MEDREG

MEDREG is co-funded by the European Union

MEDREG

WHAT IS THE ROLE FOR ENERGY REGULATORS IN CYBERSECURITY: APPROACHES AND CRITICAL POINTS

Elena Ragazzi, CNR-Ircres, elena.ragazzi@ircres.cnr.it

MEDREG training on «Regualtory implications of the digitalization of energy markets and the new role of consumers. October 28th, 2021

Consiglio Nazionale delle Ricerche
IRCRES
ISTITUTO di RICERCA sulla CRESCITA ECONOMICA SOSTENIBILE
RESEARCH INSTITUTE on SUSTAINABLE ECONOMIC GROWTH

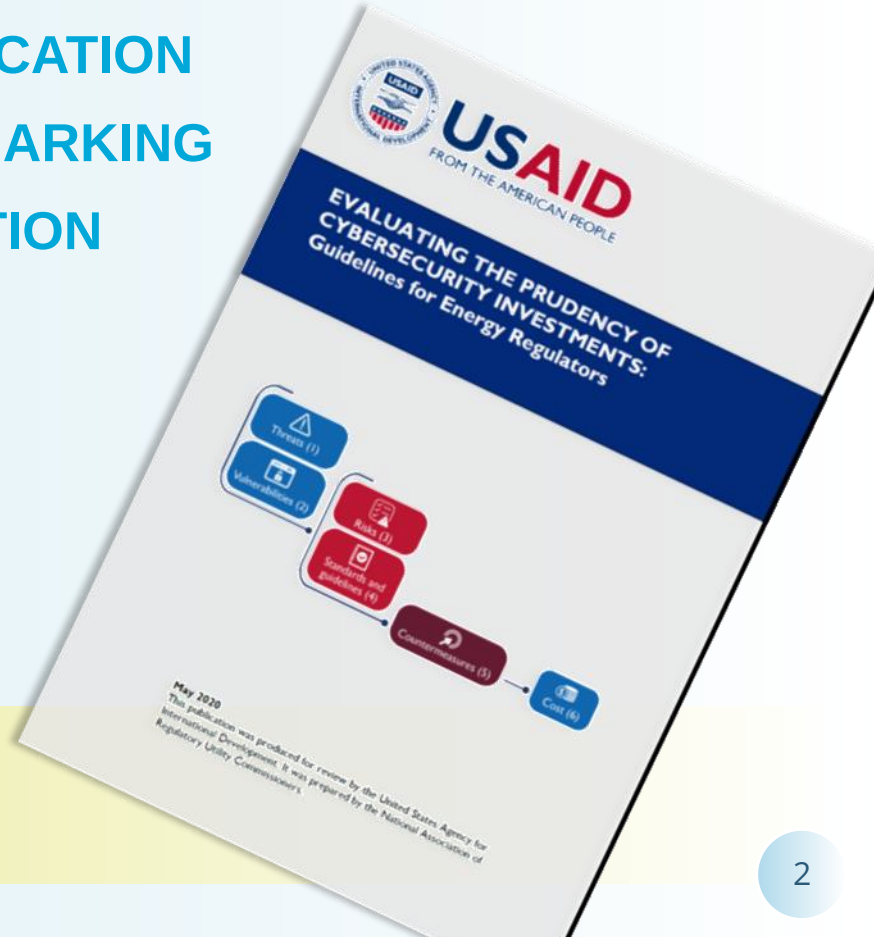
A regulatory perspective on cybersecurity

MEDREG is co-funded by the European Union

Energy regulators may be charged to enhance the cybersecurity stance of their power systems.

While the implementation of cybersecurity measures is typically the responsibility of power system operators, regulators have to ensure that cybersecurity investments are

- **reasonable** (they go in the right direction) **IDENTIFICATION**
- **prudent** (enough but not too much), **BENCHMARKING**
- **effective** (they produce what they were intended for) **EVALUATION**



This training is based on the experience done while preparing for USAID and NARUC the document “Evaluating the prudency of cybersecurity investments: guidelines for energy regulators”.

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

Regulators that want to enhance the protection and preparedness of the power systhem have not to choose the countermeasures, but have to promote reasonnable, prudent and effective investments

Enhancing cyber preparedness in different regulatory frameworks

MEDREG is co-funded by the European Union

The general approach to enhance cyber investments and to define tariffs is not independent from the general regulatory framework:

- Performance based regulation.
- Cost of service / compliance based regulation.

In the reality national regulatory frameworks are always in the grey area among these two extremes. Moreover different approaches may be used to reach different objectives.

Nevertheless I will refer to these two general frameworks to explain that they imply different ways to implement and manage a cybersecurity strategy.

The way in which a cybersecurity objective should be pursued by the regulator depends on the type of regulatory approach

Performance based regulation

MEDREG is co-funded by the European Union

In performance based regulation the regulator wants to provide regulated companies with economic signals in order to deliver the optimal level of quality of service (QoS).

In practice the regulators adopt an output based incentive scheme, fixing:

1. QoS metrics (including in our case indicators on the protection from cyber threats)
2. The level of baselines objectives,
3. The “reward” offered to the operators reaching the objectives
4. Eventually further options to take into account technological and context evolution and procedures to manage risk.

It is up to the company to decide how to reach the objectives (2)**, measured through (1), given the system of incentives** (3) **fixed by the regulator.**

Ex-post, the regulator will verify the respect of the fixed objectives, but not what investments have been carried out or what expenses have been incurred.

In PBR the regulator fixed, indicators, baselines and incentives, but not the countermeasures

Performance based regulation and cybersecurity

MEDREG is co-funded by the European Union

In principle, in a performance-based regulation context, cyber-expenses incurred by DSOs and TSOs should be treated as any other CAPEX or OPEX connected to electricity transmission and distribution.

The company is free to choose how to ensure the required level of protection.

The regulator will neither choose which expenses to approve nor check the conformity of incurred expenses to plans; but he will strictly verify that the agreed objectives have been reached

- Not investments plans and audits
- But a great relevance of performance metrics

In PBR it is fundamental to find the good indicaotrs, able to show to the regulator that the grid is protected

Performance based regulation pros & cons

MEDREG is co-funded by the European Union

+ It doesn’t require too much activity to be carried out by the regulator (light organization, reduced staff, reduced cost)

+ It doesn’t require the regulator to have cybersecurity competencies, *just* to identify correctly the objectives

+ It leaves to the company the most suitable cybersecurity strategy (eg. which standard to comply to, compliance vs risk management approach)

+ It leads to a reduction of the cost charged to the consumer (distribution and transmission costs in the final price are lower since companies have the interest to avoid excessive investments, and the cost of implementing the regulation is lower)

+ May be easily applied if there is a different regulator for cybersecurity

- It requires a fair maturity level in the company
- In general it works better in well established power systems
- Requires good metrics. It is fundamental
  - To identify the good indicators
  - To fix the good procedures to calculate the indicators and baseline levels
- Not yet applied for cybersecurity, so it is a territory to explore, not a well defined path

Cost of service regulation (cost plus)

MEDREG is co-funded by the European Union

In this framework, all the expenses incurred by the firm to supply electricity are covered, plus a fair remuneration of capital. Various systems, such as remuneration decreasing over time, may be adopted to enhance improvements in productivity by the firm.

In this regulatory framework, **cyber-expenses have to be approved by the regulator (as it happens for other costs and investments incurred by the firms).** So, the regulator will have to acquire cyber-competencies (and staff) for investment approval.

- **Cyber expenses have to be identified, assessed through benchmarking, approved and verified.**
- **Performance metrics** is to be conceived to acquire evidence for future plans (evidence based programming).

C+ implies approving the countermeasures (ex-ante) and verifying the costs (ex-post)

Regulatory framework - Conclusions

MEDREG is co-funded by the European Union

PBR: ⇨ **Metrics**

The **regulator** defines:

- **indicators**
- **procedures** to calculate indicators.
- baseline **levels for indicators** (objectives)
- **requires data** and **verifies** their validity **through inspections.**

The **firm** decides the **cybersecurity strategy** adhering to the objectives stated in the regulation. It identifies countermeasures and benchmarks costs coherently with its strategy.

C+: ⇨ **Identification, benchmarking and approval**

The **regulator**

- identifies the relevant countermeasures,
- benchmarks the costs,
- approves the plan and verifies the conformity.

The **firm**

- complies to the national cybersecurity strategy
- **or** follows its internal strategy and submits an investment plan to the regulator (depending on the regulation)

Comparison among the two approaches.

Working together with companies: a possible scenario?

MEDREG is co-funded by the European Union

(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.
- Performance metrics for cybersecurity are in an early stage of development so difficult to implement for regulation

The dilemma may be solved in collaborative approaches to the definition of the general CS strategy

- Possible?
- Effective?
- Reactive?

Collaborative approaches (company/regulator) to cybersecurity are a third way to afford cybersecurity.

MEDREG

MEDREG is co-funded by the European Union

Principles and methods for identification and benchmarking

Principles and methods for identification and benchmarking

MEDREG is co-funded by the European Union

This picture explains the process of countermeasure identification and cost quantification. It is important for the regulator because:

- This analysis is the basis of the investment choice. The regulator, when approving investment plans should ask the company to explain it, not to leave it implicit. It is the justification for the cost claim.
- It should help the regulators understand there will never be a unique definitive recipe for cybersecurity.

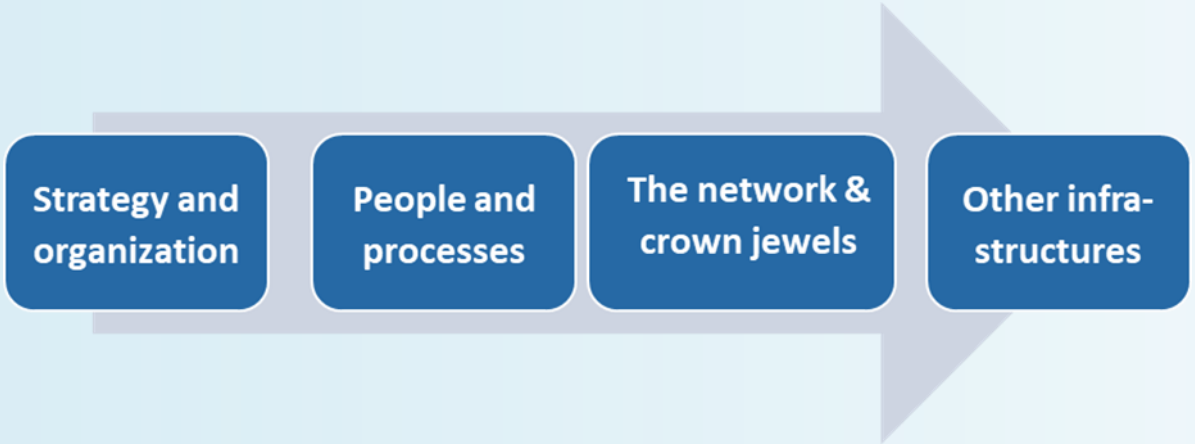
6 elements that are the rationale for investment plans

Establishing priorities

MEDREG is co-funded by the European Union

Understanding priorities is

- Fundamental when you first address the issue of cybersecurity (in power systems with low maturity)
- An important assessment when speaking of prudence (to avoid overinvestment)

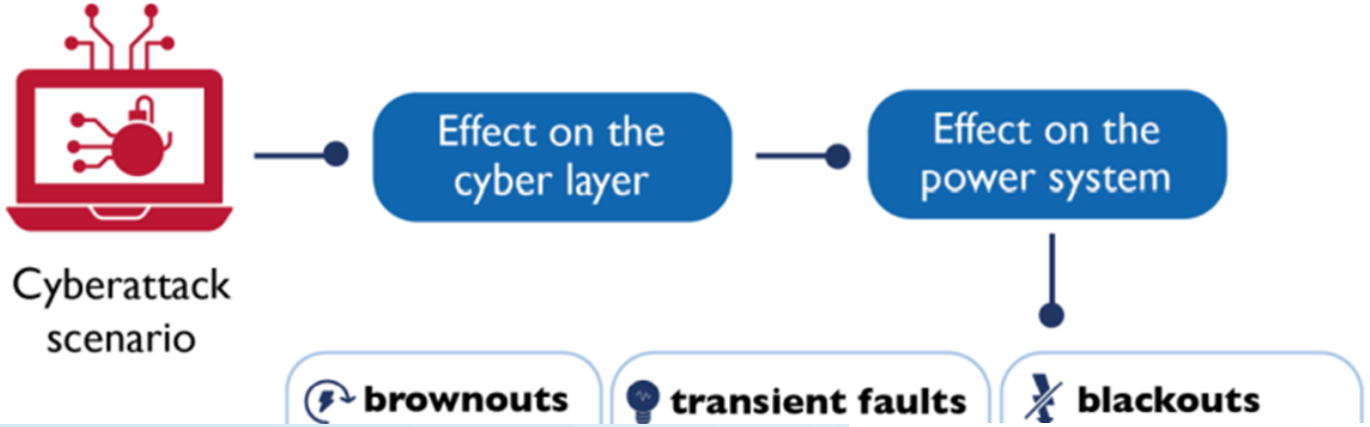


Benefit analysis is a quantitative tool to understand priorities. It aims to understand the impact that a cyberattack could have. This is called “benefit” in CBA, because it may be avoided thanks to the investment. It is the expected outcome of the investment

To invest well and avoid overinvestment, it is fundamental to establish priorities

Two steps of benefit analysis

MEDREG is co-funded by the European Union

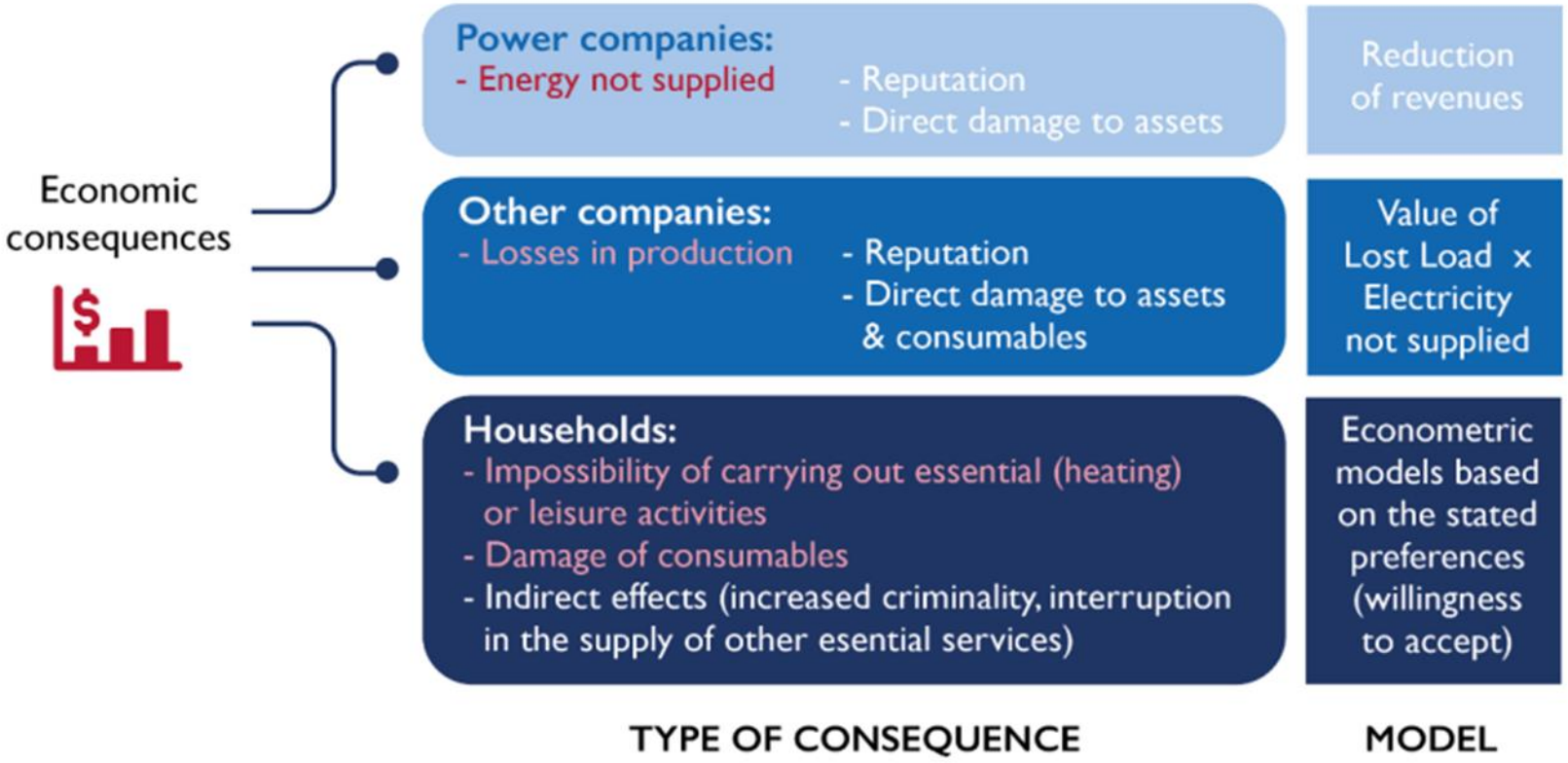


1. Technical impact of the cyberattack

Elements of the benefit analysis:

Technical impact and economic impact

2. Economic value of the impact of the cyberattack



Governance of cybersecurity

MEDREG is co-funded by the European Union

The governance of cybersecurity deserves particular mention in the context of the identification of good protection strategies. In fact they are particularly relevant and, at the same time, they difficult for the regulator to identify and for the operator to argument.

- one shortfall that explain scarce performance of cyber investments is represented by processes and people that lack the maturity to effectively use the technology
- the improvement of the security posture requires above all
  - an enrichment of competencies of the employees
  - an update of the procedures/processes (policies, procedures and organizational directives)

Governance costs are not negligible.
The Essence project calculated, for ENEL (generation multinational company), that governance costs summed up to a value ranging from 5% to 10% of hardening costs

Effectiveness of investments is ensured only if it is accompanied by the presence of aware and trained staff and of clear procedures

MEDREG

MEDREG is co-funded by the European Union

Assessing effectiveness: principles and alternatives

And the answer is… no, not only at least!

MEDREG is co-funded by the European Union

Our **problems with QoS indicators**:

- The problem of sensitivity of indicators
- The concept of risk, that mediates actions and effects (event-based metrics has to be complemented with vulnerability-based metrics)
- The maturity level interfering with performance of investments
- Cyberattacks may have different targets, not only continuity of supply (eg. sensitive data, reputation, manipulation of the public opinion)

Our problems with CS metrics:

- Designing metrics to observe the outcome
- The baseline (expectation of CS incident trends and for other metrics)
- Economic valuation (do we know the willingness-to-pay for CS?)
- Specific metrics for the power system

Problems of different types of metrics

Effectiveness: Output and outcome

MEDREG is co-funded by the European Union

So what are we looking for, to have a «**quality-like**» model for cybersecurity? Let's start from some basic concepts.

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

Where the light is! But it does not ensure that we reached our objectives

This is effectivenes, but difficult to disentangle

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

Outcomes are a tangible translation of the concept of effectiveness

Output and outcome: example

MEDREG is co-funded by the European Union

A group of beginners attends a course on safety procedures for free climbing. We want to answer the question: was the course effective in reducing the risk of accidents?

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

It measures quality and intensity of the training effort

- OUTCOME: Number of participants who make mistakes in safety procedures during climbing exits.

It measures effectiveness

- OUTCOME: Number of participants suffering from serious injuries due to an accident

X

It measures effectiveness but it is an unsensitive indicator

An indicator must have some necessary features:

- **Acknowledge a change in our objectives** and not compliance
- **Clear causal relation** between the policy (regulation/investment) and the variable measured by the indicator.
- **Measurability**

Exercise

MEDREG is co-funded by the European Union

Let's think of a policy for the power systhem (**objective/what** and **instrument/how**)

We want to increase the share of renewables (consumption) and we give incentives to prosumers to install photovoltaic roofs.

Let's think of its direct **output**

Increase in solar generation capacity

Let's think of possible **outcomes** and discuss them (**confounders**)

Increase in share of consumption of solar electricity (elasticity of demand, smart grids, storage)

Example to clarify the concepts of output, outcomes, confounders

Choosing the indicators: EPRI metrics

MEDREG is co-funded by the European Union

In the field of performance indicators for CS research is on- going, while practice is nearly non existent. EPRI indicators represent one of the most advanced studies in the field.

- Specific for electricity operators
- Outcome metrics
- 121 indicators (**measurable** and **relevant**)
- 47 operational metrics 10 tactical scores 3 strategical scores
- Tested with a North-American experiment
- Feasible. A lot of boring work but not difficult.

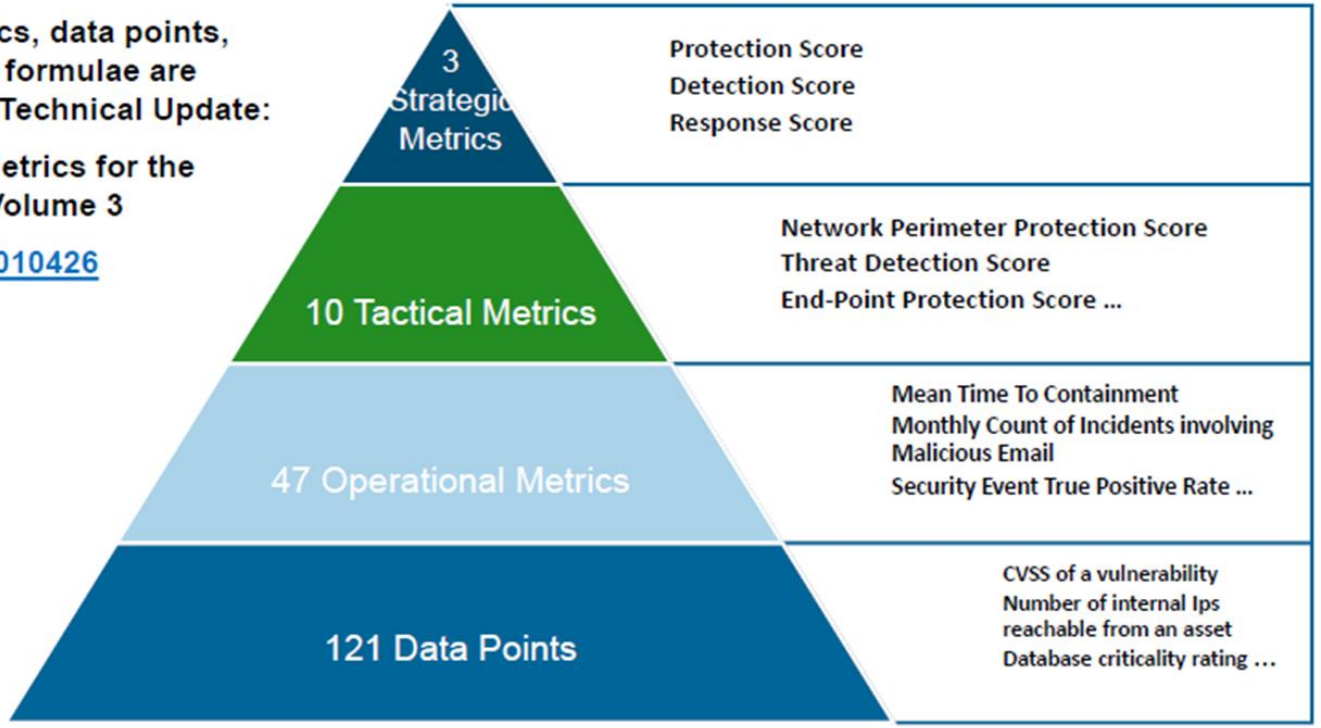
An example of performance metrics complying with our requirments for indicators.

EPRI's Security Metrics

Full lists of metrics, data points, descriptions and formulae are included in 2017 Technical Update:

Cyber Security Metrics for the Electric Sector: Volume 3

Product ID: 3002010426 (www.epri.com)



List of Security Metrics (V1)

Strategic Metrics (3)
Executive Level Summary

S-PS	Protection Score
S-DS	Detection Score
S-RS	Response Score

Tactical Metrics (10)
IT/OT Management Level Summary

T-NPS	Network Perimeter Protection Score
T-EPS	End point Protection Score
T-PAS	Physical Access Control Score
T-HSS	Human Security Score
T-NVS	Core Network Vulnerability Control Score
T-NAS	Core Network Access Control Score
T-DPS	Data Protection Score
T-TAS	Threat Awareness Score
T-THS	Threat Hunting Effectiveness Score
T-IRS	Incident Response Score

Operational Metrics (47)
Security Operations Level Summary

O-A-MAC	Mean Asset Connectivity
O-A-MACS	Mean Asset Access Control Score
O-A-MAP	Mean Asset Proximity To Hostile Network
O-A-MNACS	Mean Network Access Control Score
O-A-MNVRS	Mean Network Vulnerability Risk Score
O-A-MPACS	Mean Physical Access Control Score
O-A-MVRS	Mean Asset Vulnerability Risk Score
O-D-MDAS	Mean Data Availability Score
O-D-MDCS	Mean Data Confidentiality Score
O-D-MDIS	Mean Data Integrity Score
O-E-METP	Mean Security Event True Positive Rate
O-E-MCSE	Mean Count-M Security Events
O-H-MHSS	Mean Human Security Score
O-I-CMSI	Count-M Missed Security Incidents
O-I-MCDL	Mean Count-M Data Leak/Loss
O-I-MCH	Mean Count-M High Severity
O-I-MCM	Mean Count-M Medium Severity
O-I-MCMD	Mean Count-M Mobile End-Point
O-I-MCME	Mean Count-M Malicious Email
O-I-MCMU	Mean Count-M Malicious URL
O-I-MCMW	Mean Count-M Malware
O-I-MCNP	Mean Count-M Network Penetration
O-I-MCRM	Mean Cost of Response in Man-Hour
O-I-MCRX	Mean Cost of Response in Dollar Amount
O-I-MCSD	Mean Count-M Stationary End-Point
O-I-MCSE	Mean Count-M Social Engineering
O-I-MCT	Mean Count-M Total
O-I-MTR	Mean Time To Recovery
O-I-MTTA	Mean Time To First Action
O-I-MTTC	Mean Time To Containment
O-I-MTTD	Mean Time To Discovery
O-I-PAV	Count-M Physical Access Violation
O-N-MAPS	Mean Access Point Protection Score
O-N-MIPS	Mean Internet Traffic Protection Score
O-N-MWAPS	Mean Wireless Access Point Protection Score
O-T-IES	Organization Threat Awareness Score
O-T-MCTI	Mean Count-M Threat Intelligence
O-T-ITP	Threat Intelligence True Positive Rate
O-T-MTIA	Mean Time From Intelligence To Action
O-T-MTIP	Mean Time From Intelligence To Protection
O-T-THES	Threat Hunting Effectiveness Score
O-T-THTP	Mean Threat Hunting True Positive Rate
O-T-MCTH	Mean Count-M Threat Hunting Investigation
O-U-MMDPS	Mean Mobile End-Point Protection Score
O-U-MSDPS	Mean Stationary End-Point Protection Score

EPRI metrics: Comments

MEDREG is co-funded by the European Union

- Research is going on. EPRI metrics is still a prototype that has to be tested and tuned.
- Complex, requires a maturity level at least 1
- Works well for self assessment (eg in a performance based regulatory asset based on QoS), and helps to increase awareness.
- But many doubts it would work as a regulatory tool. Requires the full cooperation of the company. Difficult for external operators to verify the quality of information provided.

Maturity level: definition & interaction with performance

MEDREG is co-funded by the European Union

The maturity level (ML) is one element of cyber-security.

May be defined as the **readiness of an organization to respond to potential breaches**

May range in-between unprepared, reactive, proactive or anticipatory.

It must be clear that it is a dimension connected but distinct from other dimensions of cybersecurity (CS). The interactions are:

- ML is a condition for effectiveness (the same investment may have different outcomes, following the initial maturity level)
- ML is a condition for measurement of CS indicators
- ML increase is a desirable outcome of CS projects

Worthwhile monitoring it!

Maturity level: measurement

MEDREG is co-funded by the European Union

The measurement of maturity level may be done with several approaches (self-assessment tools or external assessments) :

- C2M2 (United States Department of Energy)
- NIST CSF
- Nemertes

They are all centered on the capability and time to:

- **DETECT: Identify** and **detect** something that is potentially dangerous;
- **REACT: understand** whether this occurrence represents a breach and **protect** the system;
- **RECOVER: contain** the breach (respond and recover).

MEDREG

MEDREG is co-funded by the European Union

Final remarks on metrics

Our aim

Understanding effectiveness of cyber investments to

- Improve the protection of the power system
- In an effective and cost-effective way
- With the final purpose of enhancing/maintaining the quality of service

Challenges

- Designing policies with objectives that may be evaluated
- Finding good indicators
- Feasibility of data collection
- Reliability of data obtained by companies

What is your opinion on this?

MEDREG

MEDREG is co-funded by the European Union

Summing up: regulatory approaches for cybersecurity

By regulatory approach we mean:

MEDREG is co-funded by the European Union

A regulatory approach is the **process** of how decisions can be made **starting from theory** and **leading to implementation**.

This conclusive part of my presentation shows how general regulatory principles can be applied in a regulation to improve the cybersecurity posture of a country.

- The regulatory approach for the investments in cybersecurity is not only a technical task…
- Since it is connected to a country's values, vision and law environment, without forgetting the general regulatory approach
- … but it uses technical instruments and must be designed following a correct sequence of decisions

The core of the approach is the strategy. A strategy is made of some grounded decisions on:

- **where to go** (eg.: increase the maturity level of the TSO)
- **how** (eg.: fund training courses on the use of self assessment tools).

A CS strategy should be based on strategic planning, addressing **people** (skills and awareness), **processes** (procedures and organization) and **technologies**. It should be **feasible** and **flexible** (importance of continual feedback and re-design)

A regulatory approach is an ordered sequence of decisions implementing an idea

The strategy and the regulation implementing it should be

MEDREG is co-funded by the European Union

Feasible:

- Identify clearly defined objectives
- Objectives must be reasonable
- …and proportionate to the incentive

Flexible:

- It is not possible neither suggested to change rules frequently
- So the strategy should include means to get evidence on the performance of the regulation
- …and rules for its re-design (establish procedures to update targets, indicators, incentives, accountability rules).

Good strategies are feasible and flexible

Types of measures that may be used in an approach

MEDREG is co-funded by the European Union

Minimum standards:

The regulator defines a list of required measures that must be complied with and the related consequences if these are not met. These can be either penalties or enforced actions.

Key performance indicators:

The regulator identifies a critical set of parameters (and the related thresholds) representing those capabilities and characteristics so significant that failure to meet the threshold value could cause the regulatory authority to intervene (as above, using either penalties or enforced actions).

Ex –ante projects:

The regulator sets up conditions for some activities ex-ante. He defines precise targets or investments and asks the utility to comply with the project prescriptions to receive grants or funding.

Performance regulation:

Rewards (penalties) are assigned according to the value of relevant indicators. Incentive mechanisms are very specific, so fine-tuning is fundamental. Indicators should be carefully chosen to represent the level of service improvement (degradation) for the consumers and for their practical feasibility.

Types of regulatory instruments that may be used also for cybersecurity while implementing a regulatory approach

Actions for the design of measures

MEDREG is co-funded by the European Union

Many elements of the strategy (minimum requirements, KPIs and related thresholds, features of the projects, possible risks, objectives in performance regulation) may be set by the regulator through:

- A **central decision**
- a process of **Consultations** with the relevant stakeholders.
- an **Agreement** between the regulator and the electricity operator.

The two latter enhance the engagement of the company in pursuing the desired strategy

Uncertainty Mechanisms: designed to revise the measures over time, as conditions change. It is crucial to identify ex-ante the possible risks that companies may incur and determine which types of actions should be taken.

There are many ways to design the CS approach

Building cybersecurity scenarios starting from cybersecurity objectives

MEDREG is co-funded by the European Union

The measures that best fit the characteristics of each country may not be established in a general way

Nevertheless, **the decision process must follow a clearly defined path, made of a list of steps** (decisions, definitions, and activities).

What is in the step is a political and regulatory decision and often there is not a global optimal way through.

Nevertheless, **one should not change the order of the steps or skip one of them**, because earlier decisions have implications on the next steps.

No theory may tell what is the best think to do (what and how); this is a political and regulatory decision.

But the decisions must be taken following an ordered sequence

The strategy is the starting point of any decision process

MEDREG is co-funded by the European Union

General strategy: where to go and how. This requires:

1. A vision: which values lead me to develop this regulation? What are my objectives?
2. Identifying expectations (What changes in the electricity market are expected thanks to my strategy?)
3. A clear-cut definition of the above = you have no doubt to understand if a situation responds to the definition or not.

Defining a strategy is a well defined activity!

Defining a regulation in the Cost Plus framework

MEDREG is co-funded by the European Union

1. Define a cybersecurity strategy for the power system
2. Define the countermeasures coherent with this strategy by
   - requiring compliance to a standard or
   - defining a list of required/suggested countermeasures or
   - agreeing a list of countermeasures with the operators
3. Define the regulation for the expenses connected to these countermeasures (eg: coverage of all compliance costs, fines if minimum requirements are not reached, funding if further countermeasures are adopted)

MEDREG is co-funded by the European Union

4

- Define accountability procedures. If the cybersecurity stance is one important aim of the policy-maker, the related expenses must be clearly identifiable in investment plans.

5

- Verify ex post the compliance of performed activities and of expenses to the plan. Make sure you have skilled people to accomplish these activities.

6

- Schedule a constant update of step 2, based on experts, on feedbacks by companies and on your experience. The problem with the **compliance** philosophy is that it is not reactive to environment and that it may give a false sense of security.

Defining a regulation in Performance based regulation

MEDREG is co-funded by the European Union

1

- Define a cybersecurity strategy for the power system

2

- Define objectives coherent with this strategy that must be
  - Clear-cut.
  - Measurable
  - Reasonable

3

- Define indicators
- Define targets to be reached

4

- Define procedures to calculate the indicators (Regulatory guidance for recording CS events)

5

- Perform controls and inspections on the way indicators are calculated (Audits in field and sanctions)

6

- Schedule a constant update of steps 3 and 4, based on experts, feedbacks by companies and your experience. The problem with the incentive philosophy is that incentives have to be constantly fine tuned with the evolution of the context

Goals and drivers inspiring the rulemaking process

MEDREG is co-funded by the European Union

- Ensure a smooth change towards new methods by taking into consideration the general regulatory framework, existing instruments and practices
- Build simple and coherent regulatory processes
- Assess it based on performance
- Be ready to let your regulatory strategy evolve based on the feedback you receive
- Involve the end-users, the companies and other stakeholders in the decision-making policy and inform them of the rationality of your choices.

MEDREG

MEDREG is co-funded by the European Union

Via Fieno, 3
20123 Milan, Italy

Tel: +39 340 293 80 23

E mail info@medreg-regulators.org
Web www.medreg-regulators.org

Follow us on