Cyber Security Requirements in Context of REMIT Regulation

Nikoloz Sumbadze
Georgian Energy and Water Supply
Regulatory Commission (GNERC), TF4 Leader

ECRB REMIT WG 3rd Meeting,
12 February 2020 Vienna

Importance of Cyber Security

Technological Advancements & Macro-Trends

- Industry 4.0
- Digitalisation
- “Smartification”
- 24/7 Connectivity
- Internet of Things
- Big Data, Smart Analytics
- Process & Computing Power
- Automation, Machine 2 Machine

Increasing System Complexity

- Demand Response
- Competitive Pressure
- Multiple Market Actors
- Real-Time Operations
- Multi-Directional System
- System Balancing / Volatility
- Decentralization / Renewables
- Multiple Standards / Regulations

REMIT Regulation

- Market Participants
  - Publish inside information (critical infrastructure – article 4(7))
  - Provide information to NRAs
- National NRAs
  - Market monitoring – information on wholesale products and market participants
  - Register market participants
  - ensure the confidentiality, integrity and protection of the Information
- ECRB
  - Information provided by national NRAs
  - establish a central register of market participants.

CEER on Cyber Security

- All parties interacting with the grid not included in the list of Operators of Essential Services should aim to develop and apply cybersecurity standards and measures which will support further innovation and digitalization in the energy sector.

- NRAs should proactively engage with energy stakeholders in order to encourage them to be in compliance with the (network and information systems) NIS Directive and provide support for transposing horizontal regulation into sector-specific best practices

- The Clean Energy Package should be even more effective in order to serve as a basis to define the additional cybersecurity needs of the rest of the energy sector (e.g. including the gas and oil sub-sectors).

- NRAs may also required to monitor the cybersecurity related expenditure and the effects of those cybersecurity-related investments to the risk landscape of the energy system and of individual operators.

- Management in energy-sector entities, including NRAs, should provide clear guidance on cybersecurity governance, including the role and, eventually, as in other international examples, 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: this may allow the further development of a cybersecurity culture within the energy sector.

Source: Cybersecurity Report on Europe's Electricity and Gas Sectors, CEER, 2018

ECRB Cyber Security working Group

TASK 1 – Identification and designation of critical energy infrastructures

- Review / report on the current state of CI / ES
- Common platform for regional designation of ECCI

TASK 2 – Operator Security Plans (OSP)

- Guidelines for Operator Security Plans
- Regional Implementation of Operator Security Plans

TASK 4 – Energy Cybersecurity Strategies in the Energy Community

- Report on the Cyber security Strategies of the Energy Community
- Regional Cyber security Strategy of the Energy Community

Potential Activities under TF4

- Review of best-practice experience gained on EU level by CEER and ACER
- Coordination with ECRB cyber security working group
- Identification of market participants, NRAs and their roles

  Survey of EnC NRAs
- Identification of potential risks and their evaluation

  Example: Risk (R) = Feasibility of Occurrence (F) x Probability of Occurrence (PQ) x Impact (I)
- Selection of risks, aggregation by categories and creating risk matrix
- Develop risk mitigation recommendations