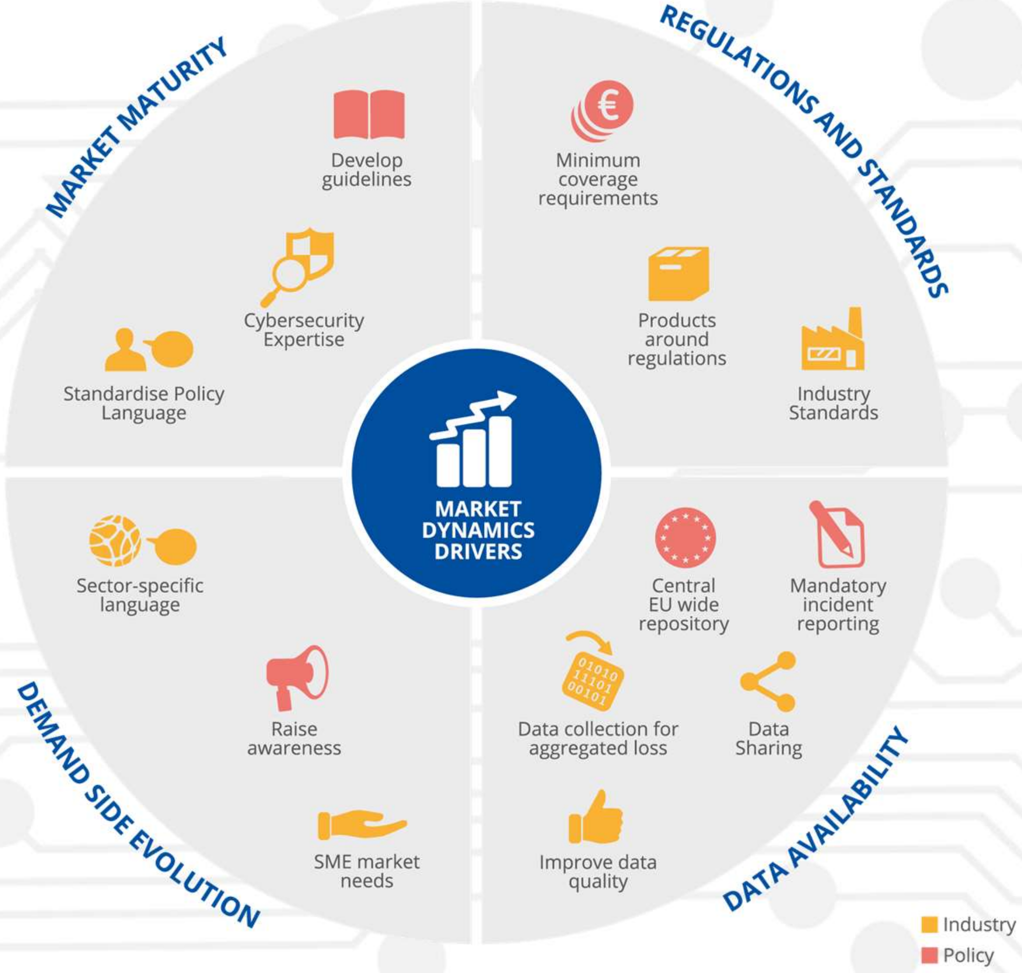
Commonality of risk assessment language in cyber insurance - Recommendations

Theodoros Nikolakopoulos | Officer in NIS | ENISA

Cyber Insurance Validation Workshop | Brussels | 6th October

European Union Agency for Network and Information Security

Mapping of recommendations to key drivers of market dynamics



Recommendations for the industry

1. Standardise policy language and underwriting questionnaires to help insurers and customers mutually understand what they are selling and buying
2. Promote data sharing between the industry stakeholders via dedicated platforms or Information Sharing and Analysis Centres (ISACs)
3. Develop industry standards to define terminology, use cases, coverage, incident types, policy trigger parameters etc.
4. Develop in-house expertise in cyber security to support all aspects of the risk assessment process and provide the link between IT risks and business risks
5. Contribute in the collection of data on aggregated loss or correlation scenarios
6. Use information security and data privacy regulations (e.g. GDPR, NIS Directive) as the basis on which to develop common product frameworks in terms of terminology, coverage and underwriting questionnaires
7. Focus language harmonization efforts on an industrial/sectorial basis to benefit from the commonalities of the specific customer bases (e.g. threat landscape, vulnerabilities, compliance requirements)
8. Address the needs of the SME market for more flexible and lightweight underwriting procedures and standardized/comparable offerings.
9. Support the cyber incident data collection process with various heterogeneous sources, such as threat analyses, open source intelligence etc. and improve overall data quality.
10. Improve communication and information sharing on affirmative or silent coverage for cyber exposures whenever policy language and conditions change.

Recommendations for policy makers

1. Create minimum coverage requirements on top of which insurers can build extra coverage
2. Leverage the upcoming mandatory incident reporting schemes via the NIS Directive and the GDPR to produce meaningful data that could be used, among others, by the cyber insurance industry to expand its evidence base
3. Create a central EU wide repository of incidents to provide aggregate data from multiple sources
4. Raise awareness about cyber security and cyber risk management in organisations to build up demand and buyer maturity and to increase the cybersecurity posture of organisations seeking to transfer risk
5. Encourage the active participation of the European Commission and ENISA in developing guidelines for cyber insurance

Recommendations for the industry #1

Standardise policy language and underwriting questionnaires to help insurers and customers mutually understand what they are selling and buying while avoiding the potential for coverage disputes and costly litigation

Recommendations for the industry #2

Promote data sharing between the industry stakeholders via dedicated platforms or Information Sharing and Analysis Centres (ISACs)

Recommendations for the industry #3

Develop industry standards to define terminology, use cases, coverage, incident types, policy trigger parameters etc. The standards need not cover the full scope of cyber insurance products but can serve as a point of reference for suppliers and buyers of cyber insurance alike

Recommendations for the industry #4

Develop in-house expertise in cyber security to support all aspects of the risk assessment process and provide the link between IT risks and business risks; develop knowledge bridge programs both for insurance experts and for Information Security experts

Recommendations for the industry #5

Contribute in the collection of data on aggregated loss or correlation scenarios

Recommendations for the industry #6

Use **information security and data privacy regulations** (e.g. GDPR, NIS Directive) as the basis on which to develop common product frameworks in terms of terminology, coverage and underwriting questionnaires

Recommendations for the industry #7

Focus language harmonization efforts on an industrial/sectorial basis to benefit from the commonalities of the specific customer bases (e.g. threat landscape, vulnerabilities, compliance requirements) and work together with customers to understand the specific needs

Recommendations for the industry #8

Address the needs of the SME market for more flexible and lightweight underwriting procedures and standardized/comparable offerings. Underwriting for SMEs can be more automated and efficient, e.g. via a score-card approach.

Recommendations for the industry #9

Support the cyber incident data collection process with various heterogeneous sources, such as threat analyses, open source intelligence etc. and **improve overall data quality**.

Recommendations for the industry #10

Improve communication and information sharing on affirmative or silent coverage for cyber exposures whenever policy language and conditions change.

Recommendations for policy makers #1

Create **minimum coverage requirements** on top of which insurers can build extra coverage

Recommendations for policy makers #2

Leverage the upcoming mandatory incident reporting schemes via the NIS Directive and the GDPR to produce meaningful data that could be used, among others, by the cyber insurance industry to expand its evidence base

Recommendations for policy makers #3

Create a central EU wide repository of incidents to provide aggregate data from multiple sources

Recommendations for policy makers #4

Raise awareness about cyber security and cyber risk management in organisations to build up demand and buyer maturity and to increase the cybersecurity posture of organisations seeking to transfer risk

Recommendations for policy makers #5

Encourage the active participation of the European Commission and ENISA in **developing guidelines for cyber insurance**

Thank you

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

CyberInsurance@enisa.europa.eu

www.enisa.europa.eu