Proposal for a Cost-Benefit Analysis of Critical Infrastructures Cybersecurity Compliance Policies

Notes for a speech delivered at the workshop organized by The University of Nicosia and the Cyprus Organization for Standardization, 11 September 2014

Alessandro Guarino

www.studioag.pro/en

a.guarino@studioag.eu

@alexsib17

Introduction

Infrastructures today, be they critical or not, are heavily dependent on Information and Communications technology for their control and operation, even in traditional sectors like for instance freshwater delivery or railway transportation. This makes assuring the continuing security of the information used a fundamental part of operations, with clear implications also for safety. Systems where IT technologies meet the real world are usually defined cyber-physical, meaning that manipulating their operations could very well spill their consequences in the "real" world, think for instance of a malfunctioning chemical plant or dam.

While information security assumes in this way a whole new dimension, we must always remember that it is not a purely technical endeavour, but it entails also organizational, management and human resources sides.

Standards and best practices are one of the means used to elevate information security levels and their implementation is more and more mandated, in various ways by governmental policies. Policies however can assume many different forms and they are not always chosen by rational means. The tools provided by economics can help policymaker to make rational choices; economics applied to the formerly purely technological field of information security has already helped better understand many phenomenons and behaviours.

Goals of this work

This (ongoing!) research aims at building a Cost-Benefit Analysis model that could be used by policymakers in order to select the correct standardization policy to apply to Critical Infrastructures operators. CBA has a long standing and tradition in policymaking but it was usually employed in the selection of infrastructural investment projects rather than in choosing policy options.

In this case the question is how to incorporate standard compliance in legislation and regulations in a case where public and private interests are at stake, from the economic well-being of operators, to a fair and open market for services, even to national security and safety of populations.

The European Union, as well as the United States government and others are already involved in

standardization policies, but (especially as far as the EU is concerned) the effort seems to be uncoordinated and lacking a strategic unity.

Infrastructures and Critical Infrastructures

- A "critical infrastructure" (paraphrasing the EU definition) consists of "physical resources and/or services whose disruption would have serious consequences for safety, security or welfare of (European) citizens"
- EU efforts began in 2006 and are centered on Directive 2008/114 and a set of other documents that all invoke a risk analysis and management concept. This is a good match for existing standards. Each state of course has its own transposing of the directive.
- Drawbacks: does not provide for standards *per se,* risk management frameworks are plenty and a choice should be made.

Cyber Security

- Debate on definition – relation with information security – networked systems (for some cyber security is ONLY cyber-physical systems)
- It surely involves security of highly interconnected information systems. Infrastructures IT systems and Industrial Control Systems are converging on cyber and common IT technologies (IP networks for example).
    - Beware: attacks are brought not only via network though – famous Stuxnet malware insertion happened by physical access and a USB stick and personnel errors or voluntary acts of sabotage by insiders are always a possibility.
- For economists IT security is a public good, and this is still more relevant for cyber security
    - non-excludable
    - non-rivalrous (use of one does not limit use by others)
- Free rider problem – the security of interconnected systems is explained by a least effort model (security level as high as the weakest element)

Policies

So, the **question facing regulators** is how to incorporate standardization in security policy and to what extent. Mandating the adoption of international (ISO) or national (NIST) standards for CI operators, regulate directly, leave complete freedom.

Cost-benefit analysis

Core concepts:

- Perspective: cost and benefits to society. Benefits must exceed costs
- Underpinning it is utilitarian thinking: benefits to society are the sum of individual benefits and measured in wealth (some social welfare functions: Pareto, Kaldor-Hicks).
- All costs and benefits are enumerated and expressed in monetary value, discounted (to compare them and to consider time – interest rates incorporate risk)
- Consumers' surplus (*what I am willing to pay less what I actually pay*): if a project reduces a product's cost, surplus raises.
- Opportunity costs – what is used in a project cannot be used in another
- Perimeter of analysis: consequences too remote are not to be taken into consideration

Process:

- Is the project feasible (are benefits > costs)?
- Is it the best options, considering alternative projects and limited resources (maximization of benefits)?
- Externalities generated should be included (and expressed in monetary/market value). Not so for purely private projects. So a market logic is applied to non-market decisions and effects
- Assigning values to externalities is extremely complex. IT security in general is in economic terms a public good (non sharable), even more so in cybersecurity. Economic value of security is not easily measured.

(basic) Options for standardization policy

This version of the model considers three policy options:

1. No mandatory standardization for security (non-intervention)
2. Voluntary standardization mandated but not specified
3. Complete regulation (mandated model, compulsory) - state intervention up to direct defence of networks

Caveat: right now the existence of many different categories of standards is not considered and basically what we are referring to are Informatin Systems Management Systems based on risk management (like the ISO 27000 series or the recent NIST cybersecurity framework).

Proposed framework

Actor	Cost	Benefit	Externalities generated

CI operators (public and private)	• Participation in the developing of standards
	  ◦ personnel (2,3)
	  ◦ overhead (2,3)
	• Implementation of standardization programs (2,3)
	• Maintaining of compliance (2,3)
	  ◦ Overhead
	  ◦ Administrative
	  ◦ Operative
	  ◦ Audits
		• Reduced number of attacks (higher security) (2,3)
		• Speedy disaster recovery (2,3)
		• Lower costs of communication with partners (esp. cross-borders) and authorities (2,3)
		• Lower liability and reduced insurance costs (2,3)
		• Incident reporting standards, threats catalogs can foster collaboration, reduce costs
			• “saner” cyberspace (2,3)
			• environmental benefits and safety of CIs (2,3)
			• knowledge/experience sharing (2,3)
			• (negative) Rigid markets, less competition (3)

Societal	• (possible) Participation in the developing of standards (consultation,	• Less downtime for CIs and users/clients (2,3)	• Heightened trust in institutions by citizens • National security and

	editing etc) (2,3)	• (possible) Lower costs of services (shared with operators) (2,3)	resilience (2,3) • Standardization is good for transnational CIs (ECIs in the Directive's parlance) – It supplies a common base → increases trust among international partners

Further work and conclusion

Of course much work is still needed to achieve a workable model, in particular in two areas: a better and more detailed model and, most of all, solving the problem of how to economically evaluate cost, benefits and externalities; this is the crux of the implementation of Cost-Benefit Analysis.

Better empirical data

- Source data for predict costs of potential damages (and what exactly damages are) by a cyber attack, the probability of their occurrence are hard to come by. Also security metrics for complex systems can be improved.
- Need of a baseline for *measurable* security, i.e. a state where no standards are implemented (basically policy option 1), with which to confront the other options.
- Policymaking is more complex than the three options presented and a more articulated set of options should be considered, as well as how to assess over time compliance by the operators.

Extension of the model:

- Incorporate different kinds of standards and standardization, including compliance models.
- More articulated actor analysis, especially for “strange federations” like the EU where different level of legislation and jurisdiction interact, the legislative process is quite cumbersome.
- Also incorporate differences in CIs (electrical grid, oil&gas, IT etc). Different usefulness of standards and different impact (e.g. smart meters, easy integration into the electrical grid, less so for gas).

While much is still needed, a workable model for rational economic policy decisions is very much a necessity, especially in the general field of security and national security where the last decades saw more of a fear-driven reaction to threats than meditated choices.