with Benchmark 1
Normative implications

- Compare laissez faire outcome with Benchmark 1

Proposition

There exists a critical $\gamma_c$, such that for $\gamma \leq \gamma_c$, there is under-investment in cybersecurity, $S^*_b < S^P_b$; while, for $\gamma > \gamma_c$, there is over-investment, $S^*_b > S^P_b$.

- For small $\gamma$ → run risk is low → weak incentives to invest in cybersecurity
  \[\therefore\] compared with Benchmark 1, free-riding exerts a stronger influence → under-investment in cybersecurity and under-provision of the public good

- For larger $\gamma$ → run risk is higher → stronger incentives to invest in cybersecurity
  Benchmark not impacted by rollover risk → influence of rollover risk dominates → over-investment in cybersecurity and a too low operational resilience.
Normative implications ($\gamma < \gamma^C$)

Benchmark outcome can be achieved by

1. Imposing at $t = 0$ banks invest optimally (e.g., stress-tests)
2. Penalising banks at $t = 2$ that did not exhibit ‘due care’ following a cyber attack (e.g., recent SEC penalties on financial institutions)
Testable hypotheses
Testable hypotheses

Prediction

An increase in intensity of cyber attacks reduces relative investment in cybersecurity.

- $\tilde{\lambda} \uparrow \rightarrow$ given $\chi$, more likely that security is breached leading to outages and disruptions $\rightarrow$ MRS decreases $\rightarrow$ less investment in cybersecurity
## Testable hypotheses

<table>
<thead>
<tr>
<th>Prediction</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>An increase in intensity of cyber attacks reduces relative investment in cybersecurity.</strong></td>
</tr>
<tr>
<td>- $\tilde{\lambda} \uparrow \rightarrow$ given $\chi$, more likely that security is breached leading to outages and disruptions $\rightarrow$ MRS decreases $\rightarrow$ less investment in cybersecurity</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Prediction</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>An increase in bank capital reduces investment in cybersecurity.</strong></td>
</tr>
<tr>
<td>- $E \uparrow \rightarrow$ banks have more to lose if they fail following a successful cyber attack $\rightarrow$ MRS decreases $\rightarrow$ less investment in cybersecurity</td>
</tr>
</tbody>
</table>
**Testable hypotheses**

**Prediction**

*An increase in intensity of cyber attacks reduces relative investment in cybersecurity.*

- $\bar{\lambda} \uparrow \rightarrow$ given $\chi$, more likely that security is breached leading to outages and disruptions $\rightarrow$ MRS decreases $\rightarrow$ less investment in cybersecurity

**Prediction**

*An increase in bank capital reduces investment in cybersecurity.*

- $E \uparrow \rightarrow$ banks have more to lose if they fail following a successful cyber attack $\rightarrow$ MRS decreases $\rightarrow$ less investment in cybersecurity

**Prediction**

*The more banks are subject to rollover risk, the more they invest in cybersecurity.*

- $\gamma \uparrow \rightarrow$ MRS increases $\rightarrow$ more investment in cybersecurity
Conclusion

- We develop a model to study cybersecurity and financial stability
  - Common IT infrastructure correlate risks across banks
  - Cybersecurity is a weakest-link public good

- Investment in cybersecurity trades-off lowering the probability of a successful cyber attack and raising fragility in the event of a successful attack

- Laissez faire outcome is constrained inefficient → role for regulation/supervision of cybersecurity

- Several testable implications for investment in cybersecurity (go through even after endogenising face value of debt)
We develop a model to study cybersecurity and financial stability

- Common IT infrastructure correlate risks across banks
- Cybersecurity is a weakest-link public good

Investment in cybersecurity trades-off lowering the probability of a successful cyber attack and raising fragility in the event of a successful attack

Laissez faire outcome is constrained inefficient → role for regulation/supervision of cybersecurity

Several testable implications for investment in cybersecurity (go through even after endogenising face value of debt)

Thank you!
Classification of cyber events

- Federal Information Security Management Act of 2002
Classification of cyber events

- **Federal Information Security Management Act of 2002**

- **Confidentiality** of data is breached
  - Losses may stem from liability due to damages caused to customers or from competitors learning about a bank’s trading strategies

- **Availability** of data is compromised
  - Losses may stem from bank capital or liquidity becoming immobilised

- **Integrity** of data is impaired
  - Losses may stem from inability to perform core activities
Recent attacks on financial institutions

- Europe & South-East Asia (May 2021): Insurance firm AXA subject to ransomware attack → integrity of data processed by a third-party IT firm compromised

- Hungary (September 2020): Telecommunications systems suffered DDoS attack → availability of data and services compromised for banks

- New Zealand (August 2020): Network provider suffered DDoS attack → NZ Stock Exchange shut down operations → availability of data and services compromised for banks
Recent attacks on financial institutions

- Europe & South-East Asia (May 2021): Insurance firm AXA subject to ransomware attack → integrity of data processed by a third-party IT firm compromised

- Hungary (September 2020): Telecommunications systems suffered DDoS attack → availability of data and services compromised for banks

- New Zealand (August 2020): Network provider suffered DDoS attack → NZ Stock Exchange shut down operations → availability of data and services compromised for banks

- Key ingredient
  ▶ Disruptions involved common IT infrastructure (platforms)