Losses due to cyber risk and concentration risks related to Cloud providers for the financial sector

Cyber Resilience: Managing the Consequences of Risk Contagion, 24 April 2020
Volatility and Risk Institute
Antoine Bouveret and Alexander Harris

The views expressed are those of the authors and do not necessarily represent the views of the European Securities and Markets Authority.
Two main issues for financial institutions:

• How to estimate losses related to cyber risk?

• What are the concentration risks associated with increased reliance on cloud providers?
  – Work in progress
Introduction
Relevance of cyber risk for financial institutions

**Threat:** financial sector among the most targeted sector

**Vulnerability:** Reliance on IT, interconnected systems, critical infrastructures and legacy systems

**Consequences:** Direct and indirect losses, contagion
Nature of cyber risk and cyber-attacks

Types of cyber-attacks

**Confidentiality: data breaches**

*Equifax data breach (145Mn records, USD 1.4bn)*

**Integrity: Fraud**

*Bangladesh central bank Swift heist (USD 81Mn)*

**Availability: Business disruption (FMIs, Cloud providers etc.)**

*NotPetya ransomware (USD 870Mn for Merck, USD 400Mn for Fedex)*
Estimation of cyber losses
Quantification of Cyber risk

How to estimate losses due to cyber risk?

**Objective:** Raise awareness, consider cyber-insurance and manage operational risk

**Method:** Distribution of aggregate losses (actuarial science)

**Data requirements:** Frequency of cyber-attacks and losses

**References:** Bouveret (2019), Shevshenko (2010)
Quantification of Cyber risk

Overview of the method
OpRisk databases: SAS, IBM Advisen, ORX

Frequency: Average number of attacks (2011-2016)

Cyber attacks: 341 events (103 with losses), 50 countries

Number of attacks per country
Frequency distribution: Poisson ($\lambda = 992$)

Distribution of losses: Spliced distribution (lognormal for the body and GPD for the right tail)

Contagion:

- Either assume independence of losses
- Introduce contagion through multiple losses (each event can lead to more losses), geometric distribution ($p = 20\%$, calibrated on ORX data)

Estimation through Monte Carlo simulations
Two scenarios:

• Baseline
• Severe with 2x more attacks

Contagion effects

Results:

• Global losses around USD 100bn/year
• Possibility of very large losses

<table>
<thead>
<tr>
<th></th>
<th>in USD bn</th>
<th>In % of banks net income</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Baseline</td>
<td>Severe scenario</td>
</tr>
<tr>
<td>Average</td>
<td>100</td>
<td>276</td>
</tr>
<tr>
<td>Median</td>
<td>88</td>
<td>254</td>
</tr>
<tr>
<td>95% VaR</td>
<td>167</td>
<td>405</td>
</tr>
<tr>
<td>95% ES</td>
<td>283</td>
<td>617</td>
</tr>
<tr>
<td>99% VaR</td>
<td>291</td>
<td>637</td>
</tr>
<tr>
<td>99% ES</td>
<td>599</td>
<td>1189</td>
</tr>
<tr>
<td></td>
<td>Baseline</td>
<td>Severe scenario</td>
</tr>
<tr>
<td>Average</td>
<td>124</td>
<td>345</td>
</tr>
<tr>
<td>Median</td>
<td>111</td>
<td>320</td>
</tr>
<tr>
<td>95% VaR</td>
<td>202</td>
<td>496</td>
</tr>
<tr>
<td>95% ES</td>
<td>324</td>
<td>736</td>
</tr>
<tr>
<td>99% VaR</td>
<td>343</td>
<td>762</td>
</tr>
<tr>
<td>99% ES</td>
<td>637</td>
<td>1372</td>
</tr>
</tbody>
</table>

With contagion

|                | Baseline  | Severe scenario          |
| Average        | 124       | 345                      |
| Median         | 111       | 320                      |
| 95% VaR        | 202       | 496                      |
| 95% ES         | 324       | 736                      |
| 99% VaR        | 343       | 762                      |
| 99% ES         | 637       | 1372                     |

Note: Aggregated losses from cyber attacks, assuming a Poisson distribution for the frequency and a spliced lognormal-GPD distribution for the losses. Estimates obtained by Monte Carlo simulations. Under the contagion scenario, each cyber attack has a 20% probability to affect two or more firms. Net income data based on a sample of 7,947 banks for 2016.

Sources: ORX News, SNL and author's calculations.
Concentration risk and cloud providers
Widespread use of Cloud services

Highly concentrated market

Main issue:
• Concentration risk

References: FSB (2019), Lloyd’s (2018)
Main questions:

• Do Cloud providers reduce the risk of outages for firms?

• Under which conditions could cloud providers increase risk to financial stability?

• How to mitigate risks to financial stability?
Concentration risk and cloud providers

Insights from a model of concentration risk

Framework and assumptions (1/2)

- Firms choose to rely (or not) on Cloud providers
- Firms and cloud providers are always in one of two states: \{0, 1\}, where 1 represents outage
- If firm does not rely on Cloud, moves from state 0 to 1 at ‘incident rate’ $\lambda$ and moves from 1 to 0 at ‘repair rate’ $\mu$
- **Cloud providers are more efficient**: less outages and of shorter duration $\rightarrow \lambda_{\text{cloud}} < \lambda, \mu_{\text{cloud}} > \mu$
- If firm relies on Cloud, then any Cloud outage causes all firms to suffer outage with probability $q$
- Outage states follow Markov process; enables closed-form steady state solutions, e.g. for average shares of time in outage (denoted $\tau$ and $\tau_{\text{cloud}}$)
Framework and assumptions (2/2)

- Individual costs for firms equal total time in outage
- Cost externalities: if more than $n'$ firms suffer an outage at the same time, where $n' \leq n$ is a model parameter, systemic cost of $\gamma n > 0$ arises
- Cloud providers charge fees
Main theoretical results

- Unique equilibrium exists in which all firms use Cloud.
- Reliance on Cloud providers can increase systemic risk due to concentration: more firms have simultaneous outages, even if outages are less frequent.
- Cloud increases expected total net costs (excluding fees) when
  \[ \gamma (\beta - \alpha) > \tau - q \tau_{\text{cloud}} \]
  where \( \alpha, \beta \) are respective probabilities that a systemic event occurs if all firms do not / do use Cloud.
- Systemic risk is mitigated when there is competition and portability among Cloud providers.
Main questions:

• Do Cloud providers reduce the risk of outages for firms?
  → Yes because they are more efficient

• Under which conditions could cloud providers increase risk to financial stability?
  → If systemic costs and probability of simultaneous outages are high

• How to mitigate risks to financial stability?
  → Reduce probability of simultaneous outages and duration of outages (diversification)
Next steps: Model calibration

• To calibrate model, need estimates of key parameters (duration and intensity of outage)

• Could also look at estimating parameters in relation to cyber-specific risks

• Data for estimation are scarce

• Our model and results above suggest what kinds of data collection would be policy-relevant
Main takeaways

1. Significant impact of cyber risk at entity-level and systemic risk

2. Reliance on cloud providers increases efficiency but could increase systemic risk due to concentration

3. Possible policy implications:
   1. Designation of Cloud providers as Critical Service Providers
   2. Diversification in terms of Cloud providers and/or service types (IaaS, SaaS etc.)
   3. Data portability and interoperability
Please send any comment or questions to:

antoine.bouveret@esma.europa.eu and alexander.harris@esma.europa.eu
Additional slides
Aggregate losses:

\[ Z = X_1 + \cdots + X_N \]

Where \( N \) is a discrete random variable (frequency) and \( X \) are random losses (severity).

Three components:

Frequency distribution of \( N \)

Distribution of losses for \( X \)

Correlation: under independence of events

\[ E[Z] = E[N] \times E[X] \]

Avg. # of attacks  Avg. loss per attack
Aggregate losses:

\[ Z = X_1 + \cdots + X_N \]

\[ N \sim \text{Poisson}(\lambda) \]

For \( x \leq u \), \( X \sim \text{LN}(\mu, \sigma) \)

\[ f(x) = \frac{1}{x \sqrt{2\pi \sigma^2}} \exp\left( -\frac{(\ln(x) - \mu)^2}{2\sigma^2} \right) \]

For \( x > u \), \( X \sim \text{GPD}(\xi, \alpha, \beta) \)

\[ f(x) = \frac{1}{\beta} \left( 1 + \frac{\xi(x - \alpha)}{\beta} \right)^{\left(\frac{1}{\xi} - 1\right)} \]
Selected References


Estimation of losses due to cyber risk and concentration risks related to Cloud providers

Cyber Resilience: Managing the Consequences of Risk Contagion, 24 April 2020
Volatility and Risk Institute
Antoine Bouveret and Alexander Harris