Commonality of risk assessment language in cyber insurance – Study Findings

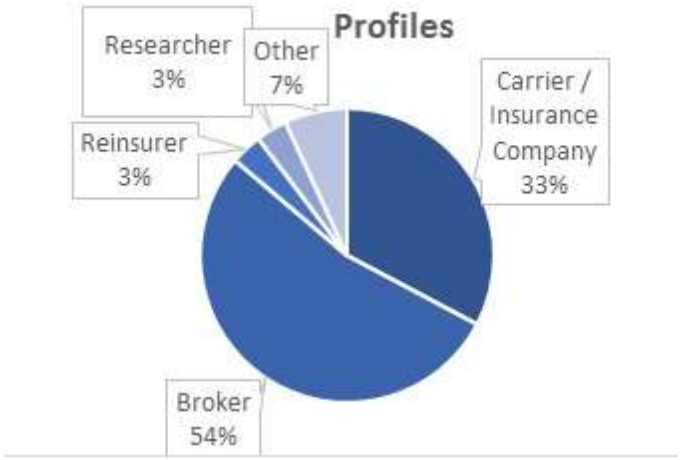
Dr. Athanasios Drougkas | Officer in NIS | ENISA

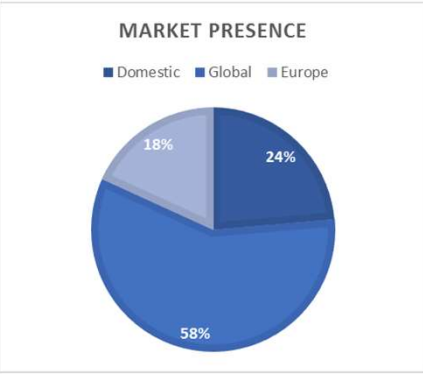
Cyber Insurance Validation Workshop | Brussels | 6th October

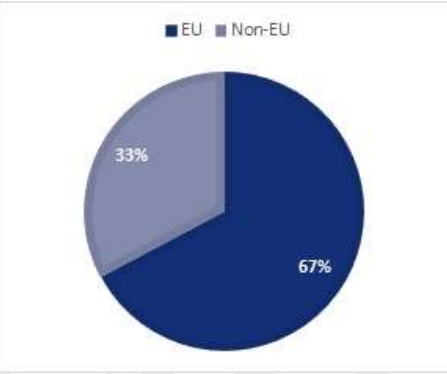
European Union Agency for Network and Information Security

Study Methodology & Demographics

- Desk research
- Commercial Documents
  - *Underwriting questionnaires*
  - *Policies*
- Interviews (19)
- Online Survey (39)
- ANOVA

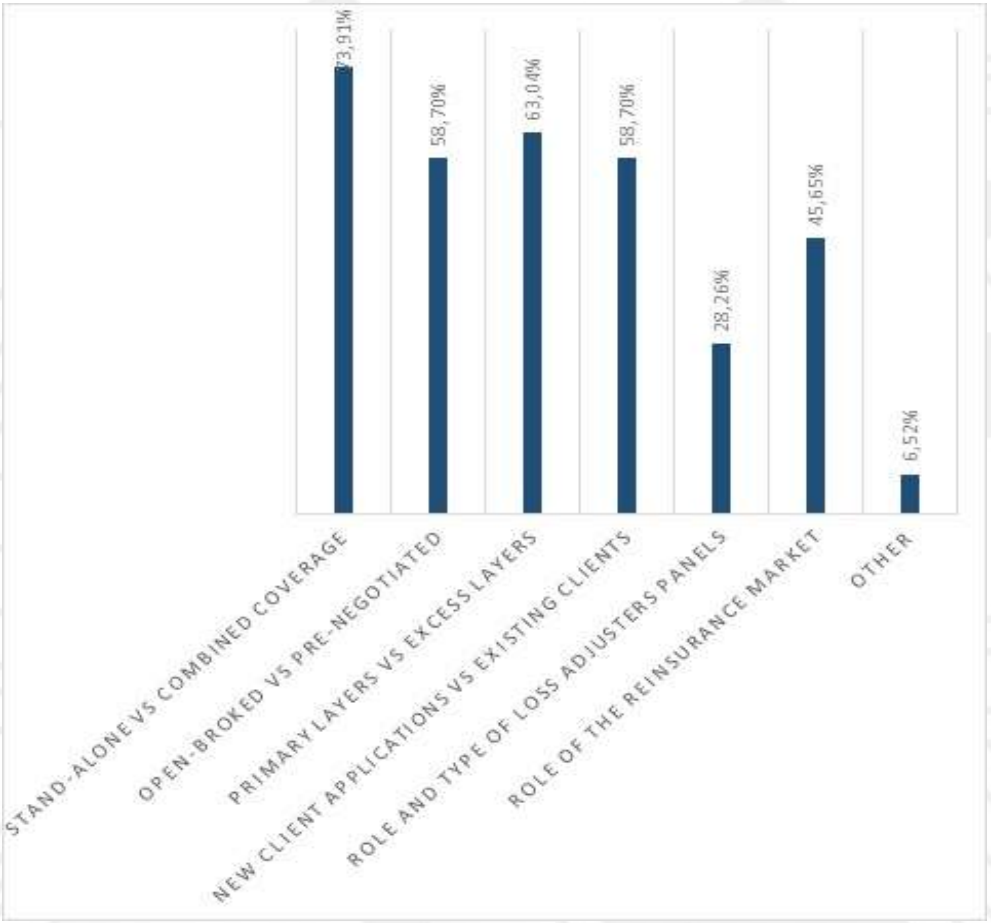




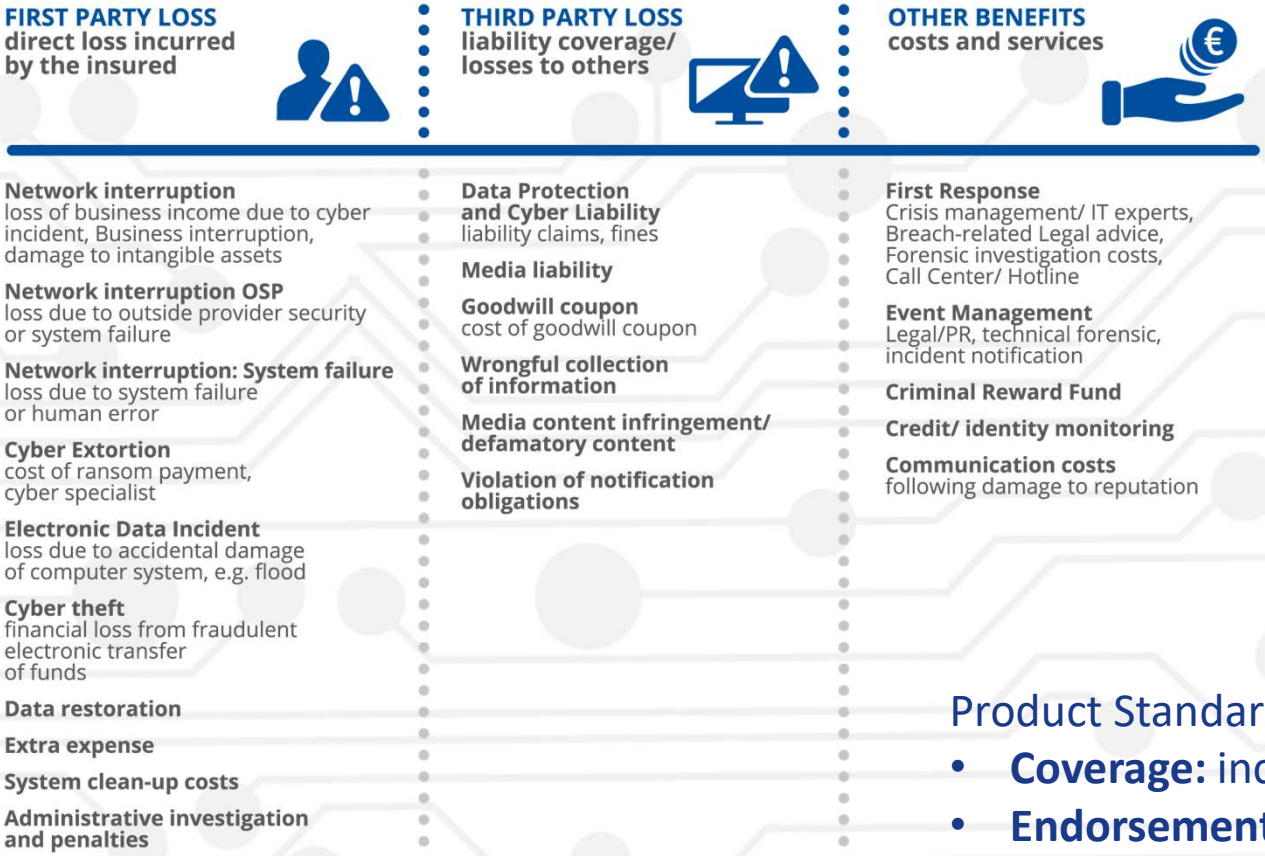


Underwriting Methods

- underwriting questionnaire – long form
- underwriting questionnaire – short form
- client meeting
- desk research
- threat intelligence
- open source intelligence (OSINT)
- risk audit or risk reports



Coverage Types



Product Standardisation

- **Coverage:** included in standard offer
- **Endorsement:** specific change to coverage
- **Extension:** optional at additional cost

Risk Assessment Language in the Cyber Insurance application process

Risk Assessment Language in Cyber Insurance

Language Harmonisation focus

- The **Underwriting Questionnaires**, i.e. what questions are asked of the insured to collect information about the risk assessment process.
- The **Cyber Insurance Coverage**, i.e. how are coverage components defined in insurance policies.

Security Standards and Cyber Insurance

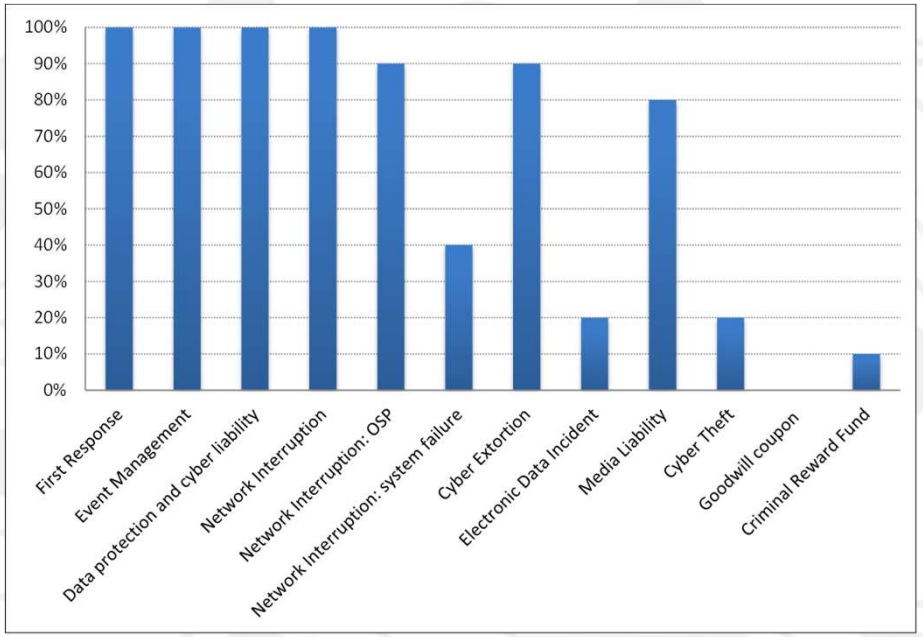
- Used as an **indicator of the insured party's cybersecurity maturity** and awareness
- Used as **reference points** by insurance carriers to support their risk assessment process
- Questions regarding compliance with such standards are often part of the underwriting process
- Questions regarding relevant security controls are typically part of the underwriting questionnaire
- Frequently used standards include **ISO 27001/2**, **NIST**, **COBIT 5**, **NCSC** and industry-specific standards such as **PCI/DSS**
- **No consensus security standards** adopted across the cyber insurance industry leading to varying underwriting questions
- Two insurers may ask **different underwriting questions** even when using the same standard to conduct risk assessment

Underwriting Information Language

- Cyber insurance underwriting is not uniform and entirely different questions may be posed to asses the same risk factor. Overall, analysis showed:
  - Different questions per carrier
  - Different definitions for similar risk areas
  - Overlapping questions for key risk areas
  - Consistent reference to cybersecurity principles
- However, the different questions cover the **same major security categories**
- Certain questions are asked by the vast majority of insurers (e.g. "*Do you have a Business Continuity plan?*")
- Little harmonization between the questionnaires and the cyber security standards
- Differences exist in application processes and forms, risk assessment methodologies and risk acceptance criteria
- Insurers who have **rich information from claims history** adapt their questionnaire to focus on mitigating those risk where they historically have had most claims
- Analysing loss scenarios and claim statistics did not reveal significant correlation with underwriting questionnaires and other type of risk assessments so far

Insurance Coverage Language

- The types of coverage insurers are offering is generally harmonized but the **policy wording itself is different** across the board
- Insurance coverage typically is not conditional to compliance with a certain security standard
- Much of the risk assessment is reflected in the coverage components that cyber insurance provides
- Insurers compete on both price and the coverage they offer but competition on coverage in most type of insurances is actually in the details not so much on what type of risks to cover



Percentage of carriers offering cyber coverage

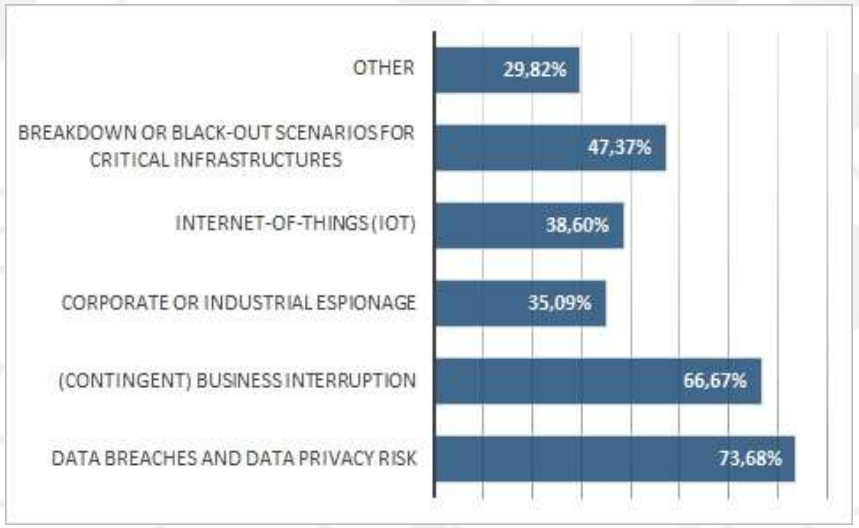
Industry Practices – Cyber Insurance Coverage Offerings

- **Types of Coverage**
  - Most insurers offer standard coverage
  - Larger insurers can offer more customised solutions, while smaller ones tend to offer more standardized products
- **Types of Customers**
  - Larger organisations favour bespoke solutions supported by internal Risk Management teams
  - SMEs favour standardized products and added value offerings (e.g. Incident Response)
- **Business Sectors covered**
  - All business sectors covered with a few exclusions due to high risk (e.g. FIs) these require more comprehensive underwriting information
  - Increasing interest from retail (GDPR)
  - Need to develop IoT and ICS/SCADA
- **Geographical Coverage**
  - Geographical Coverage
  - Mostly global coverage with independent focus on more mature markets (e.g. USA, Canada)
  - Product localisation - difference in wordings
  - Modular approach to meet specific market needs

Industry Practices – Cyber Insurance Coverage Offerings

Harmonisation aspects

- Lack of common framework for minimum requirements
- "Value judgement" models over more mature models
- Aggregation scenarios are very difficult to model
- Frequent risks are likely candidates for harmonization



Language harmonisation for coverage types – Industry perception

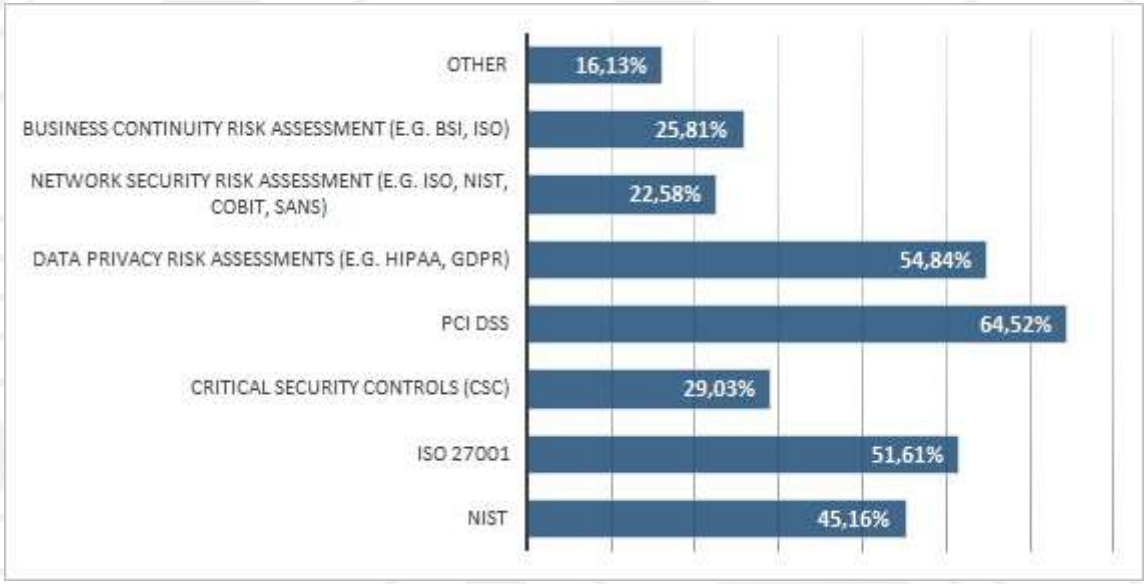
Industry Practices – Cyber Insurance Risk Assessment

- **All insurers** conduct some form of risk assessment
- **Underwriting questionnaires** (long-/short-form) is the most prevalent method (client meeting, desk research, risk audit, TPA report, threat intelligence, etc.)
- Industry perception is that **underwriting methods are insufficient** mainly due to lack of data and evolving cyber landscape
- Carriers often **lack in-house skills** to process this information and translate IT concepts to the existing underwriting methods
- **Noticed and paid claims/incidents** may lead to changes in policy wording (e.g. security patching following major ransomware incident)
- **No standard frequency or trigger** for updating wordings
- Few carriers have **specialised cyber team of underwriters**

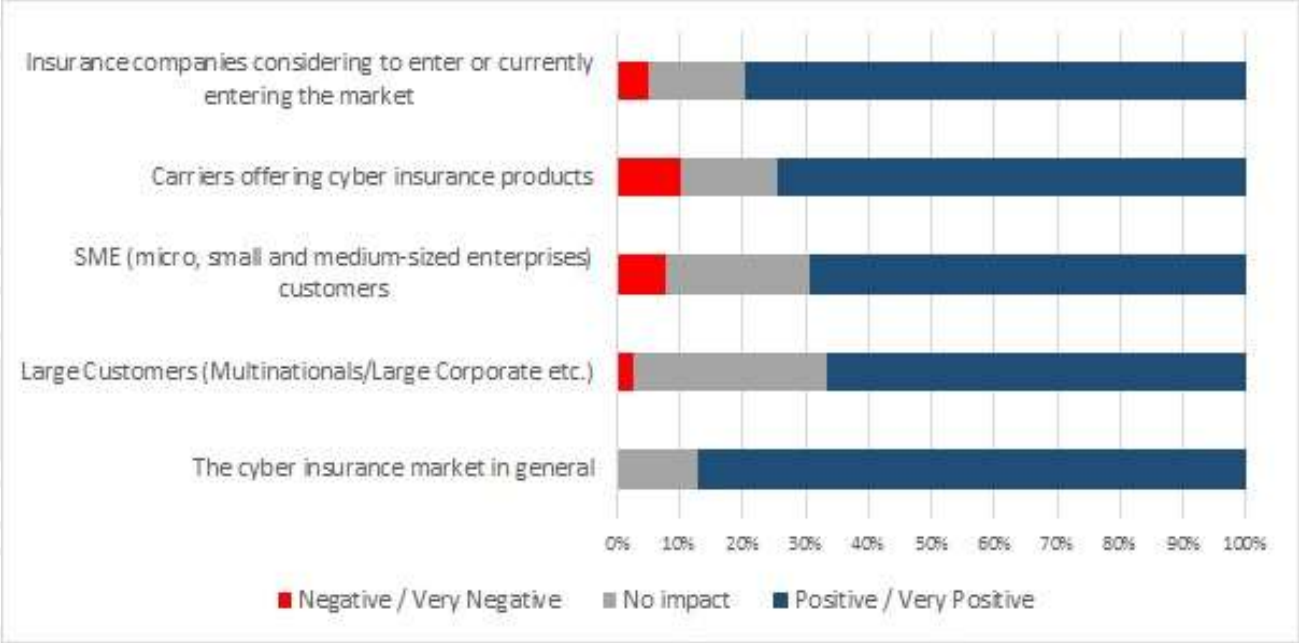
Industry Practices – Cyber Insurance Risk Assessment

Use of standards

- Application of standards is fragmented
- Industry/sector-specific and/or mandated standards are the exception
- Compliance with standards often mandated by other factors including company size (listed companies versus SME), and region.



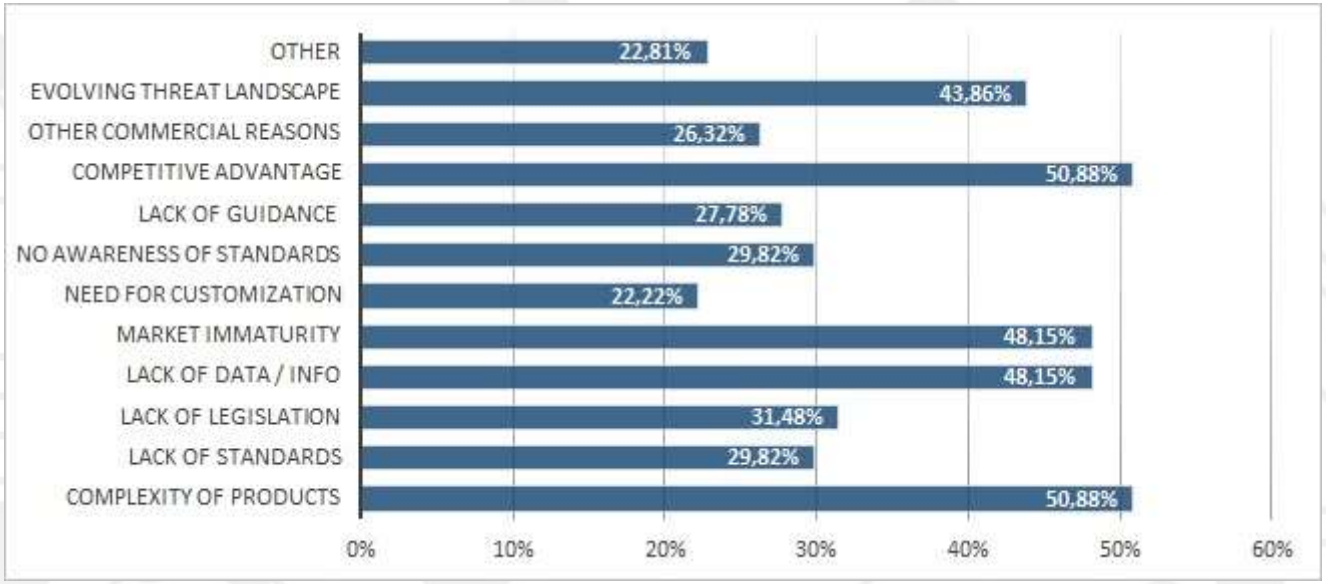
The impact of risk assessment language harmonisation



The impact of risk assessment language harmonisation

- **Increased rate of adoption** as customers better understand the products
- Standardized products will be **more attractive to SMEs** and accompanied by **simpler underwriting methods**
- Harmonisation will allow clients to **better understand the premium calculation**
- Harmonisation will provide a **point of reference for product comparison**
- Less aware customers will **better understand the options** available to them
- Competition between carriers will heavily shift to **pricing and added value offerings**
- Harmonisation will allow insurers to **commonly define risks/incidents**
- Harmonisation will **simplify the quotation process**
- Clearer framework for **developing cyber insurance products**
- Industry will become **less complex**, more reliable, and gain credibility in the eyes of the customer
- Harmonisation will **benefit brokers** as they will have less deltas to compare so they can assess the correct insurer more easily and provide the right coverage for a particular client

Barriers against harmonisation



Some key points

- **Competitive advantage –** harmonisation perceived as loss of unique selling points
- **Lack of data –** very difficult to understand threats and reluctance to share data
- **Complexity –** multiple parameters increase the difficulty of risk assessment model convergence
- **Market immaturity** - carriers compete by trying to develop the best possible product with little experience
- **Evolving threat landscape** - language convergence is slower to catch-up, and maintain, to the highly dynamic cyber risk environment

Incentives for harmonisation

- Industry understand the **potential impact on the growth** of the cyber insurance market
- The risk assessment itself is in **need of a form of harmonization** (e.g. major differences in quoted premiums)
- Addressing the **needs of un-tapped market segments**, particularly **SMEs** that can better understand more standardized products
- **Development of better products** as more data becomes available and cyber risks are better understood and quantified
- **Legislation regarding information security** and data protection creates both increased demand and uniform requirements
- Address a customer base that is maturing in terms of understanding cyber risk and has **growing expectations from risk transfer options**
- Provide offerings tailored to and understood by specific industries to address **industry-specific regulatory compliance regarding IT security**
- Carriers seeking to enter the cyber market will likely **adopt good practices** of other carriers

Market drivers towards harmonisation

Regulations and Standards

- **Common requirements** for security controls and incident reporting
- **Convergence** in terms of security practices and residual risks
- Increased adoption of **specific security standards**
- **Consistent** definitions and taxonomies

Data Availability

- **Improved risk assessment models** and understanding of risk
- **Expansion of data source** to include other feeds
- Development of **cybersecurity skillset** in the industry
- **Efficient and automated** underwriting process

Demand Side Evolution

- **Address SME market** with standardized products
- **Maturing demand side** favours comparable products
- **Compliance** with emerging regulations
- Increased customer **cyber risk awareness**

Market Maturity

- Market **convergence** and **information sharing**
- Improved **information gathering** and **benchmarking**
- Consensus on a **minimum of standards**
- Mechanics of **competition** - best practices

Supporting harmonisation and growth of the cyber insurance industry

Thank you

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

CyberInsurance@enisa.europa.eu

www.enisa.europa.eu