Towards a Digital Single Market for NIS Products and Services – RECOMMENDATIONS

Simon Forge| SCF Associates Ltd – Colin Blackman| CEPS
Athanasios Drougkas, Dimitra Liveri | ENISA

Validation Workshop| Brussels| 12 October 2016

Agenda

1. Why an NIS industrial policy is needed
2. Mapping future NIS offerings against the needs of the DSM
3. Actions to set an industrial policy in place
4. What the Industrial policy should contain
5. Implementing an EU Cybersecurity Industrial Policy in Member States
6. Guidelines for the EU NIS industry

Why an NIS Industrial policy is needed

- Europe's future is a digital but infrastructure is threatened
- Without public trust, the DSM strategy is in jeopardy
- A strong indigenous NIS sector is a strategic asset – like other sectors (eg robotics, aircraft) an industrial strategy is needed
- Purpose of industrial policy:
  - Stimulate investment – soft financing, regional funds, tax breaks
  - Support new entrants from idea through industrialisation
  - Encourage existing players to expand and prosper
  - Strengthen eco-system – promote links, clusters, centres of excellence
  - Stimulate demand – educate on the demand and supply side, legislate

NIS offerings to protect the DSM

FUTURE DSM FUNCTIONS	MEASURES OF PROTECTION NEEDED	NIS PRODUCTS AND SERVICES FOR DSM IMPLEMENTATION
Ecommerce - with high level of security to generate trust	•Removal of malware eg key loggers in endpoints and servers •Robustly encrypted sessions for transactions •Remote server authentication •Stronger user identification •Encrypted data bases of consumer financial and personal details	Endpoint security SIEM (services) for cloud and Server Managed security service for major attacks with effective IDS/IPS and Threat Intelligence
Critical infrastructure protection for non-stop operation	•Maintain integrity of control systems •Maintain network functions under attack •Encrypted data stores and sessions •Server authentication •Authorisation, access control and verifications for access, especially maintenance	Target software and systems needs to be redesigned for modern attack threats; Surveillance and responses by managed security services Authentication of all system accesses especially for remote sensors; IDS/IDP for large-scale remote networks.
Retail eBanking for all EU citizens with security	•Removal of malware such as key loggers in endpoints and servers •Encrypted sessions •Server authentication •Improved User identification & access control •Encrypted data bases for consumer financial and personal details	Endpoint security Managed security service for major attacks with effective IDS/IPS and threat intelligence – SIEM.

Implementing an EU Cybersecurity Industrial Policy

1. Recommendations for EU level Policy Makers

2. Recommendations for National Policy Makers

3. Recommendations for the NIS Industry

1. Recommendations for EU level Policy Makers

1. Conduct a needs analysis for the industrial policy – economic, DSM, social, sovereignty needs
2. Increase awareness and education of the market: Promotional planning, for public, business, SMEs
3. Focus R&D planning on NIS domain – e.g. cPPP
4. Support industrialisation of new offerings and technologies following the R&I phase with a public procurement policy
5. Support creation of industrial clusters
6. Promote NIS training and educational measures at all levels
7. Increase dedicated NIS operational support centres: e.g. CSIRTs and sector ISACs, integrating public bodies with international threat intelligence.
8. Certification of services/products to provide EU level certification.
9. Enhance the regulatory framework

Recommendations for EU level Policy Makers #1

- Conduct a needs analysis with in-depth examination of the objectives of the industrial policy, based on the risks due to technological dependence on ICTs and their consequences for:
  - An EU digital economy, following the DSM concepts
  - The DSM’s overall viability in the light of the vulnerabilities to cyber attack
  - Social impacts
  - Sovereignty issues

Recommendations for EU level Policy Makers #2

- Increase awareness and education of the market
  - Promotional planning to educate the market, with professional campaigns in public media for the citizen and for business with promotion of small business and vertical sector information and primary training.
  - SME policy for small company users to encourage NIS product sales – to improve risk awareness, change attitudes, with some funding of procurement

Recommendations for EU level Policy Makers #3

- Focus R&D planning on supporting the development of innovative ideas and technologies in the cybersecurity domain and to strengthen their link to the EU cybersecurity industry. Here, the Contractual Public Private Partnership on Cybersecurity (cPPP) offers the initial step in industrial support that will be necessary. This will need to be built on with further programmes for industrial level collaborative projects. R&D planning should include support for:
  - Start-ups
  - Incubators
  - Collaborative projects
  - Multiple EU centres of excellence for R&D and training

Recommendations for EU level Policy Makers #4

- Support the industrialisation of new offerings and technologies following the R&I phase with a public procurement policy of preferential purchases to support SME NIS suppliers moving from innovation to industrialisation:
  - A procurement plan for SME NIS suppliers to offer them early funding of products and services by the public sector and related enterprises, creating first orders for start-ups
  - Development, rather than research, funding for NIS SMEs for industrialising new technology
  - Support for users who are SMEs to procure services and products from EU providers to support the DSM initiatives, especially sourced from the SME NIS players
  - Export trade support from EU resources overseas (similar to US support in the EU), e.g. organisation of EU cybersecurity exhibition events.

Recommendations for EU level Policy Makers #5

- Support the creation of industrial clusters:
  - To create clusters of start-ups, SMEs and post-start-up ecosystems, with geographic concentration of resources and cross EU links to smaller players of all kinds, possibly around a university as a centre of NIS excellence, or other permanent institution, such as a testing and certification lab.
  - Clusters could be formed at various locations across the EU.

Recommendations for EU level Policy Makers #6

- Promote NIS training and educational measures

Recommendations for EU level Policy Makers #7

- Increase the footprint of dedicated NIS operational support centres: for instance a series of centralised EU alert centres (CSIRTs) and vertical sector ISACs for the private sector, integrating public bodies with international threat intelligence

Recommendations for EU level Policy Makers #8

- Certification of services/products to provide EU level certification. That would engender trust for users within the EU and provide a stamp of approval for international markets that other regions do not have by enabling:
  - Security certification of ICT products and services for software, hardware and firmware, ranging from apps for smartphones to data centre management utilities to real-time industrial control software to chip level security. Certification should be detailed and robust – not just a tick box exercise.
  - Certification of NIS products should be in terms of efficiency, ease of use and effort needed across the product/service lifecycle.
  - Approved centres of certification.
  - An EU security branding – a “Made in EU” label. This needs to be a harmonised qualification through local national standards, not a centralised approach.

Recommendations for EU level Policy Makers #9

- Enhance the relevant regulatory framework:
  - Enforcing protection measures for citizens and enterprises, in a manner that is appropriate, by placing a requirement on service providers to ensure a level of security commensurate with the service they are providing and significance of the personal information they are storing.
  - This might include the concept of an EU NIS regulator to monitor implementations across all Member States, with cooperation between EU-level support centres and levels of readiness of critical infrastructure.
  - Promote audits of cyber security protection levels in all sizes of company and public sector organisations.

2. Recommendations for National Policy Makers

1. Draw national guidelines for cyber protection for each industrial sector as part of this industrial policy
2. Follow a risk based approach on national critical infrastructures and set a mechanisms to monitor cyber security readiness levels i.e. as a form of a national risk register for critical infrastructure threats
3. Promote NIS training and educational measures

Recommendations for National Policy Makers #1

- Draw national guidelines for cyber protection for each industrial sector as part of this industrial policy and such a task would be consistent with an enhanced role for ENISA

Recommendations for National Policy Makers #2

- Follow a risk based approach on national critical infrastructures and set a mechanisms to monitor cyber security readiness levels i.e. as a form of a *national risk register* for critical infrastructure threats:
  - Some Member States already do this (e.g. the UK and some Nordic Member States). Such registers should be updated frequently, possibly in real time, allowing protection measures to be taken.

Recommendations for National Policy Makers #3

- Promote NIS training and educational measures:
  - University level qualifications for a new NIS workforce, with a new emphasis on security as a basic computer science
  - Education at school level on the need for cybersecurity in using ICT devices and in writing software
  - Support funds for training NIS service staff for cybersecurity incident response teams, e.g. six-month induction course for several thousand staff annually across the EU, with financial support for training courses and trainees. This would provide NIS service providers of all sizes with a solution to the gap in qualified personnel for the security operations centres (SOCs) that will be a key feature of the future EU NIS industry.

3. Recommendations for the NIS Industry

1. The NIS industry should seek support and promote awareness campaigns from the EU and at Member State and regional levels within each Member State
2. The NIS industry should push for standards, first at EU level, with ETSI being involved, and ultimately for global standards with the IEC and ISO for both services and products
3. NIS industry-led information campaigns should be created to inform the public and the business sector of the threats, with events for consumers, enterprises and government departments that promote the industry and its accomplishments
4. The industry should also push for common certification across all Member States, i.e. certification in one Member State would be valid across the EU, and promote EU-level labelling with the certification
5. On the user company side, cybersecurity should be a concern at board level of all companies
6. The industry focus should be on building an ecosystem supporting holistic security solutions

Recommendations for the NIS Industry #1

- The NIS industry should seek support and promote awareness campaigns from the EU and at Member State and regional levels within each Member State

Recommendations for the NIS Industry #2

- The NIS industry should push for standards, first at EU level, with ETSI being involved, and ultimately for global standards with the IEC and ISO for both services and products

Recommendations for the NIS Industry #3

- NIS industry-led information campaigns should be created to inform the public and the business sector of the threats, with events for consumers, enterprises and government departments that promote the industry and its accomplishments

Recommendations for the NIS Industry #4

- The industry should also push for common certification across all Member States, i.e. certification in one Member State would be valid across the EU, and promote EU-level labelling with the certification

Recommendations for the NIS Industry #5

- On the user company side, cybersecurity should be a concern at board level of all companies. To achieve this will require a cybersecurity statement in annual reports for listed organisations. This may require acknowledgement of incidents over the past year and current and future measures that have been put in place to manage risk

Recommendations for the NIS Industry #6

- There is a need to build the NIS ecosystem, as the market is moving towards holistic solutions covering the supply chain. Thus industry focus should be on building an ecosystem supporting holistic security solutions. That implies that NIS providers should quickly have a clear view of where they fit into the ecosystem, and promote formation of:
  - SME level clusters around each major player, with incubator support for start-ups.
  - Industry consortia, first from the larger players, and second to form and nurture a healthier SME segment of providers of products and services.

Thank you

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu