Building trust in the Digital Single Market – the role of international standards

Cybersecurity and Data Protection Standards in support of European Policy

CEN-CENELEC and ENISA joint workshop
Brussels, 19 September 2017

Sachiko Muto
CEO, OpenForum Europe
sachiko@openforumeurope.org

About OpenForum Europe

- Promotes an open and competitive ICT market
- Member of the EU ICT Multi-Stakeholder Platform: a unique forum for bringing all relevant stakeholders together and for establishing the linkages to all sectors for innovation and digitisation
- Co-chairs the EU Rolling Plan for ICT Standardisation
- Supports EU aims to improve cybersecurity and bolster trust

EU Cybersecurity Communication

- Joint Communication on *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*
  - Highlights the need for education – 95% of cybersecurity incidents are enabled by “some type of human error, intentional or not (IBM, 2014).
  - Recognises ENISA's role in co-ordinating EU action to enhance and promote a regional cyber-secure ecosystem
  - Introduces an EU cybersecurity certification framework

Labelling and trust in the market place

- Can certification and labelling schemes tackle dynamic security challenges or do they lead to “pseudo-security”?
- In theory (transaction economics), labels can reduce search and information costs, but for trust to be justified and not a blind leap of faith (not trust but negligence!):
  - Users must recognise the label and be able to distinguish it from other signs
  - Users must understand the contents of the scheme
- Empirical research shows a substantial proportion of users confuse symbols and do not know what Internet trust mark schemes stand for (Rüdiger 2008, 2013)
- Important to avoid proliferation of certification schemes and further fragmentation

Leveraging international standards and the European Standardisation System

- To avoid duplication of effort international standards alignment should remain priority, including ISO/IEC JTC 1, SC27 and relevant global fora/consortia active such as the IETF, W3C, and OASIS.

- In addition, there is a need for cyber security risk management frameworks. This guidance should include information as to how respective standards address security requirements laid down in EU regulation.

- Where gaps in standards and certification schemes are identified these should be pursued via the normal EU standardisation system – possibly a through a joint effort by the ESOs.

Thank you!

sachiko@openforumeurope.org