CEER

Council of European Energy Regulators

The CEER Cybersecurity Report 2018: reacting to the CS recommendations of Regulators and the way forward

CEER Cybersecurity Workshop

Roman Picard, Co-Chair, CS WS

CEER Premises, Brussels, 19 June 2019

Fostering energy markets, empowering **consumers.**

CEER

Council of European Energy Regulators

Reasoning behind this report

- Shows the world that NRAs have cybersecurity clearly in mind and that NRAs have a unique position between MS governments, the EC and operations (suppliers, TSOs/DSOs).
- Provides a public position in order to foster and facilitate an open discussion.
- Provides concrete inputs which may be included in future regulation proposals or in implementation programs for the energy sectors.

Content in brief

- Main messages included in the report:
  - All parties in the energy sector should be cyber-secure, within reasonable cost-benefit analysis
  - NRAs should actively encourage cybersecurity in the energy sector
  - Legislation could even go further than the “Clean Energy for All Europeans” Package in terms of sectoral cybersecurity
  - NRAs should be prepared for the cybersecurity expenditure discussion
  - CEER and ACER may promote culture change
  - NRAs should advocate for the role of chief information security officer (CISO) in energy-sector entities
  - TSOs/DSOs/Suppliers should all have a robust cybersecurity strategy

Conclusions

- The report proposes monitoring of costs for cybersecurity in an explicit way;
- It provides an input on rethinking the topology of the grid, having Cyber incidents in mind when we design the grid, and proposes to explore alternative ways of thinking in the smart-grid age;
- The report underlines the lack of knowledge in many key areas, which may require more work for future and may be of help for the regulators regulating innovative fields.

Recommendations (1)

- Even non-OES actors in energy sector should apply cybersecurity standards as close as possible to those of OES.
- NRAs should encourage meeting compliance with the NIS Directive and provide support in transposing horizontal regulation into sector-specific best practices.
- The CEFAE package now published provides the means to potentially cover the cybersecurity needs of entire electricity value chain (e.g. to generation). It may also serve as a basis to define the cybersecurity needs of the rest of the energy sector.
- NRAs need to be prepared to monitor and evaluate cybersecurity expenditure, particularly of regulated entities.

Recommendations (2)

- Management in energy sector entities, including NRAs, should provide clear guidance on cybersecurity governance, including, the proper place and role for the chief information security officer (CISO).
- TSOs/DSOs/Suppliers should have a cybersecurity strategy and they should set clear and effective cybersecurity measures prior embracing new technologies such as cloud computing or systems for the handling of big data.
- CEER and ACER may promote cultural change through activities such as partnerships and awareness campaigns.

Council of European Energy Regulators

Thank you for your attention!

CEER

Council of European Energy Regulators

www.ceer.eu