

Cybersecurity and financial stability^a

Kartik Anand¹ Chanelle Duley² Prasanna Gai^{2,3}

AFA PhD Student Poster Session

7-9 January 2022

¹Deutsche Bundesbank ²University of Auckland

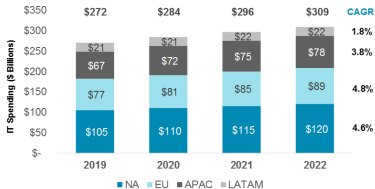
³Financial Markets Authority of New Zealand

^aThis 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 ..

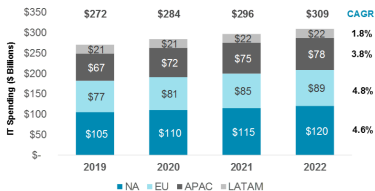
The Sum of Bank IT Spending Across North America, Europe, Asia-Pacific, and Latin America Will Grow to US\$309 billion by 2022



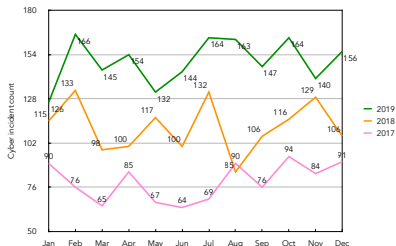
Two observations

- 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



- ... but so too are cyber attacks on financial institutions



▶ Classification of cyber attacks

▶ Recent examples

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 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

- 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

- 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)

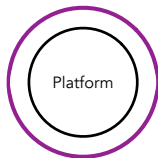
The 'cyber' ingredients

- 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

- Investment in cybersecurity (theory): Gordon and Loeb (2002), Varian (2004), Anderson and Moore, (2006), Grossklag et al (2008), Kamhoua et al (2014)
- Investment in cybersecurity (empirical): Aldasoro et al (2020), Gogolin et al (2021), Jamilov et al (2021)
- Cybersecurity and financial stability: Kashyap and Wetherilt (2019), Duffie and Younger (2019), Eisenbach et al (2021)

Model

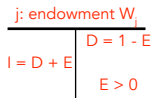
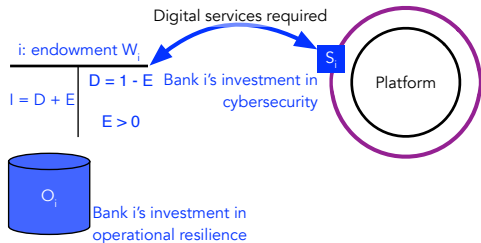
$$\begin{array}{c|c} \text{i: endowment } W_i & \\ \hline I = D + E & \begin{array}{l} D = 1 - E \\ E > 0 \end{array} \end{array}$$



$$\begin{array}{c|c} \text{j: endowment } W_j & \\ \hline I = D + E & \begin{array}{l} D = 1 - E \\ E > 0 \end{array} \end{array}$$

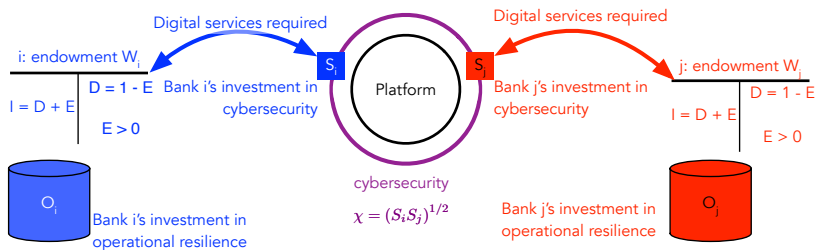
Safe investment Return $R > 1$; Face value of debt $F > 0$

Investment decisions ($t = 0$)



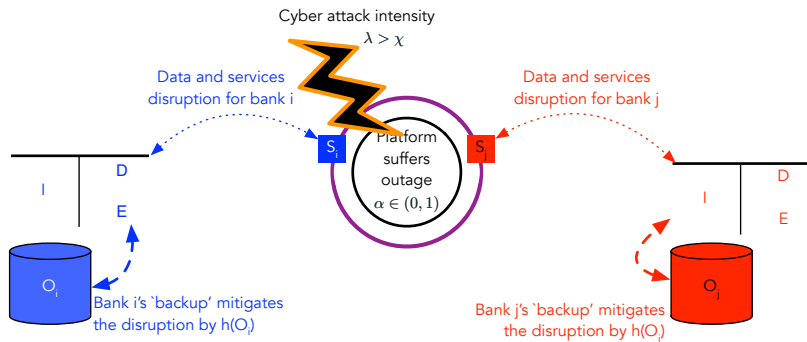
Safe investment Return $R > 1$; Face value of debt $F > 0$

Investment decisions ($t = 0$)



Safe investment Return $R > 1$; Face value of debt $F > 0$

Cyber attack and disruption to the platform ($t = 1$)



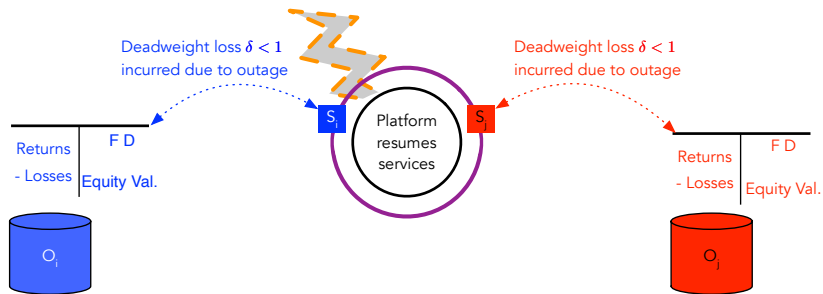
If $\ell_b \in (0, 1)$ of debt is withdrawn, bank b fails due to illiquidity whenever $R(1 - \alpha(1 - h(O_b))) - \ell_b FD < 0$

- 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

Platform resumes operations and debts mature ($t = 2$)



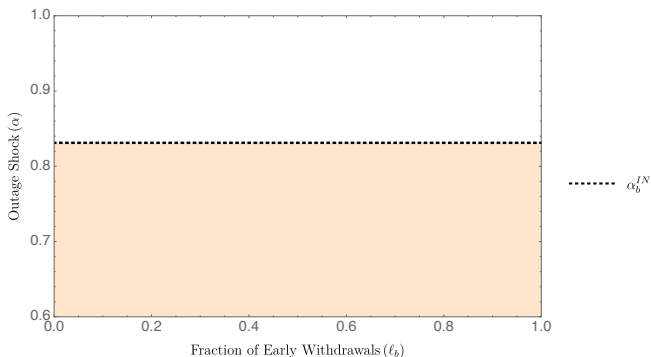
Bank b fails due to **insolvency** whenever $R(1 - \alpha\delta(1 - h(O_b))) - \ell_b FD < (1 - \ell_b)FD$

Equilibrium

- 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^*, α_b^*) , bank b chooses (O_b^*, S_b^*) to maximise expected equity value given the budget constraints, and the choices of the other bank

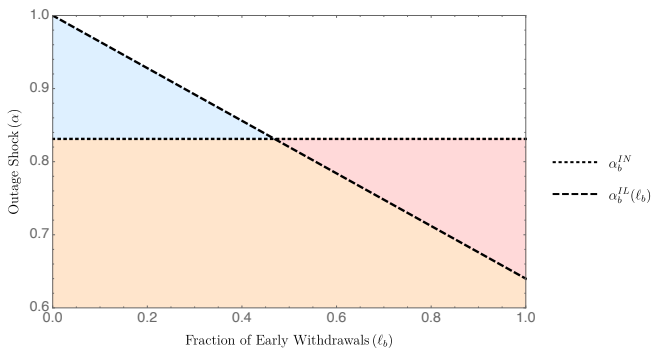
- **Illiquidity** threshold: $\alpha_b^{IL}(\ell_b) \equiv \frac{R - \ell_b FD}{R(1 - h(O_b))}$
- **Insolvency** threshold: $\alpha_b^{IN} \equiv \frac{R - FD}{R\delta(1 - h(O_b))}$

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



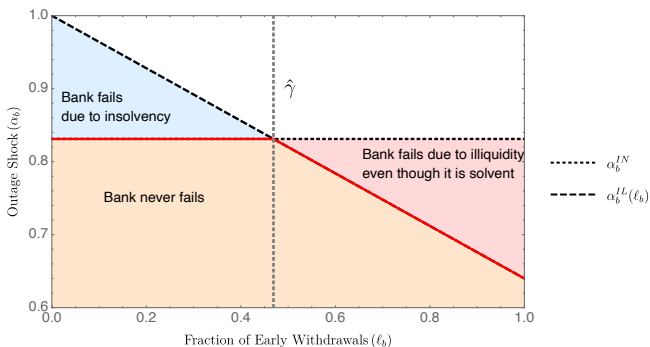
Bank failure

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



Bank failure

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



Proposition

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 γ is large
- Greater investment in cybersecurity increases fragility

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

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

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

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

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

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 α_b^{IN}
- **Samuelson Condition**

$$\sum_{b=1}^N \frac{\overbrace{(R - FD) - \int_0^{\alpha_b^{IN}} EV_2(\alpha, O_b) d\alpha}^{\equiv \partial \pi_b / \partial \chi}}{\underbrace{(\bar{\lambda} - \chi) \int_0^{\alpha_j^{IN}} (\partial EV_2 / \partial O_j) d\alpha}_{\equiv \partial \pi_j / \partial O_j}} = \frac{1}{\partial \chi / \partial S_j}.$$

- Free-riding leads to under-provision of cybersecurity

Benchmark 2: No free-riding problem but with rollover risk

- When $\gamma \geq \hat{\gamma} \rightarrow$ failure driven by illiquidity; failure threshold $\alpha_b^{LL}(\gamma)$

■ Samuelson Condition

$$\sum_{b=1}^N \frac{\overbrace{(R - FD) - \int_0^{\alpha_b^{LL}(\gamma)} EV_2(\alpha, O_b) d\alpha}^{\equiv \partial \pi_b / \partial \chi}}{(\bar{\lambda} - \chi) \underbrace{\left[EV_2(\alpha_b^{LL}(\gamma)) \frac{\partial \alpha_b^{LL}(\gamma)}{\partial O_j} + \int_0^{\alpha_b^{LL}(\gamma)} (\partial EV_2 / \partial O_j) d\alpha \right]}_{\equiv \partial \pi_j / \partial O_j}} = \frac{1}{\partial \chi / \partial S_j}$$

- Two effects of rollover risk on marginal rate of substitution
 - 1 MB from an extra unit of cybersecurity is higher ($\alpha_b^{LL}(\gamma) < \alpha_b^{LN}$)
 - 2 MB from higher operational resilience is also higher (since run is 'inefficient')
- First effect dominates \rightarrow over-provision of cybersecurity (relative to Benchmark 1)

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

Proposition

Bank b 's investments, (S_b^*, O_b^*) , given beliefs $(\vec{S}_{-b}^e, \vec{O}_{-b}^e)$, solves:

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

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

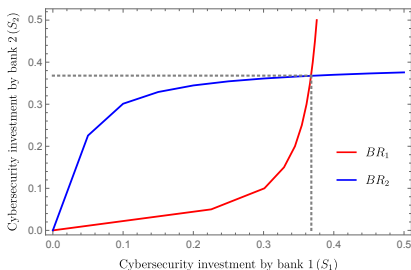
- Two countervailing effects from an increase in W_b
 - 1 Mechanical increase in O_b (for given S_b) \rightarrow reduces MRS
 - 2 Diminishing returns from investing in operational resilience \rightarrow increases MRS
- Second effect dominates when $W_b \leq \hat{W}$
- But, what are the consequences on the system level?

Proposition

There exist two Nash equilibria: all banks, $b = 1, \dots, N$

(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 $W_1 < \widehat{W} < W_2$. Following a mean-preserving spread increase in banks' endowments, equilibrium cybersecurity, $\chi^* = (S_1^* \times S_2^*)^{1/2}$, is reduced.

Normative implications

- Compare laissez faire outcome with Benchmark 1

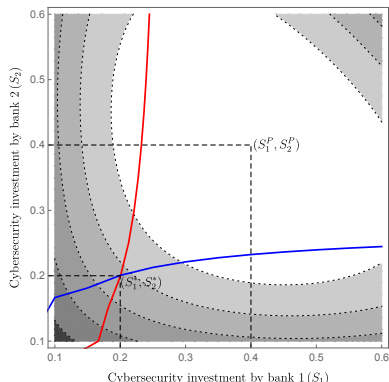
- Compare laissez faire outcome with Benchmark 1

Proposition

There exists a critical γ^c , such that for $\gamma \leq \gamma^c$, there is under-investment in cybersecurity, $S_b^ < S_b^P$; while, for $\gamma > \gamma^c$, there is over-investment, $S_b^* > S_b^P$.*

- For small $\gamma \rightarrow$ run risk is low \rightarrow weak incentives to invest in cybersecurity
 \therefore compared with Benchmark 1, free-riding exerts a stronger influence \rightarrow under-investment in cybersecurity and under-provision of the public good
- For larger $\gamma \rightarrow$ run risk is higher \rightarrow stronger incentives to invest in cybersecurity
Benchmark not impacted by rollover risk \rightarrow influence of rollover risk dominates
 \rightarrow 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

Prediction

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

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

Prediction

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

- $\bar{\lambda} \uparrow \rightarrow$ given χ , 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

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

- $\bar{\lambda} \uparrow \rightarrow$ given χ , 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

- 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

▶ return

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)