Cybersecurity and update from ENISA

ENISA Executive Director, Prof. Dr. Udo Helmbrecht

Speech at

Industry, Research and Energy Committee Meeting

European Parliament

21ST April 2016

Ladies, Gentlemen, Members of the ITRE Committee,

Thank you for the invitation and the opportunity to address you today on cybersecurity, particularly following the publication of the Commission proposal (on April 19th, 2016) to digitise the European industry, and the role ENISA can play in the delivery of a successful Digital Single Market strategy.

By way of introduction I would like to address the terms 'digital' and 'industry' and how ENISA is building partnerships for leadership in the digital technology value chain.

Firstly Digital. The world is quickly embracing digital in every part of life. E-banking, e-health, e-commerce, e- education, e-*everything* are all now totally dependent on an open, safe and secure cyberspace. We are witnessing the development and deployment of smart manufacturing, the Internet of Things and computer controlled critical infrastructure. Digital is challenging the delivery of old business models, while at the same time providing opportunities for the new world. We see new challenges to old business models, where for example mobile phone manufacturers and internet search engine companies are moving into smart transport. Europe has to embrace this challenge and take the lead in the digital revolution by delivering disruptive business models, using innovative technologies and services, in a safe and secure manner. Europe has to ensure the trust of its citizens and industry to have the necessary confidence to work with digital.

The delivery of Digital can be broken into three components, the generation of digital data, the transmission of digital data from the generator of the data to the processor, and the storage of digital data. ENISA is playing its role and is working on each of these components.

In terms of generating digital data ENISA is working on the security of smart homes/cities, the computer control of our critical infrastructures, and e-health where digital monitoring of our health on a 24 by 7 basis will improve the quality of all of our lives.

The transmission of data between the source and processor of the data is another critical part of the digital chain. ENISA has recently taken an active role in addressing the question of encryption and the importance of trusted secure communications of digital data as a key enabler of the internal market. I can not imagine that the citizens of the EU adopting digital e-health technology unless they had the trust, that their private data would only be accessible by their medical practitioners. ENISA has recently published a paper[1] on encryption on its web site and continues to contribute to the debate on encryption.

The volume of data being generated in our digital world is growing at exponential levels. The average computer for sale in the high street and online now holds terabytes of information. What this term means is that for every terabyte of storage there is 1000 million pieces of digital information to be stored. It is against this background that the term Big Data has been invented. One of the relatively new business models that has developed in the last few years to cope with the volume of Big Data is the Cloud Computing business model. In this model citizens and industry can have their data stored in a central location where the expertise, capacity and security should be

[1] https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-position-on-crypto

available to store the data in a secure manner. ENISA has been working in this area for a number of years and has produced reports on good practice and guidance in the area of cloud computing. ENISA is also conscious of the challenge for SMEs and has also produced reports tailored for their needs. These reports help SMEs to address the additional challenges that they have in embracing the digital revolution with more limited resources in comparison with large enterprises.

By way of a concluding remark on Digital, I would like to welcome and support the recent conclusion and introduction of the General Data Protection Regulation. I believe that ENISA has an important role to play in working with the EU data protection authorities and the European data protection supervisory authority and I look forward to assisting in this work.

Secondly 'Industry'. The importance of industry in the digital world cannot be underestimated. We see Commission initiatives such as Innovation for Manufacturing SME (IM4S), H2020 and Connected Europe Facility (CEF), promoting the next generation of research and development. Data breaches, theft of intellectual property, sabotage of industrial processes are not new. What is difficult is the quantifying of the losses that are occurring due to breaches in digital network and information security.

In 2015 data breaches in the health sector have been estimated at almost 320 million euro[2] and in the financial sector around 12 billion euro[3]. The growth in the cybersecurity insurance market is testament to the increasing realisation of the importance of this subject and the concern that CEOs are increasingly attaching to cyber security. What is clear, is that cyberattacks are increasing, the attacks are becoming more sophisticated, and the losses are escalating. ENISA is very conscious of this and is willing and able to work with all EU stakeholders by forming partnerships to address the challenge.

I would like to turn next to 'leadership'. Leadership can be considered in terms of structural, organisational and directional leadership. ENISA is participating in all of these aspects and is bringing additional value by creating new partnerships. ENISA as a statutory body has the legal remit to address network and information security at an EU level. At the organisational level, ENISA is bringing together key stakeholders to promote network and information security. Furthermore, ENISA continues to build capabilities and capacity by engaging with public and private sector stakeholders, to deliver pan European cyber exercises and pan European cyber training for computer security incident response teams. These activities are reinforcing community building among Member States, EU bodies and relevant Network and Information security stakeholders as set down in the current draft of the NIS Directive.

ENISA has produced cutting edge reports to raise awareness and to offer best practice in cyber security policies. All of these activities are having the effect of reducing digital silos across the Union. At the directional leadership level, ENISA has become a centre of EU expertise where it is

[2] https://www-01.ibm.com/marketing/iwm/dre/signup?source=ibm-WW_Security_Services&S_PKG=ov34982&S_TACT=000000NJ&S_OFF_CD=10000253
[3] http://www.mckinsey.com/business-functions/business-technology/our-insights/the-rising-strategic-risks-of-cyberattacks

able to leverage the knowledge and support of the EU Commission, the 28 Member States and industry participants.

I consider the diversity of different Member States approach to network and information security as an advantage for Europe, and that ENISA has the unique role of bringing together this knowledge, experience and willingness to work together for the benefit of EU industry and the citizens of the EU. ENISA as the EU focus for network and information security is building expertise and facilitating outreach to its stakeholders. ENISA is building public private partnerships with industry where the knowledge of industry is being used to assist in the development of a culture of network and information security and to encourage the importance and delivery of digital goods and services that are fit for purpose and secure in their operation.

By way of some concluding remarks I would like to make some comments in relation to ENISA's contribution to this debate.

Firstly, ENISA has repeatedly called for security by design. EU technology needs to address security of digital products as a market differentiator. Recognising that this will place an additional cost on Industry, I believe that the importance of information security will prevail and the extra cost will be justified in terms of consumer confidence. One supporting activity to achieve this objective is by the use of appropriate security standards in public procurement.

Secondly, that ENISA facilitate greater coordination of network and information security standards and certification with industry and the relevant standardisation bodies.

Thirdly, that ENISA fully participate in the Commission initiatives, such as the CEF program, to leverage the legislative mandate that ENISA has in the area of network and information security, particularly in the context of the forthcoming Network and Information Security Directive.

Fourthly, that ENISA continue to find and deliver network and information security exercises and skills enhancement that are particularly relevant to be delivered on a pan EU basis.

ENISA is now 12 years old, contributing to one of the biggest challenges that modern society is facing and is ready to work with all stakeholders to address these challenges at an EU level. I support the work of Commissioner Oettinger in the delivery of his vision of an EU digital single market.

Finally, I would like to take this opportunity to thank the ITRE Committee and the European Parliament for its support to date. I believe that ENISA is a key stakeholder in the delivery of an open and secure EU cyber space. ENISA looks forward to playing its role in this important area of network and information security for the benefit of industry and Europe's citizens.

Thank you for your attention.

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