USAID FROM THE AMERICAN PEOPLE

USEA United States Energy Association

The Relationship Between Regulators and Power Utilities:

Evaluating the Prudency of Cybersecurity Investments

Elena Ragazzi, IRCRES

elena.ragazzi@ircres.cnr.it

Consiglio Nazionale delle Ricerche

IRCrES

ISTITUTO di RICERCA sulla CRESCITA ECONOMICA SOSTENIBILE
RESEARCH INSTITUTE on SUSTAINABLE ECONOMIC GROWTH

USAID FROM THE AMERICAN PEOPLE

USEA United States Energy Association

A regulatory perspective on cybersecurity

Evaluating the prudency of cybersecurity investments: guidelines for energy regulators

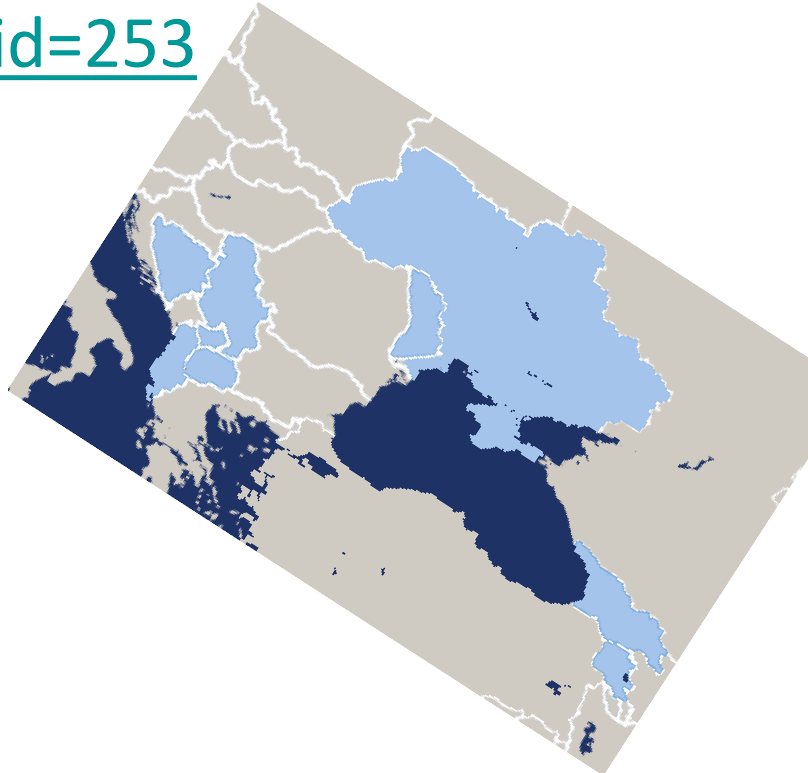
While the implementation of cybersecurity measures is typically the responsibility of power system operators, regulators have to ensure that cybersecurity investments are reasonable, prudent, and effective. The guidelines assist regulators in establishing a regulatory approach to enhance the cybersecurity stance of their power systems.

National Association of Regulatory Utility Commissioners

IRCrES

The USAID initiative for South East Europe

http://www.ircres.cnr.it/index.php/it/?option=com_content&view=article&id=253



Conceived in a specific context, but wide applicability

Different situations around the world: Power system features, regulation, economic and political context, market structure…
Priorities may differ, but principles are common.

elena.ragazzi@ircres.cnr.it

A regulatory perspective on cybersecurity

There are four main themes in the guidelines: definition of a CS strategy, identification and benchmarking of cybersecurity costs, performance assessment, regulatory approach to cybersecurity.

By cost identification we mean understanding which are the right security measures to make the power system more secure (and for the regulator identify expenses eligible for refunding); RATIONALITY OF DECISIONS

By cost benchmarking we mean establishing the right level of investment;

By regulatory approach we mean the process of how decisions can be made, starting from theory and ideas and leading to implementation.

elena.ragazzi@ircres.cnr.it

Roles – who, what and where?

	WHO (Roles)	
WHAT (Activities)	Cost plus	PBR
Definition of the cybersecurity strategy	☑ Policy maker (general objectives) ☑ Regulator (practical cybersecurity strategy) ☒ The operator just adheres to the cybersecurity strategy	☑ Policy maker (general objectives) ☑ Regulator (variables representing these objectives) ☑ The operator (practical cybersecurity strategy)
Cost identification	☑ Regulator (identifies costs to be approved in investment plans) ☑ Only if required, the operator provides a separate indication of cybersecurity costs	☒ The regulator does not assess the investments ☑ The operator identifies the most cost-effective investments to reach the objectives
Performance metrics	☑ The regulator and the policy maker may use metrics to benchmark different types of investments and better define future cybersecurity strategies ☑ The operator may use metrics for internal risk management	☑ The regulator adopts the metrics to provide incentives to companies investing in the desired direction ☑ The operator may use metrics for internal risk management

☑ Fundamental role ☑ Contribution ☒ Nothing to do

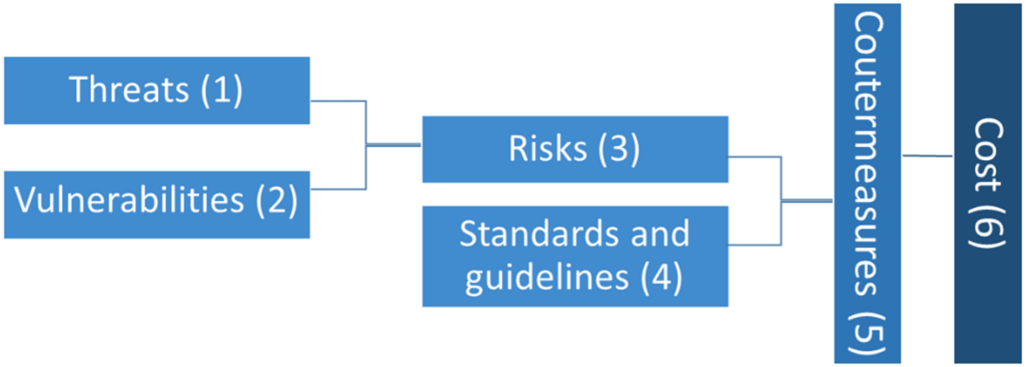
elena.ragazzi@ircres.cnr.it

Working together – a possible scenario?

- (Cyber) security is an example of market failure: for private operators, economic incentives are not enough to ensure a fair level of investments. On the other hand, ensuring the protection of any node is a must in a connected network, so regulation is fundamental.
- But in most cases operators are better skilled and more informed on evolving threats. They are in a better position to define and adapt the practical CS strategy.
- The dilemma may be solved in collaborative approaches to the definition of the general CS strategy
  - Possible?
  - Effective?
  - Reactive?

Cost identification and benchmarking:
principles, methods and (some) values

The process of cost identification and cost quantification



This picture explains the sequence to be followed to identify countermeasures and costs.

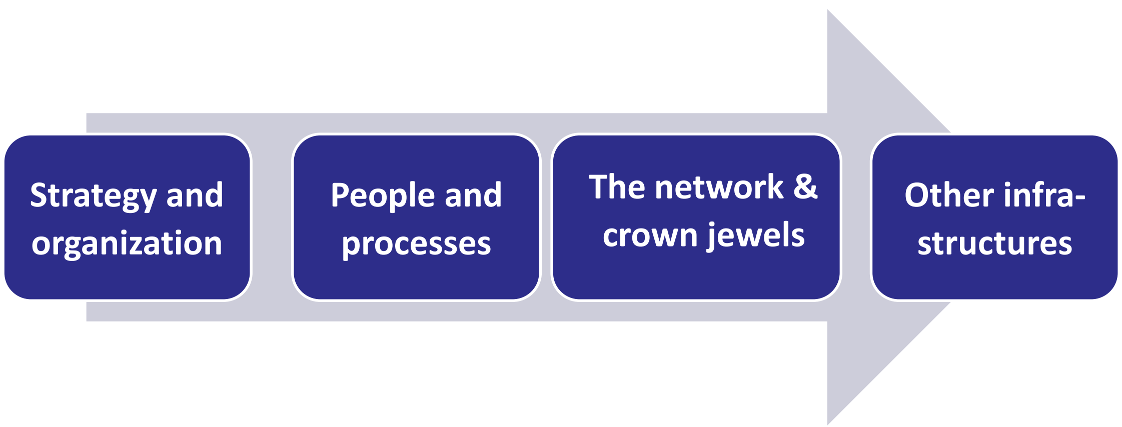
- This analysis should be at the basis of the investment choice. It should not be left implicit. The company will present it to the regulator to justify cost claim.
- It should help the regulators understand there will never be a unique definitive recipe for cybersecurity.

elena.ragazzi@ircres.cnr.it

Establishing priorities

Understanding priorities is

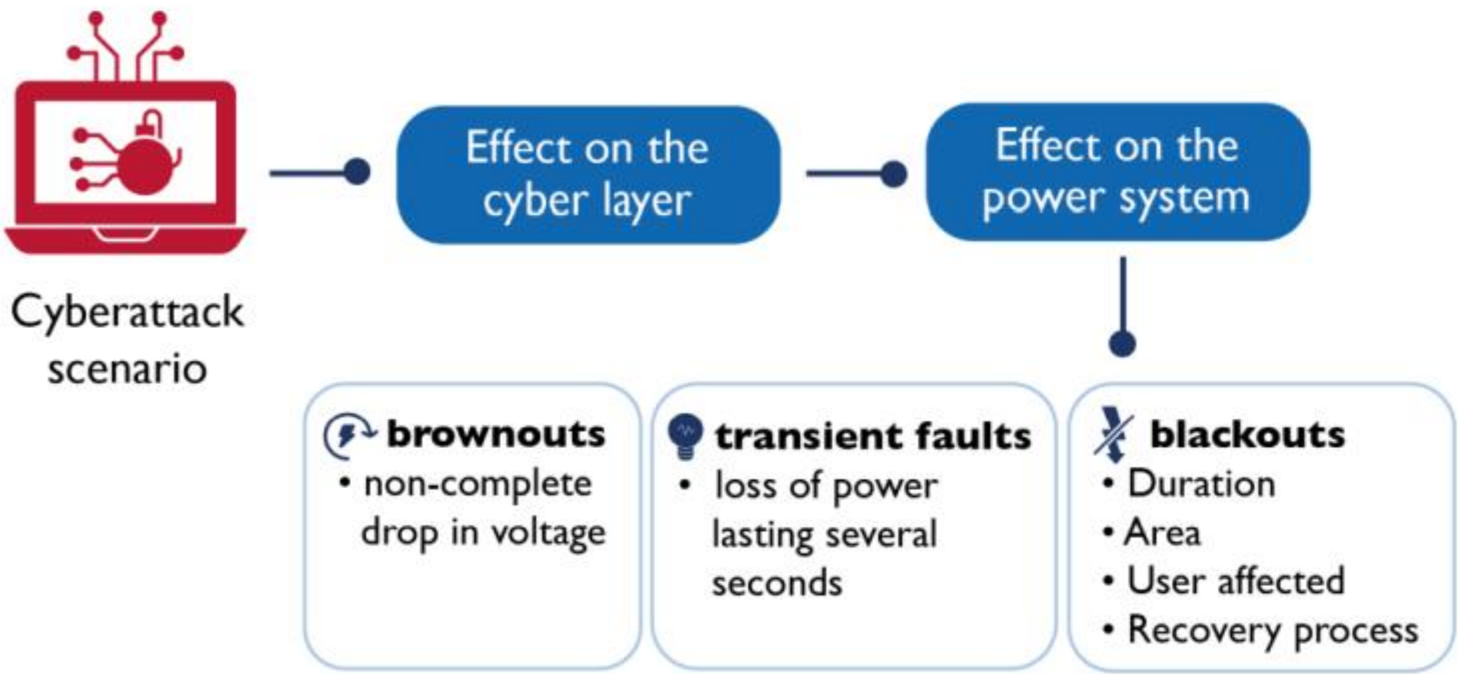
- Fundamental when you first address the issue of cybersecurity
- An important assessment when speaking of prudence



elena.ragazzi@ircres.cnr.it

Benefit analysis: a tool to understand priorities

First step: technical assessment of the impact of a cyberattack



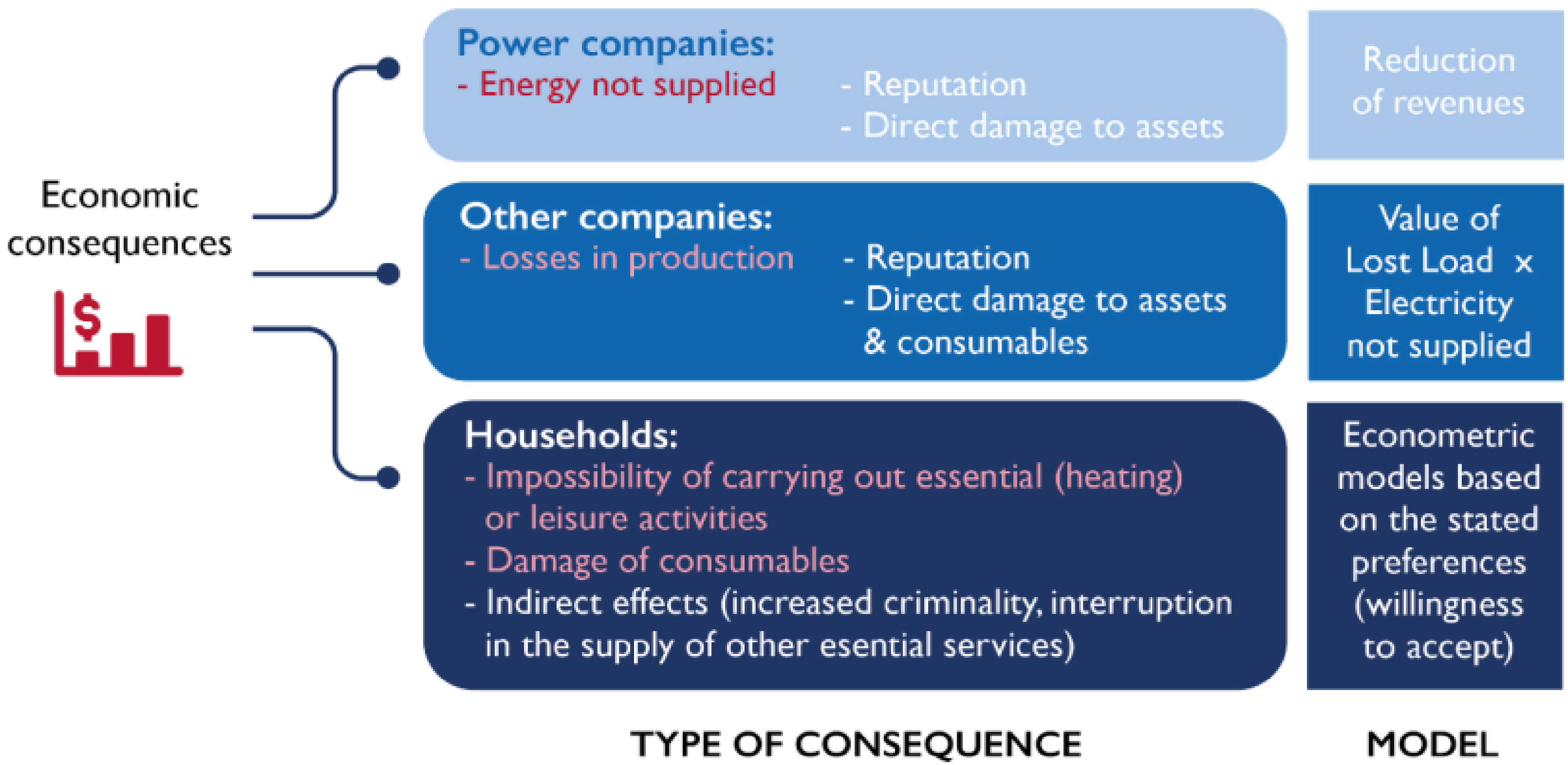
elena.ragazzi@ircres.cnr.it

USAID FROM THE AMERICAN PEOPLE

USEA United States Energy Association

Benefit analysis: economic impact of a cyberattack

Second step: economic value of the impact of a black-out



Cost-benefit analysis: the terms of the evaluation

- Any evaluation means to compare a situation with regulation to an unregulated situation
- But in the case of CS the outcome depends from an exogenous event (the cyber-attack)
- So 4 evaluation scenarios have to be assessed

		Regulation	
		NO. Every operator has freely implemented some countermeasures	**YES**. All operators are required to adopt the same countermeasures
Attack scenario	**NO** relevant attack to the system	I - Not regulated – no attack	III - Regulated – no attack
	YES, an attack is ongoing and can interfere with the system operations	II - Not regulated – attack	IV - Regulated – attack

USAID FROM THE AMERICAN PEOPLE

USEA United States Energy Association

Cost-benefit analysis: variables

1 Indicator	2 Scenario	3 Cost category	4 Information deriving from a simulation	5 Additional information from other sources
A	**I - Not regulated – no attack**	Yearly operating cost of power supply	How much does it cost to supply electricity without attack and without the regulation?	
B	**I - Not regulated – no attack**	Yearly cost of security measures		How much does it cost to manage the current security systems?
C	**II - Not regulated – attack**	*No blackout*: Increase in the operating cost of power supply (disturbed period)	How much does it cost to supply electricity in case of an attack?	
D	**II - Not regulated – attack**	*Blackout*: Cost of blackout	Which region will be affected by the blackout? For how long?	What are the characteristics of the customers not supplied
E	**II - Not regulated – attack**	Cost of emergency actions.		How much would it cost to recover from the attack?

Cost-benefit analysis: variables

1 Indicator	2 Scenario	3 Cost category	4 Information deriving from a simulation	5 Additional information from other sources
F	III - Regulated – no attack	Yearly operating cost of power supply	How much does it cost to supply electricity without attack and with the regulation?	
G	III - Regulated – no attack	Yearly cost of security measures		How much has to be spent to manage the security systems with the regulation?
H	IV - Regulated – attack	No blackout: Increase in the operating cost of power supply in the disturbed period	How much does it cost to supply electricity with the attack and with the regulation?	
I	IV - Regulated – attack	Blackout: Cost of blackout	Which region will be affected by the blackout? For how long?	Characteristics of the customers not supplied?
J	IV - Regulated – attack	Cost of emergency actions.		How much would it cost to recover from the attack?

Cost-benefit analysis: calculations

Calculation	Content	Notes
H + I + J	What happens in case of an attack when regulation is in place	These include the socioeconomic effect of the blackout, the cost of supplying electricity—if the blackout is not total—and the recovery costs (the costs associated with the actions needed to restore the normal situation).
C + D + E	What happens in case of attack with no regulation	
(H + I + J) - (C + D + E)	**BENEFIT (in terms of avoidable cost)**	**The expected value is negative (cost saving: reduction in costs and negative effects, thanks to increased security introduced by the regulation).**
F - B	Increase in the cost of security with the implementation of the regulation	These include both annual costs and depreciation of investments. Indicator B could hypothetically be zero in a theoretical "no protection" case. The expected value is positive.
G - A	Increase in the cost of electricity supply with the regulation in place	This could be positive in case extra reserve capacity or stricter operative conditions are needed.
(F + G) - (A + B)	**COST for the system of implementing the regulation**	**The expected value is positive (increased security cost).**

Results from 2 case-studies

Some quantitative benchmark from Essence project. € *Million*

ITALIAN CASE STUDY (generation system)				
BENEFIT		***COST***	***Delta***	***No protection***
Electricity not sold	2	Investment	20-40	28-53
Non-households	35-46	Maintaining	3.5-6	6.5-12.9
Household*	36-52.5-64			
TOTAL	**73-112**			
POLISH CASE STUDY (TSO)				
BENEFIT		***COST***	***Delta***	***No protection***
Electricity operators	0.7	Investment	7.5	26
Non-households	25-35	Maintaining	2.5	5
Household*	30-52-61			
TOTAL	**55.7-96.7**			

*Min-Expected-Max

Interesting insights
Difficult leveraging!

Some cost assessment from the case studies: organization and governance of CS

Field	Description	Effort (implementation)	Effort (maintenance)
Security Program	• High-level team designing the organization of the security program.	• 4 people	• 1 person
Organization of security	• Technically skilled team responsible for **internal** organization.	• 6 people	• 1 person
	• Technically skilled-team responsible for control on **external** parties.	• 6 people	• 1 person
Security policy	• Team of ICS-IT skilled people working on security policy, standards and procedures	• 3 people	• 2 people
Risk Management	• Contract with a security consultant • Team of experts	• - • 4 people half time	• 90,000€/year • 2 people half time
Asset Management	• Contract with a security consultant • Automated technical solution for asset management (optional)	• - • 500,000€ (medium-large operator)	• 90,000€/year • 2 people

Some cost assessment from the case studies: protecting a power plant

HW/SW costs for hosts and networks security of a typical 380 MWe power unit (€)

	CAPEX (hardware/software cost)	OPEX
Network requirements	370,000	20,000
Host requirements	125,000	90,000
Total	495,000	110,000

Some cost assessment from the case studies: transmission system

Total cost of implementation and maintenance of countermeasures in a TSO (€)

		30 substations	100 substations	200 substations
Implementation costs	Substations	6,047,200	15,118,000	27,212,400
	Information control systems	1,453,280	3,633,200	6,539,760
	Office systems	2,905,920	7,264,800	1,3076,640
	TOTAL CAPEX	10,406,400	26,016,000	46,828,800
	Substations	834,900	2,087,250	3,757,050

elena.ragazzi@ircres.cnr.it

USAID
FROM THE AMERICAN PEOPLE

USEA
United States Energy Association

Assessing effectiveness: principles and alternatives

IRCrES

Effectiveness: Output and outcome

Output is the direct effect of a behaviour (investment, policy, regulation).

Easy to measure, but not effectiveness!

Effectiveness

Outcome is the change in the objective variables caused by the behaviour (but mediated by contest situation)

Output and outcome:

A group of employees … e on security procedures in communi… xternal parties.

Intensity and quality of effort

- OUTPUT: Number of participants passing the final test on theory

Effectivenes

- OUTCOME: Number of mistakes in security procedures (for example: using an unauthorized USB key) in the year after the course .
- OUTCOME: Number of IT system intrusions in the year after the course.

Unsensitive indicator

USAID FROM THE AMERICAN PEOPLE

USEA United States Energy Association

Effectiveness: Change is not impact

1. After choosing the right set of outcome indicators, effectiveness (eg. of an investment) may be assessed comparing the value of one (or many) indicators before and after an investment.
2. This change should then be com registered in similar firms th named investment. This i is the suspect of a **deac** reasonable to expect ar observed indicator even

IMPACT: Difference in the number of mistakes in security procedures in the year after the course between the group of employees that have attended the course and another group of similar employees that have not attended the course.

IRCFES

USAID FROM THE AMERICAN PEOPLE

USEA United States Energy Association

Effectiveness: the problem of metrics

Outcomes have to be assessed through good indicators.

Maturity metrics.
Many experimented alternatives exist to assess the maturity level. Some are simpler, some more complex. Some are open source, other ones are offered by consulting services.
But maturity is not the full picture.

Performance metrics.
They give a comprehensive picture, but:

- complex systems of indicators;
- requiring good data collection tools and a fair level of maturity;
- research and experimentation is on-going.

elena.ragazzi@ircres.cnr.it

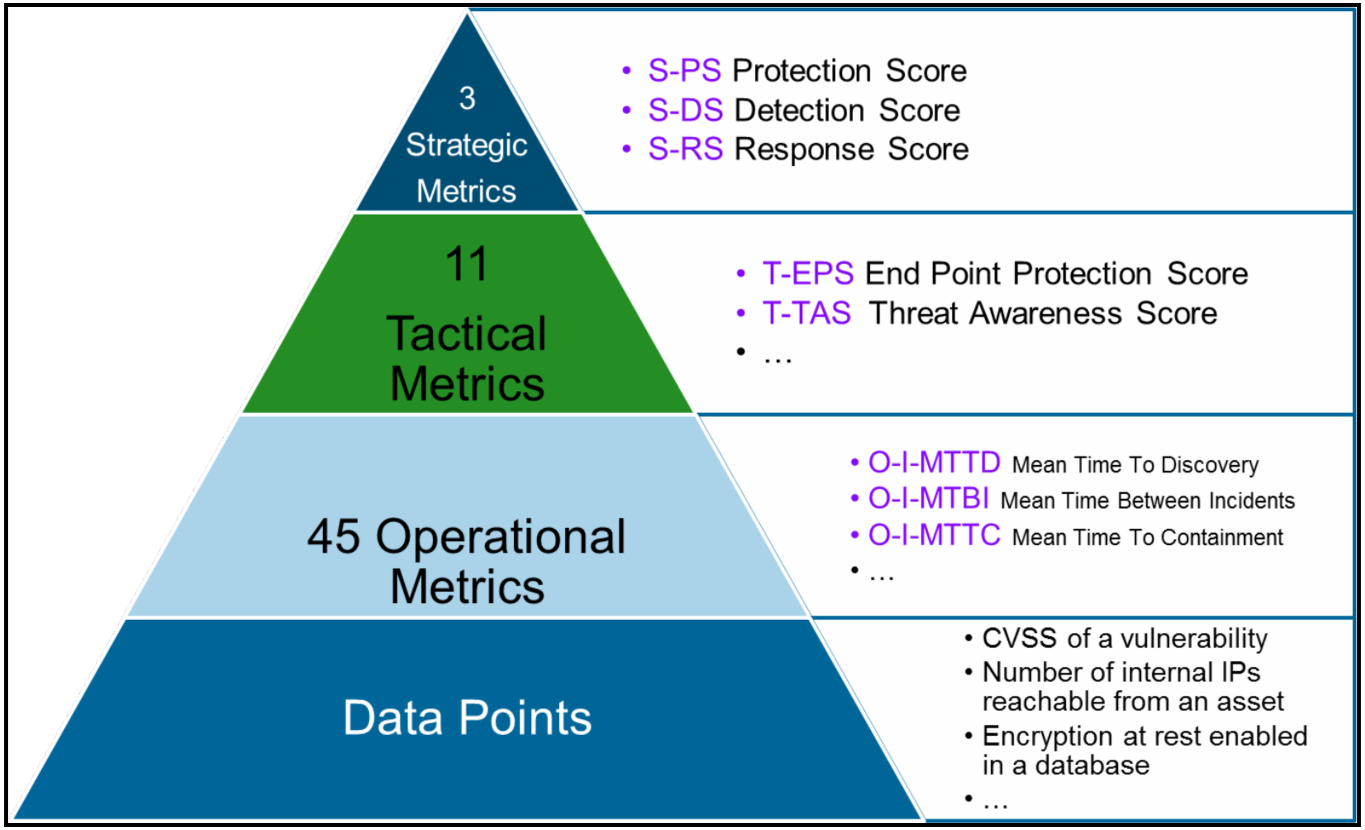
Choosing the indicators: EPRI metrics

EPRI indicators represent one of the most advanced studies in the field of performance metrics.

- 121 data points
- Indicators: 47 operational metrics, 10 tactical scores, 3 strategical scores
- Tested with a North-American experiment (→ it works).
- Feasible. A lot of boring work but not difficult.
- Wanting to carry out an European pilot (→ it scales?)
- Working to a tool

elena.ragazzi@ircres.cnr.it

The EPRI metrics



Performance metrics: Uses

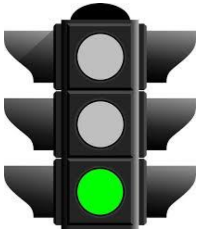
- Security team ⟹ understand what works
- IT management ⟹ decisions on security technologies
- Board ⟹ understand and manage risk
- Regulators/ consumers ⟹ is the power grid secure?

It is always a problem to use the same tool for different necessities!

elena.ragazzi@ircres.cnr.it

Performance metrics: to do what?

- Internal risk management tool



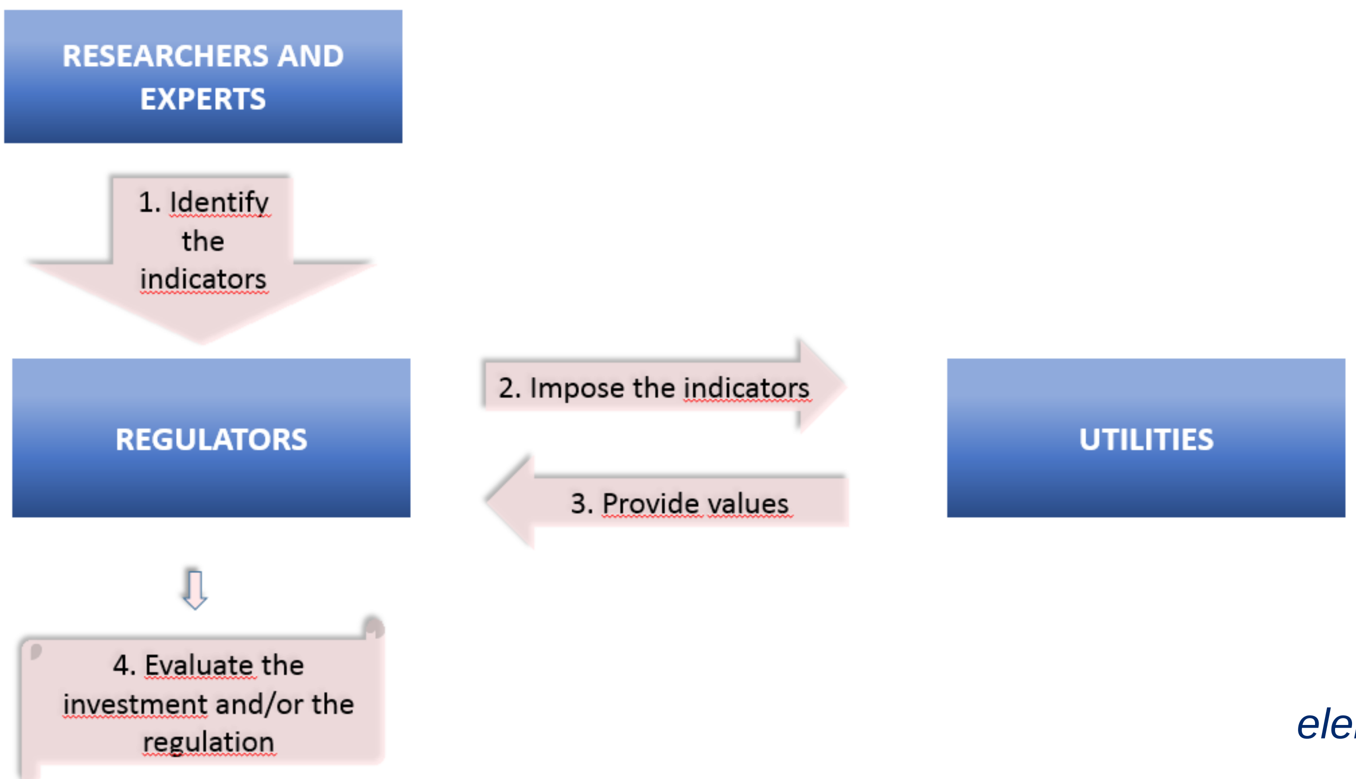
- Internal/external benchmarking

- Regulation and control (funding, approval, fines and incentives

elena.ragazzi@ircres.cnr.it

A governance for the metrics for regulatory purposes

To design an effective system to collect the values of the indicators for regulatory purposes is as important (and as difficult) than choosing the right indicators.



Is a top-down approach possible

?

elena.ragazzi@ircres.cnr.it

Thank-you for your attention!

Contacts:

Elena Ragazzi (editor) elena.ragazzi@ircres.cnr.it

Alberto Stefanini alberto.stefanini@gmail.com

Daniele Benintendi dbenintendi@gmail.com

Ugo Finardi ugo.finardi@ircres.cnr.it

Dennis K. Holstein holsteindk@ocg2u.com

Links for the download:

http://www.ircres.cnr.it/index.php/it/?option=com_content&view=article&id=253

https://www.naruc.org/international/news/evaluating-the-prudency-of-cybersecurity-investments-guidelines-for-energy-regulators/