The Need for and the Making of Cyber Insurance

CSP Forum – 27 April 2015
Stefano Nanni
R&D – www.unipol.it
The Risk

• There are two types of CEOs...

• Global impact of criminal cyber activity up to 1 trillion US$ (McAfee)

• Digital, information society, cyber physical systems

• Customers are asking insurers

• Confidentiality, integrity, availability

• First or third party losses
Banking and Finance

• 2012 “Improving NIS in the EU” public consultation: 91.1% of respondents thought it would be important to adopt NIS requirements

• Inconsistent requirements across the EU

• ENISA on regulation, supervision and cloud adoption

• NIS Directive valuable, proportionality is crucial
Cyber Insurance

- Uneven preparedness, culture, practices
- Insurance as an incentive, to bear costs and provide services
- Still limited market, particularly in the EU
- Insurability problems: evolving technology, lack of randomness and missing data
- Possible initiatives around data collection, information sharing, risk assessment frameworks
Technical Mentality Talking?

• ... *Bruce Schneier in 2001*

• Rely on the market to develop

• Insurers to talk to technology experts and industrial Risk Managers

• Need legal certainty, particularly on liability, and standardization