CEER

Council of European Energy Regulators

Session V: Cybersecurity

12th EU-US Energy Regulators Roundtable

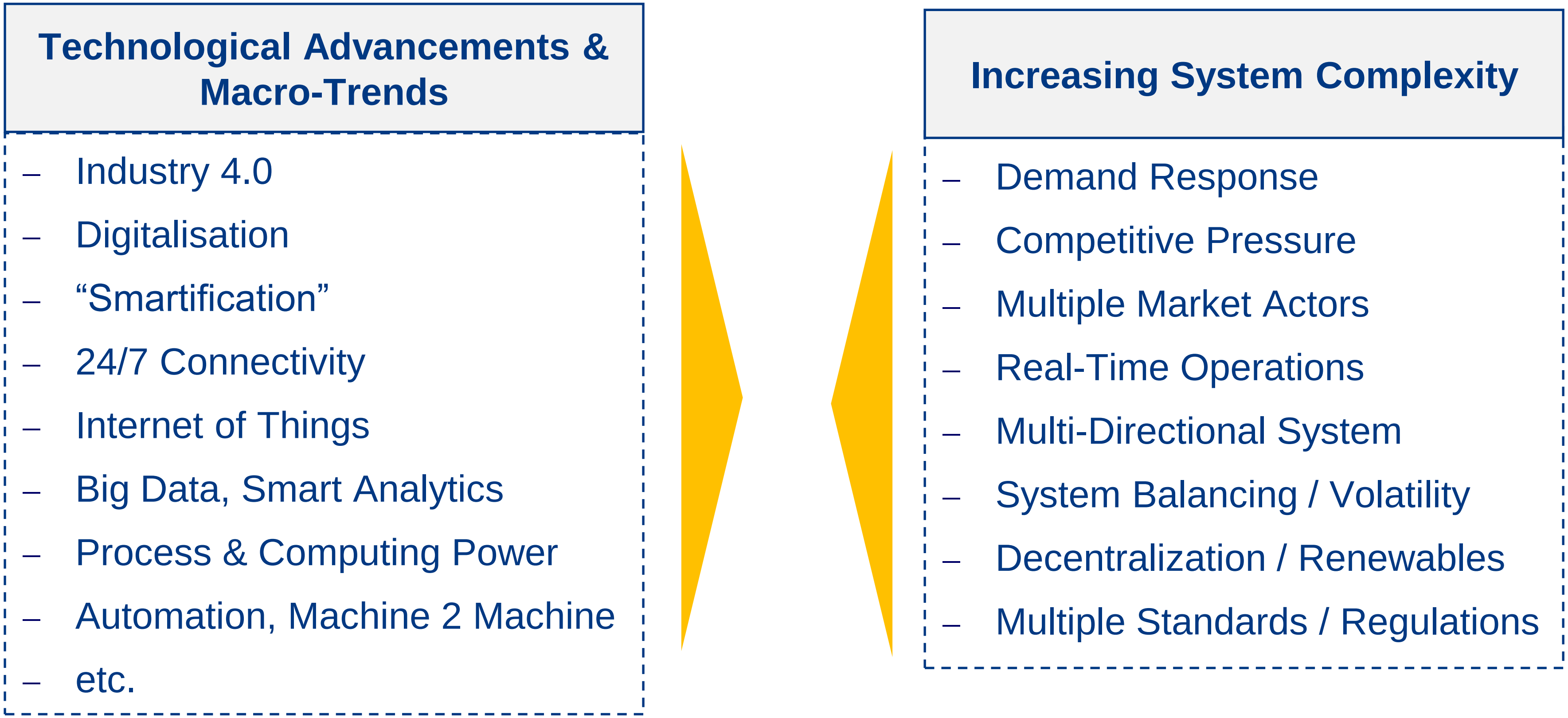
26th April 2016
Philipp Irschik, CEER, Chair Cybersecurity Workstream

Fostering energy markets, empowering **consumers.**

AGENDA

1. **Why is Cybersecurity** *(in the energy sector)* **such a “hot“ topic?**
2. **Is Cybersecurity a relevant topic to act for lawmakers & NRAs?**
3. **If so, what can or should NRAs do about Cybersecurity?**

With greater system complexity, the reliance on IT increases



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
- etc.

Increasing System Complexity

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

New interdependencies, opportunties but also vulnerabilities emerge as IT and OT continue to converge.

The importance of CS in the energy sector results from several factors

- **Motivation behind attacks** usually differs from other sectors (disruption of supply)
- **Criticality of the energy sector** to the functioning of society; **cascading effects**
- **Costs of a disruption of service** / outage to a country‘s economy
- Wide use of **old, stand-alone proprietary home-made legacy systems**
- **Few digital natives**; C-level awareness only gaining traction
- **Long investment cycles** make technology assessment difficult
- Heavy **reliance on outsourced IT-expertise**, third parties, and vendors
- **Paradigm Shift** (operational safety and reliability of supply + security against intended attacks

A rather reliable sector (energy) becomes more and more interwoven and dependent on a rather unreliable sector (IT) (i.e. n-1 criteria)

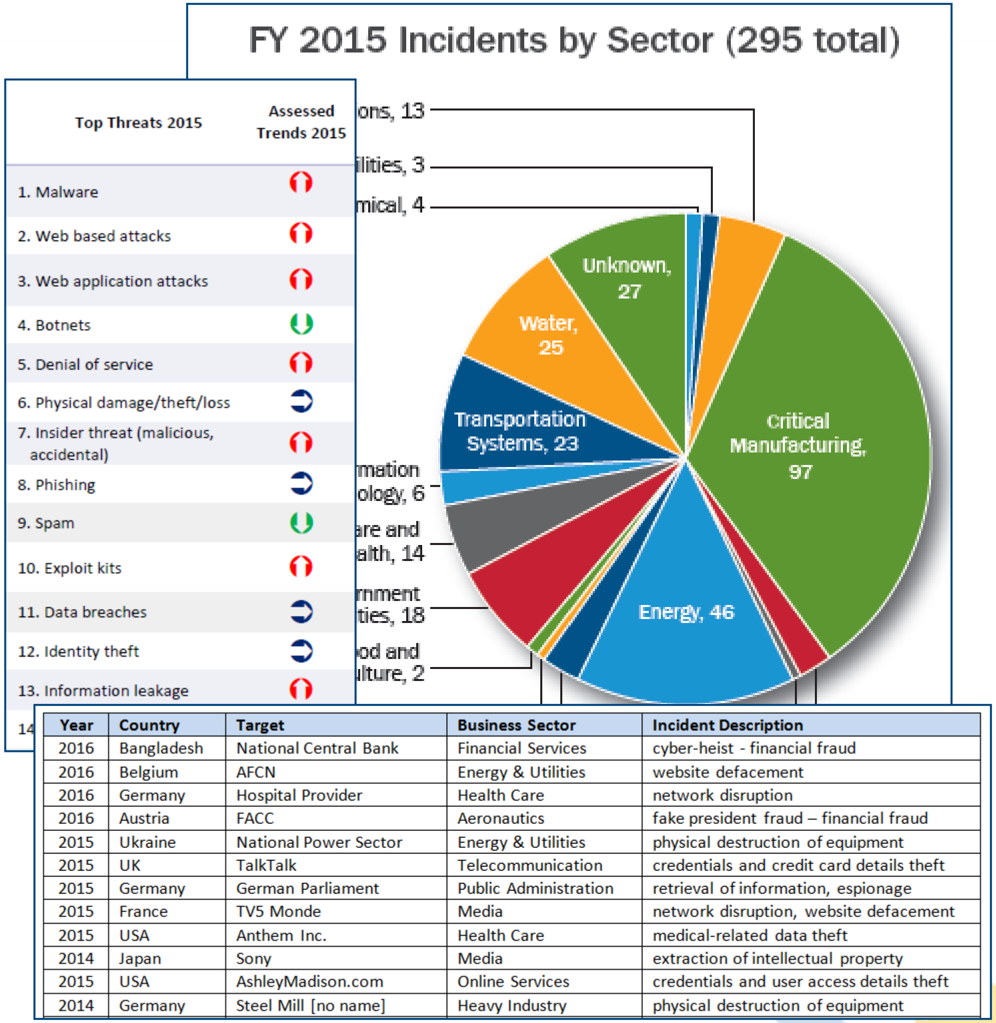
CEER
Council of European Energy Regulators

Daily experiences show that the threat of cyber-incidents is real

- Energy companies and network operators are (supposedly) amongst **the most attacked critical infrastructures providers.**

- Attacks are becoming **more sohisticated and frequent**. The **cost of ensuring IT- and Cybersecurity** is steadily augmenting. (Guesstimate: $575 bn)

- The frequency of attacks with the purpose of causing the **deliberate disruption of network services** and the **physical destruction** of equipment is real and – albeit still low - steadily augmenting.



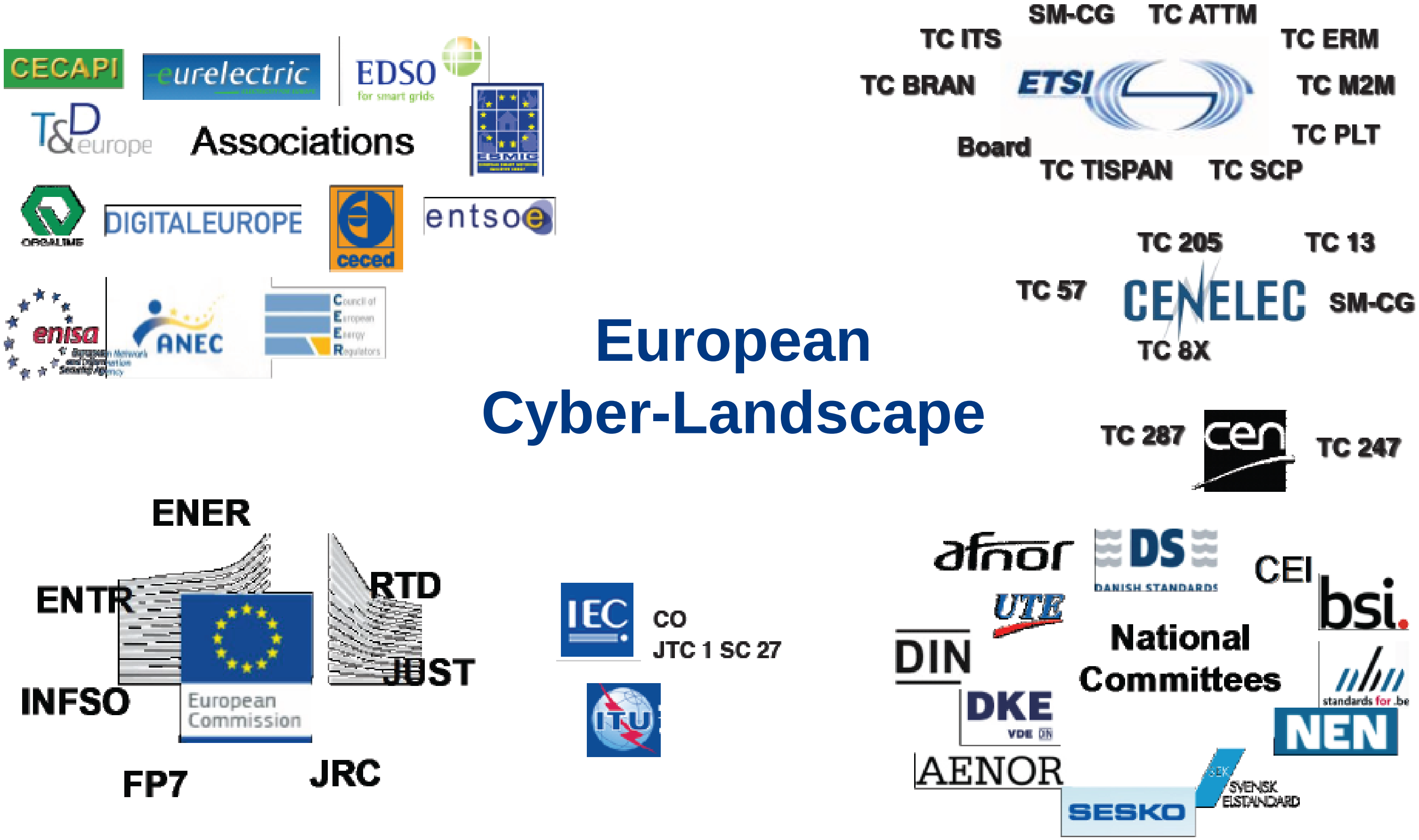
Top Threats 2015	Assessed Trends 2015
1. Malware	↑
2. Web based attacks	↑
3. Web application attacks	↑
4. Botnets	↓
5. Denial of service	↑
6. Physical damage/theft/loss	⟳
7. Insider threat (malicious, accidental)	↑
8. Phishing	⟳
9. Spam	↓
10. Exploit kits	↑
11. Data breaches	⟳
12. Identity theft	⟳
13. Information leakage	↑
14	

FY 2015 Incidents by Sector (295 total)

Year	Country	Target	Business Sector	Incident Description
2016	Bangladesh	National Central Bank	Financial Services	cyber-heist - financial fraud
2016	Belgium	AFCN	Energy & Utilities	website defacement
2016	Germany	Hospital Provider	Health Care	network disruption
2016	Austria	FACC	Aeronautics	fake president fraud – financial fraud
2015	Ukraine	National Power Sector	Energy & Utilities	physical destruction of equipment
2015	UK	TalkTalk	Telecommunication	credentials and credit card details theft
2015	Germany	German Parliament	Public Administration	retrieval of information, espionage
2015	France	TV5 Monde	Media	network disruption, website defacement
2015	USA	Anthem Inc.	Health Care	medical-related data theft
2014	Japan	Sony	Media	extraction of intellectual property
2015	USA	AshleyMadison.com	Online Services	credentials and user access details theft
2014	Germany	Steel Mill [no name]	Heavy Industry	physical destruction of equipment

Source: European Union Agency for Network Security, 2015; ICS-CERT Annual Report 2015

The good new is that CS is already addressed by a multitude of actors



European Cyber-Landscape

Associations

SM-CG TC ATTM TC ITS TC ERM TC BRAN TC M2M Board TC PLT TC TISPAN TC SCP

TC 205 TC 13 TC 57 SM-CG TC 8X

TC 287 TC 247

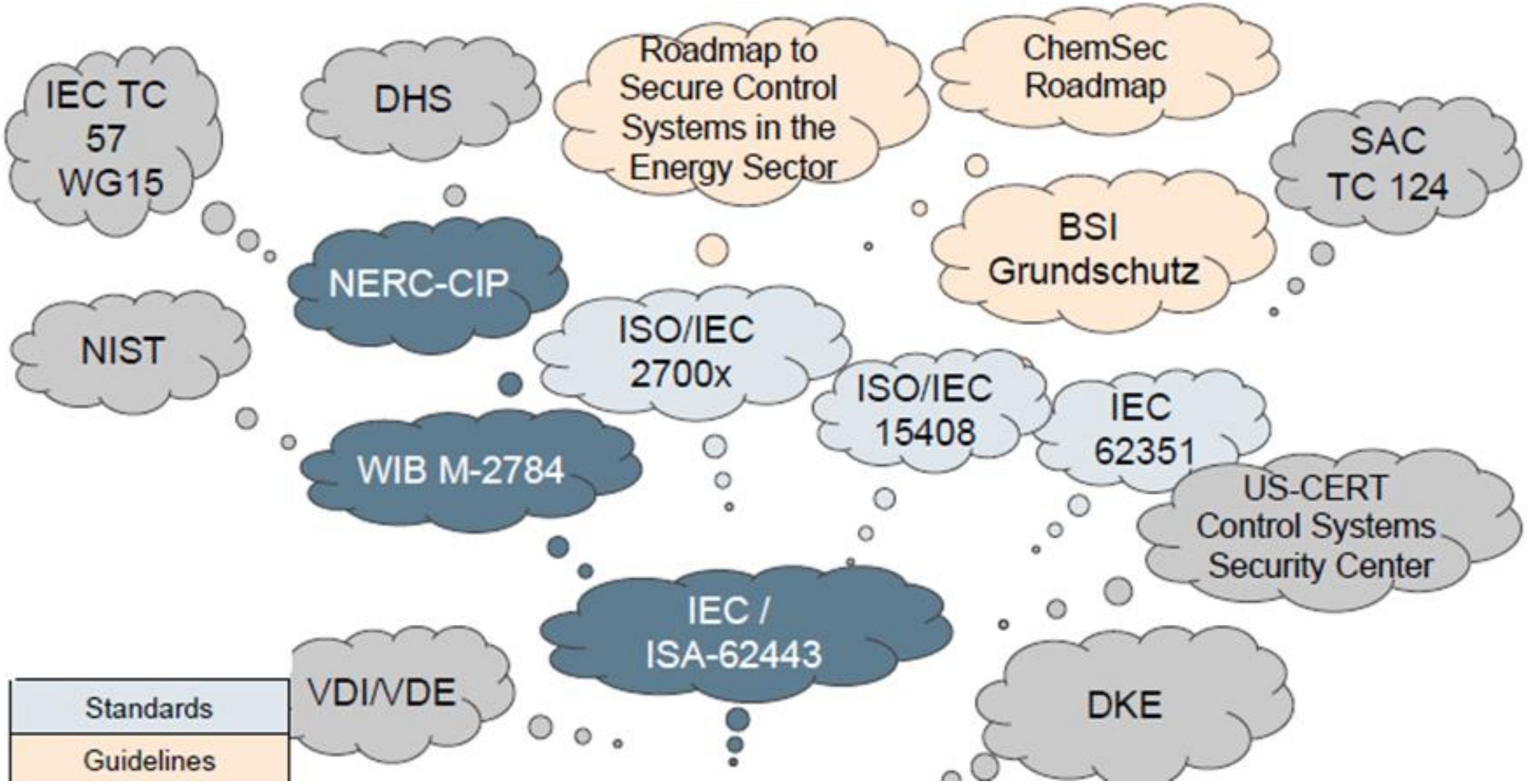
ENER ENTR RTD JUST INFSO FP7 JRC

CO
JTC 1 SC 27

National Committees

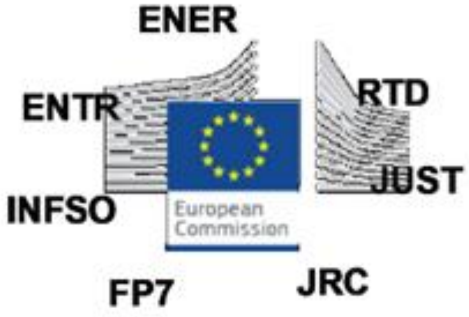
Numerous European and national initiatives are already dealing with the risk of cyber-attacks; few of them are focusing on the entire value chain (E2E).

An extensive variety of guidelines, standards and frameworks exists



Uncoordinated efforts result in a variety of heterogeneous guidelines and standards. Harmonization is often seen as the key objective. Is this true?

A comprhensive but also diverse EU policy framework is in place



EU Strategy Documents:

- Cybersecurity Strategy for the European Union
- European Agenda on Security
- Digital Single Market Strategy (DSM)
- European Cloud Computing Strategy
- Internal Security Strategy for the European Union

EU Legislation / Directive(s) / Regulation(s):

- Data Protection Directive (DPR)
- Directive on European Critical Infrastructure (ECIs)
- Regulation on Electronic Identification and Trusted Services in the Internal Market (eIDAS)

Communication(s) / Action Plans:

- Critical Information Infrastructure Protection (CIIP) Action Plan
- Commission Communication on Critical Infrastructure Protection
- Action Plan for an Innovative and Competitive Security Industry
- Internet of Things – An Action Plan for Europe

Frameworks and Programs:

- Electronic Communications Regulatory Framework
- Framework to Build Trust in the Digital Single Market (DSM) for E-Commerce and Online-Services
- European Program for Critical Infrastructure Protection (EPCIP)

Existing European legislations and strategies are often too general and unspecific and often give little reference to the energy sector.

Approaches to CS and CIP differ substantially in the European Union

- Three CIP-Profiles:
  - **Centralized Approach („*command-and-control*"):**
    - Characterisitics: central authority across sectors, comprehensive legislation and obligations for providers of critical infrastructure
    - Examples: France, Germany
  - **Decentralized Approach:**
    - Characteristics: principal of subsidiarity, strong cooperation between public and private sector, sector-specific legislation
    - Examples: Sweden, Switzerland
  - **Co-regulation with private sector:**
    - Characteristics: institutionalized cooperation between public and private sector (public private partnerships)
    - Examples: Netherlands, Austria

Source: European Union Agency for Network Security, 2015

The NIS-Directive is one key initiative to introduce baseline CS-obligations

- Network and Information Security Directive (NISD)
  - ► deemed essential for establishing a Single European Digital Market
  - ► **Objective:** Strengthen network and information security (NIS) in the European Union
  - ► **Introduction of first ever EU-wide baseline cybersecurity obligations** for
    - I) „***operators of essential services***“ (sectors include: **energy**, transport, banking, financial markets, health and water supply), and
    - II**) digital service providers** (search engines, e-commerce marketpaces, cloud-computing)
  - ► Directive focuses on **three (3) pillars**:
    - raise resilience through the **introduction of baseline cybersecurity standards**,
    - **ensure Union-wide minimum cybersecurity capabilities** through audits & penalities
      - – Introduction of NISD-competent authorities on national and sector level
    - **improve (cross-broder) information sharing and collaboration** through reporting obligations:
      - – cross-border: between EC and MS, MS and MS, with ENISA
      - – nationally: between public and private stakeholders,
  - ► Triologue-agreement on 07/12/2015 – likely formal adoption in 1HY 2016 (17.05.2016)
  - ► Time for national transposition and introduction: 27 months

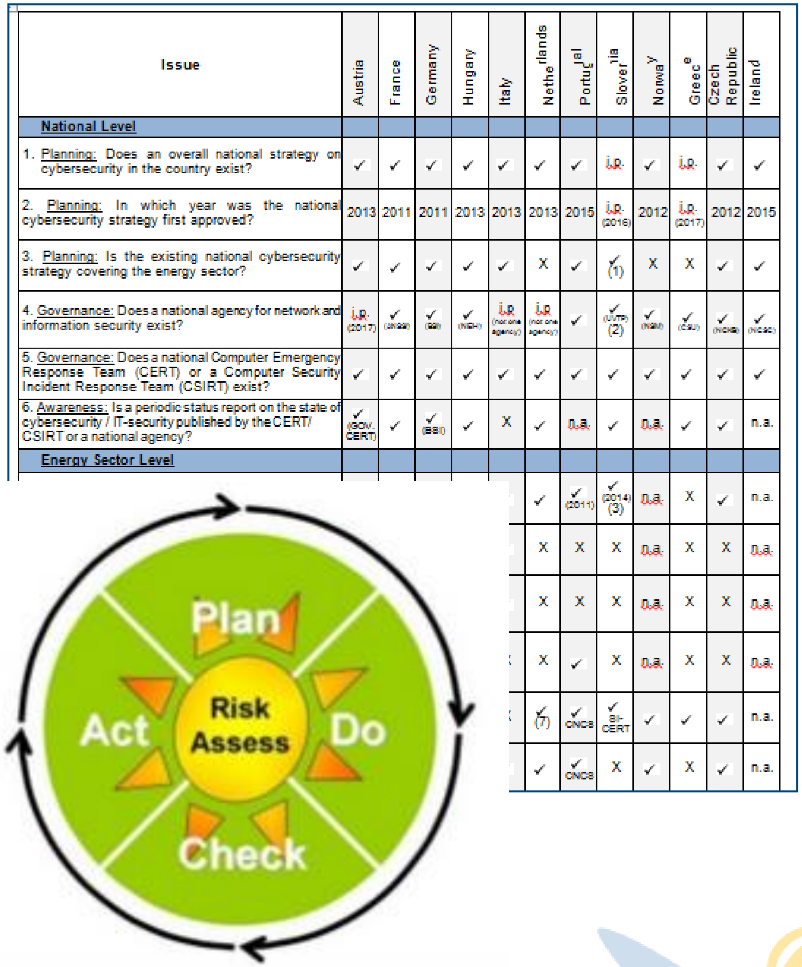
The GDPR aims to set EU-wide, baseline data protection standards

- General Data Protection Regulation (GDPR)

  - deemed essential for establishing a Single European Digital Market
  - **Objective:** Strengthen data protection rights of individuals, provide businesses with clear, modern and applicable rules
  - Main rules include:
    - easier access to private data,
    - a right to data portability,
    - „right to be forgotten“,
    - reporting obligations for „data handlers“ in case of data theft,
    - penalties in case of severe data theft incidentes
  - Triologue-agreement on 07/12/2015 – formally adopted in 04/2016
  - Legislation to take effect in 2018

The CS landscape differs substantially amongst CEER Member Countries

- Substantial differences exist in terms of:
  - Governance and Planning; Availability of a Legal Framework
  - (Sector-specific) Risk Assessment and Vulnerability Identification
  - Availability of (binding) baseline Security Standards and Obligations, (security) Audit Processes
  - Information Sharing and Incident Reporting, CERTs / CSIRTs
  - Awareness Building, Training Initiatives, Sector Excercises, PPPs



Issue	Austria	France	Germany	Hungary	Italy	Netherlands	Portugal	Slovenia	Norway	Greece	Czech Republic	Ireland
National Level												
1. Planning: Does an overall national strategy on cybersecurity in the country exist?	✓	✓	✓	✓	✓	✓	✓	i.p.	✓	i.p.	✓	✓
2. Planning: In which year was the national cybersecurity strategy first approved?	2013	2011	2011	2013	2013	2013	2015	i.p. (2016)	2012	i.p. (2017)	2012	2015
3. Planning: Is the existing national cybersecurity strategy covering the energy sector?	✓	✓	✓	✓	✓	X	✓	✓ (1)	X	X	✓	✓
4. Governance: Does a national agency for network and information security exist?	i.p. (2017)	✓ (ANSSI)	✓ (BSI)	✓ (NBH)	i.p. (not one agency)	i.p. (not one agency)	✓	✓ (UVTP) (2)	✓ (NSM)	✓ (CSU)	✓ (NCKB)	✓ (NCSC)
5. Governance: Does a national Computer Emergency Response Team (CERT) or a Computer Security Incident Response Team (CSIRT) exist?	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
6. Awareness: Is a periodic status report on the state of cybersecurity / IT-security published by the CERT/ CSIRT or a national agency?	✓ (GOV. CERT)	✓	✓ (BSI)	✓	X	✓	n.a.	✓	n.a.	✓	✓	n.a.
Energy Sector Level												
						✓	✓ (2011)	✓ (2014) (3)	n.a.	X	✓	n.a.
						X	X	X	n.a.	X	X	n.a.
						X	X	X	n.a.	X	X	n.a.
						X	✓	X	n.a.	X	X	n.a.
						✓ (7)	✓ CNCS	✓ SI-CERT	✓	✓	✓	n.a.
						✓	✓ CNCS	X	✓	X	✓	n.a.

Source: Draft Report on Cybersecurity in the Energy Sector, CEER, 2016

What NRAs may want to do - recommendations & conclusion

- Clearly define the desired role, engagement level and strategy of the Authority.
- Understand the impact of digitalization and technical advancements.
- Encourage and support national or/and energy sector-specific (quantitative) risk assessments to better understand vulnerabilities and the risk-landscape.
- Support information sharing initiatives and collaboration between public and private stakeholders and institutions; gradually build trust.
- Encourage cross-border cooperation and joint initiatives at EU level to share best-practices, knowledge, information and resources in a collective effort.
- Actively engage and support European/regional/national initiatives aimed at driving CS-awareness and/or introducing baseline security and safety standards.

Thank you for your attention.

CEER

Council of European
Energy Regulators

www.ceer.eu

CEER

Council of European Energy Regulators

What are European NRAs talking about in regard to CS and what is their opinion?

- Is there **a need for regulation, for common standards and some set of harmonized European baseline security and safety rules and standards?** What will this mean for the treatment of personal data?
- Is there a **need for a seperate treatment of critica infrastructure providers?** Do we need reporting obligations, sector specific CERTs/CIRTs, etc.?
- To **what extent will the proposed European framework help** resolve existing discrepancies between MS?
- **Who has the responsibility to act on a European / national level**?
- **What can NRAs do? (and what can we not do?)** Which legal constraints do exist? What are their capabilities?
- How can an **adequate balance between (cost) efficient behaviour** of regulated companies and security be reached?
- How can we/NRAs **ensure security along the entire value chain**? How do we interact with and overcome the dependency of suppliers?