UNIVERSITÉ PARIS SUD
université PARIS-SACLAY

European Chair on Intangibles

iC 14
Intellectual Capital
for Communities
In the Knowledge
Economy

UNESCO
United Nations
Educational, Scientific and
Cultural Organization

IFAP
Information for All
Programme

Micro and Macro Impacts of Cyberrisks:
Interim results of H2020 HERMENEUT Project

Ahmed Bounfour, Niaz Kammoun, Rokhaya Dieye,
Altay Özaygen (University of Paris-Sud), Alexander Szanto (BIGS)

Safe and Ethical Cyberspace, digital assets and risks:
How to assess the intangible impacts of a growing phenomenon?

The World Conference on Intellectual Capital for Communities

UNESCO, June 14&15 2018

European Commission
HORIZON 2020

Enterprises intangible Risk Management
via Economic models based on
simulatioN of modErn cyber-aTtacks
HERMENEUT

Agenda

1. Introduction
2. Research questions
3. Taxonomy of Intangibles
4. Research strategy
5. Intangible Asset Valuation
6. Micro estimates of intangibles cyber-risks
7. Macro estimates of intangibles cyber-risks
8. Data
9. Results

1 - Introduction: Consequences of cyber-attacks

- Data breaches are the inability of the firms to guarantee the safety and confidentiality of customer data.
- Negative publicity of the firm in the media and in the social media; word-of-mouth.
- Reduction in customer and stakeholder trust.
- The stolen data is sold in the dark market just few days after the breach (Ablon et al., 2014).
- RAND report on Consumer Attitudes Toward Data Breach (Ablon et al., 2016);
  - 11.5 million people stopped doing business with the company.
  - More than $60 billion perceived losses.
  - 77% were highly satisfied with the company’s post breach process.

1 - Introduction: Consequences of cyber-attacks

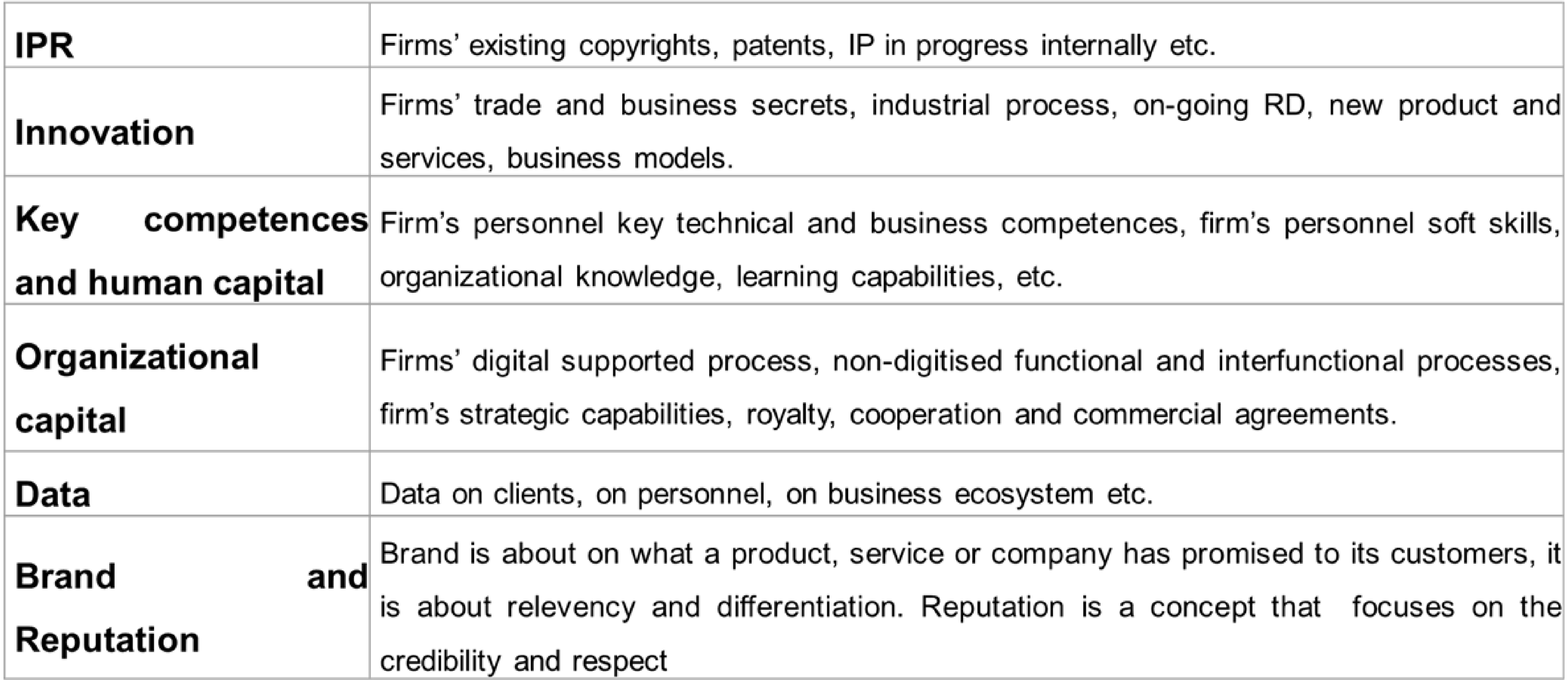
Macro Estimates and Stylized Facts

- Information disruptions
  - Petya virus (including Saint-Gobain): up to $US 1 billion
  - Equifax: $US 4 billion in September 2017 to the company
  - Ponemon Institute: $2.4 million is the average cost of malware attacks

2- Research Questions

- What are the effects of cyber-attacks on firm values and on their intangibles?
- What are the effects of cyber-attacks at the macroeconomic level?
- What characteristics of firms are linked to the type of cyber-attacks?

3- Taxonomy of Intangibles



IPR	Firms' existing copyrights, patents, IP in progress internally etc.
Innovation	Firms' trade and business secrets, industrial process, on-going RD, new product and services, business models.
Key competences and human capital	Firm's personnel key technical and business competences, firm's personnel soft skills, organizational knowledge, learning capabilities, etc.
Organizational capital	Firms' digital supported process, non-digitised functional and interfunctional processes, firm's strategic capabilities, royalty, cooperation and commercial agreements.
Data	Data on clients, on personnel, on business ecosystem etc.
Brand and Reputation	Brand is about on what a product, service or company has promised to its customers, it is about relevency and differentiation. Reputation is a concept that focuses on the credibility and respect

4- Research Strategy

1. Taxonomy of intangibles
2. Micro analysis:
   a. Valuation of intangibles
      i. Attacked firms (AF)
      ii. Non-attacked firms (NAF)
      iii. Difference => AF - NAF gives intangible loss due to cyber-attack (Counterfactual)
   b. Event Study Analysis: Obtaining the loss in stock market
   c. NLP on press articles; splitting the effect of an attack on different types intangibles.
3. Macro analysis:
   a. Inoperability I/O Model: For a given % of inoperability we obtain an economical loss value for different sectors
   b. Using step 2 “Valuation of intangibles” and step 4 “NLP analysis”: We obtain a value for different type of intangible loss after a cyber-attack.
4. Business model of cyber-attacks

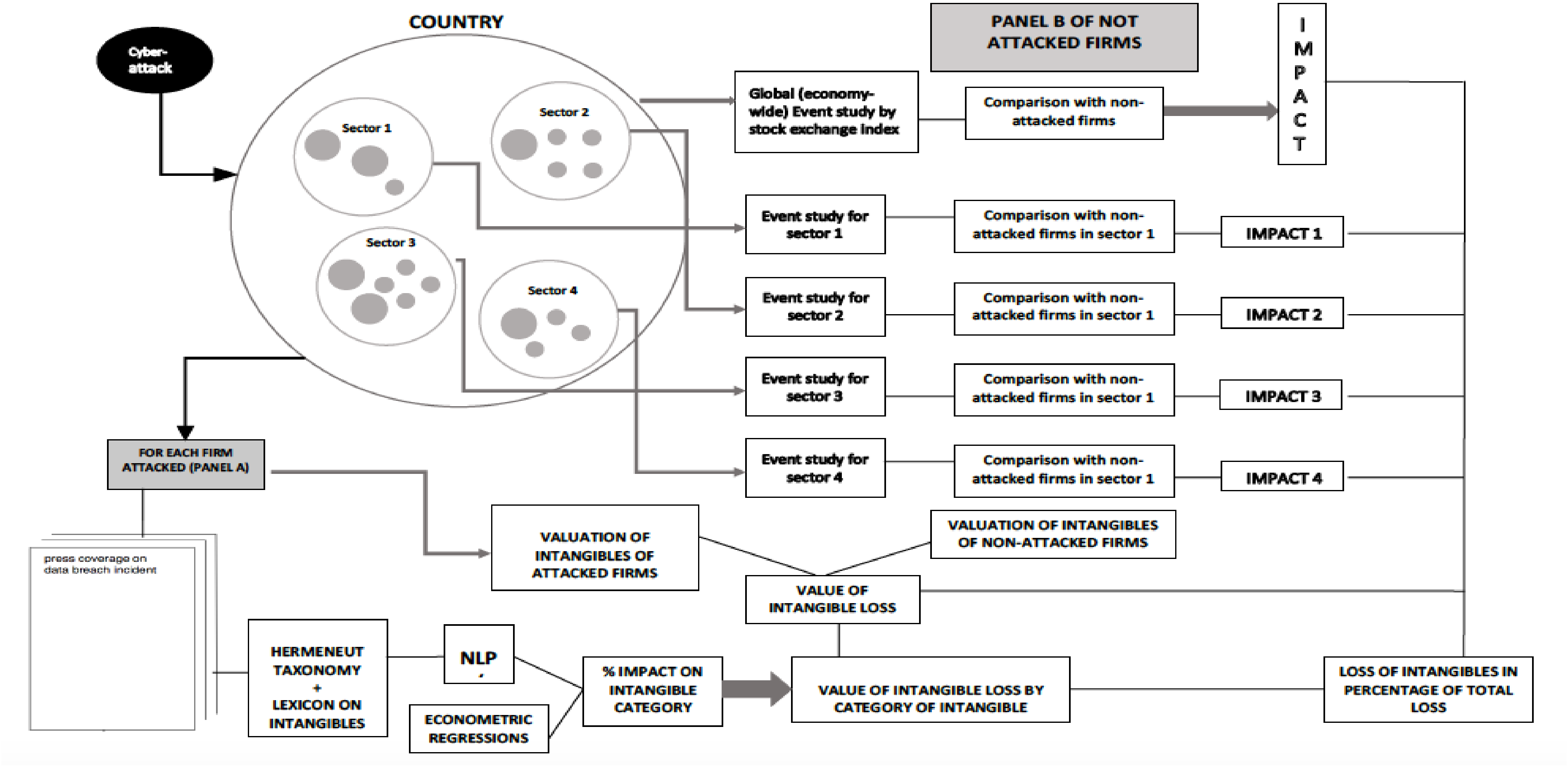
5- Intangible Asset Valuation

- We use the methodology proposed by Gu and Lev (2011) using the formula:

$$\textit{Economic performance} = \alpha \times \textit{Physical assets} + \beta \times \textit{Financial assets} + \boldsymbol{\gamma \times \textit{Intangible assets}}$$

- *Economic performance* is measured using past, present and future earnings (earning forecasts) over a 6 years period (3 years before and 3 years after)
- *Physical assets* = (property, plants and equipments + inventories - long term liabilities) * return on physical assets [7%]
- *Financial assets* = (current assets - inventories - current liabilities) * return on financial assets [5.5%]
- Use the residual method to estimate Intangible-Driven-Earnings (IDE)
- Capitalize to infinity with various growth rates according to the following sequences
  - 1-5 years(15%), 6-10 years (15%---3%), 11-inf (3%)
  - => gives a value of Intangible capital at time t

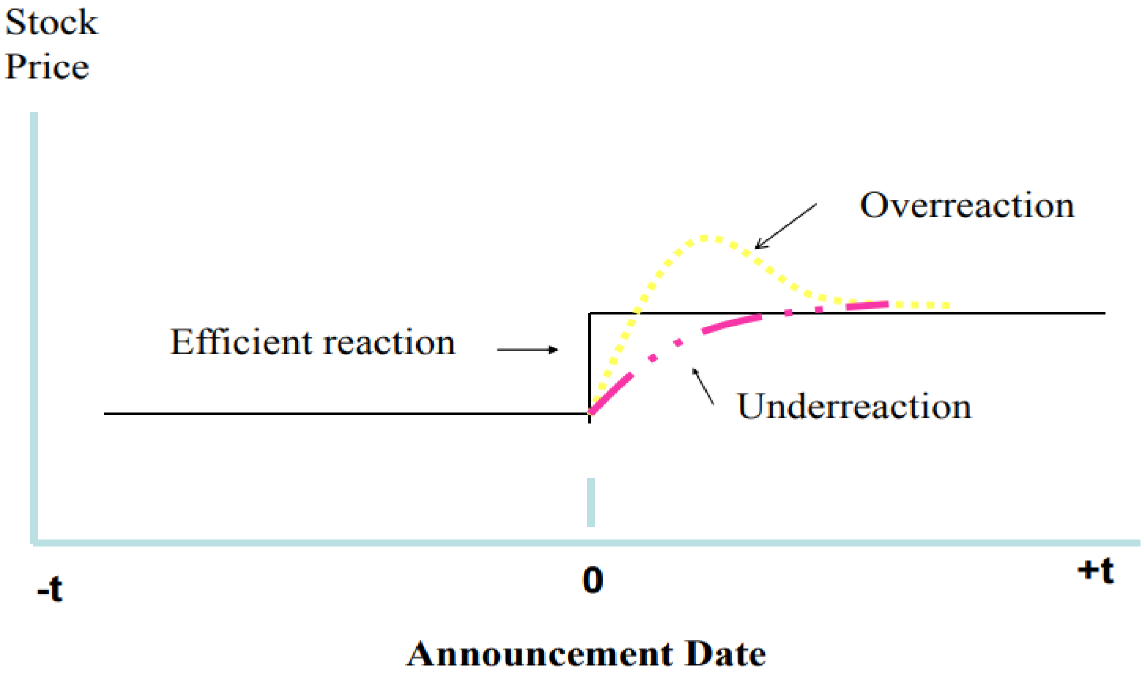
5- Intangible Asset Valuation


COUNTRY
Cyber-attack
Sector 1
Sector 2
Sector 3
Sector 4
PANEL B OF NOT ATTACKED FIRMS
Global (economy-wide) Event study by stock exchange index
Comparison with non-attacked firms
IMPACT
Event study for sector 1
Comparison with non-attacked firms in sector 1
IMPACT 1
Event study for sector 2
Comparison with non-attacked firms in sector 1
IMPACT 2
Event study for sector 3
Comparison with non-attacked firms in sector 1
IMPACT 3
Event study for sector 4
Comparison with non-attacked firms in sector 1
IMPACT 4
FOR EACH FIRM ATTACKED (PANEL A)
press coverage on data breach incident
VALUATION OF INTANGIBLES OF ATTACKED FIRMS
VALUATION OF INTANGIBLES OF NON-ATTACKED FIRMS
VALUE OF INTANGIBLE LOSS
HERMENEUT TAXONOMY + LEXICON ON INTANGIBLES
NLP
ECONOMETRIC REGRESSIONS
% IMPACT ON INTANGIBLE CATEGORY
VALUE OF INTANGIBLE LOSS BY CATEGORY OF INTANGIBLE
LOSS OF INTANGIBLES IN PERCENTAGE OF TOTAL LOSS

iC 14 Intellectual Capital for Communities In the Knowledge Economy

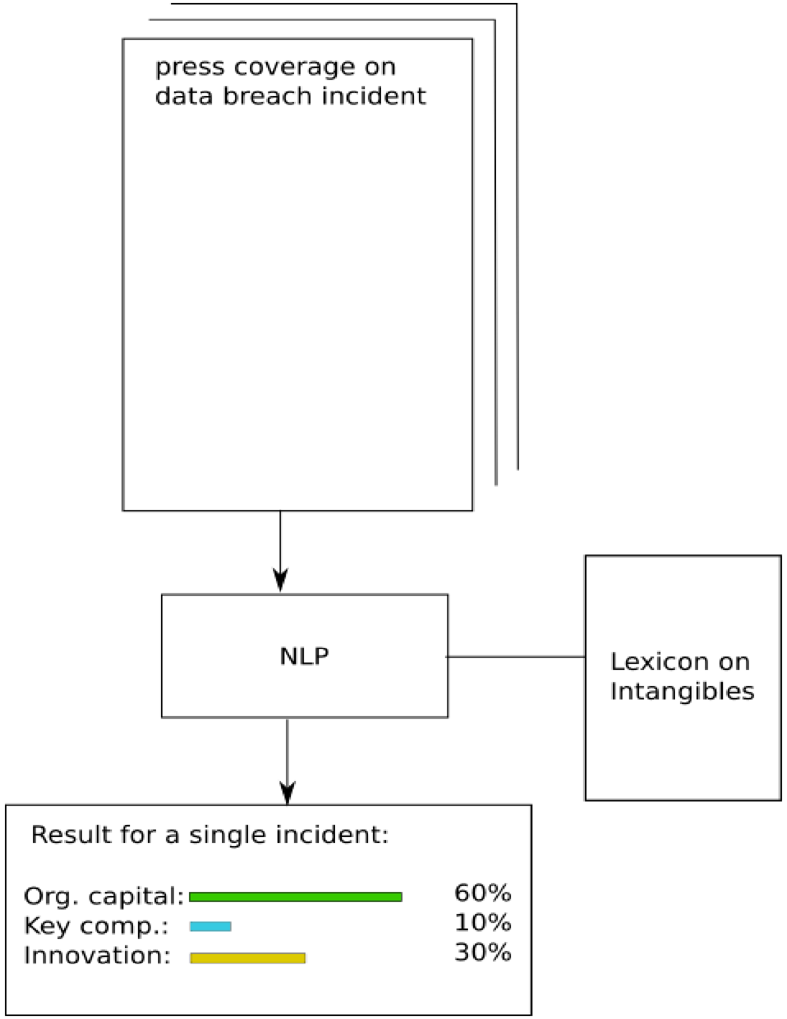
6- Micro estimates of intangibles cyber-risks: Event Study Analysis

- An event study attempts to measure the valuation effects of a corporate event, such as a merger or earnings announcement, by examining the response of the stock price around the announcement of the event.
- ***Assumption:*** Financial market efficiency (i.e. reflect all available information in an efficient and unbiased manner).

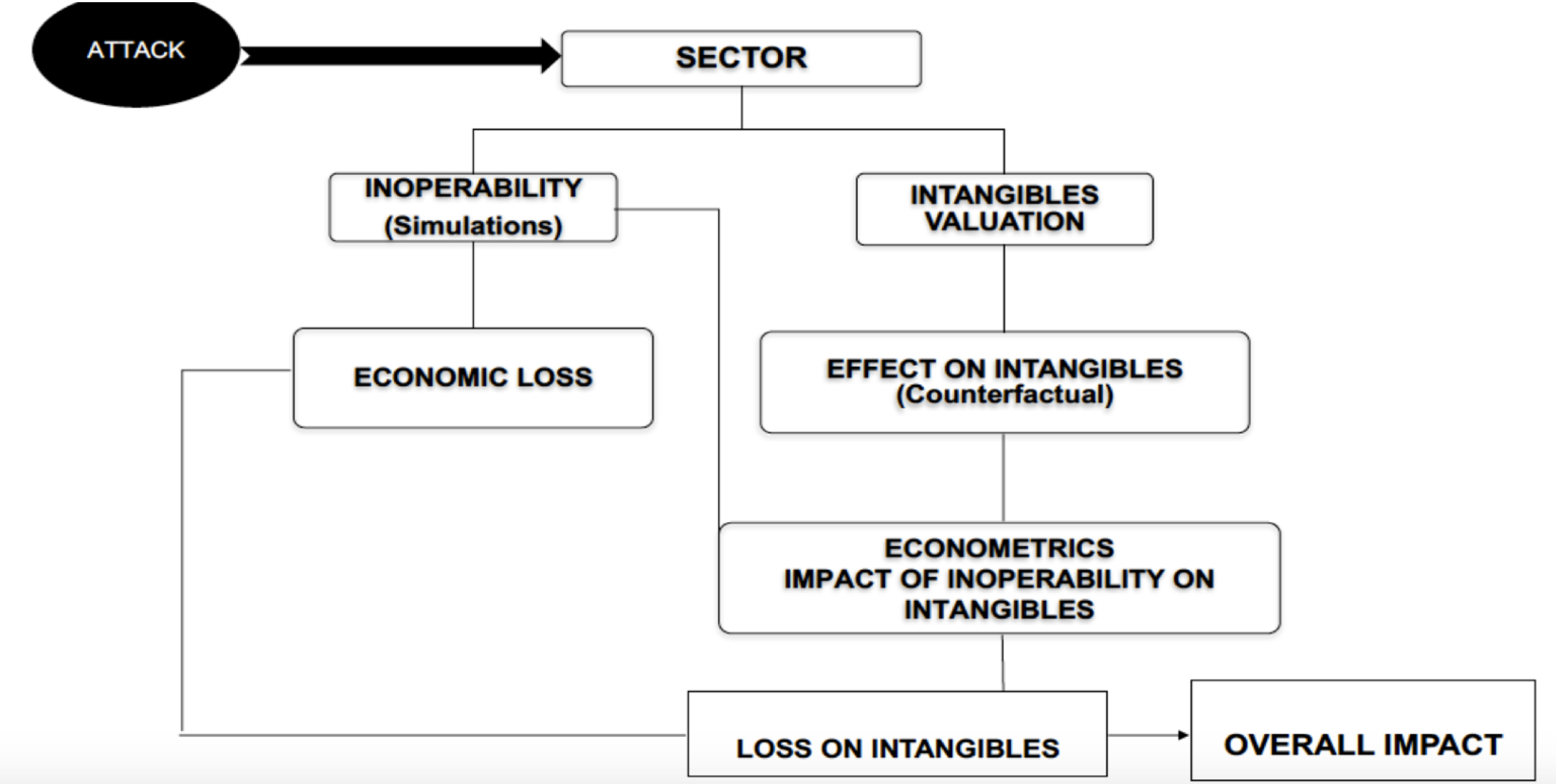


6- Micro estimates of intangibles cyber-risks: NLP Analysis

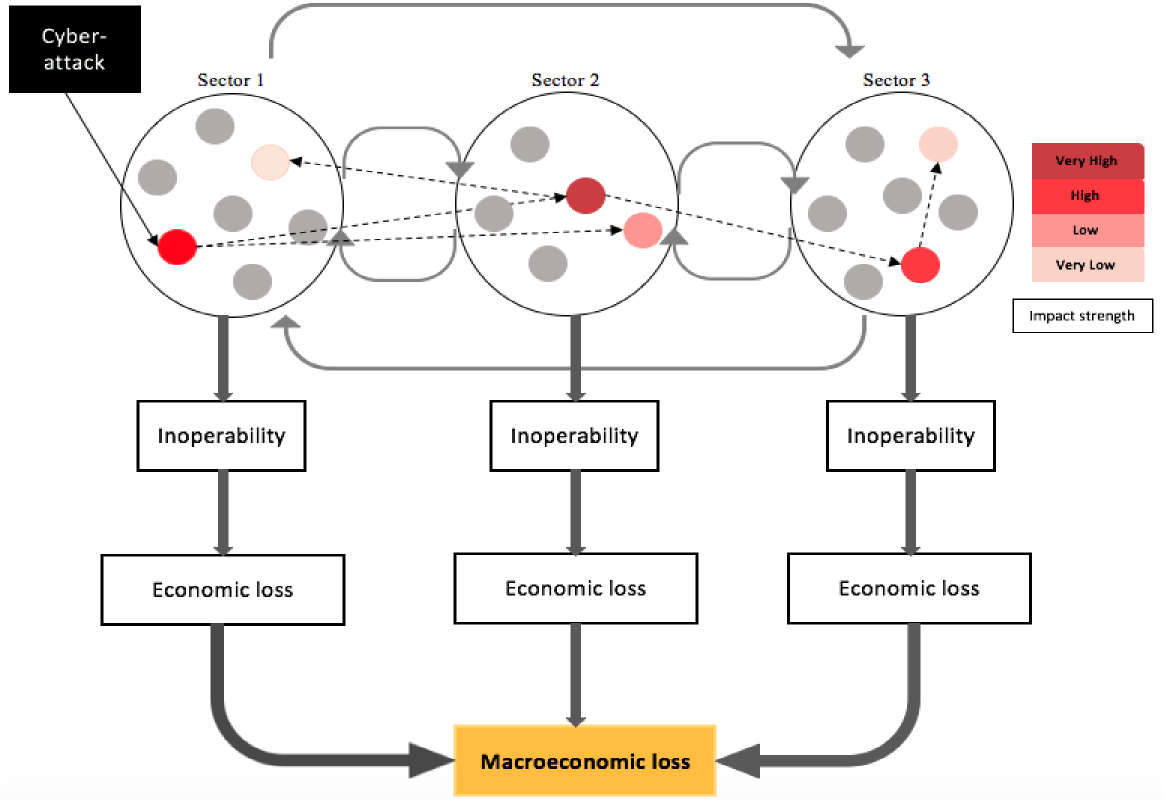
- Natural Language Processing (NLP) is carried out to understand the impact of cyber attack with respect to taxonomy of intangibles;
  - IPR and Innovation
  - Key competences and human capital
  - Organizational capital
- We uses articles which are treating the cyber-attack, published in the press and used by the cyber-event databases (Advisen and VERIS).
- The lexicon used in this study is developed by Bounfour (2007) which categorizes words by types of intangibles.



7- Macro estimates of intangibles



7- Macro estimates of intangibles: Inoperability

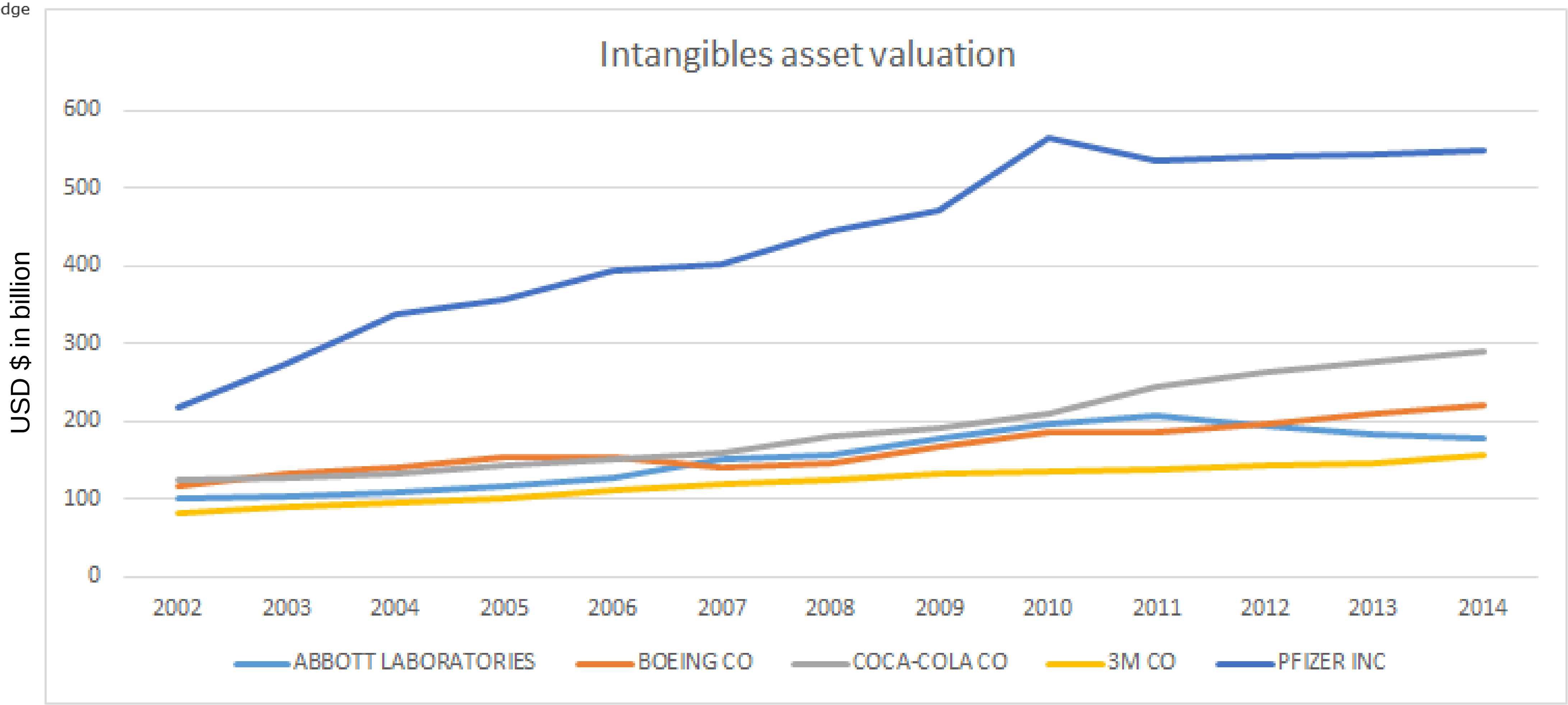


- Uses the Leontief I-O model and introduces the *Inoperability* metric
- Studies the impact of sector perturbations on terms of two metrics: inoperability and economic loss

8- Data

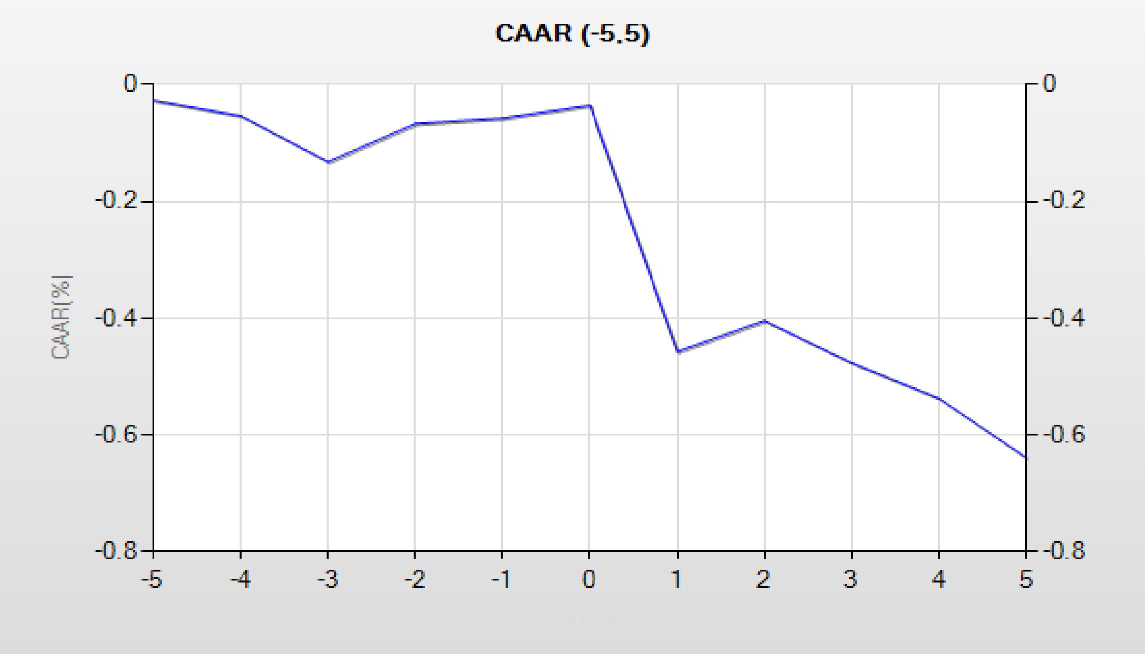
1. Cyber security event database;
    - ADVISEN Ltd. Database
    - VERIS Community Database (VCDB)
2. Compustat Database
3. World Input-Output Database (WIOD)

9- Results: Intangible valuation

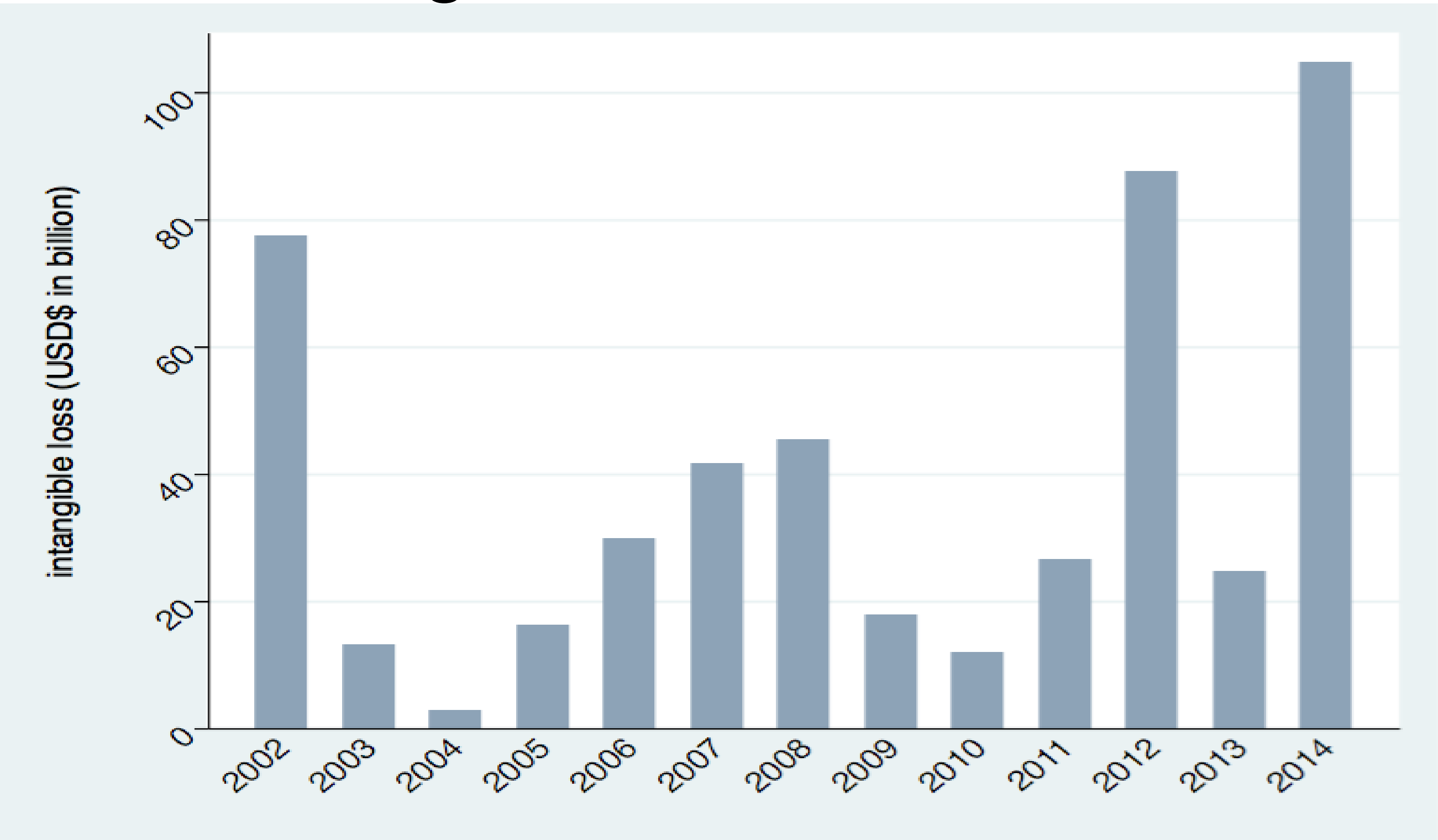


9- Results: Event Study Analysis

- The market reaction for five days before and five days after the information about a cyber-attack is disclosed.
- It is shown that the loss continues for the following 5 days.
- The estimate suggests that after an attack a firm loses around **0.6 %** of its value.

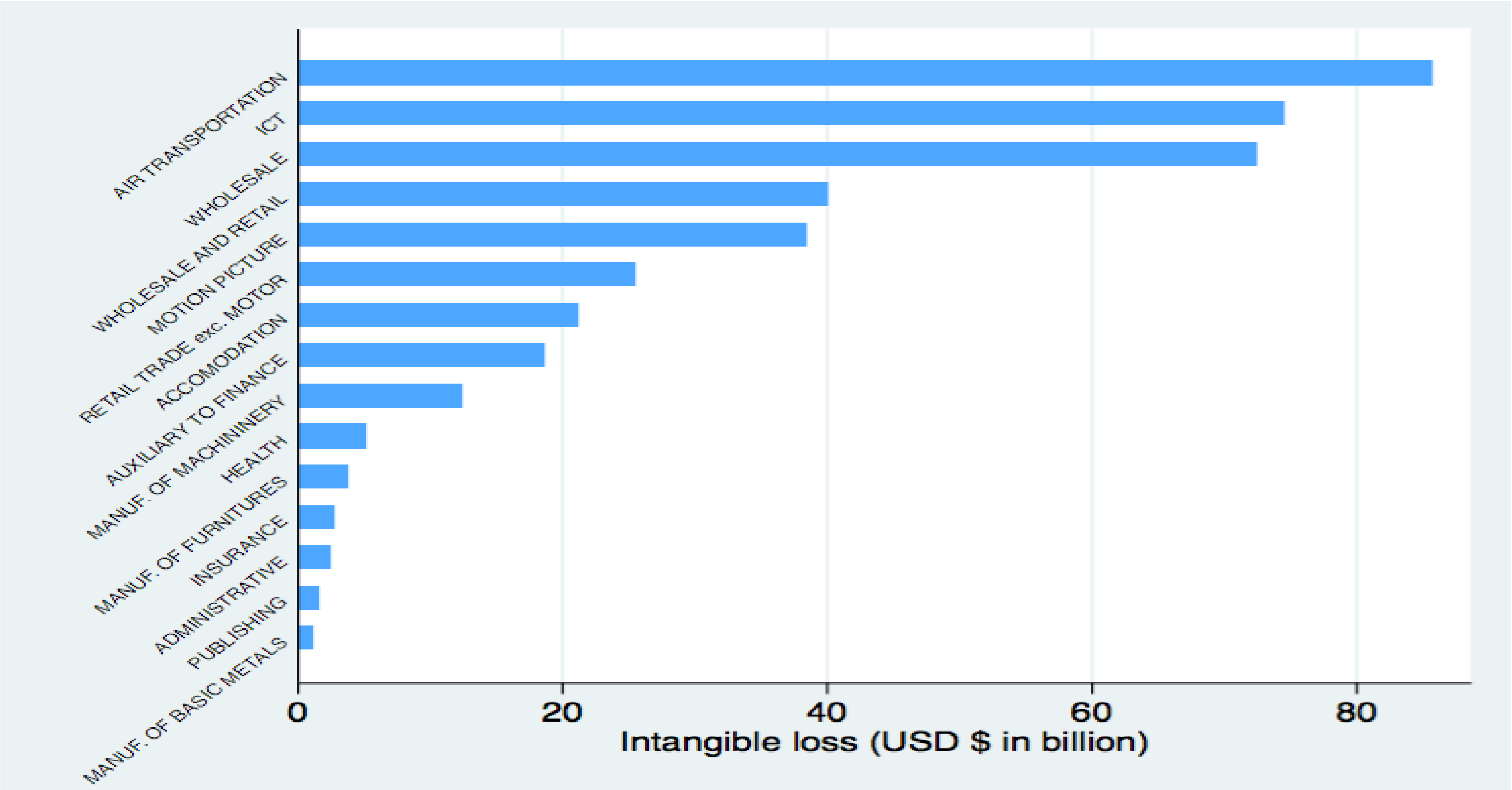


9- Results: Intangible Losses in the US



9- Results: Intangible Losses in 2013

Losses on intangibles in our sample in the ICT sector amount **USD $85.3 billion**



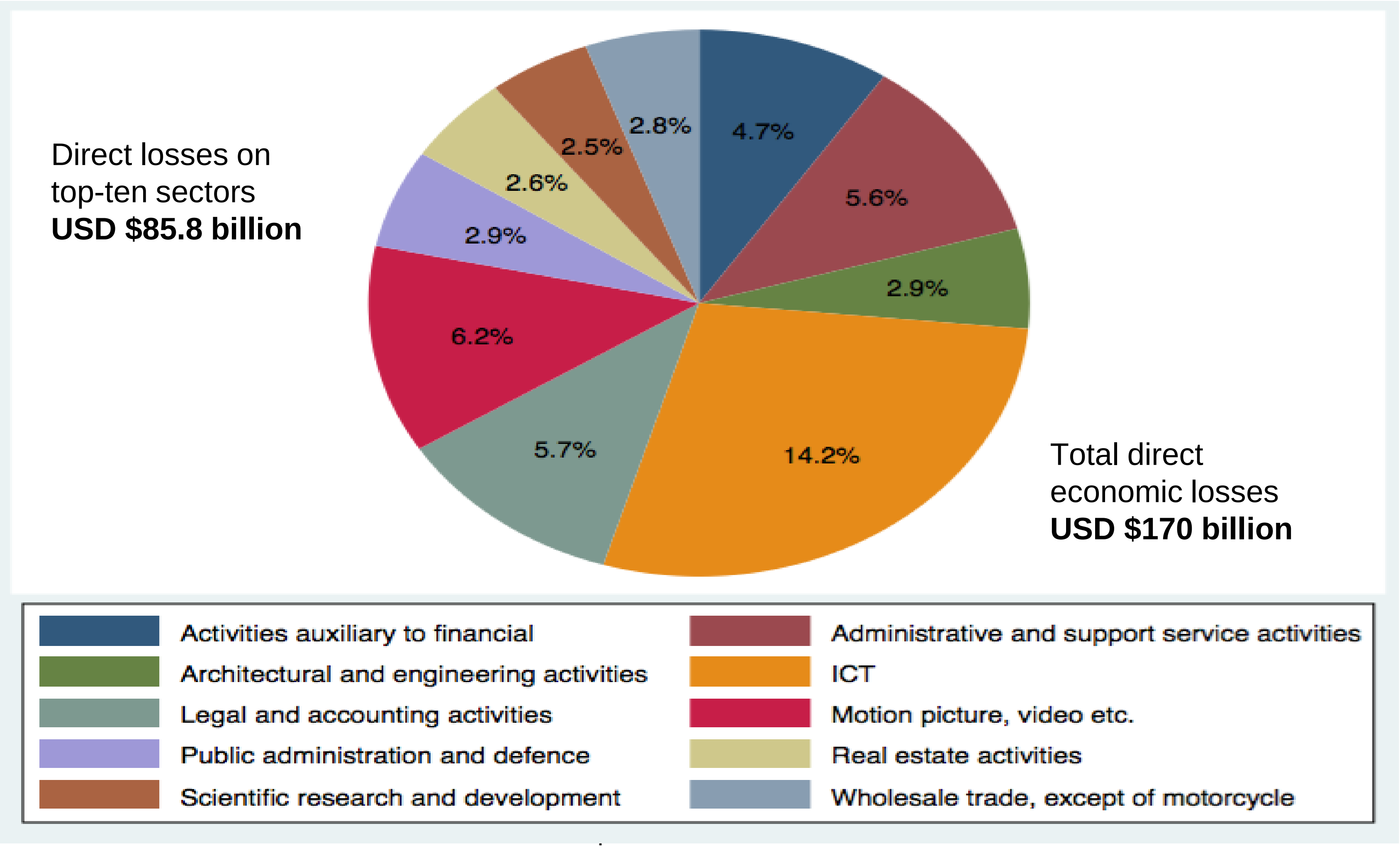
9- Results: Intangible Losses (Macro)

United States

Attacks on the ICT sector in 2013

Initial inoperability = 10%

365 Days



Direct losses on top-ten sectors
USD $85.8 billion

Total direct economic losses
USD $170 billion

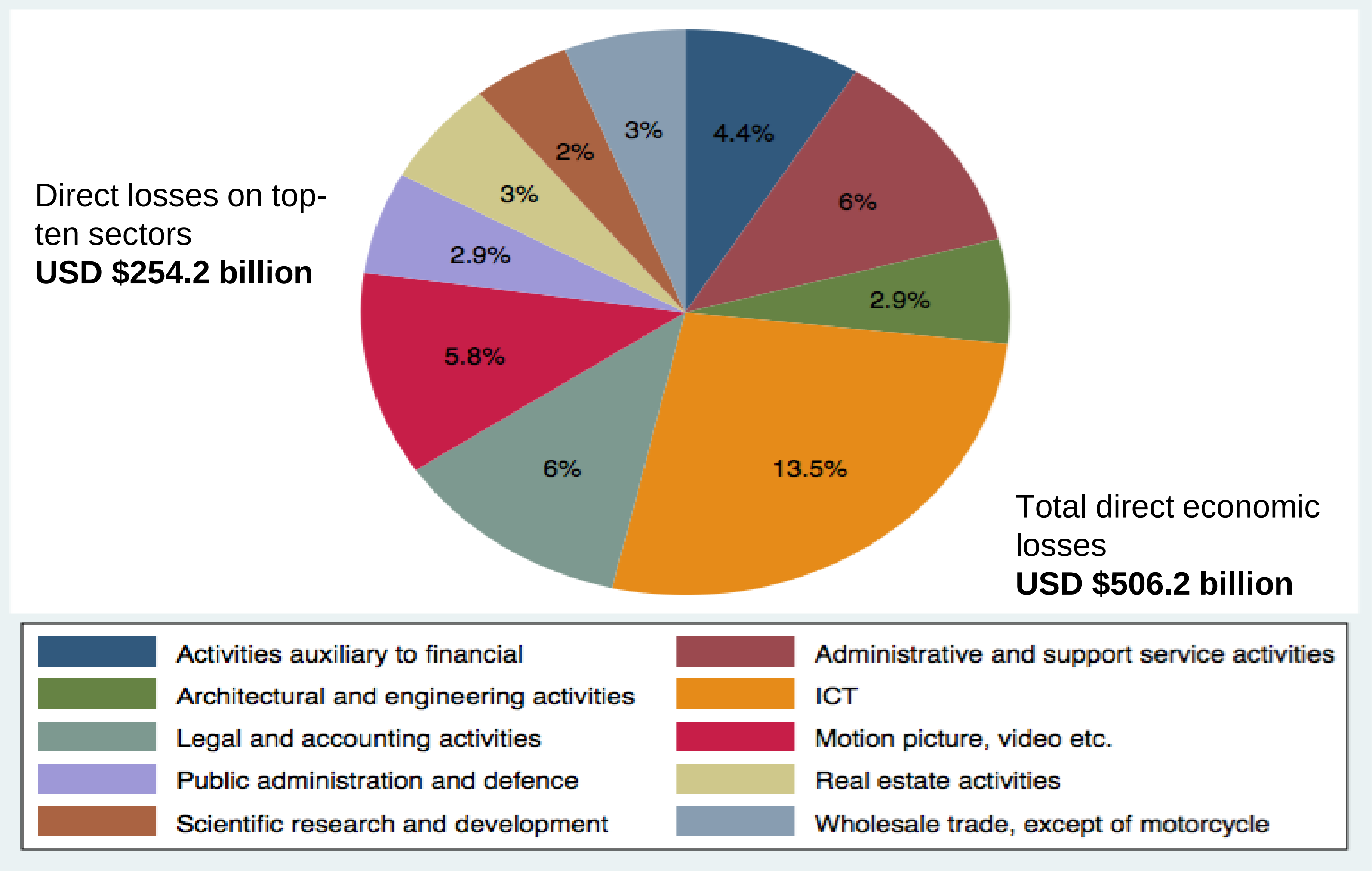
9- Results: Intangible Losses (Macro)

United States

Attacks on the ICT sector in 2013

Initial inoperability = 40%

365 Days



Direct losses on top-ten sectors
USD $254.2 billion

Total direct economic losses
USD $506.2 billion

Intellectual Capital for Communities In the Knowledge Economy

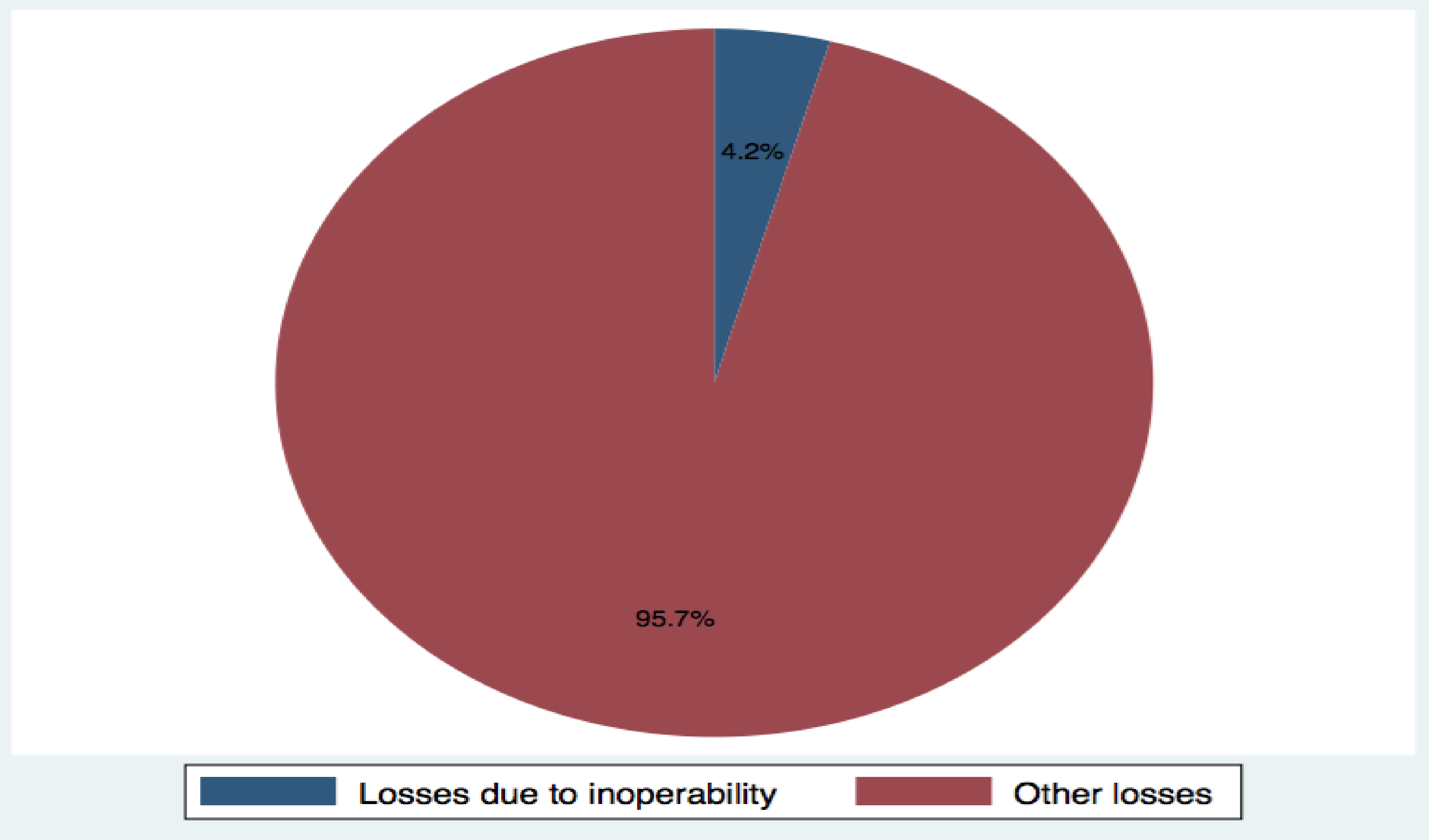
9- Results: Intangible Losses on the ICT sector in 2013

Initial inoperability = 10%

Intagible losses in our sample in the ICT sector amount **USD $85.3 billion**

Intangible losses resulting from inoperability

USD $3.5 billion



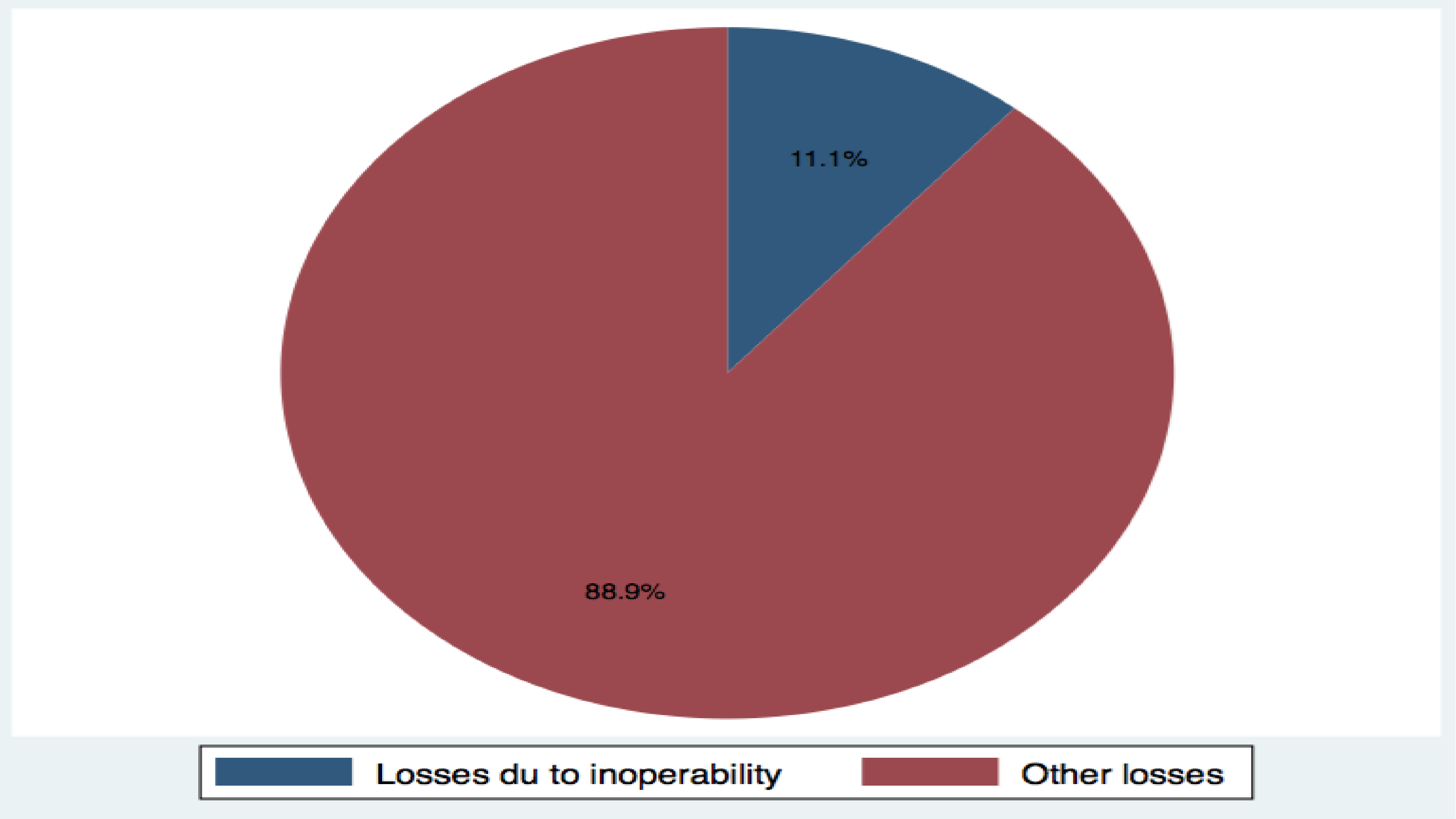
Intellectual Capital for Communities In the Knowledge Economy

9- Results: Intangible Losses on the ICT sector in 2013

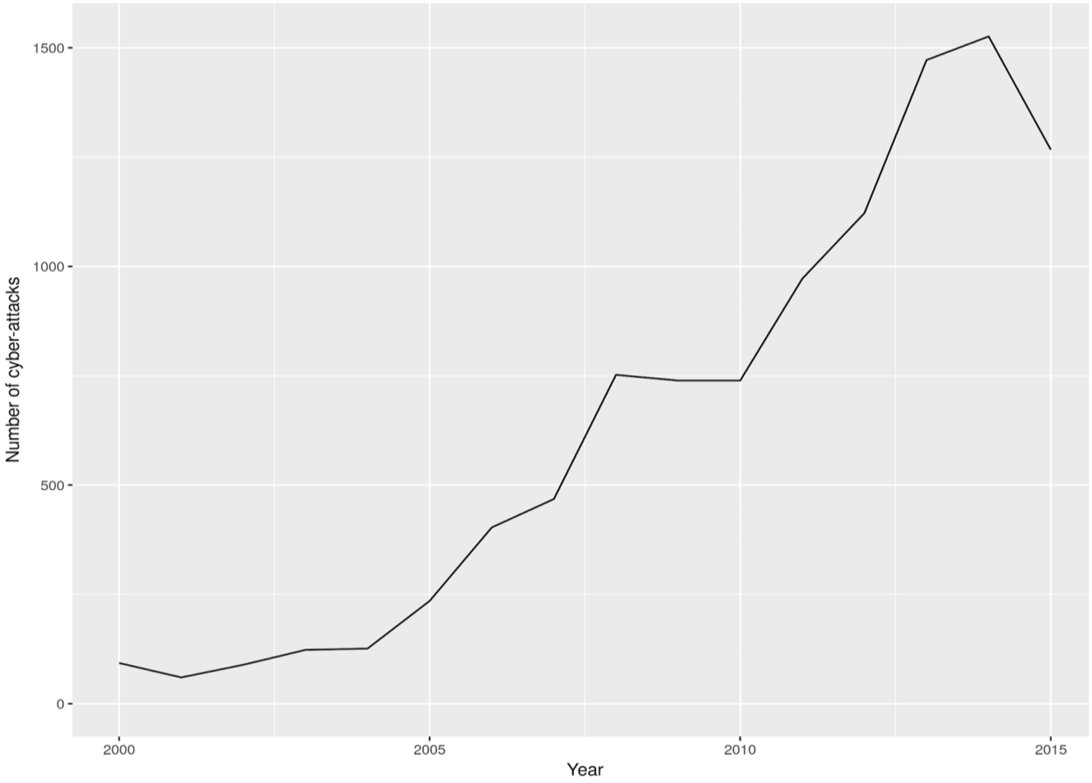
Initial inoperability = 40%

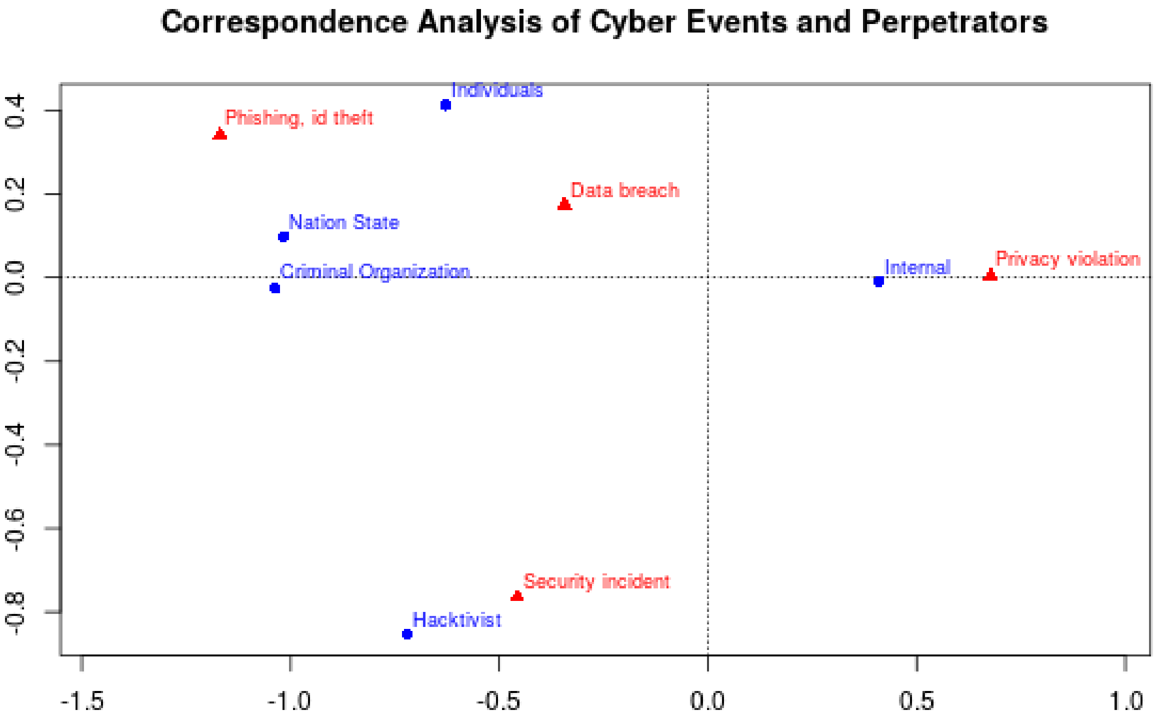
Total losses on intangibles in our sample in the ICT sector amount **USD $85.3 billion**

Intangible losses resulting from inoperability **USD $9.4 billion**



9- Results: Business Models of Cyber-Attacks




Correspondence Analysis of Cyber Events and Perpetrators

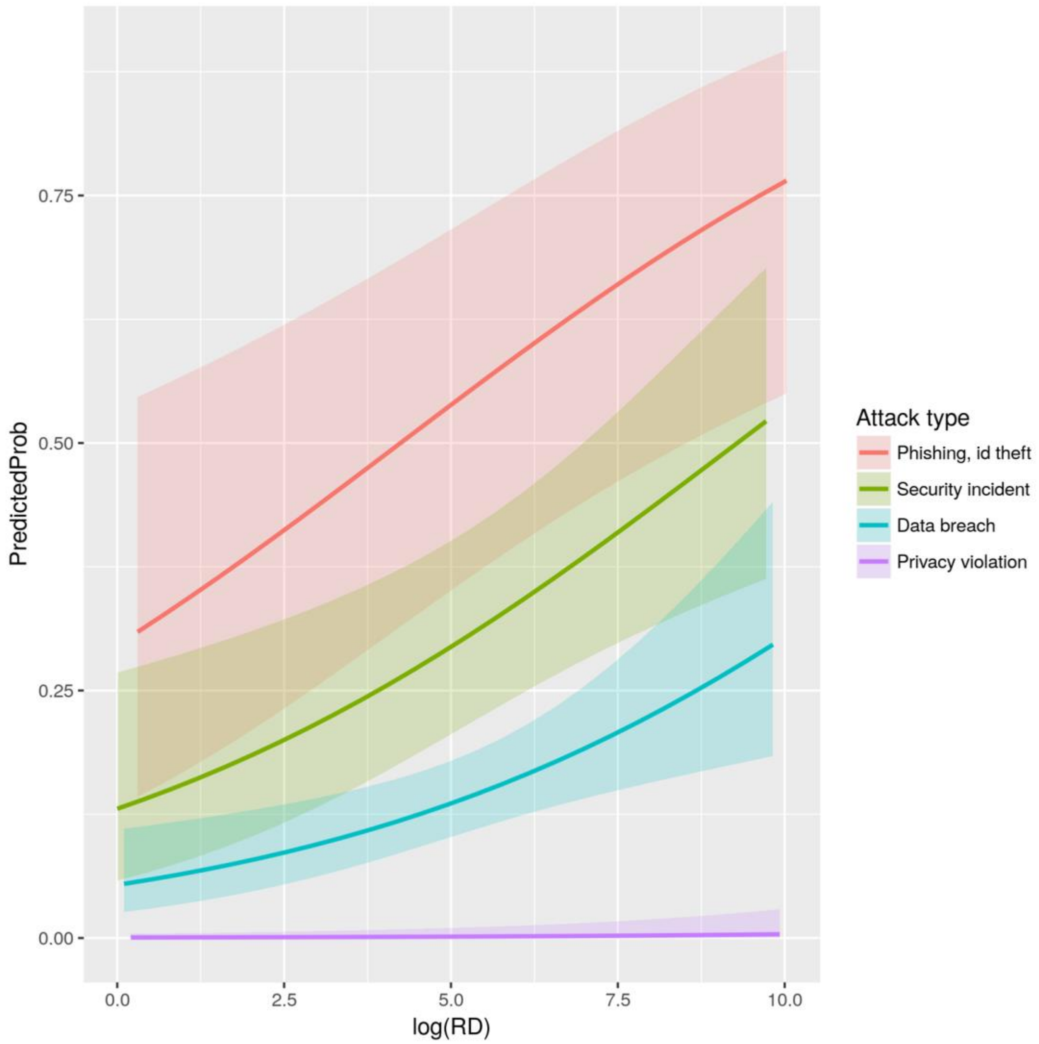
9- Results: Business Models of Cyber-Attacks

- A cyber-attack perpetrator is in general unknown (**43.1%** in Advisen database)
- However, the type of attacks and several firm characteristics are known.
  - the size of the firm (number of employee, EMP)
  - firms’ IP intensivity measured by R&D expenditure (RD)
  - firms’ total asset (ASSET.TOTAL)
  - firms’ selling, general and administrative expenses (XSGA)
- We aim to determine the type of perpetrator (Individual or Organization), with the following logit model;.

PERPETRATOR = ATTACK_TYPE + log(EMP) + log(RD) + log(ASSET.TOTAL) + log(XSGA)

9- Results: Business Models of Cyber-Attacks

- The predicted probability of a cyber-attack with respect to firms’ R&D expenditure shows that there is an increasing probability that the attack is committed by an organization which uses various attack types.
- Overall results show that the prefered attack types of organizations are
  - Phishing and ID theft
  - Security incident
  - Data breach
  - Privacy violation



Thank you!

ahmed.bounfour@u-psud.fr