# The price of cyber (in)security: evidence from the Italian private sector

Claudia Biancotti
Bank of Italy, Directorate General for Economics, Statistics and Research

Insurtech – Rome, December 15, 2017

# Outline

- The cybersecurity data gap
- Data collection at the Bank of Italy
- Expenditure on security
- Frequency of attacks
- Cost of attacks
- Preliminary evidence on cyber insurance

# The cybersecurity data gap (i)

- «[N]o point of cyberspace can be absolutely secure as long as cyber threats persist in the surrounding environment; our drive to strengthen the financial system against cyber attacks can achieve maximum results only if accompanied by measures that reduce the level of insecurity in cyberspace as a whole. In turn, economy-wide policies must be based on reliable, impartial, comprehensive and widely accessible data»

G7 finance ministers and central bank governors, final communiqué of the Bari meeting, May 2017

# The cybersecurity data gap (ii)

- Major obstacle to policy design: lack of reliable, independent data
  - Popular surveys on cyber attacks run by commercial entities (conflict of interest)


- OECD: lack of data significant issue in the design and pricing of insurance policies

- Official statistics on frequency and economic impact of cyber attacks only available in the UK (Cyber Security Breaches Survey since 2016)

# Data collection at the Bank of Italy

- BoI business surveys: sample comprising about 4,000 industrial and non-financial services firms with 20 employees or more
  - statistically representative by macro-region, size class and certain aggregations of NACE Rev.2 sectors at the two-digit level

- Routinely used in academic research; data freely available through remote access portal; fully documented methodology

- First batch of cybersecurity questions in September 2016

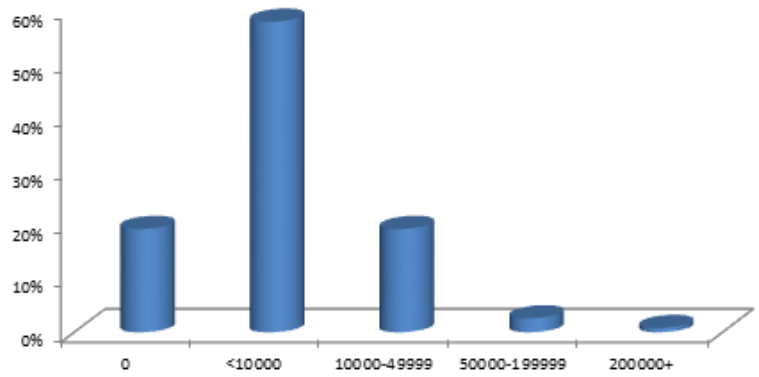
- Topics covered so far:

  - defensive measures deployed
  - expenditure on security
  - frequency of attacks
  - cost of attacks
  - insurance uptake

# Expenditure on security

- Relatively modest (overall median in 2016: €4,530, or 15 per cent of typical worker's annual gross wages)

**Firms' expenditure on cyber defence, 2016**
*(percentages of firms; expenditure brackets in euros)*




- High cross-sector variability: €19,080 for ICT firms, €3,420 for low-tech firms
- Cybersecurity training and vulnerability analysis more popular than encryption. Vendor-driven market?

# Frequency of attacks

Share of Italian manufacturing and non-financial services firms hit by at least one cyber attack that imparted damage, September 2015-September 2016

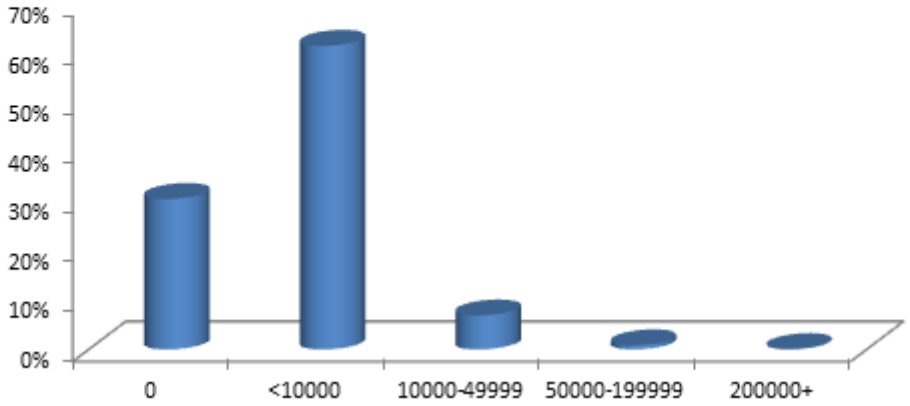
| | *Original data* | *Imputed data* |
|---|---|---|
| **Geographical area** | | |
| *North-West* | 28.5 | 44.2 |
| *North-East* | 32.5 | 47.3 |
| *Centre* | 35.3 | 52.3 |
| *South and Islands* | 24.4 | 35.9 |
| **Number of employees** | | |
| *20 – 49* | 29.2 | 42.7 |
| *50 – 199* | 31.3 | 48.4 |
| *200 – 499* | 36.7 | 56.0 |
| *500 and over* | 34.8 | 62.8 |
| **Tech / knowledge intensity** | | |
| *High and medium-high* | 30.5 | 48.8 |
| *Low and medium-low* | 30.1 | 43.8 |
| **Exports as share of turnover** | | |
| *Less than 1/3* | 29.4 | 43.0 |
| *Between 1/3 and 2/3* | 34.6 | 51.8 |
| *Over 2/3* | 29.0 | 48.5 |
| **Total** | **30.2** | **45.2** |

# Cost of attacks

- Large majority <€10,000, 1 per cent >€50,000
- 70 per cent report business interruption and r&r working hours

**Monetary costs of all cyber attacks suffered in 2016, at the firm level**

*(percentages of firms that reported an attack; cost brackets in euros)*



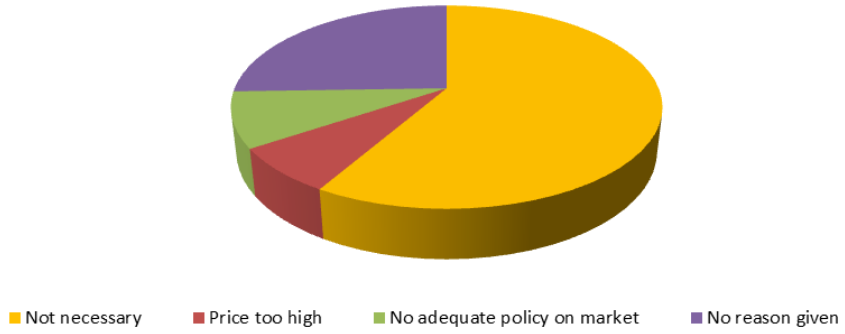

- We know from other sources that large incidents exist, but the sample is not geared towards tail events
- Large incidents are key in quantifying impact on economy: research project for 2018

# Insurance (i)

**Prevalence of cyber insurance, by technological intensity of activity sector, September 2017**
(*share of firms*)

| | *No* | *Yes, stand-alone* | *Yes, part of broader policy* |
|---|---|---|---|
| *ICT* | 59.3 | 13.5 | 27.2 |
| *High-tech, non-ICT* | 78.2 | 7.2 | 14.6 |
| *Low-tech* | 81.5 | 4.8 | 13.7 |
| **Total** | **79.8** | **5.7** | **14.5** |

**Reasons for not buying cyber insurance, September 2017**
(*share of uninsured firms*)



# Insurance (ii)

- 12.9 per cent of firms in the universe were interested in insurance, yet didn't have any coverage

- Rationing and adverse selection are a possibility:

- *firms that reported an attack in previous surveys were less likely than others to have insurance, but more likely to have investigated possibilities without finding a solution*

- *attack history, however, is not guaranteed to be a good proxy of risk, as victimization has been shown to incentivize security investment*

Thank you for your attention!