Cloud outage scenario in cyber insurance

Olivier Lopez, Ensae IP Paris (joint work with Daniel Nkameni, Detralytics)

5th European
Congress of Actuaries
www.eca2024.org

About the speaker

- **Olivier Lopez –** *Professor, Ensae IP Paris*
  Member of Institut des actuaires.
  Professor in Actuarial Sciences.
  Research topics: emerging risks, cyber, climate, AI.
  Other activities: scientific advisor at Detralytics.

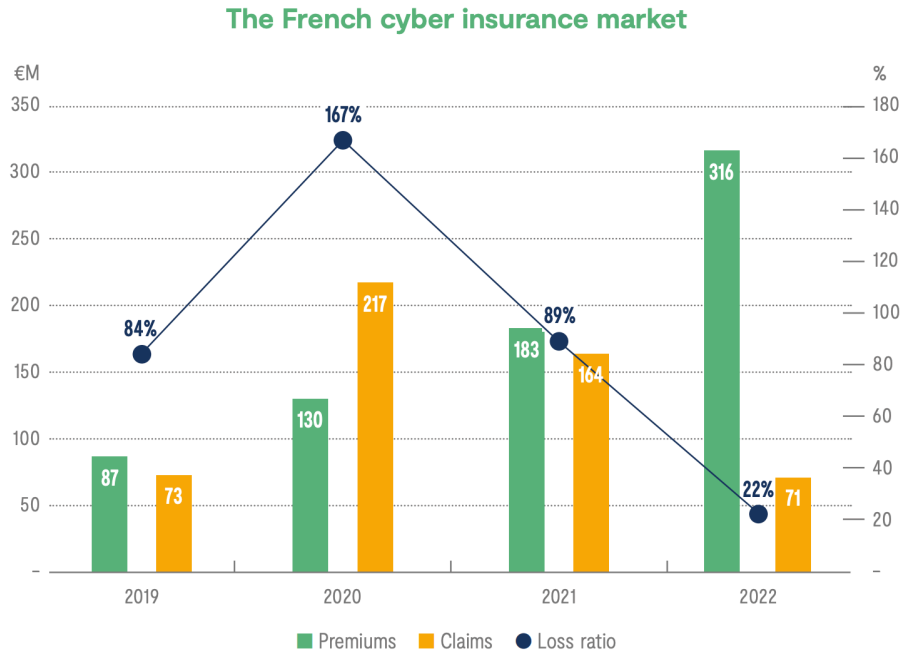
- Ensae Institut Polytechnique de Paris
  Center for Research in Economics and Statistics
  5 avenue Henri Le Chatelier
  91120 Palaiseau

Some numbers (French market, but similar patterns in other countries)

- The « Association pour le Management des Risques et des Assurances de l'Entreprise » (AMRAE) published its third version of the LUCY study in 2023.

- Some key facts in 2021:
  - Insurance capacities are smaller
  - Deductibles increase
  - Premium increases (+44,4% compared to an estimated growth of the market of 27,5%)
  - The coverage of large companies is diminishing (-4,4%)

- Key facts in 2022:
  -Loss ratio: 22%
  - Falling from 261% to 51% for « medium » companies
  - From 58% to 16% for very large ones
  - **Rising from 36% to 100% for SMEs!**



Systemic cyber

- EIOPA lists a few scenarios whose impact needs to be investigated
  - ➡ **Data center / infrastructure damage**
  - ➡ Ransomware
  - ➡ Ddos
  - ➡ Data breach
  - ➡ Power outage

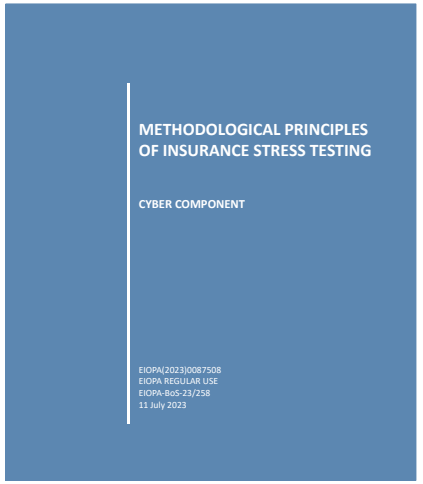


TABLE 3: RE/INSURERS' RANKING OF EXTREME CYBER SCENARIOS

Extreme cyber scenarios	Average ranking of scenario
Denial of service/interruption of operations	
Worm-like malware epidemic	1
Widespread ransomware attack	2
Mass data breach	
Exfiltration of sensitive information (PII, encrypted passwords, etc.) at key organisation/institution which has widespread effects on customers/suppliers	4
Disruption to critical infrastructure	
An extortion of supervisory control and data acquisition (SCADA) networks of industrial control systems	4
A cyberattack on a crucial participant in an industry/sector (e.g. hospital, food manufacturer/distributor, etc.)	5
A cyberattack on a key utility provider (power, water etc.)	2
A compromise of state/municipal services	5
Cross-sector IT failure	2

Refers to median ranking score assigned by survey respondents (1 being the highest-ranked scenario). Based on the results from a poll of 11 GA member cyber re/insurers

Source: The Geneva Association

- Report of Geneva association on emerging risks: identification of some key systemic scenarios for cyber.

Cloud failure

- Cloud failure is an example of critical infrastructure failure that simultaneously affects a large number of victims.
- Cloud is used essentially for:
  - data storage
  - data processing
- Essentially two type of cloud solutions:
  - private cloud: a provider (Amazon, Google…) has a technology to build a specific server for a given company. The server stays (geographically) **within the company**.
  - public cloud: a given server keeps the information of several users and is located **in the cloud provider facilities**.
- Public cloud is more susceptible to generate « systemic » events…
- … but private cloud may also, since the technologies used share the same tools.

Examples of cloud incidents

- Two recent examples in France:
  - **OVH** in Strasbourg (2021) : a fire destroyed the servers of a French cloud providers. Some back-up servers (located in the same place) also burnt. More than 400K of third party damages were paid by OVH.
  - **Google** (August 2023) : a flood in a large Google facility generated interruption of some web service impacting a large part of the territory.

- Malicious example: **CloudNordic** (already mentioned)

- **Insurance and the cloud:** is it the insurance of the cloud provider that pays or of the victim? Right now: if you exclude damages related to cloud, you do not recruit policyholders.
- Also cloud providers that develop partnerships with insurers.

TECH MONITOR 30
PROUDLY CELEBRATING 30 YEARS OF INDEPENDENT IT JOURNALISM

ctions | Cybersecurity | Digital economy | Hardware | Leadership | Events

TECHNOLOGY > CYBERSECURITY | August 25, 2023

Devastating ransomware attack hits Danish cloud hosting companies CloudNordic and AzeroCloud

A ransomware attack on the Danish hosting sites saw its back-ups encrypted and both firms lose access to all of their customers' data.

By Claudia Glover

Outline

I. Modeling the loss of the portfolio
   a) Standard regime
   b) Stressed regime
   c) Consequences of a business interruption

II. Diversification and portfolio optimization
   a) A quadratic optimization problem
   b) Illustration

Outline

I. Modeling the loss of the portfolio
   a) Standard regime
   b) Stressed regime
   c) Consequences of a business interruption

II. Diversification and portfolio optimization
   a) A quadratic optimization problem
   b) Illustration

Portfolio loss

- $i = 1, \cdots, n$ policyholders.
- $j = 1, \cdots, k$ cloud providers.
- Total loss of the portfolio:

$$\mathscr{L} = \sum_{i=1}^{n} \sum_{j=1}^{k} \delta_{i,j} w_{i,j} \tau_i L_i^{(j)},$$

with:

$\delta_{i,j} = 1$ if policyholder i experiences failure from j.

$w_{i,j} =$ proportion of activity of i in cloud provider j .

$\tau_i =$ turnover of policyholder i .

$L_i^{(j)} =$ normalized loss for i when failure of j .

Two regimes

- **Standard regime:** The defaults of the cloud provider may be correlated with each other, but the policyholders are not.
- We are in a classical framework where **average profitability** is balanced by the **variance** of the result.
- Optimizing the repartition is a standard portfolio optimization problem from Markowitz's theory (quadratic optimization).

- **Stressed regime:** All users of a given cloud provider are stroke at the same time for the same duration.
- This is a matter of bounding the total loss in this scenario.

Consequences of a cloud service interruption

- Lloyd's and AIR (2018) published a report on the effect of cloud failure.
- They do not very much focus on systemic events, but on the consequences for a victim of a cloud failure.
- They develop a framework to characterize the different step of a business interruption.
- Illustration:

Table 3: Probability of implementing a back-up plan as a function of the number of days since the start of the outage, for companies with turnovers of under $1 billion

Day	1	2	3	4	5	6	7	None/fail
Probability	0.27	0.08	0.05	0.04	0.03	0.02	0.01	0.50

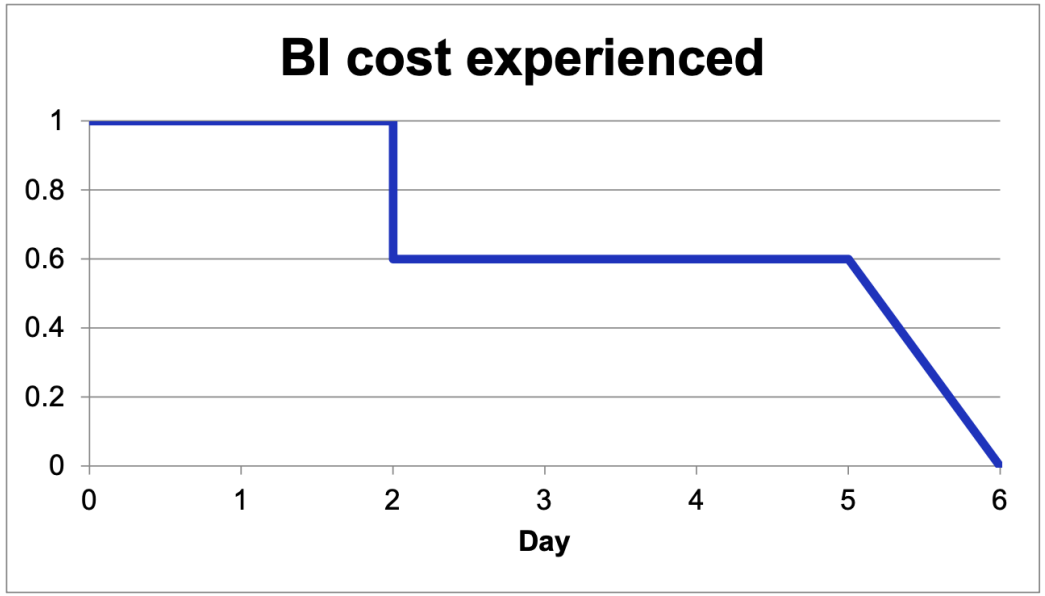
Table 4: Probability of implementing a back-up plan as a function of the number of days since the start of the outage, for companies with turnovers of over $1 billion

Day	1	2	3	4	5	6	7	None/fail
Probability	0.44	0.13	0.08	0.06	0.04	0.03	0.02	0.20

Table 5: Assumed probability distribution governing reduction of (C)BI losses upon successful implementation of a back-up plan

Loss Reduction	30%	40%	50%
Probability	0.3	0.4	0.3

Figure 11: (C)BI cost experienced as a function of time



Consequences of a cloud service interruption

- Unitary cost of 1 day business interruption for i: α_i.
- Time before restoration of the cloud service j: $T_i^{(j)}$.
- Duration before triggering back-up plan: U_i, with $\delta_i = \mathbf{1}_{U_i \leq T_i}$.
- In case of back-up plan, the cost of business interruption is reduced by a proportion $\beta_i \in (0,1)$.
- After restoration of the service, time V_i before going back to normal (linear reduction of the cost during this period).

- All together, the total loss of the episode for this policyholder is:

$$L_i = \alpha_i (T_i^{(j)} - (T_i^{(j)} - U_i)_+ (1 - \beta_i)) + \frac{\alpha_i \left\{1 - (1 - \beta_i)\delta_i\right\} V_i}{2}$$

- In case of a **systemic cloud failure:** $T_i^{(j)} = T$ is the same for all users using the service.

Risk measure in the stressed regime

- In the stressed regime, a failure of j generates a loss

$$\mathscr{L}^{(j)} = \sum_{i=1}^{n} w_{i,j}\tau_i L_i^{(j)} .$$

- One needs to introduce a risk measure to evaluate the magnitude of the loss under this regime, for example:

  - Expected value: $R_j = E\left[\mathscr{L}^{(j)}\right]$.

  - Value-at-Risk: $R_j = q_\alpha^{(j)}$ such that $\mathbb{P}\left(\mathscr{L}^{(j)} \geq q_\alpha^{(j)}\right) = \alpha$.

  - Expected shortfall: $R_j = E\left[\mathscr{L}^{(j)} \;\middle|\; \mathscr{L}^{(j)} > q_\alpha^{(j)}\right]$.

- For each of these risk measure, one can consider a **linear approximation** based on **asymptotic approximation**, that is $R_j = \bar{w}_j \mu_j$, with $\bar{w}_j = \sum_{i=1}^{n} w_{i,j}\tau_i$.

Outline

I. Modeling the loss of the portfolio
   a) Standard regime
   b) Stressed regime
   c) Consequences of a business interruption

II. Diversification and portfolio optimization
   a) A quadratic optimization problem
   b) Illustration

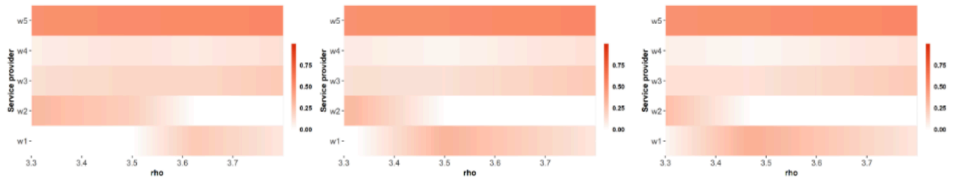
Quadratic optimization

- Risk measure in the standard regime: **variance**, that is $\bar{\mathbf{w}}^T \Sigma \bar{\mathbf{w}}$.
  Σ is related with the correlation between cloud providers.
- Risk measure under the stressed regime: **see previous slides,** that is $\bar{\mathbf{w}}^T \mu$, where $\mu = (\mu_1, \cdots, \mu_k)$.

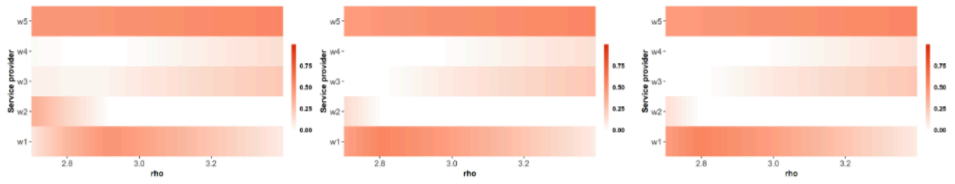
- **Final optimization problem:**
  Minimize $\bar{\mathbf{w}}^T \Sigma \bar{\mathbf{w}} + \lambda \bar{\mathbf{w}}^T \mu$
  under a profitability constraint in the standard regime (linear constraint).

- λ: possibility to determine explicitly the value of λ depending on the value of capital than one is ready to spend in case of a stressed scenario.

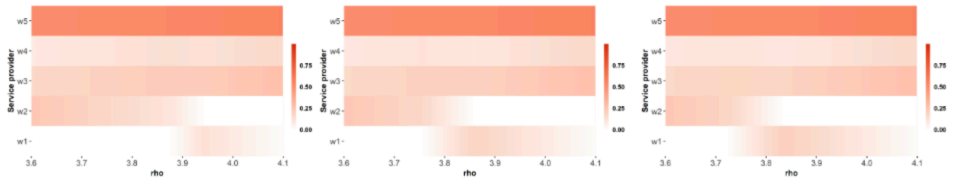
Illustration (a=1 exponential distribution for T, a=0.5 Weibull with decreasing hazard rate, a=1.5 Weibull with increasing hazard rate)



(a) $a = 1$, mean. (b) $a = 1$, quantile. (c) $a = 1$, CTE.

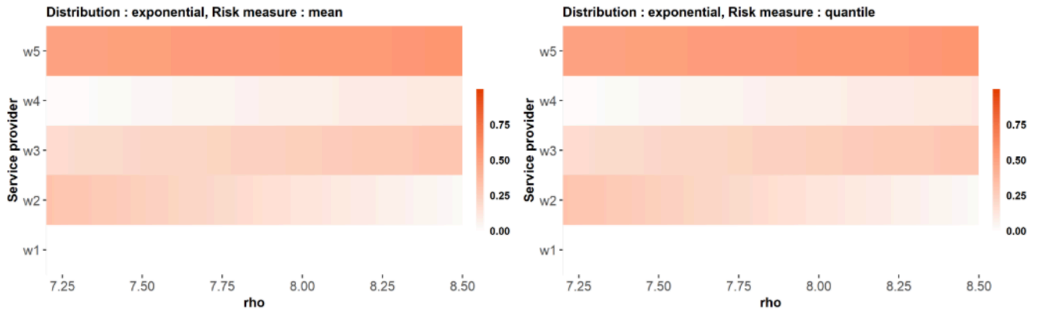


(d) $a = 0.5$, mean. (e) $a = 0.5$, quantile. (f) $a = 0.5$, CTE.

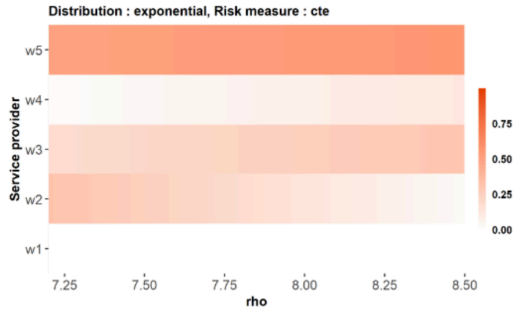


(g) $a = 1.5$, mean. (h) $a = 1.5$, quantile. (i) $a = 1.5$, CTE.

Figure 1: Evolution of the weights of the optimal portfolio depending on the value of ρ. The average duration of the interruption is set to 2 days. The left column displays the results taking the mean as risk measure, the middle column shows the results for the quantile, and the right column shows the case of Conditional Tail Expectation.



(a) $a = 1$, mean. (b) $a = 1$, quantile.



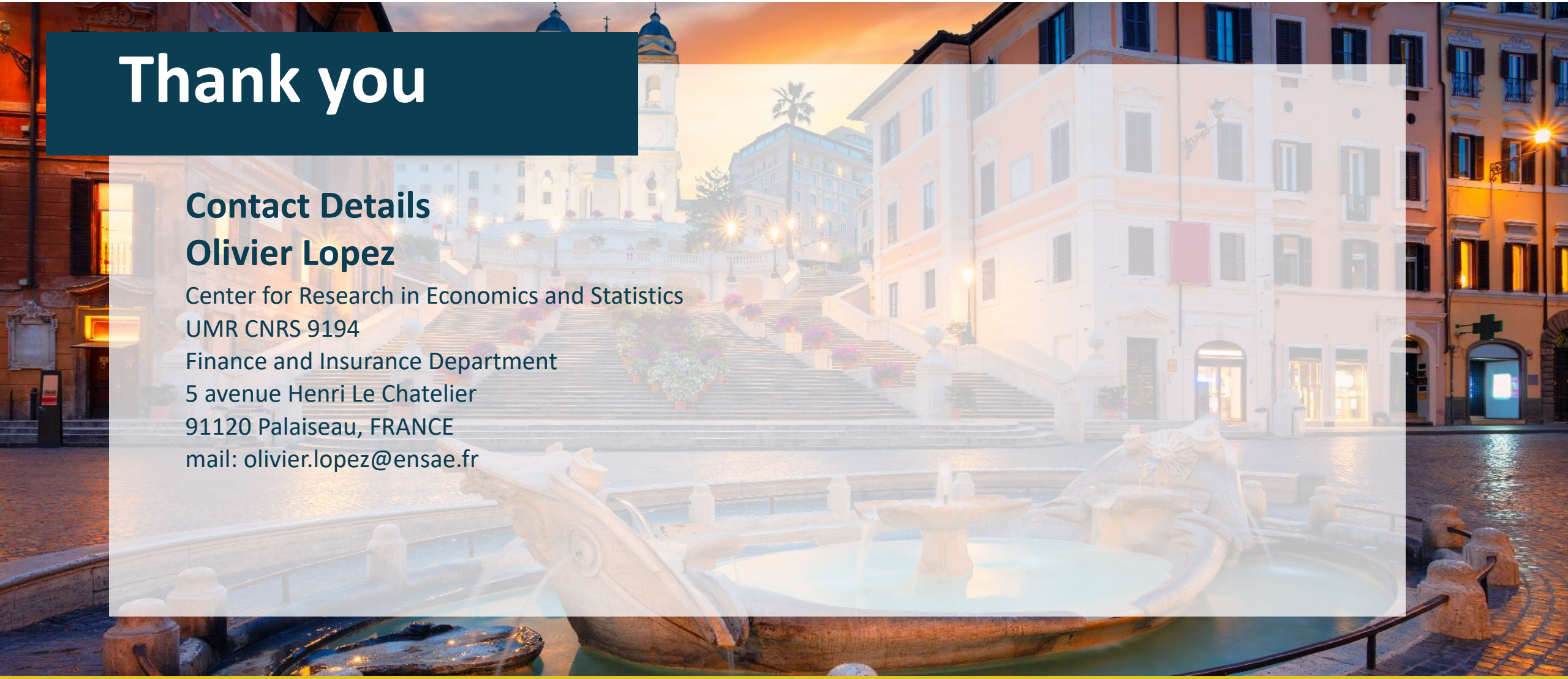
(c) $a = 1.5$, conditional tail expectation.

Figure 4: Evolution of the weights of the optimal portfolio depending on the value of ρ. The average duration of the interruption is set to 5 days. Only the results regarding the exponential distribution ($a = 1$) are reported for the different risk measures.

Conclusion

- A generic model for cloud interruption and measuring the quality of a portfolio by distinguishing standard and stressed regime.
- Optimal portfolio: can provide guidelines to underwriters and help portfolio management.
- How to feed the model:
  - distinguish between the effect of business interruption depending on the policyholder
  - data on the efficiency of backup plans
  - data on cloud failure
- An additional degree of complexity stands in the fact that some cloud servers may not be totally stroke (they have different servers).

Thank you for your attention!



Thank you

Contact Details

Olivier Lopez

Center for Research in Economics and Statistics
UMR CNRS 9194
Finance and Insurance Department
5 avenue Henri Le Chatelier
91120 Palaiseau, FRANCE
mail: olivier.lopez@ensae.fr