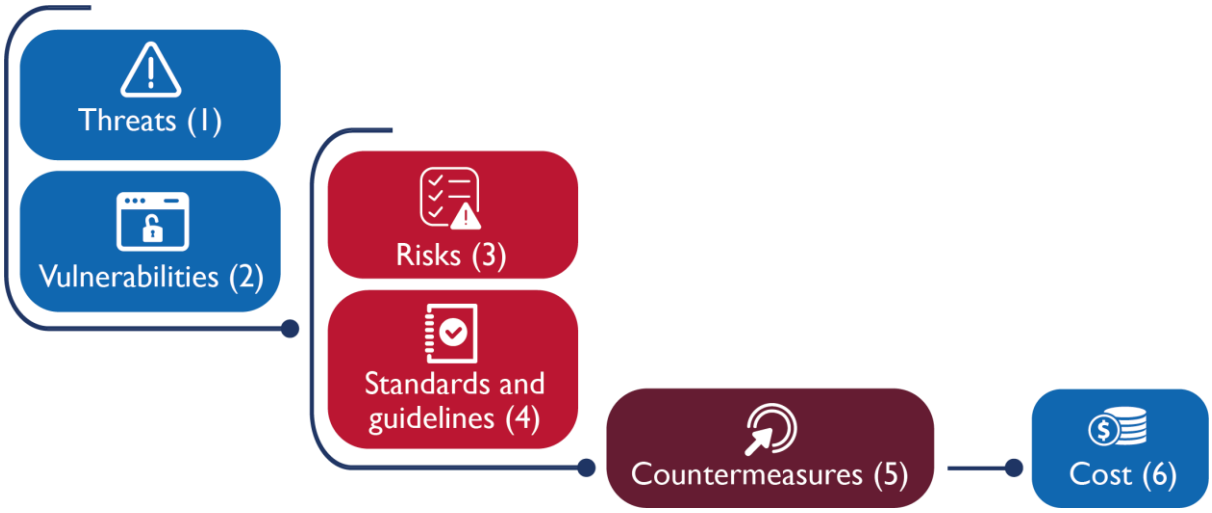
USAID
FROM THE AMERICAN PEOPLE

EVALUATING THE PRUDENCY OF CYBERSECURITY INVESTMENTS:
Guidelines for Energy Regulators



May 2020
This publication was produced for review by the United States Agency for International Development. It was prepared by the National Association of Regulatory Utility Commissioners.

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

Authors: Elena Ragazzi (project leader and editor), with contributions by Alberto Stefanini, Daniele Benintendi, Ugo Finardi, and Dennis K. Holstein under the Research Institute on Sustainable Economic Growth of the National Research Council of Italy (CNR-IRCrES)

National Association of Regulatory Utility Commissioners

This publication is made possible by the generous support of the American people through the United States Agency for International Development (USAID). The contents are the responsibility of the National Association of Regulatory Utility Commissioners (NARUC) and do not necessarily reflect the views of USAID or the United States Government.

Contents

List of Figures

List of Tables

List of Acronyms

APT	Advanced persistent threat	IRCrES	Research Institute on Sustainable Economic Growth
BSI	British Standards Institution	ISA	International Society of Automation
C2M2	Cybersecurity Capability Maturity Model	IT	Information technology
CAPEX	Capital expenses	KPI	Key performance indicator
CIP	Critical infrastructure protection	ML	Maturity level
CMM	Capability maturity model	NARUC	National Association of Regulatory Utility Commissioners
CMMI	Capability maturity model integration	NERC	North American Electric Reliability Corporation
CNR	Consiglio Nazionale delle Ricerche (National Research Council of Italy)	NIST	National Institute of Standards and Technology
DMZ	Demilitarized zone	OFGEM	Office of Gas and Electricity Markets
DSO	Distribution system operator	OPEX	Operational expenses
EPRI	Electric Power Research Institute	OT	Operational technology
GENCO	Generation operator	PBR	Performance-based regulation
ICS	Industrial control system	PSE	Polskie Sieci Electroenergetyczne (Polish TSO)
IEC	International Electrotechnical Commission	TSO	Transmission system operator

1 Context and Purpose of the Guidelines

These guidelines were developed for the National Association of Regulatory Utility Commissioners (NARUC) with funding support from the United States Agency for International Development (USAID) as part of the Europe and Eurasia Cybersecurity Partnership.

USAID and NARUC launched their work on cybersecurity in December 2016 in an effort to equip energy regulators from Armenia, Georgia, Moldova, and Ukraine with the tools and technical capacity to work with utilities in preventing and mitigating cyberattacks and to improve and safeguard overall energy security in the region. For a list of cybersecurity resources developed by USAID and NARUC, please see the footnote below.[1]

Energy regulators have a unique role to play in the field of cybersecurity. While the implementation of cybersecurity measures is typically the responsibility of power system operators, regulators have an obligation to ensure that investments made in the name of cybersecurity are reasonable, prudent, and effective. These guidelines are intended to assist regulators in defining tariffs by establishing a regulatory approach to enhance the cybersecurity stance of their power systems, and are based on literature and current practices. They attempt to answer the following questions:

- Which regulatory frameworks are best suited to evaluate the prudency of cybersecurity expenditures?
- How can regulators identify and benchmark cybersecurity costs?
- How can regulators identify good countermeasures for cybersecurity?
- How can regulators assess the reasonableness of the costs associated with these countermeasures?
- Is it possible to evaluate the effectiveness of cybersecurity investments?
- Who should identify, benchmark, measure, and evaluate the countermeasures in different regulatory frameworks?

These guidelines are a first-of-their-kind resource, and demonstrate the leadership of USAID and NARUC in empowering energy regulators to support and encourage grid resilience by ensuring prudent and effective investments in cybersecurity by their regulated entities. The guidelines strive to provide space for concepts, processes, and methods rather than prescriptive lists or ready-to-use formulas.

As power systems across the region continue to modernize, digitize, and integrate, they are increasingly exposed to additional vulnerabilities that can be exploited by cyberattacks. Attacks on the power grid can

[11] Materials developed by NARUC with USAID support include:
Black Sea Cybersecurity Strategy Development Guide, May 2017 (NARUC 2017a)
Cybersecurity Evaluative Framework for Black Sea Regulators, September 2017 (NARUC 2017b)
Additionally, the NARUC Center for Partnerships and Innovation (CPI) has developed the following materials, some concepts of which were originally developed under USAID support for the Europe & Eurasia region:
Cybersecurity Strategy Development Guide., Oct 2018 (Cadmus Group 2018)
Cybersecurity: A Primer for State Utility Regulators, January 2017 (Keogh and Thomas 2017)
Understanding Cybersecurity Preparedness: Questions for Utilities, June 2019 (Costantini and Acho 2019)
Cybersecurity Preparedness Evaluation Tool, June 2019 (Cadmus Group 2019)

have devastating effects on a nation's security, economy, and public welfare, and are a potent threat to all nations worldwide. While these guidelines were developed for the Europe and Eurasia region, much of their content can be applied universally, and NARUC encourages U.S. regulators and others to look for applicability within their own contexts and environments.

1.1 Acknowledgements:

NARUC would like to thank the following professionals for their valuable insights and for their time and expertise in designing, reviewing, and editing this document:

Stefano Bracco, Security Officer and Knowledge Manager, European Agency for the Cooperation of Energy Regulators (ACER)
Geoff Marke, Chief Economist, Missouri Office of Public Counsel
Commissioner Ann Rendahl, Washington Utilities and Transportation Commission
Commissioner Dan Scripps, Michigan Public Service Commission
Mohammed Zumla, Head NIS Competent Authority, Office of Gas and Electricity Markets
Former NARUC employees Paul Stack and Crissy Godfrey
Hisham Choueiki and Colleen Borovsky, NARUC

NARUC would also like to thank the following national regulatory authorities for their contributions:

Public Services Regulatory Commission of the Republic of Armenia (PSRC)
Georgian National Energy and Water Supply Regulatory Commission (GNERC)
National Agency for Energy Regulation of the Republic of Moldova (ANRE)
National Energy and Utilities Regulatory Commission, Ukraine (NEURC)

This publication was produced with funding from the Energy and Infrastructure Division of the Bureau for Europe and Eurasia.

2 Introduction: Preliminary Concepts for Correctly Using These Guidelines

Cybersecurity is a very diffused term, often used with different meanings. According to the U.S. National Institute of Standards and Technology (NIST) glossary, it is defined in a very comprehensive way, through a series of interconnected terms such as "the ability to protect or defend the use of cyberspace from cyber-attacks," while a cyberattack is "an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information" and cyberspace is "the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries" (NIST, n.d.b).

In these guidelines, we refer to the cybersecurity concept introduced by the NARUC *Primer*'s glossary (Keogh and Thomas 2017, 32ff.) that provides the following definition of a cybersecurity incident: "*a malicious act or suspicious event that: (1) compromises or was an attempt to compromise, the ESP (electronic security perimeter) or PSP (the physical security perimeter), or (2) disrupts or was an attempt to disrupt, the operation of a BES (bulk electric cyber system)*."

The concept of cybersecurity is closely linked to that of information security, first introduced by the BS7799, a standard originally published by the British Standards Institution (BSI) in 1995.[2] At the core of information security is information assurance, the act of maintaining the confidentiality, integrity, and availability of information, ensuring that information is not compromised in any way when critical issues arise. When dealing with critical systems, the most devastating attacks, which may have the broadest impact on the system, seek to compromise their availability by interfering with, disrupting, or disabling selected functions. Nevertheless, compromising data confidentiality and integrity, especially that of remote systems such as metering systems or remote access to protection, automation, and control systems, may also cause significant damage or be a means to prepare more devastating attacks. Later standards introduced to cope with cybersecurity in critical infrastructures and control and communication systems are basically consistent with this first definition,[3] since any one of those standards tends to define cybersecurity in its own operational terms, i.e., as a set of guidelines that—once applied—guarantee a certain level of protection to the considered target system. NARUC has taken a similar approach by introducing its *Cybersecurity. A Primer for State Utility Regulators*, now in its Version 3.0 (Keogh and Thomas 2017).

Power system controls are vulnerable to cyberattacks that can seriously affect them and even inhibit their operation. Such events, which may affect large portions of a power system and make repair difficult, can cause huge societal impact, so the pressure to ensure the protection of critical infrastructures is now strong worldwide. Several measures to counteract cyberattacks were identified, but it is rather difficult for operators and policy makers to anticipate adoption costs and benefits, and this hampers the measures' take-up. In this

[2] For more details see Appendix 2, section 5.

[3] Such as the North American Electric Reliability Corporation (NERC) CIP (critical infrastructure protection) Standards (NERC, n.d.), the International Electrotechnical Commission's (IEC's) IEC 62443 (IEC 2009), the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (NIST 2018), etc.

context, a great role may be played by regulators, who are in the position to fix rules and to provide economic incentives for the adoption of cyber-related countermeasures. Nevertheless, this is a delicate task and regulators should exercise sound judgment in deciding whether cyber-related investments are reasonable and should be recovered through the rate-setting mechanism. The assessment concerns both the rationality of decisions (the choice of measures to be implemented) and the level of expenses (are the operators under- or overinvesting in cybersecurity?).

These guidelines have been conceived as a practical tool that regulators may use in making tariff decisions to promote utilities' efforts to strengthen their cybersecurity preparedness and the security of their power systems. Nevertheless, they should not be taken as an instruction manual. The use of tools varies depending on the context, in particular on the regulatory framework adopted for public services in a country, and on the threats and vulnerabilities of a power system, which are quite diverse and keep changing. This short chapter introduces some basic concepts as to how tools should be used in different regulatory frameworks,[4] and then discusses how a cybersecurity strategy should be shaped to face ever-evolving threats.

2.1 Enhancing cyber preparedness in different regulatory frameworks

Energy regulators around the world play a critical role in setting rates that the utility can charge, balancing the interests of the consumer while also allowing the utility the opportunity to earn a fair rate of return. There are a variety of tariff methodologies that each have their own merits. However, while the threat of cyberattacks to power systems has been increasing exponentially, regulators have not had practical tools to help them evaluate and distinguish the incremental costs of investments that utilities are making to increase the security of power systems with respect to cyber prevention versus traditional infrastructure improvements.

There are two more common types of tariff methodologies that regulators can follow. The approach adopted to incentivize cyber investments can be used with both methodologies:

1. Performance-Based Regulation (PBR)
   Also known as incentive-based regulation, this method focuses on specific and measurable outcomes/goals.
2. Cost of Service
   Under this methodology, regulators determine the revenue requirement that is the amount the utility must collect to recover its costs and earn a reasonable return.

THE AIM OF THIS CHAPTER…

…is not to teach fish how to swim. General concepts about the regulatory framework are well known by regulators.

What is not self-evident is that the different instruments, pieces of information, and approaches addressed in these guidelines have different roles in the various regulatory frameworks and may be used by different stakeholders in diverse ways. Moreover, in a world of evolving threats and challenges, different tools have to be applied within a changing framework of ever evolving strategies.

[4] By analogy, these terms may be extended to other subsectors of the energy sector (e.g., gas and oil).

Reality is much more complex than this black and white picture, and many variations do exist, but a simplified view helps to understand that the role of regulators may vary a lot. In particular, these two general frameworks imply different roles for the regulators (as well as for the other operators) regarding all the activities covered by these guidelines (cost identification, cost assessment, and metrics).[5]

2.1.1 Performance-Based regulation (PBR)

In PBR, an operator (i.e., a distribution system operator [DSO] or transmission system operator [TSO]) must reach some baseline objectives described by indicators set by the regulator concerning service quality, which also involves protection from cyber threats. After the regulator sets the baseline objectives, many *carrot and stick* options may be introduced: fines if the objectives are not met, bonuses if further improvements are achieved, and fixed or decreasing tariffs over time. It is up to each individual operator to decide the most effective strategy to reach these objectives, given the system of incentives provided by the regulator and its own profit targets.[6] A good system of incentives is one that corrects market failure and makes the protection of the public's interest become an objective for profit-seeking companies too.[7] The regulator then verifies ex post that the objectives that were set have been achieved, without delving into the investments made and expenses incurred.

In a PBR context, the regulator defines indicators to assess cybersecurity performance (including protection from cyber threats and preparedness requirements) and fixes minimum levels for these indicators, following the incentive framework adopted (e.g., reducing the tariffs if a level is not reached, or granting a bonus if the operator shows better performance). Cyber expenses incurred by DSOs and TSOs are treated like any other cost connected to electricity transmission and distribution. The companies are free to decide how to ensure the required level of protection—i.e., what investments to carry out, which approach to adopt (risk management or compliance-based)—and what procedures and processes to implement.

The regulator will neither choose which expenses to approve nor check whether incurred expenses comply with previous plans; it will simply verify whether the agreed-upon objectives have been reached. Thus, no investment plans and audits are required, but great emphasis is placed on performance, which makes the way in which it is measured (performance metrics) particularly important.

[5] This is why this argument is tackled not only in the context of chapter 5, devoted to regulatory approaches, but is anticipated here.

[6] Incentives may include penalties—a negative form of incentive.

[7] Market failure is a situation in which market competition does not lead to the best allocation of resources. The presence of market failure justifies industrial policies including incentives, regulation, funding, public procurement, or direct public intervention. Defense is a perfect example of a public good (and hence, of market failure) because, once you have provided it (incurring costs), you cannot exclude anyone from enjoying its benefits, even if they refuse to pay for it. It is a useful service that has a cost, but an operator has little interest in producing it because it will not be able to sell it on the market and cover its costs.

The results of the Emerging Security Standards to the EU power Network controls and other Critical Equipment (ESSENCE) project (see Appendix 2) clearly prove this concept. They show that the benefit derived from avoiding a single successful cyberattack is enough to completely cover the cost of compliance with a standard. But the benefit is enjoyed by the whole of society (households, end-user companies, and power companies, although each for a small share only), while the whole cost is borne by the operator. Incentives are awarded to correct this situation and to provide economic benefits to companies pursuing the public interest.

In general, performance-based regulation is seen as a means to oversee public service industries by correcting market failures without completely canceling virtuous market mechanisms, and by steering processes towards efficiency. It usually leads to a reduction in costs charged to the consumers, as distribution and transmission tariffs are lower and have a more limited impact on the final price. However, what implications does it have in the case of protection from cyber risk? Which advantages and which difficulties may be foreseen? Let us survey the pros and cons of this approach to enhancing cyber protection for the power system.

Just as for any other strategic objective set by the regulator (e.g., enhancing service reliability or quality), PBR leaves it up to each individual operator to develop the most suitable cybersecurity strategy, for example, whether to comply with a standard (and if so, which standard) or to adopt a risk management approach. Therefore, PBR does not require regulators to perform many actions, allowing them to have a lighter organization with reduced staff, which results in lower costs (that in the end would be added to the consumers' tariffs). Regulators are required to have light cybersecurity competencies (mainly related to the definition of performance indicators) because they do not have to approve any specific investments. Their task is to identify feasible performance objectives and to provide incentives for the improvement of the cybersecurity posture. These may be established by relying on external experts and consultations with the operators. Finally, within this regulatory framework, the regulator may find ways to enhance the cybersecurity posture even when another entity is in charge of cybersecurity.[8]

Despite all the advantages listed above, one must be aware of certain problems and limitations that may be related to establishing a good cybersecurity strategy within this framework. In general, PBR requires all the stakeholders involved to have a fairly high level of maturity and to be able to act as competitive actors, and it works better in well-established power systems. Hence, in nascent energy markets, it should be regarded as an ideal approach to develop so that it can be easily introduced when the time is right and a reasonable period has elapsed, rather than as an imperative intervention to be implemented immediately and without assessing risks of a sudden change.

So far, the PBR approach has not been applied to cybersecurity, which makes it a new territory to explore rather than a clearly defined path. This is further complicated by the ongoing experimentation with performance indicators. At the heart of PBR are its metrics, since indicators are instruments to enhance the objectives that are set (in our case, the cybersecurity posture as depicted in the state strategy) and to reward virtuous companies by compensating their efforts. It is fundamental to identify appropriate indicators and to establish appropriate procedures to measure or calculate such indicators, but this still seems to be uncharted territory.

2.1.2 Cost-of-service regulation (cost-plus)

In this regulatory framework, tariffs cover all the expenses incurred by the companies supplying power, plus a fair remuneration of capital. Since the pure cost-plus model does not provide any incentive to improvements in productivity, to enhance operators' engagement, many variants of this model have been conceived, connected to various carrot and stick options.

[8] The regulator in charge of cybersecurity establishes the strategy and identifies objectives and targets to be reached. The regulator in charge of tariffs for the power system establishes a system of incentives rewarding operators that make progress in the desired direction. With reference to the decision process presented in section 5.3, and in particular to Figure 10, Steps 1 and 2 should be mainly performed by the cybersecurity regulator and Steps 3, 4, and 5 should be mainly performed by the power system operator, while updates based on feedback should be jointly discussed.

In this context, cyber expenses are treated like other costs and investments incurred by the utilities that have to be approved by the regulator.

The regulator has to acquire cyber competencies (and staff) for investment approval, and cyber expenses have to be identified, assessed through benchmarking, and verified. The adoption of a strategy to enhance cyber investments could be accompanied by the creation of a special procedure for their approval, making their identification easier. Where applicable, other competent national authorities should be integrated into the regulatory approach.

THIS CHAPTER

- Briefly discusses the various uses of regulatory instruments in different regulatory frameworks.
- Presents the features of strategies able to combat advanced persistent threats.
- Concludes with a table that offers a visual summary of key concepts by showing the roles of the regulators and companies in the two frameworks.

Performance metrics are needed for accountability, as a tool to improve the cybersecurity strategy and the procedure for investment approval in the subsequent investment plan, but not in order to question the individual expenditure items of an operator, which were already approved by the regulator within the context of the investment plan. The concept behind this approach is that the regulator cannot approve an investment plan and then revoke funding ex post, since this has proven to be ineffective. When the regulator approves an investment, it becomes jointly responsible with the operator for that choice. Thus, in the cost-plus context, once utilities receive approval for their investments, a metric cannot and must not be used to assess specific investments, but it must serve only to improve the cybersecurity strategy and to better choose investments in the future.

2.1.3 Regulatory framework – conclusions

Different regulatory frameworks imply different roles for regulators and operators, as summarized in Table 1.

Metrics are at the heart of PBR.

- The **regulator** defines **indicators**, the **objectives** to be reached in terms of **levels of** these **indicators**, and the **procedures** to obtain the necessary information and to calculate the indicators. It **requires data** and **verifies** their validity **through** audits or **inspections.** Inspections are intended to verify the reliability of data received.
- The **operator/utility** decides on a **cybersecurity strategy** to meet the objectives stated in the regulation. It identifies and benchmarks costs coherently with its strategy.

Cost-plus regulation is focused on cost identification, benchmarking, and approval.

- The **regulator** identifies the costs, benchmarks them, approves the plan, and verifies conformity. Metrics are used only to acquire evidence for future plans (evidence-based programming).
- The **operator/utility** incurs expenses and makes investments, as approved by the regulator, and uses performance metrics to assess the effectiveness of its strategy.

Table 1 Roles of regulators and operators in cost-plus and performance-based frameworks

	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
Cost benchmarking	☑ Regulator (benchmarks costs to be approved in investment plans) ☒ The operator is not required to benchmark costs; nevertheless, it may do it to increase the probability of investment approval	☒ The regulator does not assess the costs ☑ 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

2.2 New threats require new defense strategies

There will never be a definitive list of countermeasures or a perfect strategy to make the power system more secure. New threats emerge continuously over time, and this means that new or adaptive defense strategies must be implemented in order to counteract them. These new defense strategies have to be kept in mind when designing the cybersecurity strategy, which is the starting step of the definition of the regulatory approach.

It is not only a matter of adopting the latest network defense tools but also of changing the companies' attitude to play an active role in cyberspace as users and providers of essential services. In order to prevent cyberattacks, companies used to deploy specific network defense tools that focus on the vulnerability component of risk, while they should increasingly adopt a proactive and anticipatory response strategy.

Experts underline that advanced persistent threats (APTs) are among the most dangerous threats because they are extremely difficult to detect and defend against,[9] making them the attackers' weapon of choice. In very simple terms, an APT is an attack in which an unauthorized user gains access to a system and remains within it for an extended period of time, without being detected and identified. By doing this, hackers can have continuous access to sensitive data stored by an operator on its servers and may deploy long-term attack strategies. An APT approach implies substantial investment and effort on the attackers' part and, in fact, the attackers are often organizations endowed with means and skills, managing a number of strategies and attacks. Effort and time are needed in order to acquire sufficient knowledge, to develop a method to launch such an attack, and to probe the target's entry points so as to exploit system vulnerabilities.

The life cycle of a cyberattack conforms to a *kill-chain* model. Defending against APT deployment and execution requires careful analysis of the adversary's campaign at each stage of the kill chain. This is not a simple task, as advanced tools and a high degree of maturity and diligence are needed. According to the kill-chain model, a hacker must execute all the eight stages of the life cycle of the attack to be successful. On the other hand, in order to prevent the attack from being successful, the defender must either thwart it during any of the eight stages or break the chain. The eight stages of a (successful) cyberattack are:

1. *Initial reconnaissance*. The attacker identifies operating systems, security, applications, protocols, addresses, and other runtime characteristics.
2. *Initial compromise*. The attacker uses an exploit or an attack to probe and break through cybersecurity system defenses. This compromise could be achieved through social engineering, phishing, extortion, or other means.
3. *Establishment of a foothold*. The attacker establishes or creates persistence on an IT or operational technology (OT) system of a power unit, perhaps by installing a backdoor or utilities or malware to maintain access.
4. *Escalation of privileges*. The attacker gains greater access to systems and data by obtaining credentials, leveraging privileges, or exploiting vulnerable software.
5. *Internal reconnaissance*. The attacker explores other systems and networks to map the entire environment, identify the roles and responsibilities of key IT and OT staff, and locate interesting or valuable data needed to execute the attack scenarios.
6. *Lateral movement*. The attacker jumps from system to system on IT and OT networks, using network shares, scheduled tasks, and remote access tools or clients.
7. *Maintaining a presence*. The attacker maintains ongoing access and activity on IT and OT networks using backdoors or remote access tools.
8. *Completion of the mission*. The attacker achieves the attack objectives, such as stealing sensitive data or executing a scenario that interferes with, disrupts, or disables mission-critical functions.

In order to prevent cyberattacks, companies used to deploy conventional network defense tools. These include, for instance, firewalls, intrusion detection/prevention systems, and antivirus systems. Conventional tools focus on the *vulnerability* component of risk and are deployed in a defense-in-depth strategy, based on

[9] For a definition of APT see (NIST, n.d.a). For additional information, see (Huang and Zhu 2019; Huang and Zhu 2020).

the supposition that a successful intrusion is possible. But it is important to note that, in the case of an APT, this strategy could prove insufficient. Well-resourced and well-trained enemies have the patience, skills, and resources to conduct multiyear intrusion campaigns that target operational networks, intelligent electronic devices, or workstations. Moreover, they use the most advanced tools and techniques designed to defeat or hide from existing security measures in order to accomplish their goals.

Defenders (either internal security staff or defenders in a federated security operations center) need to continuously increase their level of maturity by using the most advanced tools and strategies. Proactive anticipatory maturity is necessary to gather and effectively operate cyber-physical system protection tools. It is recommended to perform regular audits in order to identify gaps in the solutions offered to effectively respond to APTs. It is also necessary to gather, prioritize, and process data in a timely manner.

Summing up, defenders need to switch from a purely defense-in-depth siege mentality to a proactive and anticipatory response strategy, which in turn requires the tools to reconstruct an intrusion scenario at every stage of the kill chain. Such reconstruction is essential in order to predict the attackers' next steps, and thus establish a mitigation strategy to either disrupt, degrade, deceive, or destroy the attackers' kill chain.

3 Evaluating Cyber-Related Expenditures Incurred by Utilities: Cost Identification and Benchmarking

THE AIM OF THIS CHAPTER…

…is to assist regulators in understanding whether utilities have identified the right security measures to make the power system more secure and whether the level of expenditure associated with those countermeasures is reasonable. Therefore, the various categories of countermeasures are presented with information on relevant costs.

Identification ⟷ Benchmarking

This chapter aims to assist regulators in understanding whether utility investments made to address cybersecurity issues are effective in rendering the power system more secure.[10] Since investments to address cybersecurity issues often fall into other categories and are seldom explicitly "cyber-specific," it may be hard to differentiate them from other running or investment costs. This chapter highlights the areas where cybersecurity spending can be found, with the objective of justifying the expenditure needed to improve cyber protection capabilities for the assets identified during risk assessment. From the regulators' perspective, the main question concerns **rationality in decision-making**: have utilities identified the right security measures and controls to be put in place in order to mitigate the risks previously detected?

A literature review revealed that many catalogs of countermeasures are available, but they do not provide guidance for regulators about how to identify specific cybersecurity expenditure items in the context of investment plans. In particular, existing documents summarized in the *Technical Review* that accompanies this document offer hardly any hints on how cyber costs may be allocated (e.g., in terms of manpower costs, software and license costs, or hardware upgrades). Most papers feature theoretical frameworks applicable to wide domains but very limited data about their practical application. The most concrete results about cybersecurity costs actually incurred came from the Emerging Security Standards to the EU power Network controls and other Critical Equipment (ESSENCE) project.[11]

THIS CHAPTER

- Presents principles and approaches for cost identification and cost calculation.
- Presents the most important and diffused countermeasures referring to each category of costs.
- Discusses the issues connected to their identification.
- Provides information on benchmarking and discusses the available values, based on their transferability to other contexts.

Cybersecurity cost assessment cannot be separated from benchmarking: benchmarking starts with identifying a baseline, that is, the minimum cost categories required. After discussing different cost categories, this chapter aims to help regulators identify the existing categories of cybersecurity expenditure. When determining which investments should be made, regulators must also establish the **right level of investment,** and **check**

[10] The term "grid" is used in this section to refer to the electricity transmission and distribution network, while elsewhere in this document the term "network" is used as an overarching term both for the electricity transport and distribution grid and for communication and control networks.

[11] See (CNR-IRCrES, n.d.)

whether the expenses are reasonable for the size of the operator and the threats to which they are exposed, and are in line with market prices.

In the following sections (3.1 to 3.4), we introduce some fundamental concepts for the identification of the countermeasures required and illustrate the approaches that may be used. The final sections of the chapter (3.5 and 3.6) are more practical and include a discussion of the main security areas and of some cost values that can be used for benchmarking. Further information may be found in Appendix 2.

3.1 From cost identification to cost calculation

There is no definitive reference book for cost identification in the cybersecurity domain in the energy sector. The actions needed to protect the power system evolve over time and depend on many aspects, such as the national context or the level of maturity of organizations.

Figure 1: Sequential analysis for cost identification and quantification

Cost identification should be performed following the approach shown in Figure 1. Industrial Control Systems (ICS)[12] for power generation plants and distribution or transmission grids display significant vulnerabilities (2) that can be exploited by attackers. Considering these vulnerabilities jointly with the threats (1) associated with specific attack scenarios) allows understanding of which assets are subject to higher risk (3). Standards, best practices, and guidelines (4) help identify the key organizational and technical countermeasures (5) needed to increase the security level of the infrastructures involved, so as to neutralize possible attacks. The final result is the quantification of both the cash flow for the implementation (investment costs—CAPEX) and maintenance (annual operating costs—OPEX) of the countermeasures identified (6).[13]

There are two approaches to implementing cybersecurity on a networked grid:

- Creating a **checklist of actions** that address known security risks to which the operators are obliged to adhere (**compliance-based approach**)

[12] Nowadays there are not only ICS, there are a consistent number of IT platforms on which the operators may rely, and they all suffer from the same problems.

[13] The total cost is represented by the sum of operational expenses and annualized investment cost.

- **Prioritizing actions** based on continually updating the answer to the question, "What makes my system more secure?", or more precisely: "What are the risks I'm exposed to, and how do I make sure they are controlled?" (**risk-based approach**).

Both approaches have merits and they complement each other. The **compliance-based approach** helps to easily identify/determine countermeasures since it is based on standards or guidelines (i.e., NERC CIP, NIST *Framework*, and IEC 62443) that present sets of countermeasures and list associated expenses. These standards represent the most important source of information for section 3.5, aimed at describing and discussing the main cost items connected to power system protection. On the other hand, a **risk-based approach** focuses on the assets to be protected and helps regulators to look for effective and efficient cyber expenditures, since investments are to be expected where the risk is supposed to be higher.

Cost categories may be identified in a general way, with small variations among the types of operators. However, it is not possible to rely on a general method, such as the application of fixed parameters, for:

- Choosing the right **order of priority** (which investments a country should begin with if its budget is insufficient to cover all needs).
- **Quantifying** the effort required to protect the power system or one of its subsystems, such as generation or transmission at the national level or distribution in one region.
- Deciding which countermeasures are a baseline; this would imply that there is no need to remunerate them as they are common practice.

The assessment of critical assets to be protected (and the estimation of the relevant security investments and their maintenance costs) will prove more complex in the case of generation and distribution (due to the presence of multiple operators and a number of assets with a high level of intrinsic complexity). Selecting which infrastructures need protection depends on the size of the facilities (power systems are resilient in case of faults of small generation units), their use (cold reserve has low priority regardless of its size), and the features of the socioeconomic systems they serve. This assessment may be carried out following the benefit analysis described in section 3.3. The presence of multiple operators, acting as competitors in the case of generation and retail sales, suggests that the assessment should not be done by the operator itself, but by policy makers or regulators while defining the power system cybersecurity strategy.

Cost assessment includes calculating the cost of purchasing equipment, such as ICS and related backup systems, and identifying the types of professionals needed to implement the countermeasures, as well as their cost per hour and the hours of work required. The total cost of initial implementation (CAPEX) has to be supplemented with operational expenses to maintain each of the embedded countermeasures.

Nearly all countermeasures imply a cost that is made up of different components, so they will never appear in accounts as single operations. They include not only hardware and software, consultancies, training of existing staff, and hiring of new staff, but also intangibles, such as new rules and procedures and the redesigning of systems. In many cases, the cost of countermeasures may be partially hidden, even to the operator, inside more general accounting items. Personnel costs connected to cybersecurity are usually very difficult to separate from the overall cost of labor. At a more granular level, some cybersecurity countermeasures are based on processes, that is, operating costs, rather than capital investments. Hence, they do not have direct costs but could imply losses in productivity because some activities (like personnel access to secured areas) will take longer. In other cases, to comply with some of the requirements included in the standards, it will be necessary to hire employees with higher qualifications (and higher salaries). Another example is that of goods and services bought to upgrade the power system. The purchase of more powerful and expensive hardware or software may be beneficial, as these products often embed cybersecurity measures; however,

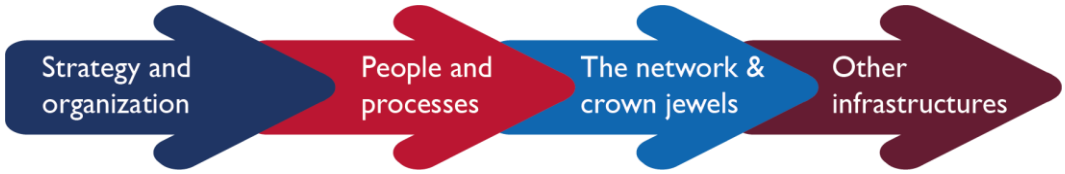
these are not normally labeled as cyber investments. In practical terms, we can offer the following operational observations:

- The regulator can gather evidence of cybersecurity expenses only if these are carefully extrapolated from other costs and investments. The regulator can deduce that an operator has adopted some cybersecurity countermeasures by consulting its documents ex post, in particular, if they come with a certification by the vendor, but their economic value can be obtained only if this had been foreseen.
- The operator must be instructed ex ante as to which information it will be asked to provide and with what level of detail. Not all information will be available in general accounting.
- The operator must provide full cooperation.
- An approach to cybersecurity based on ex ante projects (see section 5.2) is particularly suited to cost identification. An ex ante project will prescribe both the features of the cybersecurity investment and the types of costs that will be funded, along with the type of information required for cost justification.

3.2 Identifying priorities

When analyzing a standard, it is difficult to distinguish the most important requirements from the ones that can be postponed. Cybersecurity standards enable organizations to deploy effective security techniques in order to minimize the number of successful cyberattacks; a cybersecurity standard is a comprehensive and heuristic approach that ensures a given level of protection if the operator complies with all countermeasures required. Nevertheless, not all actions are the same, and some of them have an "enabling" role; that is, they are necessary to make the other countermeasures effective.

Figure 2: Priorities in the strategic planning of cybersecurity protection



The starting point, as shown in Figure 2, is the definition of cybersecurity objectives and of the plan to reach them. This means adopting a specific strategy and architecture and organizing a management structure for the implementation and management of the strategy.

The second priority has to do with personnel and working processes. "Securing" personnel is an essential point. First, all employees must be made fully aware of cyber risks and the importance of properly using physical assets. They must be skilled enough to avoid, or to intervene to mitigate the effect of, cyber threats, such as phishing and malware, and the improper use of physical assets, such as using USB keys or other devices to transfer data or connecting personal devices to the network. Skilled personnel are needed to take full advantage of the technology installed. Another issue concerns the selection, management, and supervision of people since employees might cause security breaches not only by the incorrect use of physical or information systems, but also deliberately. In practice, to address this second priority, an operator must invest in personnel selection, training, and awareness and in processes for correct information management.

Priority should be given to critical assets, often referred to as ***crown jewels***, on which the functioning of critical infrastructures relies.[14] However, it is also important to protect the system itself, including the network connecting the various devices (e.g., controls and smart meters), and not just single assets. These assets can be identified based on their function, through an analysis of the network topology and of its connections with the external world. This last step implies adequately protecting all the relevant infrastructures while avoiding investments when the cost of protection exceeds the potential benefits, which highlights the importance of the benefit analysis (see section 3.3) in cost prioritization.

A final remark on cost identification: everything described above has a cost. The security of physical assets has a cost, and so do training personnel on a continuous basis, hiring *trained* personnel, and developing and enforcing procedures to ensure that the personnel is trustworthy. Regulators must keep these points in mind and consider total expenditures, because if only CAPEX items are eligible for recovery, operators might be tempted to disregard the most important priorities, which actually involve operational and maintenance costs.

3.3 Benefit analysis

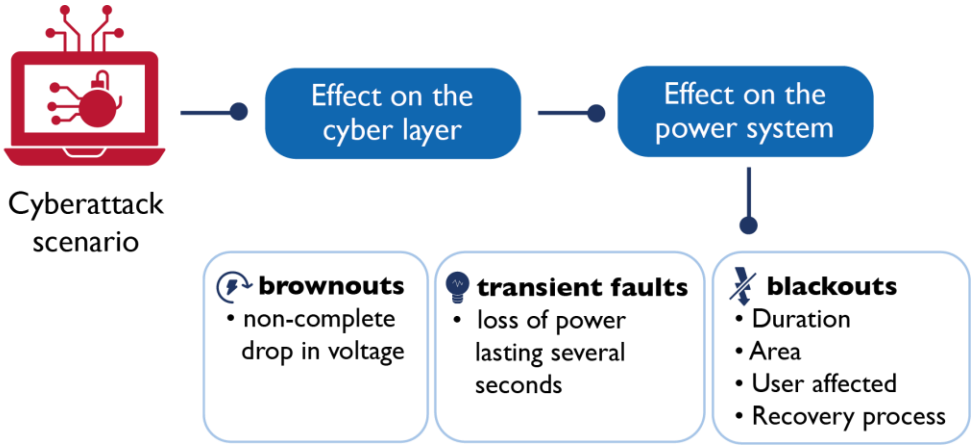
Evaluating the benefit of implementing countermeasures means assessing the impact of a successful cyberattack. The benefit in question is the possibility that this (negative) impact may be avoided or minimized.

While cost assessment is a calculation, benefit assessment is an estimate that requires technical and economic assumptions. Why should a regulator or an electric grid operator assess the impact of a successful cyberattack scenario? Why take the trouble to evaluate the benefits of applying countermeasures, which is complex and methodologically difficult? There are two reasons for this:

- *Accountability*: justifying the funding of cybersecurity investments to the government and the public.
- *Prioritization*: allocating limited resources to high-risk assets or high-impact scenarios, which means assessing the probability of an event, the impact of that event (its effect on the power system) and the economic value of that impact on the society as a whole.

[14] Although there are several definitions of critical infrastructures, official sources agree that power systems are among them. According to the U.S. Department of Homeland Security, "Critical infrastructure describes the physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety" (DHS, n.d.). The related U.S. Department of Homeland Security Cybersecurity & Infrastructure Security Agency (CISA) site provides a list of 16 critical infrastructure sectors, including energy systems (CISA, n.d.). In Europe, the Council Directive 2008/114/EC (EU 2008), which applies only to the energy and transport sector, establishes a procedure for identifying and designating European Critical Infrastructures (ECI) and a common approach for assessing the need to improve their protection.

Figure 3: Impact of a cyberattack – technical assessment



The technical assessment of the impact of a pure cyberattack is shown in ***Figure 3***. First, the effect on the cyber layer must be evaluated, which requires cybersecurity skills. If the existing countermeasures have failed to block the attack, the effect on the power system must also be evaluated. This implies combining cybersecurity skills (to assess the propagation and escalation of the attack and the time needed to block it) and engineering skills (to assess the effects on the power supply).

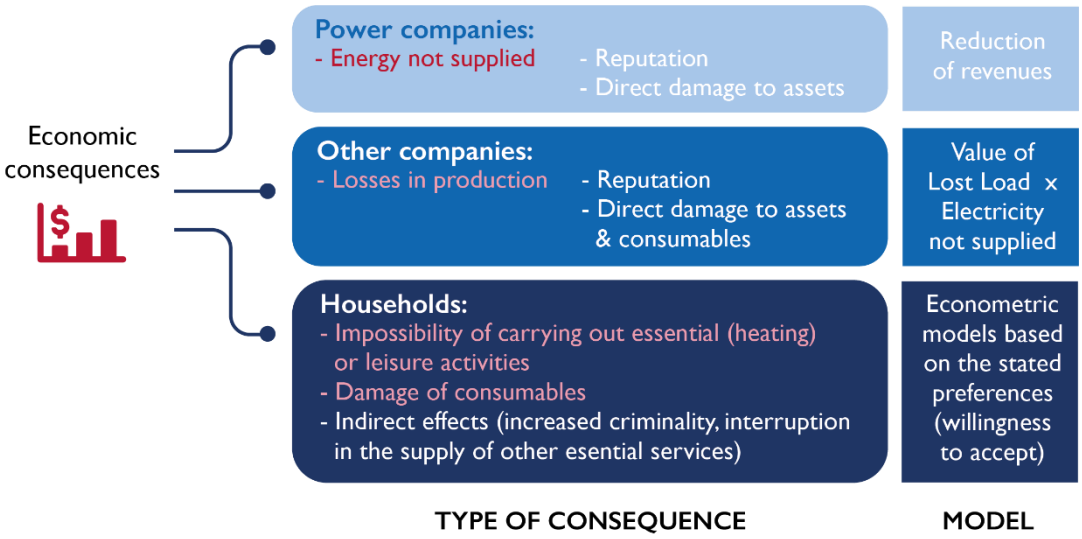
The impact of the cyberattack on the power system must be translated into economic value, to be used for the cost-benefit analysis (3.4). This evaluation,[15] illustrated in Figure 4, comprises three aspects:

- *Impact on the operators of the power system*. This has to do mainly with reductions in revenues (for all suppliers: generation operators [GENCOs], TSOs, and DSOs) deriving from electricity not sold or not delivered to end customers. More refined evaluations may also include values for loss of reputation and possible damage to the equipment.
- *Impact on productive end users*. In this case, the main damage is due to the fact that it is impossible to continue production processes, expressed as "Value of Lost Load." For this reason, the evaluation should also take into account how heavily different industries rely on electricity. More refined evaluations may also include values for loss of reputation and possible damage to equipment and consumables.
- *Impact on domestic end users.* In this case, the impact mostly derives from the impossibility of carrying out essential activities or practicing leisure activities, although direct damage to consumables must also be taken into account. In order to accurately calculate an economic value, it is necessary to understand how much value people place on power-dependent activities. This may be done through surveys of

[15] This assessment involves many technicalities, which are exhaustively described in (Bruno et al. 2014). The report also provides a list of relevant references to methodological papers and similar analyses. In Figure 4, the main effect is written in red, while secondary effects are written in white.

representative samples based on the "stated preference" principle.[16] The data collected must then be transformed into a cost through econometric models.

Figure 4: Impact of a cyberattack – economic assessment



3.4 Costs and benefits of cybersecurity countermeasures

This section discusses how to approach a comprehensive economic analysis of cybersecurity countermeasures in the electricity sector.[17] The objective is to evaluate the suitability of a particular type of policy, such as a regulation imposing the adoption of some countermeasures (e.g., those listed in a standard), by comparing the cost of its implementation with the benefits it may bring to the power system. To this end, an impact analysis perspective (see section 4.2) is employed, which requires assessing the effect of a policy on an outcome variable. In order to correctly isolate the effect of the policy, one must compare two situations that differ only in whether the regulation is in place or not. For this reason, the first dimension of the evaluation concerns the *implementation of regulation* and compares:

- A *situation with no regulation*, where each operator sets its own level of protection and invests accordingly to implement certain countermeasures, which thus turn into security costs.
- A *regulated situation*, in which the minimum level of protection is set by the regulation itself, and may consist of the adoption of a certain security standard or a list of countermeasures, or of a performance score to be reached. We expect this security cost to be higher. Otherwise, there would be no need for regulation, as companies would already have a good protection strategy in place.

However, security countermeasures are much more complex to assess than other aspects of regulation. This is because security costs are incurred in any case when regulation is in place, but their related security benefits

[16] i.e., based on methods that involve asking individuals questions that can be used to infer economic values through either direct or indirect expressions of economic value.

[17] More details, such as step-by-step guidance on the application of this approach and a hypothetical exercise showing its application, are provided in Appendix I.

emerge only in case of an attack, the consequences of which the countermeasures were designed to nullify or mitigate. In order to assess the benefits, it will then be necessary to introduce a new dimension of evaluation concerning the attack scenario. The performance of the electricity system is evaluated in two situations: ongoing cyberattack and no cyberattack. Four scenarios derive from combining the two dimensions. For each scenario included in Table 2, one has to calculate:

- The cost of running security measures. They should be the same per column except for costs associated with taking emergency actions in response to attacks (so-called recovery costs).
- The economic cash flows connected to electricity production in various situations:
    - The cost of producing (or purchasing) electricity and the cost of supplying it (cost in normal conditions *versus* the cost when an attack causes disturbances able to affect the operational management of electricity supply). *In this case, the attack disturbs the system but does not cause a blackout.*
    - Or the effect of interruptions in supply on the economy and on society. *In this case, the attack causes major disturbances that turn into a blackout.*

Table 2: Scenarios for cost-benefit analysis

		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[18]	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

Table 3 (below) defines these monetary indicators and describes how to calculate them. For all calculations, the whole electricity system must be considered, not just a single operator or part. This, of course, introduces some difficulty in the assessment, because costs and benefits have to be estimated taking into account what happens all along the production chain, even when this involves several different operators. Analyzing only a part of the system is not only incomplete, but might, in some particular cases, prove misleading. For example, it might happen that, thanks to the attack, which causes a reduction in general supply, local market prices increase. As a consequence, some companies might earn more, and even take advantage of the situation strategically by hampering the restoration of normal conditions.

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

Table 3: Economic indicators for the cost-benefit analysis

1 Indicator	2 Scenario	3 Cost category	4 Information deriving from a simulation	5 Additional information from other sources	6 Description of indicator and type of information
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?		Total cost of production (or price of purchase) of the energy (generation + imports) exchanged in the scenario.
B	**I - Not regulated – no attack**	Yearly cost of security measures		How much does it cost to manage the current security systems?	Cost of implementing and maintaining countermeasures associated with the present level of protection against cyberattacks. It includes both operative costs (personnel, material) and asset depreciation.
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?		Total cost of production or price of purchase of the energy used in the scenario compared to the unperturbed situation.[19]
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	The cost of the blackout may be divided into the cost for the power operators, the cost for other companies, and the cost for households.[20]
E	**II - Not regulated – attack**	Cost of emergency actions.		How much would it cost to recover from the attack?	This item is associated with taking emergency actions in response to attacks (recovery costs).

[19] The expected increase in costs is associated with the difficulty in supplying power and the necessity to rely on more expensive sources/plants.

[20] It depends on users' characteristics and on blackout duration, time, and venue. This item mainly assesses the direct or indirect costs faced in case of interruption. This effect varies according to the types of customers. So, a lot of heterogeneous information has to be collected: number of consumers involved and their locations, type of consumers (industrial by size, commercial and services, residential, agriculture), data to estimate the economic and social impact (value of lost load, willingness to accept). See section 3.3.

1 Indicator	2 Scenario	3 Cost category	4 Information deriving from a simulation	5 Additional information from other sources	6 Description of indicator and type of information
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?		Total cost of production (or price of purchase) of the energy (generation + imports) exchanged in the scenario.[21]
G	**III - Regulated – no attack**	Yearly cost of security measures		How much has to be spent to manage the security systems with the regulation?	Cost of implementing and maintaining countermeasures associated with the level of protection against cyberattacks required by the regulation. It includes both operative costs (personnel, material) and asset depreciation.[22]
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?		Total cost (generation or purchase) of the electricity exchanged in the scenario.
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?	The cost of the blackout may be divided into the cost for the power operators, the cost for other companies, and the cost for households (see section 3.3).[23]
J	**IV - Regulated – attack**	Cost of emergency actions.		How much would it cost to recover from the attack?	The cost of taking emergency actions in response to attacks (recovery costs).

[21] This could be higher than without regulation because it could require backup facilities or more time-consuming procedures.

[22] We expect that there will be an increase in security cost and, in particular in asset depreciation, due to investments made to comply with the regulation.

[23] We expect that the blackout may be avoided or at least that there will be a reduction in the cost of the blackout (due to shorter duration, fewer users involved) with respect to the unregulated situation.

In Table 3, the second column refers to the evaluation scenarios described in Table 2. Column 3 concerns the types of costs or effects to be considered. These encompass the cost of power (production, purchase, and supply) in case the attack disturbs the system without causing an interruption in supply, or the effects on the economy in case of blackout, plus the cost of running security countermeasures (with or without the regulation in place, also including recovery costs). The values must be calculated for each specific case. In particular, there might be wide differences in the actual levels of countermeasures. A hypothetical situation in which no security countermeasures are implemented would imply that the current cost of security (Indicator B in Table 3) is zero. The cost of security includes both the annual operating costs of management and maintenance and the depreciation of investments.

The information for these calculations comes from two different types of sources:

- A simulation showing what would happen in the electricity system in a particular situation (time, day of the year, location) with or without an attack. This will yield the real flows of electricity exchanged, the cost of power supply, and, eventually, the impact of the blackout generated by the disturbance.
- Information coming from other sources, concerning the types of customers involved in the blackout and the technical and organizational cost of security.

The final assessment consists of comparing the different indicators, as shown in Table 4.

Table 4: Relevant indicators for the impact evaluation

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).**

3.5 Security areas

By understanding and discussing the main categories of countermeasures, regulators can better identify cost categories in investment plans and understand whether utility investments are prudent and useful.

International security standards, as well as best practices and policies (generally related to ICS security for the energy sector), describe technical requirements for various security areas. Standards list uniform engineering or technical criteria, methods, processes, and practices.

The complexity of controls for electric power generation, transmission and distribution activities is reflected in the number of security standards for the power system, which classify security areas in several ways. This uncoordinated proliferation of standards and guidance for electric power system cybersecurity has understandably made it more difficult for individual utilities to quickly determine what is required of them. In addition, it certainly poses a challenge for those who would like to shed light on their many parallel efforts. Where no standard is imposed by law, common practice, as highlighted by the ESSENCE project, goes in the direction of following the soft guidance of one or more standards, and the most relevant standards for transmission and generation are not the same. Although the prescriptions that an organization must comply with are not so different, the classification of countermeasures does not fully overlap. Different security standards entail the use of different countermeasures that are classified in different ways. A comprehensive list of these categories and a comparison of possible classifications are included in Appendix 2.

The sections below describe the most relevant groups of countermeasures. These lists, mostly inspired by the prescriptions of International Society of Automation (ISA) standard ISA-99.02.01-2009, which later became IEC 62443-2-1, do not claim to be complete and have a twofold aim. The first is to offer a simple review of relevant countermeasures to be applied in order to achieve basic improvements in security. The second is to introduce the reader to the complexity of the use of security standards in power utilities.

3.5.1 The governance of cybersecurity

The costs of the governance of cybersecurity deserve particular mention, as they seem especially relevant for transitioning economies. The main costs to improve an operator's security posture result from updating and maintaining organizational processes (policies, procedures, and organizational directives) and personnel training (awareness, and ability to respond in a timely manner).[24]

Due to their nature, governance costs might be less evident than the costs of other countermeasures. Nevertheless, they might represent a significant fraction of the total, in particular, when necessary for

[24] This is underlined by relevant standards. According to NERC, "The purpose of a security management program (SMP) is to ensure that the organization creates and maintains the policies, standards, and procedures necessary to ensure that all applicable aspects of the security domain are adequately covered" (NERC 2016, 4). The NIST *Framework for Improving Critical Infrastructure Cybersecurity* addresses cybersecurity governance, defining it as follows: "The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk" (NIST 2018, 25–26).

steps forward in maturity. In section 3.2, the organization of a management structure is indicated as the primary priority, followed by personnel and procedures. The need to update and maintain processes and personnel skills (awareness, timeliness, etc.) might entail relevant costs, as will be shown in practice in the next section. The lack of proper governance might impact the efficacy of security systems, and the behavior of poorly trained personnel might even bypass their effect. Proper procedures are countermeasures themselves. Thus, the level of maturity of a system, which is a consequence of security governance, is a condition for efficacy.

Governance countermeasures, the main categories of which are described in Table 5, display little scalability, on the whole. For this reason, a specific arm in charge of cybersecurity should be organized in large and medium-sized operators, such as big utilities and TSOs, while small organizations may choose to rely on the services of a federated security operations center.

Table 5: Areas of cybersecurity governance countermeasures

Security programs. Directives related to vision, objectives, goals, strategies, directions, and plans of security systems.
Organization of security. Requirements concerning both internal and external (third-party) roles, responsibilities and organization suited to guaranteeing security.
Security policy. Provisions concerning policies, plans of actions, and procedures on security.
Risk management. Requirements concerning the approach to risk management and its methodology.
Asset management. Provisions concerning asset management to achieve and maintain protection.

3.5.2 Hardening

System hardening is the process of checking and securing a system. It is performed via the adoption of specific techniques aimed at reducing the surface that is exposed to attack. As most systems may still be vulnerable to access from the outside, hardening is necessary even when network security features, such as antivirus programs and spyware blockers, are present. Hardening methodologies may involve selecting the services to be used, software package updating, optimization of configurations, elimination of unneeded users, closing network ports, installing a system of intrusion detection and prevention, and firewalls. Hardening cost categories may fall under several cost classes, as summarized in Table 6.

The meaning of some of these keywords (e.g., configuration management, business continuity) does not require any specific explanation. However, some of them deserve clarification:

- *Malicious software prevention* requires a good, up-to-date understanding of your system vulnerabilities vis-à-vis the threat landscape (who are the likely attackers, their preferred way of operation, patterns of attacks, etc.)
- *Cryptography* is another area where technological progress has made giant leaps so that code breaking is now possible on cryptographic schemes until recently deemed secure.

- *Access Control*, both physical and electronic, must be determined in view of the many personnel categories that must be granted access to plant facilities, such as the plant crew, maintenance and service personnel, plant management, administrative officers, business controllers, and auditors.
- *Compliance and improvement* require up-to-date knowledge of the standards and guidelines one wishes to apply. Complex standard frameworks are being updated on a continuous basis.
- *Network security* is a separate function from *host* (i.e., plant control) *security*. This concept is especially stressed by IEC 62443, where a key concept is the assessment of the conduits to carry data and information through several application areas within a complex ICS.[25]

Quite clearly, most of these categories are not fully independent, but are interrelated; for example, human resource security organization, security levels, personnel knowledge of the current cybersecurity landscape, and access granted to facilities are mutually dependent.

Table 6: Hardening cost classes

Malicious software prevention	Human resources security
Configuration management	Physical and environmental security
Cryptography and key management	Business continuity management
Backup and recovery	Incident management
Network and host security	Compliance and improvement
System acquisition, development, and maintenance	Access control

3.6 Estimating the cost of countermeasures

Very little evidence is available in the literature about the costs involved in assuring compliance with existing cybersecurity standards. The ESSENCE project is a noteworthy exception because it calculated the costs connected to the key organizational and technical countermeasures needed to increase the security of the infrastructures involved in the case studies (generation and transmission) (Calabrese, Finardi, and Ragazzi 2014). This section presents the results of these calculations, offering the maximum level of detail compatible with confidentiality issues, and discusses their transferability to the context of transitioning economies, such as the Black Sea countries.

[25] For further details on the description on security areas, please consult Appendix 2: "Summary of the main results of ESSENCE project," Section 2.

3.6.1 The costs calculated in the ESSENCE project

The costs evaluated in the case studies and extrapolated to all the countries involved are presented in Table 7.[26]

In both cases, two situations are considered: costs to be borne in a hypothetical scenario where no security standards have been implemented (cost starting from 0), and costs to be borne starting from the current situation, in order to manage supplementary security (Delta cost). The first column is reported as a reference, to understand the share of total investment which has already been made, since no power system is deprived of any protection. This information is interesting since it provides a basis for assessing scalability to other contexts.

The adopted methodology quantifies cash flows for the implementation and maintenance of security standards. Some of the costs, specifically the ones related to the design, acquisition, and implementation of countermeasures, are investment costs to be borne only once, upon first introduction (CAPEX); other costs, specifically those related to the maintenance of countermeasures, are operating costs to be borne annually (OPEX).

Table 7: Total cost of implementing and maintaining countermeasures in ESSENCE case studies (€, '000)

	COST STARTING FROM 0		DELTA COST	
	CAPEX	OPEX	CAPEX	OPEX
Electricity transmission in Poland	26,016	5,016	7,486	2,457
Electricity generation in Italy	27,730–52,480	6,480–11,980	20,000–40,000	3,480–5,980

Source: (Calabrese, Finardi, and Ragazzi 2014)

As discussed in section 3.1, since the Italian case concerns generation, some assumptions were necessary to assess the number of plants (belonging to several operators) to be protected. Conversely, in the Polish case study concerning the national TSO, the protection of the whole national transmission grid was included in the assessment. This explains why, in Table 7, the cost is estimated precisely in the Polish case, as a single transmission system operator is in charge of the system. Instead, in the Italian case, an estimation range is presented, as several power GENCOs operate on the system.[27]

[26] More information (with a level of detail compatible with the need to avoid exposure of confidential critical information) on attack scenarios, selected countermeasures, and cost calculations may be found in the case study reports.
For the Italian case study: (Angeletti et al. 2014). For the Polish case study: (Bartosewicz-Burczy et al. 2014).
[27] To have a sense of the size of the two case studies, the Italian population is 60 million, and the Polish population is 38 million.

3.6.2 How to transfer ESSENCE results to other contests?

It is not easy to calculate the real effort required to ensure the acceptable protection of a power system since it depends on many specific variables related to the local context. This is why it is not possible to calculate its cost by means of a formula with fixed parameters. Nevertheless, the ESSENCE calculations used to obtain the total values included in Table 7 provide some parameters of general interest. With reference to governance costs, Table 8 reports the resources required to implement a comprehensive plan.

Table 8: Resources required to implement a cybersecurity governance plan (€ or no. of people)

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

Source: (Angeletti et al. 2014)

The information about Effort refers to the number of people, as far as internal staff is concerned, and/or to expenditure in Euros for the purchase of goods and services (values calculated in 2014 in the context of the Italian case study). The table underlines both the initial effort to implement the plan and the yearly expenses necessary for its maintenance. It may be worth a reminder that governance costs suffer from little scalability and so, for very small operators, the suggested solution is to refer to a federated security operations center.

The Italian case study also provides some information on the cost necessary to protect a typical 380 MW unit (Table 9), which can be used to assess, after assessing scalability (above all in multiunit generators), the cost of protecting the generation system.

Table 9: Hardware/software costs for hosts and networks security of a typical 380 MW power unit (€)

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

Source: (Angeletti et al. 2014)

As for the transmission system, the Polish case study indicated that the cost of protecting a substation was equal to €151,180 for initial implementation and €27,830 for maintenance. Yet it must be noted that costs do not scale up linearly, due to economies of scale. Hence, a nonlinear scale must be adopted, considering both scalable and non-scalable costs. Table 10 shows more detailed data on Polskie Sieci Electroenergetyczne (PSE), the Polish TSO, equivalent to a country with 100 substations. Moreover, as a tool for the generalization of the results, we provide a quantification of the total effort (no implemented protection) necessary for a smaller TSO (30 substations) and a larger one (200 substations), based on an assessment of scalable costs.[28]

Table 10: 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

[28] To better assess these values, consider that, in the case study, the average labor cost of skilled staff was 20€ per hour (2014 prices), and that PSE ICS systems included 100 servers, plus a redundant Internet node with total of 40 servers. PSE employed 2,000 workers.

		30 substations	100 substations	200 substations
Maintenance costs/software	Information control systems	155,216	388,040	698,472
	Office systems	510,496	1,276,240	2,297,232
	Total maintenance/software	1,500,612	3,751,530	6,752,754
Maintenance costs/labor	Substations	208,800	696,000	1,392,000
	Information control systems	54,000	180,000	360,000
	Office systems	116,700	389,000	778,000
	Total maintenance/labor	379,500	1,265,000	2,530,000
	TOTAL OPEX	1,880,112	5,016,530	9,282,754

Source: (Calabrese, Finardi, and Ragazzi 2014)

4 Effectiveness Metrics

This section introduces approaches to measuring the performance of cyber expenses, to help determine if investments are effective in making the power system more secure. The goal is to provide regulators (and utilities) with means to track and monitor the effectiveness of investments.

Regulators will assess cyber performance and track improvement (security benchmarking), and then evaluate performance as a function of the expenses incurred.

THE AIM OF THIS CHAPTER…

…is to present and compare the tools available to assess the effectiveness of cybersecurity investments.
The chapter also introduces some basic concepts concerning effectiveness assessment and discusses the way in which a system of performance indicators should be managed in order to obtain a reliable picture.

The term *metric* can refer to either a system or method of measurement, or to a unit of measurement to assess, control, rank, and select objects (phenomena, processes, or people). This chapter deals with both layers, explaining both the *what* (measures of the variables, i.e., the indicators) and the *how* (the system, the method to calculate indicators and to collect data), so as to provide a toolkit of measurement instruments along with instructions on how to apply them.

As discussed in section 2.1, the role (use and purpose) of metrics depends on the regulatory framework. The metrics described in this chapter could be used, for example, to identify key performance indicators (KPIs),[29] in order to evaluate whether the cybersecurity solution currently in place ensures the desired level of protection. Regulators can adopt these metrics to benchmark the effectiveness of investments in alternative cybersecurity solutions. Given the rapidly evolving threat landscape, these benchmarks should provide a reasonable basis to strategically plan future cybersecurity investments. Or, in performance-based regulation, performance metrics may represent the instruments to create appropriate incentives to ensure an adequate level of protection. The next chapter discusses in greater detail how metrics may be used in different ways when building an overall regulatory approach.

Developing metrics to evaluate effectiveness is challenging because it requires an in-depth understanding of the context of the system of interest and a well-described situational assessment. As a preliminary point, we must observe that research and experimentation are ongoing in this field, so many suggestions are available, but no established practice can be singled out.

4.1 Identifying good effectiveness indicators

Effectiveness evaluation is not limited to cyber investments but may concern any public policy, pilot project, innovative approach, or investment. Consequently, researchers and practitioners have developed general wisdom that helps to understand the "how-to," i.e., the correct approach to selecting indicators.

[29] KPIs are the critical subset of performance parameters representing those capabilities and characteristics so significant that failure to meet the threshold value of performance could cause the regulatory authority to reevaluate the cost justification for the utility's cybersecurity system of interest.

Nevertheless, the quality and appropriateness of the indicators are closely linked to the evaluation approach and jointly determine the success of the evaluative exercise. Selecting the wrong indicators may nullify a wonderful evaluation design, to the same extent as the most sophisticated indicator may lead to the wrong conclusions if it is not measured and used correctly. This is why it is important to underline general requirements and features for effectiveness indicators. An indicator must have particular features in order to be used to assess performance metrics:

- *Clear causal relation*. The causal link between the investment and the variable describing the expected outcome measured by the indicator must be clear, and the indicator must capture the essence of the desired result. The causal link must also be clear with respect to other possible variables affecting the outcome (absence of confounders).
- *Measurability*. The variable describing the outcome should be well represented by indicators that can be observed and recorded. Also, it must be easy and not too costly to collect data to calculate the indicator. The cost and effort of evaluation must be proportional to the value of the evaluated phenomenon.
- *Specificity*. The object of measurement must be clear, and the level of disaggregation must be appropriate to observe the outcome and its variations in space and time (sensitiveness).

Output, outcome and impact: an example

A group of employees attends a course on security procedures in communication with external parties.

- **OUTPUT**: Number of participants passing the final test on theoretical aspects → **It shows effort intensity and quality, but it is not a measure of effectiveness**
- **OUTCOME 1**: Number of mistakes in security procedures (for example: using an unauthorized USB key) in the year after the course → **effectiveness metrics**
- **OUTCOME 2**: Number of IT system intrusions in the year after the course → **effectiveness metric but insensitive indicator**
- **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.

4.2 What is effectiveness? The concepts of output, outcome, and impact

Effectiveness has to do with the results of an action, but one has to clarify what these results consist of. **Output** is the direct effect of an action (an investment, a training program, a new procedure, a regulation, a policy, or an incentive). **Outcome** is the change in the objective variables that may be observed after that action. This change is indirect, because it is mediated by the context and by subjective variables, and often occurs only with a certain time lag.

To assess the effectiveness of any planned action (an investment, a training program, a new procedure, a regulation, a policy, or an incentive), it is necessary to check whether:

1. The action has been carried out and has produced the expected results. A badly managed policy will never be effective.
2. A change in the desired outcome has occurred.

3. This change may be ascribed to the action.

All three points are relevant, but addressing the third one is a thorny issue. The problem is that change is not impact. After choosing the right set of indicators, effectiveness assessment continues by comparing the value of one or many indicators before and after an action. To make sure that the observed change can actually be ascribed to the action and is not merely the result of an endogenous process that would have occurred anyway, it is necessary to assess the **impact** of the action on the objective variable. To determine the impact, the observed change should also be compared to the change recorded in similar situations in which the action was not carried out. This **counterfactual approach** is fundamental when there is suspicion of a deadweight effect, that is, when it is reasonable to expect an improvement in the observed indicator even without the action.[30] Counterfactual impact evaluation is particularly important in case of experimental adoption of particular countermeasures in pilot studies, before the experimentation is extended, because it is the only way to gather sound and reliable evidence on the effectiveness of an innovative policy instrument.

4.3 The governance of metrics

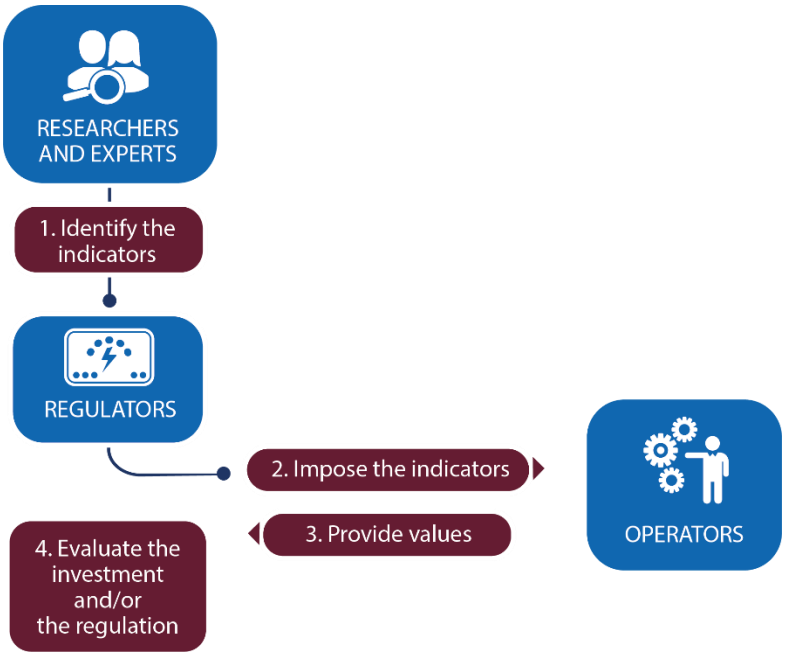
The title of this section could also be "How to avoid deception." Performance measurement is an exercise whose difficulty is often underestimated. This is because it is regarded as an apolitical application of the use of information, collected and analyzed to demonstrate effectiveness against a set of criteria. In reality, many complexities hide behind this apparently rational and technical endeavor, since measurement is connected not only to comprehension but also to judgment. If the evaluation involves an interinstitutional relationship (two different entities concerned, or even just two different departments in an operator), performance measurement is also a political matter affecting decisions on what should be measured, how, why, and by whom (Lewis 2015). Designing an effective system to collect the values of the indicators is as important (and as difficult) as selecting the right indicators.

When regulators implement effectiveness metrics, the logical process that we expect (depicted in Figure 5) is the following:

1. The literature identifies, explains, and justifies the use of a list of effectiveness indicators.
2. The regulator adopts an approach and imposes the calculation of a list of metrics on the regulated companies.
3. The companies provide the values of these indicators to the regulator on a periodic basis.
4. The regulator analyzes these values and, based on its conclusions, assesses future investments claimed by the regulated companies.

[30] For example, in the field of cybersecurity, an improvement in the observed metrics may occur without any positive action, simply thanks to the increased awareness of cyber risk that employees may develop by following the cyber debate in the media.

Figure 5: The process of developing metrics for regulatory purposes



Past experience in evaluation shows that the steps involving both the regulator and the regulated companies (Steps 2 and 3) may prove critical. To wit:

- Step 2: Even though the calculation of some indicator may be declared compulsory by the regulation, this does not mean that its formula can be automatically applied. The final toolkit is the result of a process rather than of one-off adoption. The fine-tuning of the measurement can be achieved by experimenting and then drawing conclusions from the lessons learned, taking the input of both the regulators and the operators into account.
- Step 3: Data collection is difficult, time-consuming, and requires specific competencies—in a word, it is costly. Moreover, providing information on internal activities exposes companies to external judgment. An operator (or a lower-level public entity) may fear that other, undeclared purposes of control could be hidden behind the explicit purpose of performance measurement (i.e., to improve performance). So, evaluators may face overt or tacit opposition when they ask the evaluated entity to provide the necessary data for their activity. The governance of data collection should not be underestimated, and different scenarios (e.g., the establishment of a system of sanctions in case of noncompliance or the creation of an independent body for the collection and management of such information) should be analyzed.

4.4 Cybersecurity metrics

The two main categories of cybersecurity metrics are:

- Maturity level (ML) indicators, focusing on the level of preparedness of an organization; and
- General cybersecurity performance indicators, aimed at assessing the overall effectiveness of the implemented countermeasures.

As discussed below, in section 4.4.1, the two categories have many points of contact and some overlap but are separate concepts. Research concerning cybersecurity performance indicators is ongoing, while established practices are nearly nonexistent. The Electric Power Research Institute (EPRI) metrics represent one of the most advanced studies in the field, while other approaches are in an even more preliminary phase. ML metrics seem to be at a more mature stage, even though their widespread application is far from established.

4.4.1 Maturity metrics

Since the discipline of analyzing the ML of organizations is rather mature, it is possible to compare some different approaches. From a governance and regulation point of view, maturity metrics attract more interest, probably because they properly balance the contribution of specialized people skills, well-formed organizational policies and procedures, and technical controls. However, maturity metrics give a qualitative appreciation of the maturity of an operator and, like any such metrics, their evaluation gives space for interpretation.

ML, which may also be applied to other domains and not only to power systems, is one element of cybersecurity. In our context, it may be defined as the readiness of an organization to respond to potential breaches and may be measured along different scales, in which a label describes each level. For example, a four-level scale may range from unprepared through reactive, proactive, and anticipatory.

It must be clear that this dimension is connected to but distinct from other dimensions of cybersecurity. The interactions are:

- ML is a condition for effectiveness (the same investment may have different outcomes, depending on the initial maturity level)
- An increase in ML is a desirable outcome of cybersecurity projects (readiness and awareness are fundamental elements of cybersecurity)

This interaction loop is a strong argument in favor of the importance of investing in people and processes (governance), above all in contexts where the initial ML is low. However, these direct and inverse causal relations also explain why it is worthwhile to develop and implement specific ML metrics, without limiting the assessment to technical metrics.

In the following sections, we will present some relevant approaches, chosen among the many that have been developed, with small variations, by different consultancy companies.

Carnegie-Mellon Maturity Index

The Carnegie Mellon maturity model, originally known as the Capability Maturity Model (CMM) and later evolved into the Capability Maturity Model Integration (CMMI), was initially developed as a tool to assess the ability to develop a software project. It is the most well-known maturity model and may be applied to almost any situation, not only to cybersecurity (CMMI Institute 2019). This multidimensional approach is very complex to put into practice. The term "maturity" relates to the degree of formality and optimization of processes and is assessed on a five-level scale: *Initial* (chaotic, ad hoc, individual heroics), *Repeatable, Defined, Managed* (capable), and *Optimizing* (efficient).

The levels are identified along a maturity continuum, where the highest level is an ideal state in which processes are systematically managed through a combination of process optimization and continuous process improvement. The list below transposes the above levels to the field of cybersecurity maturity:

- *Initial.* There is no structure and no organization of security processes. Protection relies on individual efforts and is neither repeatable nor scalable.
- *Repeatable.* Security countermeasures are repeatable; basic procedures are established, defined, and documented.
- *Defined.* Greater attention is paid to documentation, standardization, and maintenance support.
- *Managed.* The organization monitors and controls its security processes through data collection and analysis.
- *Optimizing.* Monitoring operational feedback makes it possible to constantly improve security procedures and to introduce new ones.

The creators of IEC 62443 are currently investigating a simplified version of the CMM Index and combining maturity with its definition of security levels. The resulting combination is called the "protection level." This approach is still in the experimental phase and no steps have been taken so far to integrate it into the named standard (IEC 2009).

Cybersecurity Capability Maturity Model (C2M2)

The Cybersecurity Capability Maturity Model (C2M2) program is the result of a public–private partnership that was established to improve electricity sector cybersecurity capabilities and understand the cybersecurity posture of the grid (Christopher et al. 2014). This model focuses on the implementation and management of cybersecurity practices associated with the operation and use of IT and OT assets and the environments in which they operate.

The C2M2 program is comprised of three cybersecurity capability maturity models, a core model (C2M2) for all organizations and two specific models for the electricity subsector (ES-C2M2) and the oil and gas subsector (ONG-C2M2), including additional reference material and implementation guidance specifically tailored for the operators in those sectors. The model is made of a set of cybersecurity practices, grouped into 10 domains and arranged according to maturity level. Companies and organizations can use a tool in which their cybersecurity practices are compared to C2M2 cybersecurity practices. Based on this comparison, a score is assigned to each domain. Scores can then be benchmarked against the desired score, reflecting the organization's risk tolerance for each domain. All models are publicly and freely available. Even though they are conceived as a self-assessment approach, their application might present some challenges. For this reason, organizations may participate in facilitated one-day self-assessment sessions, designed to let them conduct evaluations with the aid of experienced facilitators.

Nemertes Maturity Model

Another approach is Nemertes Research's maturity model (Nemertes 2017). When compared to CMMI and C2M2, this model has the advantage of being easy to understand and apply. The simplicity of this approach (which aligns well with IEC 62443's trinity of people, process, and technology) is captured in

Table 11. Organizations can use a simple index (ranging from 0 to 3) to rate the maturity of their staff's ability to deal with the evolving cyber threat landscape. Policies, procedures and organizational directives can be rated in terms of this process index. Furthermore, skills and processes need to be aligned with technologies deployed by the organization, assessed through a technology index.

Table 11: The Nemertes Maturity Model

	Unprepared Maturity 0	Reactive Maturity 1	Proactive Maturity 2	Anticipatory Maturity 3
STAFF (Skill level)	0	1	2	3
PROCESS	Ad hoc	Basic	Zero-thrust	Emerging threats
TECHNOLOGY	Perimeter defense	Traditional	Cutting-edge	Advanced prototypes

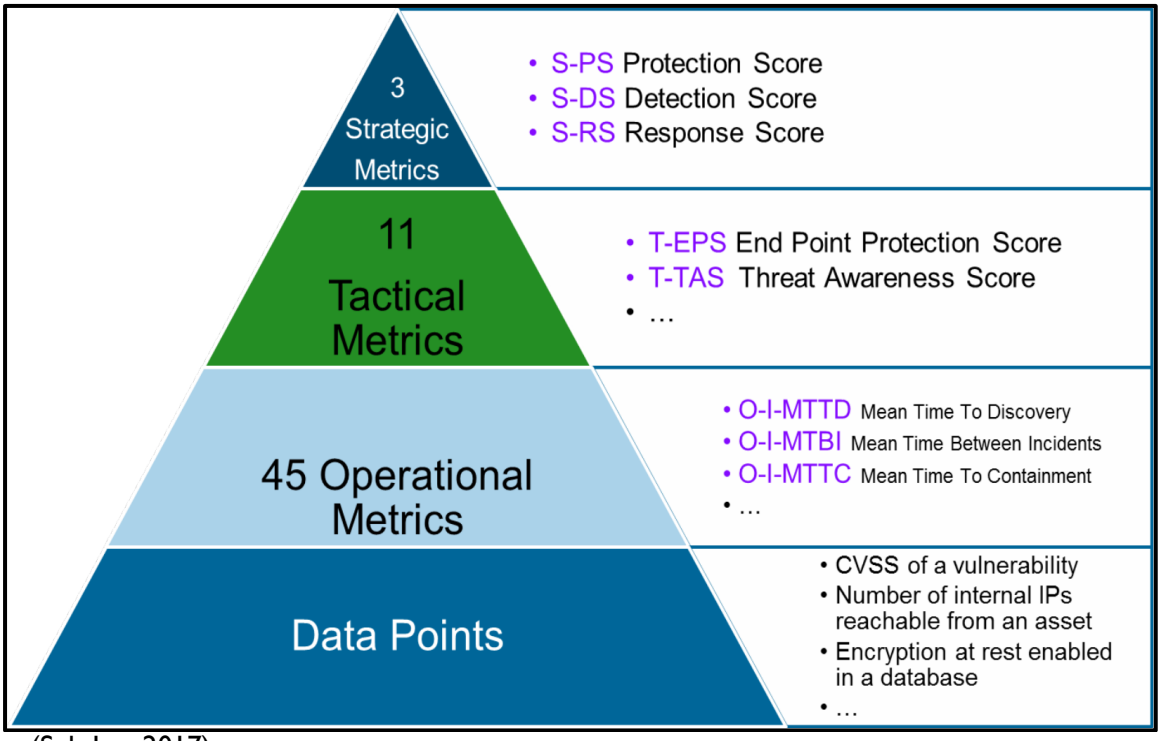
An organization's maturity level derives from the combination of these indexes. For example, the lowest level (unprepared) is assigned when the staff skill level is rudimentary, processes are for the most part ad hoc, and cybersecurity protection relies on perimeter defense in the form of firewalls and air gaps between the operational networks and the business networks.

4.4.2 The EPRI metrics: the most comprehensive and mature approach to assess general cybersecurity performance

According to the EPRI Cyber Security Metrics for the Electric Sector: Volume 3 (Suh-Lee 2017),[31] the EPRI metrics consist of 3 strategic level metrics, 10 tactical level metrics, and 45 operational level metrics, for a total of 58 metrics. A summary and a rationale for the EPRI metrics hierarchy are graphically depicted in Figure 6 below, also taken from the above-mentioned publication.

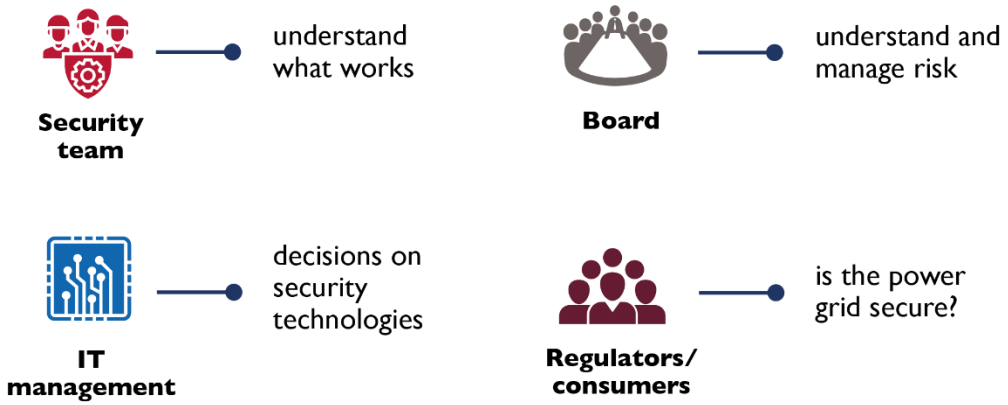
[31] The full EPRI approach to metrics is available in the following reports: (Suh-Lee 2017; Lee and Lee and Suh-Lee 2016).

Figure 6: EPRI cybersecurity metrics hierarchy



Source: (Suh-Lee 2017)
Note: "CVSS" stands for a Common Vulnerability Scoring System score.

Figure 7: EPRI metrics uses



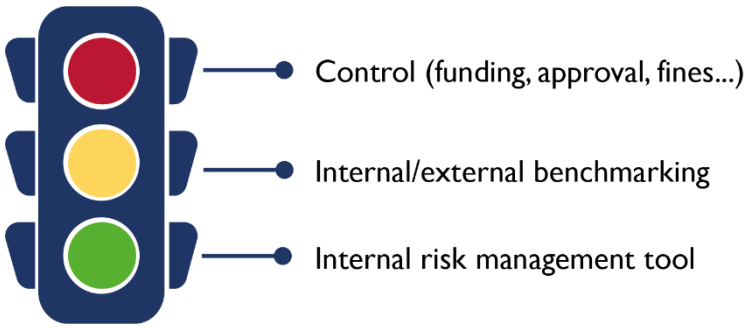
The quantitative foundations of the metrics are based on 120 data points (the full list of data points and metrics is presented in Appendix 3); these include operational statistics collected from various points in utility operations. Operational metrics measure day-to-day operations by using company logs and other certified documents. Tactical metrics offer an overview of programmatic health and progress within the

organization. Strategic metrics measure corporate risk and alignment of the metrics with the direction of the business. The data points that provide the metrics foundations are all measurable quantities; thus, after an external assessment of the approach proposed in the report, the metrics appear operational.[32]

Of course, some of the above claims may prove difficult to support without practical hands-on experimentation. This is the main aim of a current EPRI pilot project, in which five U.S. utilities (which are EPRI members) are testing the metrics. EPRI is currently trying to disseminate the metrics across the European Union, possibly launching a similar exercise to the one run in the United States.

Although the collection of 120–150 measures may seem burdensome, EPRI has stated that, based on its U.S. experiment, it is feasible with a minimal level of maturity (starting from ML 1. It is not suitable for "unprepared" organizations). EPRI has also announced the forthcoming release of an open-source tool to operationalize the calculations. The tool is in the form of an information and communication technology dashboard and is expected to expedite measure collection. However, it is quite clear that the full understanding and practical deployment of the metrics may take a long time and require experienced staff (not less than six months for a large organization, according to the EPRI team).

Figure 8: Internal and external uses of EPRI metrics



It is no wonder that measuring such a complex and multifaceted quality as the cybersecurity posture of an operator requires evaluating so many different quantities. However, 120–150 measures is presumably an upper threshold, likely to apply only to large-size companies. It will be necessary to understand if the number of measures could scale downward for smaller companies and less complex organizations. Finally, it must be noted that EPRI explicitly envisages the adoption of a maturity model as a prerequisite for deploying and applying their metrics.

According to the EPRI product brief, the EPRI cybersecurity metrics program can help improve utility posture by:

- supplying quantifiable information about cybersecurity to support enterprise risk management decisions;
- tracking progress towards goals by means of a repeatable method;
- increasing accountability by identifying gaps or ineffective security practices; and

[32] Of course, the final judgment could only be made following a pilot application of the approach; this is highly suggested since it could highlight critical points and possible improvements.

- providing an objective context to compare and benchmark cybersecurity-related practices.

These features suggest that it should be a powerful risk-management tool. However, EPRI has expressed a more prudent opinion on the use of the metrics program from outside a company, either for external benchmarking or for regulatory control (Figure 7 and Figure 8). In fact, especially in this preliminary experimental phase, the approach has to rely on the full cooperation of the company under assessment.

4.4.3 A critical issue of the EPRI metrics: data aggregation

Various aggregation techniques were used in developing the EPRI metrics, especially when calculating higher-level metrics from a number of lower-level metrics (for example, a tactical metric from a number of operational metrics). The most common aggregation technique used is a combination of scoring and weighted average.[33] Table 12 shows an example of a tactical metric: Incident Response Score.

There are five inputs, all of which are operational metrics. Each metric has a defined minimum and maximum value. Using a negative scoring function,[34] the score for each input metric is calculated. Finally, the Incident Response Score (T-IRS) is calculated as the weighted average of the input scores, normalized to a value between 0 and 10.

Table 12: Incident Response Score with Weighting.

Incident Response Score with weighting	Value	Min	Max	Score (-)	Weight	Score X Weight
O-I-MTTC Mean Time to Containment	8.4	0	30	0.7200	3	2.1600
O-I-MTTR Mean Time to Recovery	21.4	0	60	0.6433	3	1.9300
O-I-MTTA Mean Time to Action	3.8	0	7	0.4571	3	1.3714
O-I-MCRM Mean Cost of Response (man-hours)	11.1	0	480	0.9769	0.5	0.4884
O-I-MCRX Mean Cost of Response ($)	400	0	48,000	0.9917	0.5	0.4958
T-IRS Incident Response Score			6.4457			

Source: (Suh-Lee 2017)

As observed by the authors of the metrics, "Generally, EPRI security metrics are defined with a set of default weights for each input metric, when aggregating to a higher-level metric.…These are standard values that are rather arbitrarily chosen. It is expected that users of the metric will review these default values and adjust them according to the specifics of their environment." This introduces a degree of specificity in any company's metrics that is an obstacle to benchmarking. Also, it may take a long time and

[33] Aggregation is a process in which several related values are grouped to form a single value of more significant meaning or measurement.

[34] In negative scoring, the distance from the value to the maximum is measured, and the resulting score represents the ratio of the maximum distance. Therefore, a higher value results in a lower score. The relevant formula is: Score = (Max-Val)/(Max-Min).

require a rather complex consultation process before various stakeholders agree on the score and weights to be attributed when aggregating base values, or operational metrics, into a tactical metric, as in the above example. On the other hand, such a process is required before a metric can become a shared and comparable milestone among a set of different subjects. If the above process is unavoidable in order to reach an agreement on a large number of different metrics (45 operational and 11 tactical), it becomes clear that there is still a long way to go before such metrics become practical, shared milestones for the energy community.

4.5 Comparative assessment and conclusions

At the end of this presentation of cybersecurity metrics, one may conclude that only maturity metrics and EPRI metrics are sufficiently well defined to be considered for practical applications. Other cybersecurity performance metrics, such as the IEC 62443 metrics, are in the formative stage. Until mature drafts exist, it will be impossible to apply those approaches to justify costs or for other regulatory purposes. Several models to assess an organization's maturity level are available and have been applied for some time. Private consultancy companies have developed many of them (so they are available for purchase), but C2M2 is available for free. Nevertheless, maturity level models cannot be the only metrics adopted to assess the performance of investments, as they do not address all dimensions of a cybersecurity posture and are based mostly on self-assessment rather than on objective evidence.

EPRI metrics are a comprehensive (and consequently complex) approach and, considering the critical issues discussed in 4.4.3, they appear well designed and engineered. If current and future experimentation definitely shows that these metrics are feasible and operable, they may prove a breakthrough, not only for the energy sector but also for any mission-critical application and for industry and business at large. In fact, although the EPRI metrics program is developed for the energy sector, there is no measurable quantity that is energy-specific. Notwithstanding all this, one has to consider that:

- As EPRI metrics are still a prototype that has to be tested and fine-tuned, it may take several years and much more experimental testing and assessment before they become an accepted yardstick worldwide.
- At present, they are mostly used as an internal benchmarking tool in companies that believe in the validity of their conceptual layout. They have not been vetted to the degree needed for a standard or best practice to assess and communicate data about an operator's cybersecurity posture.
- A maturity model such as C2M2 is suggested as a preliminary assessment, to be able to measure improvements, especially on energy branches that are not yet regulated, basically as a way to measure the posture and evaluate improvements after a risk assessment. Maturity models and EPRI models appear to be complementary instruments necessary to get the full picture of the performance of a cybersecurity strategy.

Based on the assessment above, our recommendation is to adopt a maturity model and carefully monitor the progress of the EPRI method. Although the latter is still a prototype, there are good prospects that it may become widely used in the power industry in the short to medium term.

To design a possible approach for power regulators, the question is whether to suggest implementing the whole EPRI method or whether, in our context, a few tactical and operational metrics might suffice, among

the 11 plus 45 included in the complete EPRI approach. A simplified strategy is an appealing idea, as it might have a higher probability of being implemented. The problem with this is that the state-of-the-art of cybersecurity metrics has not yet converged on a common, "public" reference standard. So, further research is needed to understand whether the simplified strategy will return a correct, albeit less defined, picture of a situation,[35] or if this incompleteness will turn into a biased picture. This is why regulators—while waiting for research to provide a clearer picture—might prefer to start by adopting some simple maturity model. In this case, from a regulation point of view, cost justification may be supported simply by improvements in the cybersecurity posture of the applicant. This posture may be determined by using one of several means, such as EPRI metrics, ES-C2M2, as well as parallel approaches being devised within relevant standards like IEC 62443 and IEC 62351.

[35] Further evidence could be gathered by using statistical models to process anonymized data obtained through pilot implementations of the EPRI approach.

5 An Approach to Investments in Cybersecurity

THE AIM OF THIS CHAPTER…

… is to show the process of how decisions can be made from theory to implementation.
It examines a series of regulatory principles and tools, and demonstrates how they can be applied to improve the cybersecurity posture of European and Eurasian countries by describing some reference regulatory scenarios.

The objective of this chapter is to assist regulators in devising an overall approach to assessing prudence in investment plans and tariff setting (including concrete solutions to regulatory processes, procedures, rulemaking, and rules). The development of this approach requires considering existing tools and mechanisms to identify a smooth transition towards new methods, and it relies on the toolkit provided by national power system regulations. These tools are linked to the general regulatory framework and may encompass rules on licenses, privacy, data access, and procurement processes and rules, as well as requirements for the utilities concerning quality of service, like public evidence on activities performed in the public interest (accountability).

In countries where the power system is still in a transition phase towards competitive market solutions, the regulatory frameworks and the operational rules are still undergoing a process of definition; this might represent an advantage. In Western democracies, laws, regulations, and directives look like stratified sediments that originated over time that are very difficult to integrate and to comply with. Transitioning countries have the opportunity to build good, simple regulatory frameworks, learning from the U.S. and EU experience without imitating it uncritically, even though this requires strong political will and a strategic vision.

The starting point is the definition of a cybersecurity strategy, based on a strategic planning vision and addressing three components: people skills (training and awareness); coherent processes embodied in policies, procedures, and organizational directives; and deployment of technologies over the planning horizon (10 to 20 years).

Each component requires significant investment, which must be qualified by its expected effectiveness. In this chapter, we examine a series of regulatory tools and principles and show how they can be applied to some reference regulatory scenarios. We essentially aim to describe the decision-making process from theory to implementation and to clarify it by means of example scenarios. These should be used as guidance to tackle other types of objectives or policies too.

5.1 Background

This section presents the goals that should inspire regulatory action in this period of radical transformation of the power system. They are the drivers that should be behind all regulatory decisions, including those on cybersecurity.

Network regulation is being put under scrutiny by the evolution of the electricity sector, occurring in a rapidly evolving environment. The power system keeps adopting technologies that are modifying the way electricity is produced and consumed. This change is even more dramatic considering that, in the previous

situation, regulation had to deal with a system that had very little innovation and offered a limited number of well-defined services.

THIS CHAPTER

- Summarizes the main regulatory objectives and principles that will shape regulatory scenarios.
- Offers an overview of types of measures and regulatory tools.
- Discusses how to design an effective regulation to enhance cybersecurity protection.
- Provides some examples and alternative scenarios combining the above tools that may represent a pathway for power regulators.

Overall, the objectives of modern electricity service regulation address three aspects:

- Meeting consumer needs and ensuring quality of service;
- Maintaining a safe and resilient network; and
- Providing a network that is able to integrate low-carbon technologies.

The current trend is toward a system where consumers at all levels (from residential to large industrial) have a central role, which means, for example, that:

- They must be involved in decision-making processes, in which they can evaluate the types of services offered by companies and their business practices;
- They should pay adequate service prices; and
- They have the right to participate in the energy system directly through their actions and investments.

The first point mainly concerns the regulator, which must set up a process to collect the consumers' views and make them public. This activity is in line with its role as a representative of the public and can be carried out using various forms of consultation; its importance is even greater in areas that evolve rapidly, like cybersecurity. The current system presents many opportunities, but these also increase the number of possible risks—an aspect that underlines the importance of the opinions of the relevant stakeholders for the decision-making process. It is then a priority to establish clear communication channels with the stakeholders, for example by having dedicated personnel for public relations with business and consumer associations and medium to large companies.[36]

5.2 Types of measures and actions

Given the above general objectives, here is a list of the main types of measures or regulatory instruments, with a definition of the items. Most measures can be combined whenever necessary, either for a specific objective or to target different objectives within the same strategy.

[36] For more information, please see the NARUC *Communications Primer for Utility Regulators* (Choueiki 2019).

Minimum standards: the regulator defines minimum standards (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 aim of these is similar to that of minimum standards (ensuring that companies reach at least a minimum standard), but it is implemented differently. The regulator identifies a critical subset of parameters (and 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 penalties or enforced actions).

Ex ante projects: the regulator clearly sets up conditions for some activities ex ante. In the context of PBR, this type of measure is introduced when the objectives of regulation cannot be accomplished through the general mechanism of allowing the utility to choose how to reach a global output. The regulator defines precise targets or investments and asks the utility to comply with the project prescriptions. KPIs could be adopted in this context too; failure to meet the threshold may cause the regulator to reevaluate the operator's cost justification.

Incentives: in the case of PBR, rewards/penalties are assigned according to the value of relevant indicators. These variables should represent the level of service improvement or degradation for the consumers. Incentive mechanisms are very specific to each activity/sector and should be carefully chosen, as there are potential side effects: for example, strict benchmarking may induce companies not to share relevant information.

Besides the measures above, we would like to mention other factors that should be taken into consideration in the regulatory process:

Uncertainty mechanisms: they make it possible to revise the measures described above 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 to redefine objectives.

Public or stakeholders' consultations: instead of relying only on the opinion of internal or external experts, many elements of the measures described above (minimum requirements, KPIs and related thresholds, detailed features of the projects, possible risks) might be set by the regulator, after a process of public or stakeholders' consultations with the relevant stakeholders.

Agreements: some elements of the above measures, such as KPIs and their thresholds or objectives in output regulation, can be determined by means of an agreement between the regulator and the electricity operator. The regulator and the operator jointly agree on the values that will be the basis for economic rewards. This enhances the engagement of the operator in pursuing the desired strategy.

5.3 Building cybersecurity scenarios starting from cybersecurity objectives

The objective of this chapter is to provide insights into the process of establishing measures to address the cybersecurity protection of a power system from a regulatory point of view. Even though the measures that best fit the characteristics of each country may not be established in a general way in these guidelines, the decision process must follow a clearly defined path, consisting of steps (decisions, definitions, and activities). The order of the steps may not be inverted, because it represents the practical process that leads from principles to realistic application, and every decision sets the perimeter of options for the subsequent step. The process is described in Figure 9, for what concerns the cost-plus regulatory framework, and in Figure 10, for what concerns PBR.

Both approaches start from the definition of a cybersecurity strategy and, in particular, of an objective to be reached. Before addressing the different phases of the implementation process, the regulator should define an overall cybersecurity strategy for the power sector.[37] Nothing consistent can be done without having a clear indication of where to go. A good regulation needs the objectives for which it has been conceived to be clearly identified, along with the tools and strategies adopted to reach them. Establishing a strategy involves a policy maker's vision (Which values lead me to develop this regulation? What are my objectives?) and expectations (What changes in the electricity market are expected thanks to my strategy?).[38]

[37] In compliance with the overall cybersecurity strategy of the country, as stated by the governing laws and dispositions. The regulator, starting from the governmental level, shall define specific objectives for the electricity sector in line with the overall national strategy, keeping in mind the financial impact of such changes, and the priorities.

[38] REMARKS ON THE FIGURES:

Cost-plus – Step 4: Cyber cost identification is rather difficult, unless it is compulsory to have a separate indication in plans submitted for approval. For example, cybersecurity is often purchased embedded in new equipment, hidden in the choice to buy more expensive equipment/software, and therefore is not labelled as a cyber cost. Also, the costs connected to governance and security procedures are included in other cost categories, unless the operator itself provides special justification for those resources. Rules for an easier identification should be established ex ante. However, if Step 2 is carried out with enough care and detail, this task will become less challenging.

Cost-plus/PBR – Step 6: Updates are fundamental when cybersecurity is being guaranteed through the implementation of a list of countermeasures. The problem with the compliance philosophy is that it is not reactive to the environment and it may give a false sense of security. Also, in PBR, updates of the strategy based on feedback from experience are fundamental. The problem with the incentive philosophy is that incentives have to be constantly fine-tuned as the context evolves.

PBR – Step 2. *Clear-cut* means that, based on the chosen definition, you always know whether or not a situation corresponds to the definition. If you think that the answer is "partly" or "it depends," the definition does not work. *Measurable* means that the defined objective (e.g., reducing unemployment) must be associated with a measurable variable (e.g., employment rate and not employability). *Reasonable* means that the quantitative objective is set at a level that can be reached with an effort proportionate to the incentive given.

PBR – Step 3. This step should be managed as a process (through workshops and consultations) rather than as a one-step decision.

Figure 9: Defining a regulatory scenario in the cost-plus framework

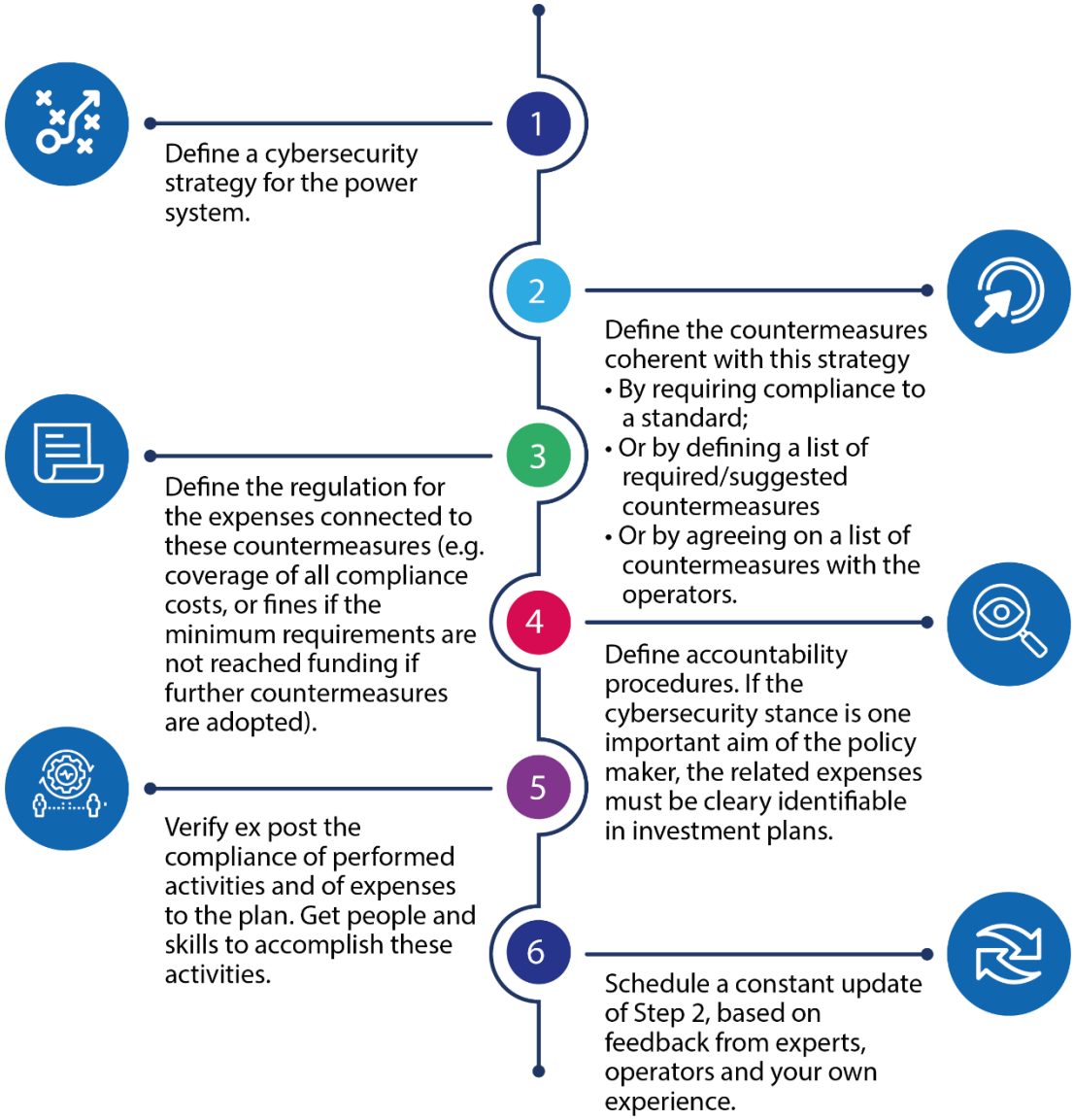
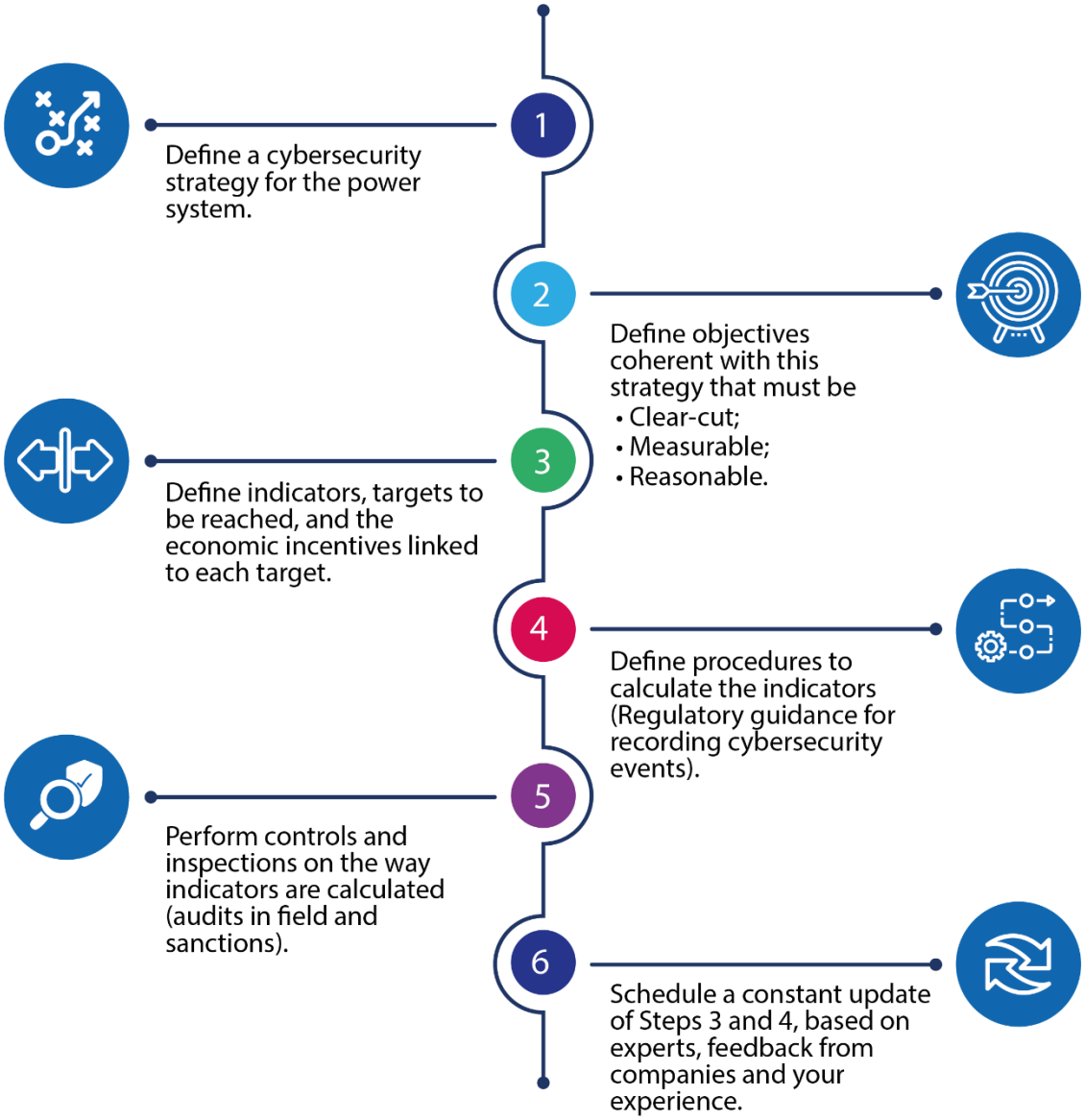


Figure 10: Defining a regulatory scenario in performance-based regulation (PBR)



5.4 Cybersecurity scenarios

This section presents examples of regulatory scenarios,[39] all referring to the same cybersecurity objective. The goal is to show how the same principle can be implemented in practice by adopting different regulatory approaches. Some of these applications, including the regulatory tools to be adopted, are defined by a country's regulatory framework.

Step 1: Define a cybersecurity strategy for the power system

The issue: The policy maker (assisted by the regulator) realizes that the utilities are making investments in cybersecurity without clear rationality, as they lack both a strategic vision and culture and skills to effectively put countermeasures into practice.

The Strategy: The regulator intervenes by encouraging the utilities to define a strategy and an internal process that includes preparation, awareness, and appropriate procedures.

In the subsections below, we present five scenarios, following the steps listed in section 5.3, which define a regulatory plan. The scenarios describe categories of actions (one for each step) in the order in which they should be taken. The result should ensure coherence in the approach and account for why certain options are chosen.

All scenarios address the same challenge, which means that Step 1 is common to all of them. The selected objective concerns the governance aspect of cybersecurity because it seems to be a critical issue, conditioning the effectiveness of other cybersecurity investments. Moreover, it is a field in which metrics (namely maturity metrics) are more "ready to adopt" and so it makes sense to try to apply PBR.

5.4.1 Scenario 1: a compliance-based approach in cost-plus

This scenario is a possible path to reach the objective selected in Step 1 in a cost-plus framework.

- **Step 2** *Define countermeasures* coherent with the strategy. The regulator identifies a list of countermeasures related to security areas listed in Table 5. Companies are required to implement them.
- **Step 3** *Define regulation for the expenses* related to the strategy. All the expenses incurred by the companies to adopt the countermeasures are covered.
- **Step 4** *Define accountability procedures*. The regulator defines a procedure to report admissible costs. Cost categories (compensation for new personnel, consulting expenses, training costs) are carefully identified and companies are asked to clearly extrapolate the costs of cybersecurity from other costs and investments.
- **Step 5** *Verify incurred expenses ex post* and compliance of the activities performed. The regulator verifies ex post that expenses correspond to admissible categories. This can also be carried out

[39] As explained above, scenarios present types of actions that should be taken in a certain order. Actions of the same type can be found in different scenarios; nonetheless, their implications vary according to the specific context. We suggest that regulators place great emphasis on communication activities related to cybersecurity, and extensively use consultations to verify the degree of awareness of companies and the possible issues raised by the decisions made.

thorough inspections to check if and how the measures have been implemented. The regulator can also ask for the support of external experts to perform tests to assess how measures have been implemented. The companies and the regulator have the possibility of hiring external experts to support them in this auditing process.

- **Step 6** *Schedule updates* of Step 2. After the process is completed, the regulator organizes a series of consultations and open debates with companies and experts to establish whether the measures planned so far are still valid or whether others should be introduced. This also applies to the reporting and auditing methods.

5.4.2 Scenario 2: a semi-participatory approach in cost-plus

This scenario is an alternative to the one above and also implements a cost-plus framework.

- **Step 2** *Define countermeasures.* The regulator sets up an open consultation process with the companies to discuss a list of countermeasures related to the governance security areas listed in Table 5. Based on these consultations, the regulator defines a set of minimum requirements; the remaining ones are optional measures. The regulator collects and analyzes the opinions of the companies but is ultimately responsible for the final decisions.
- **Step 3** *Define regulation for expenses.* The regulator covers only expenses for the additional optional measures defined ex ante, while minimum requirements are covered by the operator. The procedure also contemplates the possibility that, in exceptional circumstances, other expenses (not included in the list from Step 2) connected to technological innovation or new needs may be covered.
- **Step 4** *Define accountability procedures*. The regulator defines a procedure to report costs linked to additional expenditures and one to apply for reimbursement of exceptional expenses. Once a year, companies have the opportunity to apply for additional expenses.
- **Step 5** *Verify incurred expenses ex post.* The regulator verifies ex post that minimum requirements are respected and that the reported expenses correspond to the measures exceeding minimum requirements. This is carried out through inspections to check if and how the measures have been implemented. The regulator will also verify whether the requests comply with expense regulation.
- **Step 6** *Schedule updates.* To receive feedback on the performance of the policy, companies are required to apply the C2M2 model; the regulator offers guidance and support to companies that have to perform a self-assessment of their level of cybersecurity maturity. The overall results of the self-assessment exercise are analyzed and discussed in order to evaluate the policy, update minimum standards, and define admissible additional expenditure. The impact evaluation checks whether companies that have obtained funding for additional measures show a higher level of maturity than companies that have adopted only minimum requirements. It also explores if and how companies have availed themselves of the option to apply for exceptional expenditure and discusses how this option has been managed by the regulator. On the basis of these results, the regulator and the policy maker redesign the strategy for the following years.

5.4.3 Scenario 3: a participatory approach in cost-plus

This scenario integrates Scenario 2 and concerns the possibility of adopting a special approach and agreeing to separate conditions for one operator that shows a higher level of awareness compared with the average situation of other operators.

- **Step 2** *Define countermeasures.* The regulator and the company discuss and agree on the minimum requirements for the company, according to the list of countermeasures established in the former scenario, and which additional measures will be subject to funding. The final agreement foresees that:
    - The company is subject to the same minimum requirements as other companies;
    - Funding may be received for a wider list of optional countermeasures; and
    - The company organizes practical training workshops for other companies.
- **Step 3** *Define regulation for expenses.* The regulator covers only expenses for the additional optional measures defined ex ante, while minimum requirements are covered by the operator. Since the company may receive a large amount of funding even if it is already more mature and organized, it engages in a training campaign for the other companies at its expense.
- **Step 4** *Define accountability procedures*. The same as for Scenario 2. The company will submit the program for the training campaign and obtain approval.
- **Step 5** *Verify incurred expenses ex post.* The same as for Scenario 2.
- **Step 6** *Schedule updates.* Since the company is experienced in applying maturity metrics, it will provide guidance and data for benchmarking. In particular, the company was already applying the C2M2 model before the regulation was launched, so it agrees to include guidance and support on maturity assessments to other companies in the training campaign. It also agrees to provide a list of metrics (statistics and anonymized data) for benchmarking to the regulator.

5.4.4 Scenario 4: experimenting with incentives to enhance the maturity level

This scenario is a possible path to reach the objective selected in Step 1 in a PBR framework.

- **Step 2** *Define* clear-cut, measurable, and reasonable *objectives* that are coherent with the strategy. Companies are required to reach a minimum level of maturity. To define maturity, the regulator refers to the C2M2 model.
- **Step 3** *Define indicators, targets to be reached and incentives*. Companies are required to apply the C2M2 model (or a subset of its domains). The regulator sets a target or a minimum level of maturity to be reached (for example, 1); the companies are penalized if this is not reached, while they receive bonuses if a higher level is achieved.
- **Step 4** *Define procedures to calculate the indicators*. To provide regulatory guidance, the regulator first organizes sessions to introduce the logic and functioning of C2M2. Then, companies perform self-assessments using the freely available C2M2 tool. Companies may be asked to participate in facilitated one-day self-evaluation sessions (offered by the regulator) and conduct their evaluations with the aid of experienced facilitators.
- **Step 5** *Perform checks* on the way indicators are calculated. In this phase, the regulator organizes audits in which experts (paid by the regulator) check that the values declared by the operator (provided through the self-assessment) actually correspond to the operator's operating reality. Operators are sanctioned whenever significant discrepancies are found.

- **Step 6** *Schedule updates*. The regulator reviews Steps 3 and 4, based on external experts' assessments, feedback from companies, and its own experience. The regulator performs an overall analysis of the sector to better assess the level of maturity achieved by companies. This activity relies on a consultation process in which companies and consumer representatives are asked to comment on the regulator's findings and suggest improvements in view of the established objectives. The discussion should cover the technical content of the strategy and its practical management, in particular:
  - **The choice of indicators**: is C2M2 a good model? Is it easy to apply? Is it sensitive enough to be used to provide incentives?
  - **The level of targets**: what is the average maturity level after the regulation? Should the minimum requirement be increased?

  It is also possible to organize physical or virtual meetings to engage in collective discussion. The regulator should collect the inputs and consider them in a decision-making process leading to a possible revision of previously adopted measures. Even though the final decisions are taken by the regulator (or the policy maker), all the input from the companies should be documented and the regulator should explain how it was taken into account (or why it was not).

5.4.5 Scenario 5: relying on companies' strategies without relying on metrics

This scenario also refers to a PBR framework but, in this case, the regulator thinks that cybersecurity performance metrics are not sufficiently mature to be applied for regulatory purposes. Moreover, since they are based on self-assessments, the information is not reliable enough to be used to give incentives. Hence, the regulator decides to rely on ex ante projects (this is why the steps are those used for the cost-plus framework); these allow the regulator to respect the philosophy of PBR, believing that the operators have competencies and information to make better decisions than the regulator.

- **Step 2** *Define countermeasures*. The objective is to have companies adopt their own cybersecurity strategies, invest in improving internal organization and awareness, and acquire skills. The regulator identifies four fields in which companies are invited to submit proposals:
  - Design and implementation of a cybersecurity organization model;
  - Definition and implementation of a set of rules and procedures for the daily management of cybersecurity;
  - Improvements in the skills of cybersecurity staff; and
  - General awareness campaigns.
- **Step 3** *Define regulation for expenses*. The regulator recognizes costs for (1) technical training, (2) general awareness programs, (3) setting up a special security unit, and (4) hardware and software as related to the projects. Applications are granted up to 65% funding, as this is estimated to be an expansion of the business-as-usual business plan, and a fixed upper limit on total expenses is defined according to operator characteristics and size. The regulator defines a budget. Companies present applications by following an online procedure. All applications complying with the requirements are funded in chronological order until the budget is exhausted. The regulator defines rules for monitoring, evaluating, and sharing the results of the projects within the sector so that the innovation introduced is disseminated among all power system operators.

- **Step 4** *Define accountability procedures*. All costs should be documented and justified. Apart from normal cost reporting, the companies are requested to show that the project activities exceed business as usual.
- **Step 5** *Verify expenses and compliance*. The regulator performs audits to verify ex post the compliance of performed activities and expenses to the proposed plans.
- **Step 6** *Schedule updates*. Companies are asked to participate in one-day self-evaluation sessions organized by the regulator and conduct evaluations of their maturity levels with the aid of experienced facilitators. The results of these sessions are used by the companies to update their internal cybersecurity strategies and by the regulator to receive feedback that may be used for the design of future policies.

5.4.6 Comparison among scenarios

The above scenarios should not be taken as best practices to follow, but as examples showing that the same objective may be reached in several ways. The analysis of the actual situation will provide the regulator with hints on how best to undertake them.

For example, in Scenario 1, the regulator decides that the maturity level of power operators is too low and decides to keep direct control over the practical cybersecurity strategy. For this reason, the regulator adopts a compliance-based approach. Since the initial level is very low, to overcome the resistance of the operators to this new regulation, all expenses are covered.

Conversely, in Scenario 2, the regulator is not worried about the maturity level but wants to start a change in the attitude of operators. The approach is labeled as semi-participatory because the regulator will have the final word on the decisions. Since the regulator thinks that the awareness of the companies may be enhanced by involving them in the decision-making process, he/she launches an open consultation process, even though the regulator will have the last word. Since the initial level of maturity of the operators is not zero, a list of minimum requirements is defined and only optional measures and exceeding minimum requirements will be covered.

Scenario 3 shows that multiple approaches may be adopted by the same regulator, to cope with different attitudes among operators. The approach is labeled participatory because the elements of the agreement between the regulator and the mature company are established on equal terms. In this scenario, the company is recognized as a key actor for the implementation of the national cybersecurity strategy and will cooperate in implementing it.

Scenarios 4 and 5 deal with a PBR context. In Scenario 4, the regulator knows that many companies in the country are experimenting with the use of maturity metrics. So, he thinks that a pilot application of PBR could be done to address awareness and governance. Companies are offered economic incentives if they reach a certain level of maturity.

Conversely, in Scenario 5 the regulator thinks that cybersecurity performance metrics are not sufficiently mature and objective to be applied to give incentives. The decision to rely on ex ante projects, is nevertheless coherent with the philosophy of PBR, as it is grounded in the belief that the operators have better competencies and information than the regulator and so are in a position to make better decisions.

6 Conclusions

The present guidelines provide European and Eurasian regulators with a set of suggestions and recipes to deal with cybersecurity in their countries, namely:

- A discussion of the principles of cost identification and some reference values for cost benchmarking; this is mostly based on the cybersecurity costs results actually recorded in the ESSENCE project.
- A summary of the terms of evaluation of the economic effects of a regulation imposing compliance to a standard or to a list of countermeasures—that is, increased and saved costs—with an exercise showing how to apply these terms of evaluation to calculate the costs and benefits of a hypothetical implementation of a regulation.
- A discussion of the way to assess whether operators' investments made to address cybersecurity issues are effective in rendering the power system more secure. A review of current cybersecurity metrics, concluding with the recommendation to complement maturity metrics by experimentation with the recent EPRI performance metrics, although this is still immature.
- A template for the definition of a regulatory approach to deal with cybersecurity according to a cost-plus and a PBR framework. The basic concept is to show a process from principles to realistic application that must be based on empirical evidence from the power system's situation. All scenarios start with the same step: the definition of a cybersecurity strategy. This strategy follows the vision of the regulator, that is, the values inspiring the regulation; its objectives, and the expectations about the changes in the electricity market that should occur based on the strategy.
- Five possible scenarios applying the decision process described earlier. It must be emphasized that they represent only five possible outcomes out of hundreds of possible combinations. Their merit is to show how to apply the template practically, and to show that the choice depends on the initial situation and on the values at the basis of the regulatory activity. The scenarios also show that different approaches may coexist in the same country, for example, a general regulation based on cost-plus and a pilot application of PBR for a very specific objective.

In conclusion, these guidelines provide tools and approaches, often discussing several alternatives for each action. The philosophy behind their application is frequently discussed as well, but unique turnkey solutions are never suggested. So, how can a regulator understand what to do—particularly a regulator who is at the beginning of his or her journey towards a structured intervention for cybersecurity? How should he or she choose from the various options available? We believe regulators should start from a series of reflections on their status quo, and provide responses to a number of issues that may have a significant influence on the approach they will choose. This is a possible list of questions to start with in this assessment:

- *What are my objectives? Where do I want to start?* The definition of a strategy and of priorities will help to focus on the initial steps of a very engaging process. Start with a plan, and don't waste time trying to make it perfect; this will also help to get the operators thinking strategically. The U.S. experience of many state regulators shows that starting to do something, even when it seems to be a drop in the ocean, provides expertise, feedback, and engagement that are precious for shaping continuously improved strategies.

- What *strengths, weaknesses, opportunities, and threats* are apparent in the cyber landscape for the key power operators and utilities in my country? The actual situation of the power system provides hints to make better decisions. If the situation is not clear, it is important to start to ask questions of the operators, without being worried about asking the right questions. In turn, they will start to reflect on their cybersecurity stances, which is an achievement in itself.
- *Are there governing laws or administrative rules* in place that limit or expand my influence in this area? Taking into consideration the general regulatory framework and existing instruments may facilitate a smooth transition to new methods.
- *What mutual aid agreements* are in place (if any)? The initial steps of a process are very costly and suffer from a lot of inertia. Nevertheless, cybersecurity is not the private matter of a country, but is a mutual issue of an interconnected region, so including this objective inside wider aid agreements should be natural.
- Do I have enough *skilled personnel in-house* to address cybersecurity cost identification and benchmarking (for cost-plus)? What experience on *performance metrics* (cyber or not) do the operators and my staff have (for PBR)? These questions are designed to provoke reflection on the pros and cons of the different approaches.

EU countries (and the individual states of the United States) have adopted different regulatory strategies; some of them are still in an early phase of initial engagement with the problem. This shows that no gold standard has emerged at present.[40] Likely it will never appear because the design of a regulatory approach is not a technical task, but it is truly connected to a country's values, vision, and legal environment. It is useless to let time pass, waiting for a clear, complete, and even tailored picture to appear. Regulators must get started immediately and learn lessons along the way because experience will answer more questions than a 1,000-page book that would become outdated in six months' time. These guidelines are intended to help regulators think through this new paradigm and learn to constantly adapt to change, with the goal of making power operators better prepared and able to react.

[40] However, in this context the OFGEM (UK) example, addressed in Appendix 4, is outstanding because its process to establish a comprehensive regulatory approach for cybersecurity is at a very advanced state.

7 References

Angeletti, Valentino, Luca Guidi, Daniela Pestonesi, Marco Biancardi, Marco Alessi, Graziano Abrate, Clementina Bruno, Fabrizio Erbetta, Giovanni Fraquelli, and Azahara Lorite-Espejo. 2014. *Italian Case Study: Socio-Economic Impact Analysis of a Cyberattack to a Power Plant in an Italian Scenario. Cost and Benefit Estimation of CIPS Standard Adoptions. A Reduced Version*. Ceris Technical Reports - Special ESSENCE series on Security Standards for Critical Infrastructures, no. 55. National Research Council of Italy, Research Institute on Business and Development (CNR-CERIS). http://essence.ceris.cnr.it/images/documenti/RT_55.pdf

Bartosewicz-Burczy, H., C. Bruno, F. Garcia, and T. Wlodarczyk. 2014. *Polish Case Study. Scenario Based Assessment of Costs and Benefits of Adoption of Comprehensive CIP Standards*. Ceris Technical Reports - Special ESSENCE Series on Security Standards for Critical Infrastructures, no. 56. National Research Council of Italy, Research Institute on Business and Development (CNR-CERIS). http://essence.ceris.cnr.it/images/documenti/RT_56.pdf

Bruno C., A. Lorite-Espejo, H. Bartoszewicz-Burczy, A. Cortes, E. Doheijo, A. Diu, U. Finardi, E. Ragazzi, G. Falavigna, V. Moiso, L. Guidi, D. Pestonesi, T. Wlodarczyk, G. Abrate, F. Erbetta, and G. Fraquelli. 2014. *Benefit Analysis. Assessing the Cost of Blackouts in Case of Attack. Evaluation Based on Italian and Polish Case Studies*. Ceris Technical Reports - Special ESSENCE Series on Security Standards for Critical Infrastructures, no. 52. National Research Council of Italy, Research Institute on Business and Development (CNR-CERIS). http://www.ceris.cnr.it/ceris/rt/RT_52.pdf.

Cadmus Group. 2018. *Cybersecurity Strategy Development Guide*. NARUC Center for Partnerships and Innovation. https://pubs.naruc.org/pub/8C1D5CDD-A2C8-DA11-6DF8-FCC89B5A3204.

Cadmus Group. 2019. *Cybersecurity Preparedness Evaluation Tool*. NARUC Center for Partnerships and Innovation. https://pubs.naruc.org/pub/3B93F1D2-BF62-E6BB-5107-E1A030CF09A0.

Calabrese G., U. Finardi, and E. Ragazzi. 2014. *Cost Analysis of Standard Implementation in the SCADA Systems of Electric Critical Infrastructures*. Ceris Technical Reports - Special ESSENCE Series on Security Standards for Critical Infrastructures, no. 53. National Research Council of Italy, Research Institute on Business and Development (CNR-CERIS). http://essence.ceris.cnr.it/images/documenti/RT_53.pdf

Choueiki, Hisham. 2019. *Promoting Transparency and Public Participation in Energy Regulation: A Communications Primer for Utility Regulators*. NARUC. https://www.naruc.org/international/news/promoting-transparency-and-public-participation-in-energy-regulation-a-communications-primer-for-utility-regulators/.

Christopher, Jason D., Fowad Muneer, John Fry, and Paul Skare. 2014. *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) - Version 1.1*. Washington DC: U.S. Department of Energy. https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0.

CISA (U.S. Department of Homeland Security Cybersecurity & Infrastructure Security Agency). n.d. "Critical Infrastructure Sectors." Accessed January 17, 2020. https://www.cisa.gov/critical-infrastructure-sectors.

CMMI Institute. 2019. "What is CMMI?" https://cmmiinstitute.com/cmmi/intro.

CNR-IRCrES (The National Research Council of Italy, Research Institute on Sustainable Economic Growth). n.d. Emerging Security Standards to the EU power Network controls and other Critical Equipment (ESSENCE) (website). Accessed January 17, 2020. http://essence.ceris.cnr.it/.

Costantini, Lynn P., and Matthew Acho. 2019. *Understanding Cybersecurity Preparedness: Questions for Utilities*. NARUC Center for Partnerships and Innovation. https://pubs.naruc.org/pub/3BACB84B-AA8A-0191-61FB-E9546E77F220.

DHS (U.S. Department of Homeland Security). n.d. "Critical Infrastructure Security." Accessed January 17, 2020. https://www.dhs.gov/topic/critical-infrastructure-security.

EPRI (Electric Power Research Institute), 2017, "Cyber Security Metrics for the Electric Sector." Accessed February 6, 2020, https://www.epri.com/#/pages/product/000000003002010426/?lang=en-US

EU (European Union). 2008. "Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance)." *Official Journal of the European Union* L no. 345 (2008): 75–82. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF.

Huang L. and Q. Zhu. 2019. "Adaptive Strategic Cyber Defense for Advanced Persistent Threats in Critical Infrastructure Networks." In *Performance Evaluation Review* 46, no. 2: 52-56, https://doi.org/10.1145/3305218.3305239.

Huang L. and Q. Zhu. 2020. "A Dynamic Games Approach to Proactive Defense Strategies against Advanced Persistent Threats in Cyber-Physical Systems." In *Computers and Security* 89 (2020). https://doi.org/10.1016/j.cose.2019.101660.

IEC (International Electrotechnical Commission). 2009. *IEC TS 62443-1-1:2009*. IEC. https://webstore.iec.ch/publication/7029#additionalinfo.

Keogh M., Thomas S. 2017. *Cybersecurity. A Primer for State Utility Regulators. Version 3.0*. NARUC Center for Partnerships and Innovation. https://pubs.naruc.org/pub/66D17AE4-A46F-B543-58EF-68B04E8B180F.

Lee, A. and C. Suh-Lee. 2016. *Creating Security Metrics for the Electric Sector, Version 2.0*. Palo Alto, CA: Electric Power Research Institute. https://www.epri.com/#/pages/product/3002007886/?lang=en-US.

Lewis, J. M. 2015. "The Politics and Consequences of Performance Measurement." *Policy and Society* 34 no. 1: 1–12. https://doi.org/10.1016/j.polsoc.2015.03.001.

NARUC (National Association of Regulatory Utility Commissioners). 2017a. *Black Sea Cybersecurity Strategy Development Guide*. NARUC. https://pubs.naruc.org/pub.cfm?id=E20048B4-155D-0A36-3117-F2F0A7A692F4.

NARUC. 2017b. *Cybersecurity Evaluative Framework for Black Sea Regulators*. NARUC. https://pubs.naruc.org/pub.cfm?id=E3CE75B5-155D-0A36-31FD-1B268F7BD125

Nemertes 2017. *The Nemertes Security Maturity Model*. Nemertes Research. https://nemertes.com/research/nemertes-security-maturity-model/

NERC (North American Electric Reliability Corporation). 2016. *Security Management in the Electricity Sub-Sector Version 1.1*. NERC. https://www.mro.net/MRODocuments/Security%20Management%20in%20the%20Electricity%20Sub-Sector%20Version%201.1%20September%202016.pdf.

NERC. n.d. "CIP Standards." Standards. NERC. https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

NIST (National Institute of Standards and Technology). 2018. *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*. NIST. https://www.nist.gov/cyberframework/framework.

NIST. n.d.a. "Advanced Persistent Threat." Computer Security Resource Center Glossary. Accessed January 17, 2020. https://csrc.nist.gov/glossary/term/advanced-persistent-threat.

NIST. n.d.b. "Cyber Security." Computer Security Resource Center Glossary. Accessed January 17, 2020. https://csrc.nist.gov/glossary/term/Cyber-Security.

Suh-Lee, C. 2017. *Cyber Security Metrics for the Electric Sector: Volume 3*. Palo Alto, CA: Electric Power Research Institute. https://www.epri.com/#/pages/product/3002010426/?lang=en-US

For questions regarding this publication, please contact
Colleen Borovsky (cborovsky@naruc.org)
Erin Hammel (ehammel@naruc.org).

National Association of Regulatory Utility Commissioners (NARUC)
1101 Vermont Ave, NW, Suite 200
Washington, DC 20005 USA
Tel: +1-202-898-2210
www.naruc.org