Cybersecurity as an Economic Enabler

1 Introduction

In this short paper, ENISA puts forward several ideas on how to align good cybersecurity practices with economic policy. The ultimate goals behind these ideas are to ensure that cybersecurity is an enabler and not an inhibitor of a more efficient market whilst continuing to to encourage the establishment of a high level of cybersecurity across all industry segments.

The essential arguments are structured as follows:

- A brief review of macroeconomic and microeconomic drivers for cybersecurity in the EU is presented.
- The current policy context is then summarised
- Areas in which ENISA could contribute to the DSM are presented and discussed.

2 Macroeconomic Considerations

A small number of new technologies (such as big data, mobile computing and cloud) are revolutionizing IT markets and enabling new trends in the IT market. Whilst these trends can rightly be seen as economic enablers they also present significant cybersecurity challenges. If the EU fails to respond to these challenges, it could sacrifice up to €640bn of potential EU economic value.

The EU Cybersecurity Market is estimated at €20.1bn and compares favourably with the cybersecurity market of other global regions. The Compound Annual Growth Rate (CAGR) of the EU market however is 6%, whereas the average growth rate is around 8%, and is growing slower than all other major regions.

3 Microeconomic Considerations

From a microeconomic perspective, cybersecurity maturity of large European companies is approximately equivalent to those in other regions. Interestingly, large European companies are typically more concerned about cyber security related risks than rest of world. Matching the global growth forecast would increase the European market by EUR 1.0 bn in 2018. In parallel, ITSEC professionals in the EU are forecast to grow at 6% p.a., which could grow the workforce by up to 0.3m jobs in 2018.

The rapid development of new technologies however has made it clear that traditional approaches to Cyber Security are insufficient. Security concerns are slowing adoption of some technologies, especially mobile and cloud, which is preventing the EU from making the most of innovation to boost its economic efficiency.

4 EU Cybersecurity policy & legislation

Although there have been many policy initiatives related to cybersecurity over the past five years, the EU Cybersecurity Strategy, the NIS Directive and the General Data Protection Regulation (GDPR) are the most significant developments in terms of impact on ENISA's work. These policy developments however are not particularly linked to EU economic policy.

The Digital Single Market (DSM) initiative on the other hand clearly deals with market issues and includes a cybersecurity component. The comments in this paper can be seen as ideas for supporting the DSM strategy.

5 Engaging with Industry to Support the Digital Single Market

For the vast majority of its deliverables, ENISA achieves impact by working together with industry and the public sector to identify issues and propose acceptable solutions. This approach enables the Agency to achieve scalability (by leveraging experts in the member States) and results in a greater sense of ownership by the target communities. In this sense, ENISA is continually fostering public-private cooperation.

ENISA believes that the EU needs to become the single market of preference for governments and industry where cybersecurity is concerned. Achieving this will require the EU to achieve a reasonable balance between strong ethical principles and effective business practices that could more effectively stimulate economic growth. Given the key role of modern technology in supporting future growth, cybersecurity should be an integral part of the EU industrial policy approach. ENISA will continue to promote and support such an approach in the area of cybersecurity by providing the platform to bring together public and private sector.

6 Cybersecurity Issues in the Digital Single Market

The following tables identifies a number of key cybersecurity issues that are associated with the Digital Single market and proposes a number of mechanisms for resolving them.

Issue	Proposed Resolution Mechanisms
Current attempts to improve NIS throughout the EU often do not achieve an optimal balance between opportunity and risk. This reduces the effectiveness of the overall approach and increases costs for both the public and private sector.	• Assist the Commission and the Member States in ensuring that EU cybersecurity strategy and EU industrial policy are strongly aligned. Identify areas where the EU is well positioned to be a global leader and assist in defining long-term plans for building up these competencies. • Promote industry to reason in terms of the balance between opportunities and risks and not just to concentrate on risk.
The internal market for security products and services is not functioning correctly. The EU security market is dominated by US companies and functions on a 'supply push' principle rather than a 'demand pull' principle.	• Stimulate 'collective demand' by getting different industry sectors to define security requirements on a sector-by-sector basis. Use these requirements to drive procurement policies in these sectors. • Work together with industry to define and disseminate security requirements adapted to the needs of SMEs.
The area of privacy and data protection is moving from a legal and principle-based debate to an implementation phase. The EU has a strong policy in this area but is very weak in terms of implemented solutions.	• Help the Commission and Member States to move the privacy and data protection debate towards implementation strategies. • Identify existing methods and tools that could be used to implement the proposals of the regulation.

Current EU research & development activities in the area of cybersecurity are not giving rise to successful services and products .	• Work together with universities and EU cybersecurity companies to define and implement a framework for rapid implementation of EU research ideas in industry environments. Ensure a feedback mechanism to enable research to improve products together with industry. • ENISA should be given a stronger role in H2020 projects in the area of NIS. In order to achieve scalability, the ENISA regulation should be changed so as to allow the Agency to receive funds for this.
Cybersecurity standardisation and certification activities are not sufficiently aligned with modern needs of the industry.	• ENISA should proactively foster the development of relevant standards by active participation in ISO, ETSI, CEN/CENELEC and other relevant standardisation groups. • Promote certification schemes by active contribution to initiatives such as the SOGIS[1] group and facilitate industry involvement.
Knowledge and skills related to network and information security are developed and maintained in a fragmented manner. There is no coherent approach for educating citizens, private sector and government.	• Work together with schools, universities and professional associations to create a coherent framework for raising awareness and education in NIS. Assist industry in aligning skill sets with career paths.
The EU has many agencies in the area of ICT and security : EU Lisa, Frontex, Europol/EC3, CEPOL, Eurojust, EEAS, EDA, ENISA.	• Future EU policies, legislation and programmes should recognize the central coordination role of ENISA in ensuring a coherent approach to cybersecurity across the EU, both in terms of Member States and in terms of communities.

7 Key Messages to Industry

In the light of the above comments, ENISA has published the following key messages to industry:

- Consider new business models that capitalise on security as a differentiator of products and services.
- Establish sectorial requirements for information security in order to move the cybersecurity market.
- Invest more in awareness and education on security at all levels.
- Reduce Operational Expenditure by Improving Risk Management.
- Secure the whole lifecycle of products by using security and privacy by design.
- Improve cooperation within and across industry segments and national borders to improve threat intelligence and promote the application of good practices.
- Consider new business models that capitalise on security as a differentiator of products and services.
- Proactively drive standardisation through strong industry representation.
- Support cybersecurity and privacy certification schemes to improve customer confidence
- Collaborate with academia to ensure that quality research results in concrete products and services.

[1] http://www.sogisportal.eu