APPENDIX 1:
COSTS AND BENEFITS OF CYBERSECURITY REGULATION
THE TERMS OF A COMPLEX ASSESSMENT

Appendix to **Evaluating the Prudency of Cybersecurity Investments: Guidelines for Energy Regulators**

Project Title:	Europe and Eurasia Cybersecurity Partnership
Sponsoring USAID Office:	USAID Bureau for Europe and Eurasia
Cooperative Agreement #:	AID – OAA-A-16-00049
Recipient:	National Association of Regulatory Utility Commissioners (NARUC)
Date of Publication:	May 2020
Author:	CNR-IRCrES, The National Research Council of Italy, Research Institute on Sustainable Economic Growth[1]

[1] The present document has been prepared by Elena Ragazzi

This appendix will explain the terms of an evaluation of the economic effects (increased and saved costs) of a regulation imposing the compliance to a standard or to a list of countermeasures. The reference is the cost-benefit approach presented in section 3.4 of the guidelines.

An exercise based on hypothetical data will show how to apply these definitions in order to calculate the costs and the benefits connected to the implementation of the regulation.

1 Cost-benefit analysis of cybersecurity countermeasures

It must be underlined that in this context:

- **Costs** are represented by expenses associated with running security measures.
- **Benefits** are represented by the economic effect of cyberattacks that can be avoided by running security countermeasures.

Evaluating a regulation means to **compare**:

- A situation with **no regulation**. Each company freely decides which countermeasures to implement.
- A **regulated situation**. The regulation sets the minimum level of requirements to be reached. These minimum requirements may consist of measures to implement or in objectives (scores) to be reached.

1.1 Scenarios

However, with respect to other types of regulations, the analysis of benefits is more complicated in the case of cybersecurity regulation. In fact, the concept of risk mediates actions and effects. The impact is based on the occurrence of an event that is out of the control of both the policymaker and the power operator.

As a result, the economic items that compose the evaluation have to be calculated in four possible scenarios, described in Table 1. The four scenarios derive from the application of two dimensions: the application of regulation, and the presence/absence of a relevant tack. By relevant attack, we mean an attack that threatens the system operations and could circumvent present countermeasures. In Table 1, the green color identifies an unperturbed situation, while the red color identifies situations in which there is a relevant attack. Light colors identify situations without regulation, and bright colors identify regulated situations.

Table 1: Scenarios for cost-benefit analysis

		Regulation	
		NO. Every company has freely implemented some countermeasures	**YES**. All companies are required to adopt the same countermeasures
Attack scenario	**NO** relevant[2] 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

In particular, Table 2 lists the classes of economic items (values) that have to be calculated in each scenario.

[2] By relevant attack, we mean an attack that threatens the system operations and could circumvent present countermeasures.

Table 2: Types of calculations in the four scenarios

To be calculated in all scenarios	To be calculated only in scenarios with a relevant attack (red scenarios)	To be calculated only in scenarios with an attack causing a blackout
▪ The cost of security measures, including the operational expenses and the annualized cost of investments ▪ The cost of supplying electricity	▪ Cost of running emergency actions under attack	▪ The economic impact of the blackout

1.2 Data sources

The first data source is represented by a **simulation**.

Each policy evaluation is based on a comparison between a situation with the policy and a situation without the policy (counterfactual). But in the case of regulation, in most situations the policy concerns the whole country and so you miss a counterfactual. For this reason, you may not rely on real data, comparing ex-post metrics, and must use data from a simulation. Referring to a precise scenario (day of the year, time of day) the simulation must show the quantity of power supplied, the users (type, location) the energy sources, and the costs of production. To build this simulation, you have to rely on a simulator of the national system, or on precise data obtained by the body/company that manages the power market.

The information offered by the simulation has to be integrated with information from other sources. These include:

- Information concerning the cost of security measures. Obtaining this type of information requires the cooperation of the power operator and of a vendor of security technologies and services;
- Information on the features of the users (e.g.: sector for companies, willingness to pay for households), which are necessary to estimate the economic value of a blackout. This type of information may, in general, be obtained by the body/company that manages the power market.

2 Calculations for cost-benefit analysis

2.1 The baseline: not regulated – no attack

The first scenario represents the baseline for the comparisons. It concerns the actual situation, and for this reason, the calculations for the baseline scenario may refer to real costs incurred by companies. The time-frame is the operating year.

I - Not regulated – no attack		
Item	**Cost category**	**Information**
A	Yearly operating cost of power supply	How much does it cost to supply electricity without an attack and without the standard?
B	Yearly cost of security measures	How much does it cost to manage the current security systems?

2.2 Attack without sufficient protection: not regulated and attack

This scenario represents a situation of attack before the regulation is implemented. In this situation, we expect that there is a partial (option no blackout) or total (option blackout) reduction of power supply and an increase in the cost of supply respect to the situation without attack (scenario I). The cost of carrying out actions for the recovery of the normal situation also has to be considered. The timeframe is the length of the perturbed situation.

II - Not regulated -attack		
Item	**Cost category**	**Information**
C	*Option no blackout*: Increase in the operating cost of power supply during the disturbed period	How much does it cost to supply electricity in case of an attack?
D	*Option 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	Cost of emergency actions	

2.3 Normal conditions under regulation: regulated and no attack

This scenario represents the normal operating conditions when the regulation is implemented. In this situation, with respect to the baseline depicted in scenario I, we expect an increase of security cost due to the implementation of a wider range of countermeasures. We expect an increase in the cost of power supply as well, because of new procedures that require more time to accomplish the same activities and in case the regulation requires an increase in reserve capacity. The timeframe is the operating year.

III - Regulated – no attack		
Item	**Cost category**	**Information**
F	Yearly operating cost of power supply	How much does it cost to supply electricity without attack and with the regulation?
G	Yearly cost of security measures	How much does it cost to manage the countermeasures necessary to comply with the regulation?

2.4 We are prepared: regulated and attack

This scenario represents a situation in which a relevant attack occurs when the regulation is implemented.

With respect to the regulated situation without attack (scenario III), we expect that there is a partial or total reduction of power supply and an increase in the cost of power supply.

We also expect that the blackout duration is shorter or zero, and that the cost increase is lower with respect to an attack in an unregulated scenario (scenario II).

The timeframe is the length of the perturbed situation.

IV Regulated - attack		
Item	**Cost category**	**Information**
H	*Option no blackout*: increase in the operating cost of power supply during the disturbed period	How much does it cost to supply electricity with the attack and with the regulation?
I	*Option blackout*: Cost of blackout	Which region will be affected by the blackout? For how long? What are the characteristics of the customers not supplied?
J	Cost of emergency actions	

2.5 Relevant comparisons

Once one has defined the scenarios and calculated the relevant variables, the impact analysis and the cost-benefit analysis derive simply from the comparison between scenarios. In particular:

1. Scenario 2 describes the **impact of an attack without regulation.**
2. Scenario 4 describes the **impact of an attack with regulation** (we expect it is lower compared to point 1).
3. **Cost**: is the increase in security and power supply costs passing from scenario 1 to scenario 3.
4. **Benefit**: is the difference between the impacts in scenario 4 and scenario 3 (benefit related to one relevant cyberattack).

3 Hypothetical exercise on the cost-benefit analysis

This exercise is not based on real data, neither concerning normal operating conditions nor the effect of a cyberattack. Nevertheless, it should be noted that the scale of values, fixed starting from the Essence experience, is reasonable. So, in the context of the exercise, if a proposed value is five, the real value could be seven or even 10, but not 50.

3.1 Description and data

For our exercise, we imagine a country whose power system is divided into two regions. We also imagine that a relevant cyberattack occurs.

Without regulation, the attack causes serious disturbance resulting in a complete blackout in one region lasting several hours. In the other region, the attack causes difficulties in supplying power that is afforded thanks to the presence of reserve capacity (resulting in an increased cost for the power supply). An attack scenario is when a relevant cyberattack affects a country made of two regions.

With regulation, the attack causes serious disturbance as well. But the effect is limited to an increase in the cost of power supply, without causing a blackout.

Table 3: Hypothetical data of the variables for cost-benefit analysis

A	**Yearly cost of power supply I**	**590**	**F**	**Yearly cost of power supply III**	**600**
B	**Yearly cost of security measures I**	**4**	**G**	**Yearly cost of security measures III**	**12**
C	**Cost of power supply II**	**1**	H	**Cost of power supply IV**	**4**
D	**Value of blackout II**	**40**	**I**	**Value of blackout IV**	**0**
E	**Emergency action II**	**0.5**	**J**	**Emergency action IV**	**0.2**

Comparing the situation with and without regulation, hypothetical data are based on the following assumptions:

- Passing from a non-regulated to a regulated situation in an unperturbed situation (scenario I vs. scenario III), there is a small increase in the cost of power supply (first line of the table) and a sharp increase in the cost of security measures (second line of the table).
- The economic cost of a blackout for the society is huge. This cost may be avoided in our hypothetical exercises thanks to the measures adopted under the regulation (fourth line of the table).
- When the attack does not turn into a blackout, it causes an increase in the cost of power supply (third line). This increase is smaller in the non-regulated situation, because in one of the regions no power is supplied during the blackout timeframe.
- The cost of emergency action after the attack (last line) is lower in the regulated situation, because the recovery is easier and faster thanks to well-designed procedures.

3.2 Cost

The cost of a regulation imposing the adoption of cybersecurity measures is represented by the increase in costs for security measures and for power supply in normal situations (no attack) passing from an unregulated situation (scenario I) to a situation with regulation (scenario III).

We expect that the difference in costs of scenario III vs. scenario I is positive. If there is no difference, it means that operators were already implementing the required measures, so either it would not have been necessary to implement a regulation, or the regulation was too loose.

The cost of implementing the regulation of the utilities can be calculated through the formula:

(F + G) - (A + B) **(scenario III vs scenario I)**

With regulation			Without regulation		
F	Cost of power supply III	600	A	Cost of power supply I	590
G	Cost of security measures III	12	B	Cost of security measures I	4
SUM		**612**			**594**
				Δ Costs	**18**

3.3 Benefit

The benefit is measured by the difference between what happens in the case of a relevant attack when regulation is imposed (scenario IV) and what happens without regulation (scenario II).

Relevant cyberattacks are those that will have an impact, in terms of increased costs for the operator and for the society, at least in the unregulated scenario. We expect that this impact is reduced or nullified by the implementation of the regulation. So, the difference is expected to be negative, and the benefit is represented by cost savings.

(H + I + J) - (C + D + E) **(scenario IV vs scenario II)**

With regulation			Without regulation		
H	Cost of power supply IV	4	C	Cost of power supply III	1
I	Cost of black-out IV	0	D	Cost of black-out III	40
J	Cost of emergency actions IV	0.2	E	Cost of emergency actions III	0.5
SUM		**4.2**			**41.5**
				Δ Costs (Savings)	**-37.3**

3.4 Summing up the results

The comparison of the results in the exercise shows that benefits connected to one single event largely compensate yearly costs.

Nevertheless, the costs of measuring implementation and the benefits connected to one cyberattack may not be summed up, because costs concern an event (the implementation of the regulation) that is certain in a probabilistic sense, while benefits concern one among *n* several possible events, each occurring with a probability π_n.

The correct assessment would imply to estimate *n* benefits B_i connected to *n* possible events and to sum them up, weighted with their probability π_i:

$$Benefit = \sum_{i=1}^{n} B_i \pi_i$$

In the most advanced stage, this appears to be feasible because the probability connected to various attack scenarios is unknown. Its objective estimate would require access to reliable statistics on cyber-related incidents that are not presently available.