ENISA Recommendations to IT Industry

JANUARY 2016

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Steve Purser Head of Core Operations Department

Contact

For media enquiries about this paper, please use press@enisa.europa.eu.

Table of Contents

1. Background

As a direct result of current economic necessities, ongoing technological developments and changes to EU policy, the IT industry is undergoing a number of fundamental shifts. Growth has slowed for many IT industry vendors that aren't delivering the innovative solutions that consumers expect, this is a sign that the nature of the industry is changing. Legacy vendors are feeling the pressure from new dominant vendors and are therefore consolidating or divesting[1] (HP split[2] & Dell buying EMC[3]).

Technological developments such as Internet of Things, Big Data and Smart Devices have the potential to significantly change the EU way of life, but are hampered by issues related to security and privacy. Nevertheless, these technologies are becoming the driving force behind many IT companies in the foreseeable future.

Where EU policy is concerned, the adoption of the NIS Directive will impose new network and information security requirements on operators of essential services and digital service providers and will require them to report certain security incidents to competent authorities or Computer Security Incident Response Teams. At the same time, the European General Data Protection Regulation, which outlines security requirements and requires privacy breach reporting, subject to penalties and fines, will require companies in the EU to change their operating model to comply to more stringent requirements. Last but not least, the Digital Single Market initiative is expected to boost the competitiveness of industry through a number of mechanisms. However, none of these policy changes will be successful without the strong support of industry.

In this short paper, ENISA puts forward 10 messages to industry. The ultimate goals behind these messages are (a) to encourage the establishment of a high level of cybersecurity across all industry segments and (b) to ensure that cybersecurity is an enabler and not an inhibitor of a more efficient market.

2. Key messages to Industry

ENISA's key messages to EU industry are as follows:

1. Consider new business models that capitalise on security as a differentiator of products and services.

   The EU has a strong background in information security coupled with extensive experience in implementing trust models. EU industry is therefore well-positioned to offer cybersecurity products and services to a broad consumer base. In order to do this however, it will be necessary to conceive new business models, which are not simply replicating successful approaches pioneered outside the EU.

2. Establish sectorial requirements for information security in order to move the cybersecurity market.

   The EU cybersecurity market is currently a 'supply push' market. Even large industry players may not have enough purchasing power to move the cybersecurity market to reflect their needs. By creating common

[1] http://www.cio.com/article/3006976/it-industry/5-it-industry-predictions-for-2016-from-forrester-and-idc.html
[2] http://recode.net/2015/11/02/hewlett-packard-splits-in-two-today-now-what/
[3] http://www.bloomberg.com/news/articles/2015-10-12/dell-to-acquire-emc-for-67-billion-to-add-data-storage-devices

requirements representative of entire industry sectors, industry can influence supply and move the market to reflect their needs.

3. Invest more in awareness and education on security at all levels.

   Work together with the public sector, academia and professional organisations that specialise in training to ensure that education schemes are closely aligned with industry expectations. The ultimate objective is to ensure that such training results in knowledgeable and qualified personnel for all important security-related industry functions (and is not restricted to the CISO).

   Invest in people as well as technology. The various data breaches in 2015 show that the "insider threat" is still underestimated.

   Empower "informed customers" in order for them to be able to ask the right questions to the providers and understand where their responsibilities lie.

4. Reduce Operational Expenditure by Improving Risk Management

   Industry must comply with legal obligations and regulatory requirements, but outside this framework companies are free to select an approach that optimises opportunity for a given set of risks. By investing in proven risk management techniques, companies can reduce their overall expenditure whilst still achieving an appropriate level of security.

5. Secure the whole lifecycle of products by using security and privacy by design.

   Industry can offer a high level of security whilst significantly reducing costs by deploying methods that build security and privacy into their products and services starting from the design phase. In addition, where ICT devices and services rely on third-party components, it is important to validate the security of the supply chain and to ensure the secure integration of all components together.

   Security design should be based on a solid understanding of the threats that are likely to affect products and services and such threat assessments should be carried out at regular intervals in order to keep up with threat evolution.

   Where deployed products are concerned, vendors must provide security updates in a timely manner.

6. Improve cooperation within and across industry segments and national borders to improve threat intelligence and promote the application of good practices.

   Industry actors should increase cooperation on all areas of cybersecurity to the extent that it does not affect their competitiveness (suppliers of cybersecurity products and services being a special category here). Improving threat intelligence and spreading best practice benefits all industry players and reduces unnecessary costs due to 'reinventing the wheel'.

   Opportunities exist for closer collaboration with EU policy makers, which could improve the competitiveness of EU industry in the global market. Notable examples of such opportunities are the Digital Single Market initiative as well as the General Data Protection Regulation that was recently agreed between the European Commission, the European Parliament and the Council.

7. Proactively drive standardisation through strong industry representation.

   ENISA believes that standards should be industry driven and should be a mechanism for improving market efficiency by providing for high levels of security whilst stimulating competition and ensuring interoperability of products.

   Industry should proactively contribute to the standards development process by clarifying the requirements for new or evolving standards and ensuring that they help promote best of breed solutions.

8. Support cybersecurity and privacy certification schemes to improve customer confidence

   Security concerns are still seen as a major barrier to deploying the latest technologies in the EU market – often rightly so. By agreeing on suitable certification schemes for security and privacy, industry can play a role in increasing consumer confidence thereby increasing the uptake of new technologies.

9. Collaborate with academia to ensure that quality research results in concrete products and services.

   ENISA notes that there is still a large gap between innovative resource ideas that come out of EU funded research projects and commercial products and services that turn these ideas into pragmatic solutions for consumers.

   Industry should work together with academia to improve the mechanism for ensuring that good ideas result in good products. In particular, there should be a framework for introducing research ideas to EU companies and for ensuring adequate support by those who developed the ideas throughout the product or service lifecycle.

10. Make the resolution of societal issues a concern for engineers as well as public affairs specialists.

    Engineers and operational staff tend to be greatly under-represented in EU collaboration efforts on cybersecurity. Industry should allocate more operational experience to initiatives that seek to resolve key societal issues. By doing so, they will help remove barriers that prevent EU industry from realising its true potential.

3. Concluding remarks:

The role of ENISA is to guide experts towards security solutions that are adapted to the needs of the internal market. By encouraging strong cooperation across national borders and across communities, the Agency promotes the development of approaches to security that are not hampered by national restrictions or the ideas of particular communities. This results in solutions that are interoperable across the EU, thereby decreasing costs and enabling EU industry to benefit from a wider market.

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu