



Preliminary Workshop comparing U.S. Cybersecurity framework and EU NIS Platform approaches

Brussels, 24th November 2014

Summary report

On 24.11.2014 a preliminary workshop comparing US Cybersecurity Framework and EU NIS Platform approaches was held in Brussels, under the umbrella of the EU-US Working Group on cybersecurity and cybercrime/Public-Private Partnership Expert Sub-Group.

US NIST¹ presented the US Cybersecurity Framework, which was issued on February 12, 2014, as directed by President Obama in Executive Order 13636². European Commission DG CNECT³ presented the EU NIS Platform⁴, which was established in June 2013 under the EU Cybersecurity Strategy⁵.

Two cross-sectorial industry panels, one on risk management and the other on voluntary information sharing, shared their experiences and views about the US and EU approaches.

Risk management

In the risk management panel there was wide consensus on the need to engage in open, inclusive processes when elaborating frameworks and guidance, thus maximising the potential for interested organisations to contribute. Sufficient efforts should be devoted to raising awareness about the existence of voluntary good practice guidance initiatives and frameworks, as a precondition for them being applied by the targeted constituency.

In the experience of panellists, frameworks and guidance documents provide a useful basis for organisations when putting in place cybersecurity risk management approaches. Organisations tailor them to their needs and operational environment; some parts may not be relevant for all organisations. Many use them as a means to engage with CEOs. The simpler the framework the better the chances are of them being applied successfully. There was broad agreement that CEO-level engagement is an absolute necessity for cybersecurity to be addressed within an organisation. There was certain disagreement on whether executive boards or CEOs should be liable for cyber incidents; some US participants were totally opposed, arguing that cybersecurity depends on a much wider

¹ National Institute of Standards and Technology

² <http://www.nist.gov/cyberframework/#>

³ Directorate General for Communications Networks, Content & Technology

⁴ <https://resilience.enisa.europa.eu/nis-platform>

⁵ <http://ec.europa.eu/digital-agenda/en/news/communication-cybersecurity-strategy-european-union-%E2%80%93-open-safe-and-secure-cyberspace>

range of actors and factors than for instance financial irregularities; while some EU participants argued for some kind of responsibility.

There were diverging views on what the role of the public sector is. Some US participants raised the risk of ending up with a minimum compliance approach by companies as a result of government intervention; while some EU participants argued that a minimum compliance approach is not tenable for organisations that rely on high security for their business offering. Such organisations will be naturally inclined to put in place more ambitious measures.

Regulatory requirements, including standards, tend to be sector-specific while cyber-security risks are cross-sectorial. Industries from US side shared experiences on how a horizontal framework such as the US Cybersecurity Framework can apply to different sectors: US industry sectors, such as financial and energy, have issued their own sector specific guidance to map the cross-sectorial framework to the requirements in their own sector, e.g. payment card industry requirements.

For SME specific needs the usefulness of lighter guidance, such as the UK cyber essentials, were mentioned.

Voluntary information sharing

In the panel there was broad agreement on the importance of voluntary information sharing. There were, however, some different views and experiences on the most useful ways to cooperate. On EU side the high number (possibly up to 900) and fragmentation of information sharing schemes is confusing users. In the US the landscape is more coherent with Information Sharing and Analysis Centres (ISACs) existing in 16 sectors and discussions ongoing on whether to 'standardise' the set-up of ISACs to make their cooperation smoother. In US ever more sectors are establishing ISACs, recently retail. There was general agreement that the EU would benefit from more coherence, through some kind of strategic or meta-guidance for information sharing arrangements.

Based on US experience some suggested that it is very difficult to include SMEs on an equal footing with big organisations in information sharing arrangements, because of differing resources. From EU side it was pointed out that SMEs are already sharing information by using anti-virus tools.

The government has a useful role as a convenor or trusted third party in information sharing arrangements, in the views of both US and EU participants. There are some difficult areas though, raised by EU participants, such as sharing with law enforcement bodies, where practices differ from country to country. Positive results of close public-private cooperation and sharing of information were mentioned, e.g. in the Nordic countries and the Netherlands.

Conclusion

US and EU concluded that all of the above topics merit to be further discussed and taken into account in their approaches. The US will issue a report⁶ on views expressed during the Request For Information, which will also refer to international aspects. The EU NIS Platform Plenary on 25.11.2014⁷ will be an occasion to input into the EU process since organisational risk management approaches and voluntary information sharing mechanisms in the EU context will be discussed then.

⁶ <http://www.nist.gov/cyberframework/upload/nist-cybersecurity-framework-update-120514.pdf>

⁷ <https://resilience.enisa.europa.eu/nis-platform/shared-documents/4th-plenary-meeting>

The event concluded with a discussion of possible topics for future US-EU stakeholder collaboration, based on the feedback heard throughout the day:

- Awareness
 - Best Practices and Next Steps
- Board of Directors / CEO
 - Responsibilities
 - Guidance
- Relationship to Existing Regulations
 - Information Sharing
 - Compliance vs. Best Practice
 - Steps to move from compliance-based to Risk Management
 - Country- and sector-specific needs
- International Policies
 - Alignment of country specific and other Approaches
- “Actionable” Guidance
 - The needs for the development of more detailed use cases
- Small and Medium organizations
 - What are the steps to best assist?
- The need for Trust – and related mechanisms to show trust
- Sharing across ISACs/Types/Voluntary vs. Mandatory sharing
 - Sectors growing and public roles of ISACs and CERTs working together.