EEF.NGO/14/18
6 September 2018

ENGLISH only

Organization for Security and Co-operation in Europe
Secretariat

Conference Services

DISCLAIMER

The OSCE Secretariat bears no responsibility for the content of this document and circulates it without altering its content. The distribution by OSCE Conference Services of this document is without prejudice to OSCE decisions, as set out in documents agreed by OSCE participating States.

EEF.NGO/14/18
6 September 2018

ENGLISH only

BANCA D'ITALIA
EUROSISTEMA

Measuring cyber (in)security

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

September 6, 2018
26th OSCE Economic and Environmental Forum, Prague

BANCA D'ITALIA
EUROSISTEMA

The cybersecurity data gap

- «[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 2017 ITALIA

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

Addressing the data gap: an example from Italy

A first response to the data gap for Italy: two questions in the Bank of Italy's 2016 Business Outlook Survey of Industrial and Nonfinancial Service Firms

Cybersecurity section
1. In your firm, cybersecurity is…
1 = Handled by internal resources; 2 = Outsourced to an external company, belonging to the same group; 3 = Outsourced to an external company, not belonging to the same group; 4 = Partly handled by internal resources, partly outsourced; 5 = Not applicable, as no cybersecurity activities exist; 9 = I don't know / I refuse to answer
2. The number of cyber attacks against firms, including small and medium ones, is increasing. Over the last year, how many times were you hit by a cyber attack? Only consider the attacks that had consequences, no matter how limited and/or short-lived and/or easily reversible, on the functioning of the firms' systems and/or on the integrity and confidentiality of data therein stored.
1 = No attacks; 2 = One attack; 3 = Between 2 and 5 attacks; 4 = Between 6 and 10 attacks; 5 = More than 10 attacks; 9 = I don't know / I refuse to answer

Frequency of attacks

Firms hit by at least one cyber attack: data corrected for misdetection, reticence
(percentages; estimates on full sample)

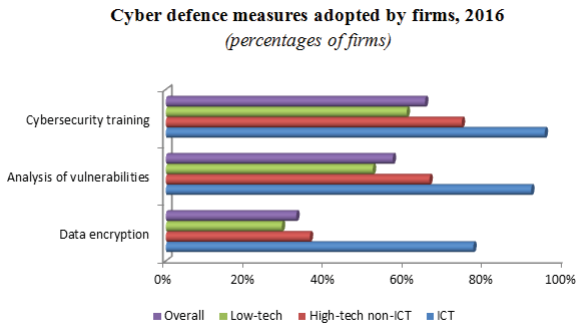
	Share of firms	*Total correction (percentage points)*	*Misdetection (share of total correction)*	*Reticence (share of total correction)*	*Share of employees*
Geographical area					
North-West	44.2	15.7	40.1	59.9	54.8
North-East	47.3	14.8	28.4	71.6	57.5
Centre	52.3	17.0	35.9	64.1	63.9
South and Islands	35.9	11.5	51.3	48.7	42.6
Number of employees					
20 – 49	42.7	13.5	43.7	56.3	44.0
50 – 199	48.4	17.1	35.1	64.9	48.2
200 – 499	56.0	19.3	7.3	92.7	56.2
500 and over	62.8	28.0	7.5	92.5	67.6
Tech / knowledge intensity of sector (*)					
High and medium-high	48.8	18.3	33.9	66.1	62.7
Low and medium-low	43.8	13.7	39.4	60.6	52.4
Exports as share of turnover					
Less than 1/3	43.0	13.6	40.4	59.6	55.1
Between 1/3 and 2/3	51.8	17.2	35.5	64.5	59.2
Over 2/3	48.3	19.5	28.2	71.8	57.6
Total	**45.2**	**15.0**	**37.3**	**62.7**	**56.0**

(*) High and medium-high: manufacturing firms with high or medium-high technological intensity, and service firms with high knowledge intensity, according to OECD/Eurostat classification. Low and medium-low: all other firms. Firms in the energy sector, not covered by the original classification, are reclassified as high-technology.

More questions (2017)

Cybersecurity Section
1. Does your firm adopt any of the following cybersecurity measures? (y/n)
a) Use of security hardware / software (e.g. anti-virus, firewall) b) Cybersecurity training for employees c) Data encryption, total or partial d) Analysis and management of vulnerabilities in the firm's IT systems
2. In 2016, approximately how much did you spend to prevent cyber attacks?
3. In 2016, were you hit by a cyber attack?
4. At least one of these attacks implied… (y/n) a) Interruption of ordinary business activities? b) Extra working hours to recover from technical damage and/or manage stakeholder communication? c) Theft or destruction of data, including intellectual property
5. In 2016, what was the approximate monetary value of the damage done by these cyber attacks?
6. Did you adopt extra cybersecurity measures as a consequence of these attacks?

Defensive measures

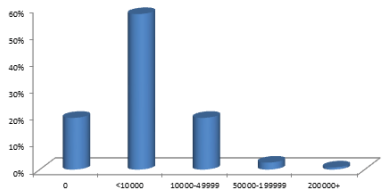


- Cybersecurity training and vulnerability analysis more popular than encryption. Vendor-driven market?

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)

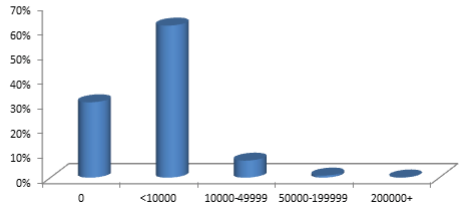


- High cross-sector variability: €19,080 for ICT firms, €3,420 for low-tech firms
- Southern Italy lags behind the rest of the country: median expenditure €2,700

Cost of attacks (and more measurement challenges)

- 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 2018-2019

BANCA D'ITALIA
EUROSISTEMA

Thank you for your attention!