REPORT

Cybersecurity – an opportunity for Europe to be a global leader

On 29 March 2019, Orgalim, together with the Association of Swedish Engineering Industries, Teknikföretagen, and RISE, Research Institutes of Sweden, held a lunch debate on how industry, EU countries, Research and Technology Organisations (RTOs) and European institutions should collaborate to develop a world leading and efficient cybersecurity system.

Introduction

The **moderator Mr Joakim Jakobsson, Head of Public Affairs at RISE**, welcomed participants to the panel discussion before **Mr Malte Lohan, Orgalim's Director General** gave some opening remarks.

Lohan maintained that cybersecurity is a vital issue for Orgalim. It is at the heart of the transition towards a transformed European economy driven by technology and digitisation. He also spoke about Orgalim's vision towards 2030, which at its core is about embracing technology and transforming societal challenges such as climate change into drivers of growth and prosperity.

He welcomed the European Commission's work on the Cybersecurity Act, saying that it is a good first step, adding that Orgalim was and will continue to be involved in the transition, and implementation phase.

Europe has a golden opportunity to be a thought, technological and policy leader in cyber security, he said, adding that cybersecurity could be a European success story, benefiting industry, the citizen and society.

Panel interventions

Ms Vivian Loonela, member of Vice President Ansip's cabinet, stressed that close consultation with stakeholders is vital to ensure that the European Commission's work on cybersecurity remains consistent.

She gave a snapshot of what the current Commission has achieved over the past five years: The security of network and information systems (NIS) Directive encourages the exchange of information and sets minimum standards for protecting digital infrastructure. The Cybersecurity Act, which sets up a certification framework was established, while the cybersecurity strategy was reviewed. A network of cybersecurity competence centres is proposed and will carry out cyber security research and development and just last week, the Commission issued a recommendation on 5G security.

She added that the Commission's work has been comprehensive and cybersecurity is now at the heart of EU policy making.

Ms Maija Rönkä, Senior Specialist, Permanent Representation of Finland to the EU said that cooperation between national cybersecurity centres and ENISA is essential for building trust.

Through the EU's work in the area, European Union Agency for Network and Information Security (ENISA) today has a stronger mandate and a key role in facilitating cooperation between Member States. She stressed the importance of exchanging information on cyber incidents and learning from successes and mistakes. The importance of sharing information

with the public and private sector and even to citizens is also vital. She mentioned that ENISA's awareness raising actions and its policy studies would be important moving forward.

Mr Shahid Raza, Director Cyber Security Lab, RISE elaborated on the role of RTOs like RISE, saying that they perform strategic research, bridging the gap between industry and academia. RISE engages in projects with industry to solve specific technological problems with a big focus currently on Internet of Things (IoT) standardisation.

His lab also works closely with the competence centres and the European Cyber Security Organisation (ECSO). As the Cybersecurity Act is now agreed, RISE will link its cybersecurity certification work with ENISA. RISE Cybersecurity Lab is also developing an automated cybersecurity certification system for use by RISE members.

Mr Johannes Nitschke, Director EU Affairs at Siemens gave an overview of the Charter of Trust for cybersecurity launched one year ago. He said that in 12 months, it has doubled to 16 members and has 10 principles, including ownership, certification and collaboration.

The Charter was launched due to an explosion in cyberattacks over the past 10 years, which are the biggest challenges for consumers and industry. It aims at protecting the data of individuals and companies, reducing harm to companies and infrastructure, and building a foundation for trust.

Much focus is on supply chain security. 17 baseline requirements have been set out for participating companies.

On Critical infrastructure, Nitschke said that there are good ideas and definitions from the Commission and the US. However, he called for any Critical IoT definition/certification to be more dynamic and less static.

Mr Alexander Eisenberg, Senior Expert EU Technical Government Affairs, BSH (Bosch) Home Appliance stressed that we must go beyond the existing certification framework, saying there is a need for a holistic view, a kind of cybersecurity policy 2.0.

This is difficult due to the wide variety of stakeholders and legislative backgrounds involved. The ICT industry is different to consumer products – both have different regulations and laws.

He suggested that all parties should agree on five basic principles to reach an EU consensus on this 2.0 version: National coherence, legal consistency, requirements, vertical and horizontal discussions, and internationally agreed standards.

Mr Jacques Kruse Brandao, Global Head of Advocay at SGS/IFIA, representing the Testing, Inspection and Certification (TIC) industry, gave his views on a successful EU-wide cyber security certification framework.

He said that the Commission's Cybersecurity Act is a good start and creates more of a level playing field. However, much more collaboration between stakeholders is needed to fill in the gaps.

He stressed that there will be 20 billion IoT devices next year and not all of them will be secure. He therefore urged swift action to have a complete framework in place.

Europe has an advantage over other regions as most of the component manufacturers are based here. As well as having a company's view, a cybersecurity framework should also take into consideration both the citizen and the social view - only then can the framework make sense.

On a question from the audience on how the Cybersecurity Act addresses consumer safety, Jaques Kruse Brandao said that companies would initially follow baseline requirements and over time, brands themselves would come up with their own additional solutions.

Alexander Eisenberg added that there is an EU Safety Directive already in place, and that certificates will help but it's too early to say how much.

Vivian Loonela maintained that certified doesn't mean that a product is 100% safe – there is no such thing as a cyber-secure product, she said.

Asked about the Permanent Cyber security Certification Stakeholder Group, Loonela affirmed that it is an ambitious project but that ENISA will deliver. Stakeholders must buy into it so it has to be, she added.

On the upcoming Finnish Presidency of the European Union, Finland will follow the implementation of the Cybersecurity Act together with the Commission and ENISA to prepare the work programme. Work has been completed at Council level.

Shahid Raza then spoke about RISE's involvement in the Concordia project, which aims to implement a common Cybersecurity Research & Innovation Roadmap for Europe. The 46-member project is unique as it goes beyond research and all the way to commercialisation of potential products. It is also inclusive and community driven.

On the issue of third party or self-assessment, there were differing views. It was mentioned that third party assessment generates trust between two parties. Another view is that very few companies in the world can do self-assessment in house and it should be done by a third party.

However, for SMEs both third-party and self-assessment can prove to be costly and complicated. RISE can help here to make these smaller companies compliant.

On what spurs innovation in cybersecurity, there was some discussion on whether a hack causes companies to take steps to be more cyber secure. It was also noted that GDPR has also spurred companies into action. Baseline requirements such as training and protecting your PC were once again mentioned as important to follow.

Panel's views on Cybersecurity Act opportunities:

- The Cybersecurity Act generates a level playing field for the benefit of companies, citizens and society.
- It is a great starting point but best results will only come through collaboration.
- It will result in more competitiveness to benefit everyone

- Europe can become market leader in area, giving it a competitive edge.
- It can support the Digital Single Market if certificates are harmonised in the EU.
- It gives more confidence for consumers and opportunities for business.

Conclusions

In closing, Pia Sandvik, CEO, RISE, said that cybersecurity is a key challenge but also a pre-condition for building trust in the Digital Single Market and for the digitisation of public services. Europe has the opportunity to take leadership on cybersecurity in the global arena. Strengthening trust for citizens and businesses should be the core objective, she said.

Sandvik added that Europe needs a simple and user-friendly framework and with few regulations or requirements. Ensuring consistency in legal requirements for cybersecurity is key to have a true digital single market. National fragmentation should be avoided, while standards should also play a core role in the Cybersecurity Act.

Many large companies have the resources and competences to handle cyber threats. However, for SMEs it is vital to have the right support to tackle these threats. This role can be played by RTOs, she maintained.

To realise the European Commission's reform package on Cybersecurity, Horizon Europe must have a clear industrial focus and conditions, which will allow industry and RTOs to contribute to the package's implementation through applied research. She added that a European strategy for technology infrastructure should be developed in order to utilise existing test beds.

Sandvik ended by saying that further discussions on the Cybersecurity Act are required so that it can be implemented in a way, which supports European competitiveness and innovation.