


ACER

 Agency for the Cooperation
of Energy Regulators

Cyber Security – EU developments

Prepared by: Stefano Bracco – Stefano.BRACCO@acer.europa.eu
(Security Officer and Knowledge Manager at the Agency for the Cooperation of
Energy Regulators)

Ljubljana, 10 December 2018



This presentation was prepared by Stefano Bracco in his personal capacity and at his best knowledge as an expert. The facts are provided with sources, when available, the opinions expressed in this presentation are the author's own and may not reflect the view of the Agency for the Cooperation of Energy Regulators, or of the European Union Institutions.

Thank you for your patience in reading this disclaimer



- Fundamentals – Why do we do this?
- What have European policymakers done to date?
- What are we planning to do in the future?
- What not to do?



Technological Advancements

- Industry 4.0
- Digitalisation
- "Smartification"
- 24/7 Connectivity
- **Internet of Things (IoT and IIOT)**
- Big Data, Smart Analytics
- Process & Computing Power
- Automation, Machine 2 Machine
- **Blockchain**
- **Artificial Intelligence**
- **Quantum Computing**
- **E-Mobility**



Increased System Complexity

- Demand Response
- Competitive Pressure
- Multiple Market Actors
- Real-Time Operations
- Multi-Directional System
- System Balancing / Volatility
- Decentralization / Renewables
- Multiple Standards / Regulations
- **More regulations covering the same markets in a non-coherent way**
- **Non-coordinated markets Energy Markets (Systems)**
- **Smart Contracts**



New interdependencies and opportunities, but vulnerabilities as IT (Information Technology) and OT (Operational Technology) continue to converge and interoperate

Reality check on a cyber attack to the grid: Ukraine 2015

23 Dec 2015 h 15:35



**3 DSOs
affected**



225.000



**103
Cities
and
Towns
Affected**



**135 MW
Impact**



**7 x 110 KV
SubStations
23 x 35 KV
SubStations
(up to 50)**



**3.5 to 7
hours
Outage
Duration**



**100s
Damaged**



**10s Field
Device
Affectes**



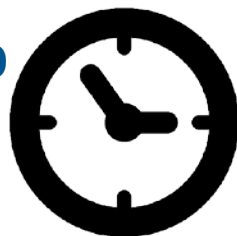
**Outside
Temp.
Between
4 and
-8° Cent.**

(Source: SANS ICS - ICS.SANS.ORG)

Saturday, November 4, 2006



15.000.000



Around 2
hours
Outage
Duration



More
than ten
Nation
States
were
involved

Root cause after the analysis

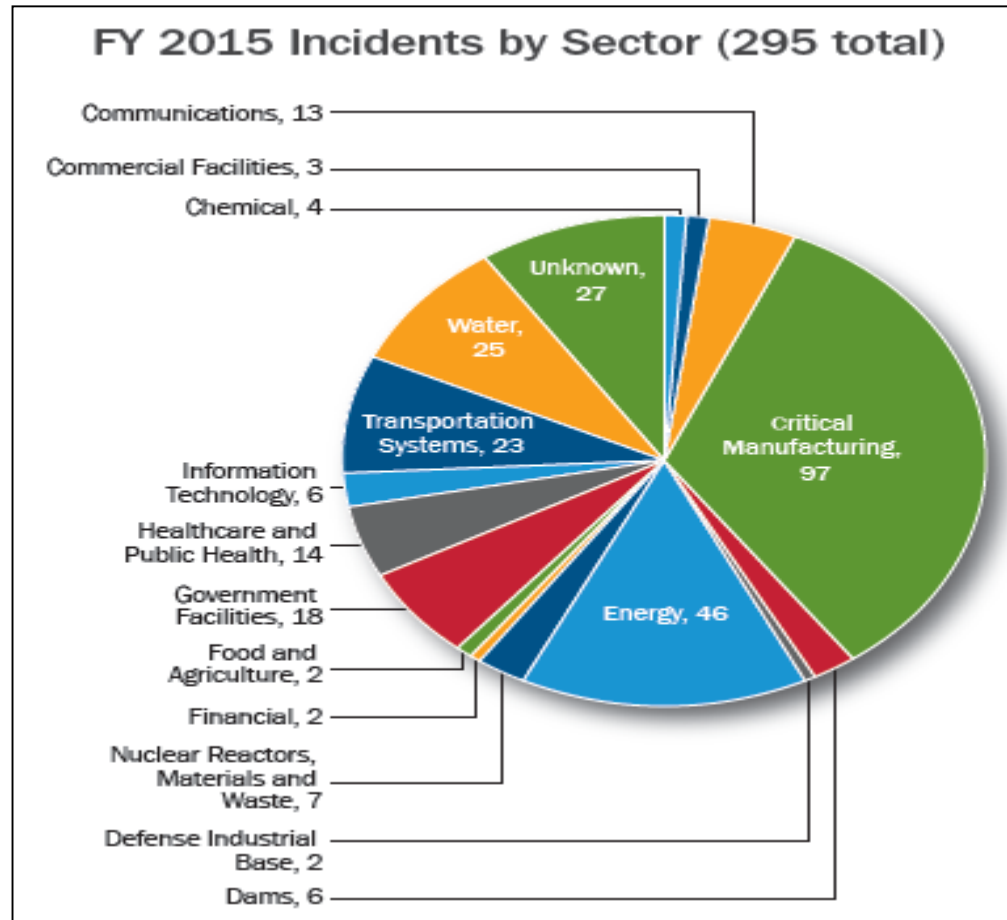
- Non-fulfilment of the N-1 criterion
- Insufficient inter-TSO co-ordination

NOTE: This was not a Cyber incident/attack. It is just used as a term of comparison.

(Source:

https://www.entsoe.eu/fileadmin/user_upload/_library/publications/ce/otherreports/Final-Report-20070130.pdf)

- Energy companies (excluding Nuclear Fuel Lifecycle) and network operators are potentially among the most attacked critical infrastructures providers
- Attacks are becoming structured, coordinated, sophisticated and frequent
- The cost of ensuring IT and cybersecurity is increasing; at the same time there are difficulties to assess costs for regulated entities
- The frequency of disrupting network services and destroying equipment is considered to be low - but research forecast an increase in frequency and magnitude of attacks, and there are initial signals that some equipment may start breaking in future



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

As cyber attacks and costs increase, CS is more in focus (and also its interdependencies)

Table 1: Assessments by sector, March/April 2017.

Assessments by Sector	March 2017	April 2017	March/April Totals
Chemical			
Commercial Facilities			
Communications			
Critical Manufacturing			
Dams	10	4	14
Defense Industrial Base			
Emergency Services			
Energy		1	1
Financial Services			
Food and Agriculture			
Government Facilities			
Healthcare and Public Health			
Information Technology			
Nuclear Reactors, Materials, and Waste			
Transportation Systems			
Water and Wastewater Systems			
Monthly Totals	10	5	15 Total Assessments

Table 1: Assessments by sector, May/June 2017.

Assessments by Sector	May 2017	June 2017	May/June Totals
Chemical			
Commercial Facilities			
Communications			
Critical Manufacturing	2		2
Dams		6	6
Defense Industrial Base			
Emergency Services	3		3
Energy		8	8
Financial Services			
Food and Agriculture			
Government Facilities			
Healthcare and Public Health			
Information Technology			
Nuclear Reactors, Materials, and Waste			
Transportation Systems			
Water and Wastewater Systems	9	6	15
Monthly Totals	14	20	34 Total Assessments

Table 1: Assessments by sector, July/August 2017.

Assessments by Sector	July 2017	August 2017	July/August Totals
Chemical			
Commercial Facilities	4	3	7
Communications			
Critical Manufacturing			
Dams	1		1
Defense Industrial Base			
Emergency Services			
Energy	1	9	10
Financial Services			
Food and Agriculture			
Government Facilities	3	5	8
Healthcare and Public Health			
Information Technology			
Nuclear Reactors, Materials, and Waste			
Transportation Systems		5	5
Water and Wastewater Systems	4	3	7
Monthly Totals	13	25	38 Total Assessments

Table 1: Assessments by sector, November/December 2017.

Assessments by Sector	November 2017	December 2017	November/December Totals
Chemical			
Commercial Facilities			
Communications			
Critical Manufacturing			
Dams			
Defense Industrial Base			
Emergency Services			
Energy	7	6	13
Financial Services			
Food and Agriculture			
Government Facilities		3	3
Healthcare and Public Health			
Information Technology			
Nuclear Reactors, Materials, and Waste			
Transportation Systems	3	3	6
Water and Wastewater Systems			
Monthly Totals	10	12	22 Total Assessments

Table 1: Assessments by sector, September/October 2017.

Assessments by Sector	September 2017	October 2017	September/October Totals
Chemical			
Commercial Facilities			
Communications			
Critical Manufacturing	3		3
Dams			
Defense Industrial Base			
Emergency Services			
Energy	11		11
Financial Services			
Food and Agriculture			
Government Facilities			
Healthcare and Public Health			
Information Technology			
Nuclear Reactors, Materials, and Waste			
Transportation Systems			
Water and Wastewater Systems	8	8	16
Monthly Totals	22	8	30 Total Assessments

Source: US ICS-CERT Monitor Newsletters

What are the most significant drivers behind your spending on information security?

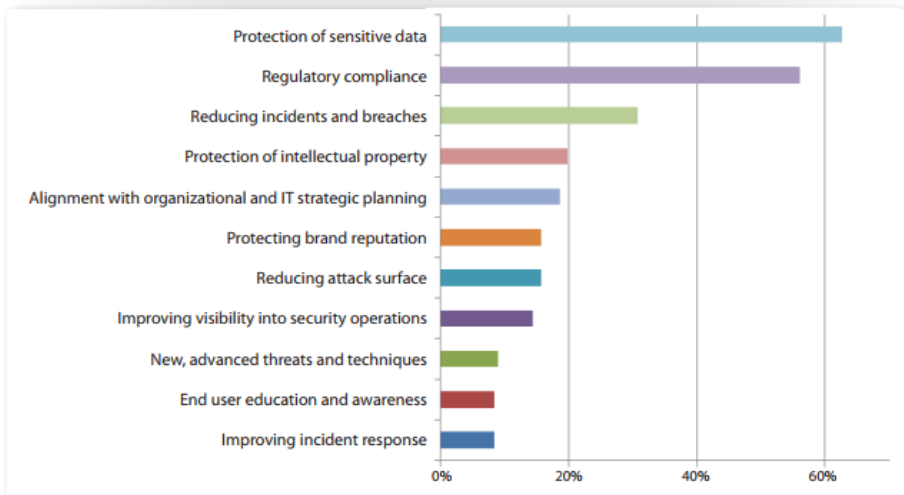
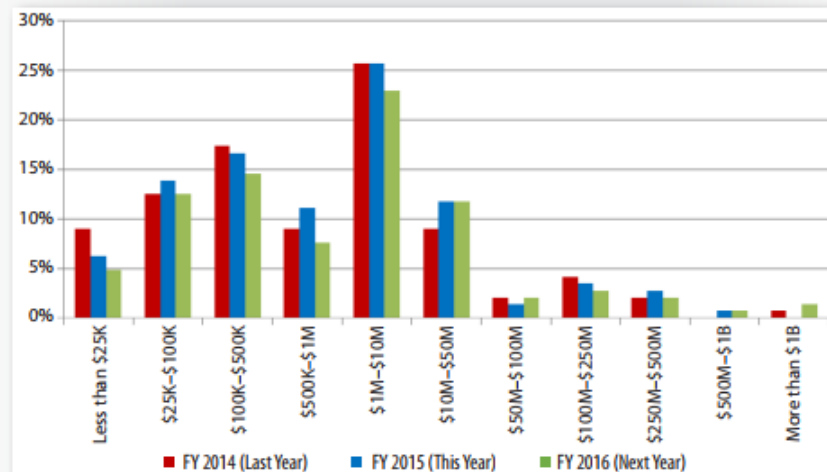


Table 2. Overall Median Budget and Percentage Allocated to Security by Year

	FY 2014	FY 2014	FY 2016 (Projected)
IT Budget	\$500K-\$1M	\$500K-\$1M	\$500K-\$1M
% Budget for Security	4%-6%	4%-6%	7%-9%

Source: <https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697>

IT Budget Range



Percentage of IT Budget Spent Annually on Security

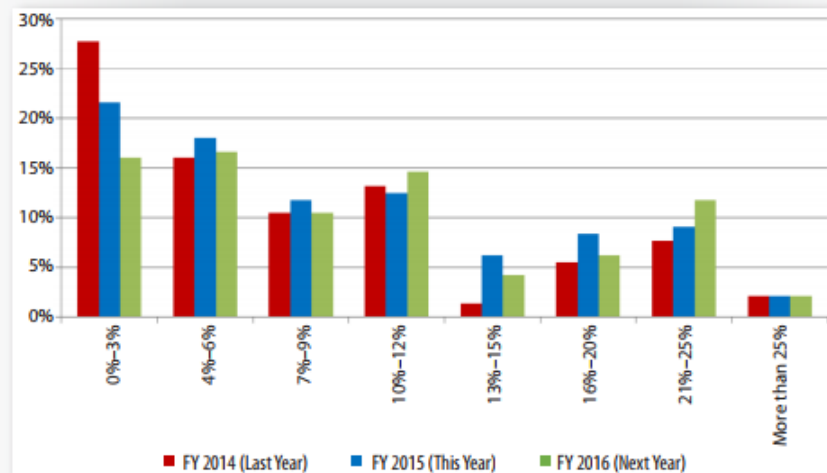
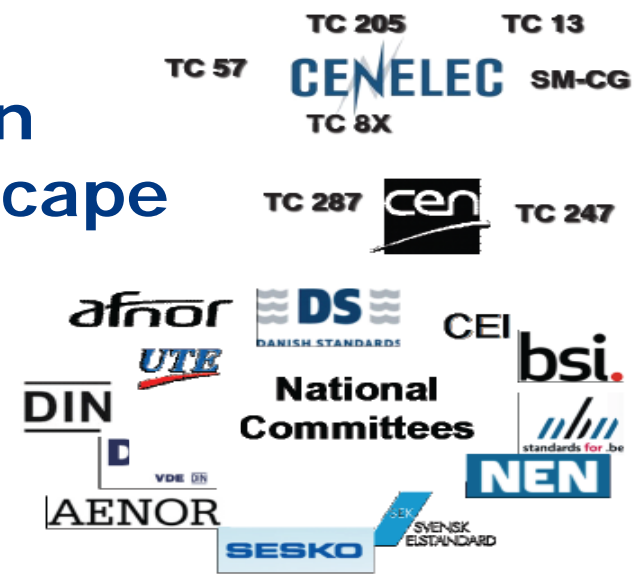
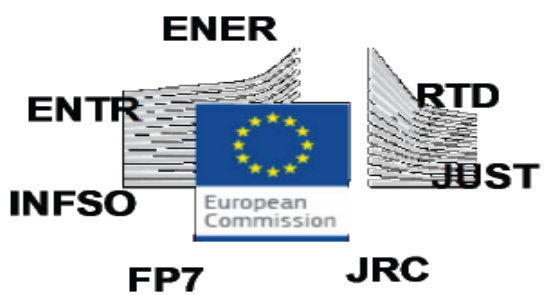


Figure 3. IT Annual Budget Ranges and the Percentage Spent on Security

- ✓ **Political changes within the European Union** (BREXIT and need to review Treaties) do not help
- ✓ **Third Package didn't include certain topics** (the main focus of the 3rd Energy Package was on unbundling, Independent regulators, ACER, Cross-border cooperation through ENTSO-E and ENTSG, open and fair retail markets)
- ✓ We move from „Single Energy Market“ against **„Single Energy Market with a strong Regional Identity“**
- ✓ „Single Energy Market“ vs **„Single Digital Energy Market“**
- ✓ **Dependency of the EU Energy Sector on Third Countries – Security of Supply**
- ✓ Need to have **inclusive policies to allow all actors to enter the market and to have equal opportunities**, as well as assure that consumers are not penalized by a too open inclusive policy
- ✓ Need to change the Energy Mix (**decarbonisation and Paris Agreement are a priority**)
- ✓ Cybersecurity is heavily considered; but scarcely understood as the **number of experts is very low**
- ✓ **„Clean energy for all Europeans“ and the „Cybersecurity Act“ are the future but they do not come at zero cost**



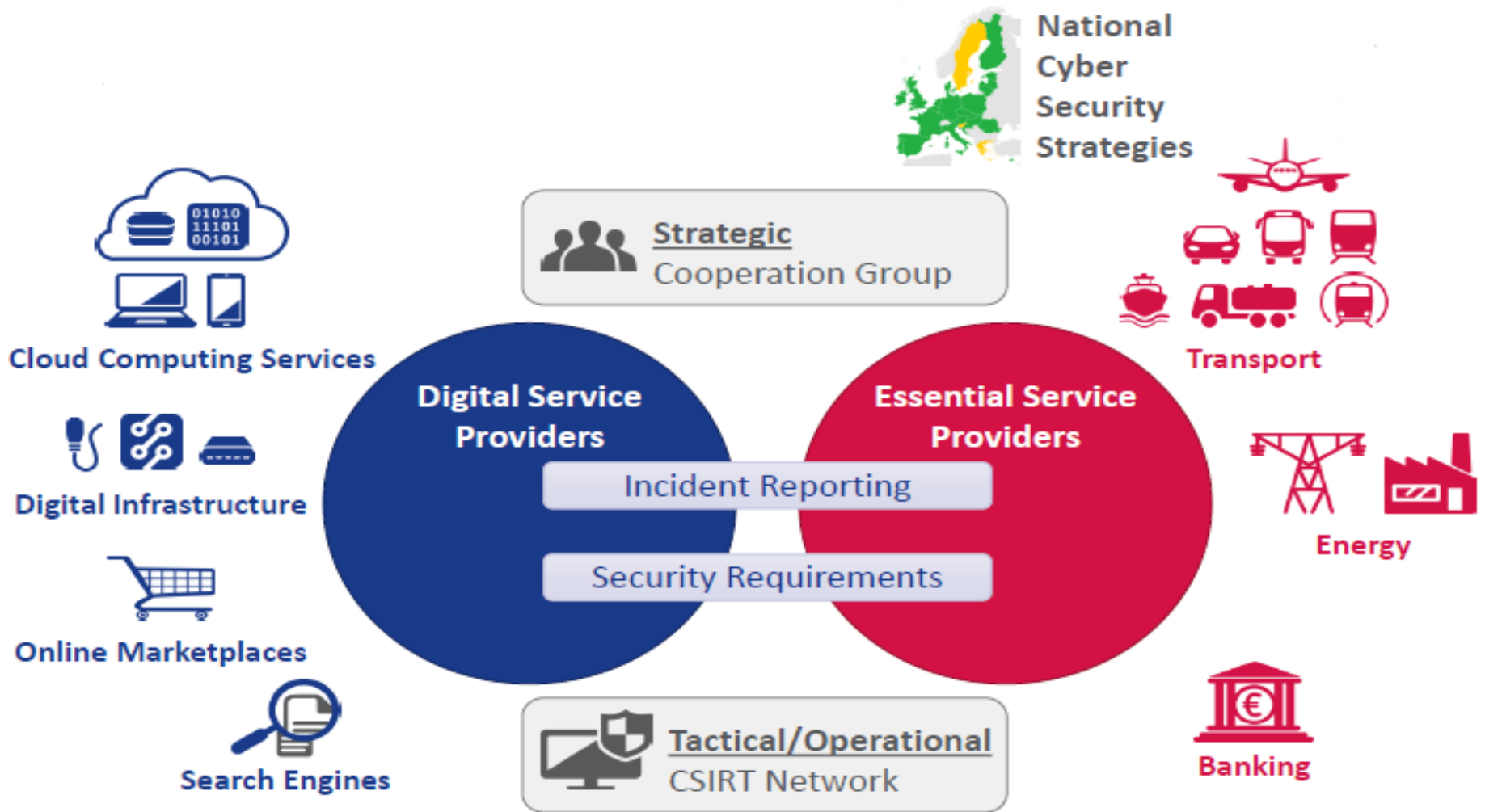
European Cyber Landscape



- Different guidelines / standards, often not energy specific, and not converging
- Sometimes unclear governance
- No clear ownership and responsibility of the issue
- **New emerging standards and old known problems (use of NIST, ISO - ISO/IEC 27019:2017 Information technology - Security techniques - Information security controls for the energy utility industry)**

- JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (7.2.2013)
- JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL - Resilience, Deterrence and Defence: Building strong cybersecurity for the EU (13.9.2017)

- New legislation to strengthen EU network and information security
- Important to create a secure EU Digital Single Market
- Introduces new EU-wide baseline CS obligations for:
 - » Operators of essential services in energy, transport, banking, etc
 - » Digital service providers - search engines, online marketplaces, cloud-computing
- Directive focuses on 3 pillars:
 - » Raising **resilience** through **baseline CS standards**
 - » Ensuring EU-wide minimum CS **capabilities** through **audits** and **penalties**
 - NIS competent authorities on national and sector level
 - » Improving **information-sharing** and **collaboration through reporting obligations**
 - Cross-border between the EC and MS, MS and MS, with the help of ENISA
 - Nationally between public and private stakeholders



Source: European Union Agency for Network Security, 2016

Improved National Capabilities

- National strategy on the security of network and information systems
- National competent authorities for Cyber Security
- Computer Security Incident Response Teams (CSIRTs)

Improved EU Cooperation

- Cooperation Group
- Network of the national CSIRTs

Date	Entry into force +	Milestone
Aug 2016	-	Entry into force
Feb 2017	6 months	Cooperation Group begins tasks
Aug 2017	12 months	Security and notification requirements for DSPs
Feb 2018	18 months	Cooperation Group establishes work programme
May 2018	21 months	Transposition into national law
Nov 2018	27 months	Member States to identify operators of essential services
May 2019	33 months i.e. 1 year after transposition	Commission report assessing the consistency of Member States' identification of operators of essential services
May 2021	57 months i.e. 3 years after transposition	Commission review of Directive functioning, with a focus on strategic and operational cooperation and the scope in relation to operators of essential services / digital service providers

Directive on Security of Network and Information Systems (NIS Directive)

- General Data Protection Regulation is seen “as a component” of NIS – It is about Data Protection (Entry into force was in May 2018)
- NIS was a Directive, not a Regulation, and it may have generated some discrepancies
- They were both very general, so there is a general need to adapt them to the specific field

Gaps

Cybersecurity specific (from Energy Expert Cyber Security Platform Expert Group)

» Threat and risk management system

- Pursue a harmonized, structured and comprehensive way to identify operators of essential services for the energy sector at EU level*
- A structured risk analysis and risk treatment plan specific for the highly interdependent European energy sector*
- Regional cooperation on cyber security topics controlled and secure disclosure of vulnerabilities and incidents affecting the energy sector in its crucial role*

ENERGY EXPERT CYBER SECURITY PLATFORM

Cyber Security in the Energy Sector

Recommendations for the European Commission
on a
European Strategic Framework and Potential Future
Legislative Acts for the Energy Sector

EECSP Report
February 2017

The mission of the EECSP-Expert Group is to provide guidance to the Commission on policy and regulatory directions at European level, addressing the energy sector key points including infrastructural issues, security of supply, smart grids technologies and nuclear.

Directive on Security of Network and Information Systems (NIS Directive)

Gaps

Cybersecurity specific (from Energy Expert Cyber Security Platform Expert Group)

- » Effective cyber response framework
 - Define and implement a cyber response and coordination framework*
 - Implementation and the strengthening of regional cooperation for efficient handling of cyber emergencies when energy is involved and affected*
- » Improve cyber resilience in the energy sector
 - European cyber security maturity framework*
 - cPPP for supply chain integrity*
 - Foster internal coordination and pursue international cooperation
- » Build-up the adequate capacity and competences
 - Building competences
 - Providing knowledge
 - Promoting research

ENERGY EXPERT CYBER SECURITY PLATFORM

Cyber Security in the Energy Sector
Recommendations for the European Commission
on a
European Strategic Framework and Potential Future
Legislative Acts for the Energy Sector

EECSP Report
February 2017

The mission of the EECSP-Expert Group is to provide guidance to the Commission on policy and regulatory directions at European level, addressing the energy sector key points including infrastructural issues, security of supply, smart grids technologies and nuclear.

- EU DSO entity will be also responsible for ensuring data management, cyber security and data protection and participation in the elaboration of network codes;
- Network Codes on cyber security rules and rules concerning regional operational centres;
- Guarantee of security of supply against the risk of an electricity crisis also depending on malicious attacks having regard to some scenarios:
 - Simultaneous
 - Cross Border
 - At Regional Level
 - At National Level
 - All which goes beyond N-1 security criterion

New

- » Cyber Security is mentioned several times, but with very little details on the final strategy;
- » Absolute priority is given to risk preparedness in the electricity sub-sector;
- » Key role for DSOs in cybersecurity;

Gaps (Analytic review of the Winter Package, NIS and GDPR)

- » Gas, Oil, other sub-sectors related to Energy are not explicitly mentioned;
- » Cybersecurity will move on two parallel tracks: technical standards (sometimes high level), risk management and preparedness;
- » No clear way on how the two elements may align in the future, and no governance to assure that this will be achieved and kept consistent;
- » No clear statement on the suggested approach (prescriptive or relaxed?)

- New permanent mandate for ENISA;
- European framework for certification;
- Full implementation of the Directive on the Security of Network and Information Systems;
- A Joint Commission/industry initiative to define a "duty of care" principle for reducing product/software vulnerabilities and promoting "security by design";
- **Swift implementation of the blueprint for cross-border major incident response.**

- Understand and analyze the impact of digitalisation and technical advancements, and keep up to date with them: you need to lead regulation on technology!
- Encourage, facilitate and support national, regional and/or energy sector-specific quantitative risk assessments:
 - » Better understand vulnerabilities and the risk landscape;
 - » Propose methodologies for the consistent identification of risks among all MSs.
- Support information-sharing initiatives and collaboration between public and private stakeholders and institutions at any level:
 - » Gradually build trust between actors;
 - » EE-ISAC is on the radar;
 - » Promote an open environment .

Further actions for European energy Regulators to consider (in a realistic way)

- Encourage cross-border cooperation and joint initiatives to share best-practice, knowledge and resources in a collective effort, try some shared exercises, when possible;
- Actively engage and support national/regional initiatives:
 - » To drive CS-awareness and/or introduce baseline security and safety standards;
 - » Take part to the introduction of a Maturity Framework;
 - » Take part to research projects or education activities to offer also a Regulator perspective.
- Measure the effectiveness of the Cyber Expenditure and try to aim to achieve prudent investments;
- Do not re-invent: when possible, re-use what you have! This was the right spirit of the open source communities (and the way the hackers make their attacks efficient).

- The **EU Legal Framework is rather complex**, but we tried to keep it comprehensive in an already too complex legal architecture.
- **NIS** was just one initial step, and it is alone a very ambitious program, together with the other actions.
- Some more activities may follow, but we need to be extremely careful with resources (**human** and financial).
- Evaluate if we are **over-regulating** all of us.
- **Standards** are important and a communication channel with the standard communities is already in place;
- **Time** is the most **critical factor**: it will happen, it is just a matter of “when” it will happen. Be ready to manage the crises.
- Between Cybersecurity and innovation we must be optimists: **“The future's just a place we've never been”** (*Sting*)

Thank you!

**Security, your
responsibility**



www.acer.europa.eu

Thank you for your attention!



www.acer.europa.eu