When standards and regulations are not enough: 
Why industrial cybersecurity is different in Critical Infrastructures?

Samuel Linares
Munich, June 2018
Society
Critical Infrastructures
Interdependencies: the impact of a major attack on any critical sector in the region would be devastating with widespread implications.
Cyber attacks now threatening critical infrastructures can disrupt business operations and destroy data and infrastructures on larger scales.
Information Theft vs Infrastructure Destruction
...on the lookout
Risk = f (threat, vulnerability, impact, probability)
Probability is irrelevant
Probability is irrelevant for critical infrastructures protection and national security

Moreover, there is a lack of objective and relevant historical data of cybersecurity incidents, making probability/likelihood completely subjective and irrelevant.

“Traditional” risk assessments focus on the top results of the impact and likelihood product. This means that harmless or rare events are not taken into account.

Black swans are unexpected events of so huge consequences that can not be neglected in critical infrastructures and national security since they are able to cause huge impact in the physical world, with the potential of harming the environment and damaging human lives.

In environments with the potential of damaging human lives, the assessment of low probability events cannot be neglected.

The black swan theory was developed by Nassim Nicholas Taleb in his 2007 book “The black swan: The impact of the Highly Improbable”.

Samuel Linares | @infosecmanblog | +34 639656519
Standards are not enough
Standards and regulations are baselines and not sufficient

1. Comply = Comply + Lie
2. Compliant != Protected
3. Standards are slow...
Protection is not only about cyber
Cybersecurity is only one leg of the chair of the protection.
We have a complex ecosystem
The ecosystem is complex, with multiple and deep supply chains
No way to go it alone
Dealing with giants is not easy
How a real mega-project looks like?

8 years  $3.5 billion

Design

4 million man hours
50,000 design drawings

Construction

20 million man hours
10,000 workers

66,000 tons in weight
250 km of piping

6000 valves
225 km of cabling

64% facing cost overruns
73% reporting schedules delays
100% facing budget overruns

4 million man hours
50,000 design drawings
20 million man hours
10,000 workers
66,000 tons in weight
250 km of piping
6000 valves
225 km of cabling

8 years $3.5 billion

Design

4 million man hours
50,000 design drawings

Construction

20 million man hours
10,000 workers

66,000 tons in weight
250 km of piping

6000 valves
225 km of cabling

64% facing cost overruns
73% reporting schedules delays
100% facing budget overruns

4 million man hours
50,000 design drawings
20 million man hours
10,000 workers
66,000 tons in weight
250 km of piping
6000 valves
225 km of cabling

64% facing cost overruns
73% reporting schedules delays
100% facing budget overruns
Cybersecurity is only a very small part of these mega projects and EPCs deal with it from a general compliance perspective rather than a core project element.
People are the key to success
It is difficult (and will be more difficult) to find available cybersecurity talent in the market.
Probability is irrelevant
Standards are not enough
Protection is not only about cyber
We have a complex ecosystem
Dealing with giants is not easy
People are the key to success

So what?
There is light at the end of the tunnel...
... but we need to work hard
One reality, multiple perceptions
It all starts by harnessing collaboration, coordination and commitment between all the (internal and external) stakeholders

- **Collaboration**: Encouraging information sharing within sectors and across industry verticals
- **Coordination**: All of us is stronger than one of us. Coordination among producers, distribution, regulators, government agencies and industry experts
- **Commitment**: Dedicated, motivated, and knowledgeable resources, along with senior leadership support are key
Increase inside (full infrastructure monitoring) and outside (threat intelligence) visibility.
Build your own industrial cybersecurity framework by adapting and adopting applicable standards and regulations

Your strategy, governance, management and evaluation approaches should be built on your Cybersecurity Framework, aligned with international standards and best practices, and providing the key principles for managing cybersecurity.
Inject cybersecurity into the design, development, deployment and operations of your infrastructures and projects

- **PLAN**
  - Conceptual Design
  - Initial Specifications
  - Evaluate Cybersecurity and Develop Initial Specifications

- **DESIGN**
  - Front End Engineering Design
  - Detail Design
  - Develop Reference Architecture, Detail Cybersecurity Specifications and Procurement Support

- **BUILD**
  - Procurement and Acquisition
  - Provision (FAT, iFAT)
  - Conduct Cybersecurity Tests during FAT, iFAT y SAT

- **OPERATE**
  - Execution (SAT)
  - Manage and Operate
Enable an independent Cybersecurity Trusted Contractor as an unbiased Trusted Advisor, thus reducing implementation risk

Acts as a catalyst and oversees cybersecurity activities

Manages and interfaces with key stakeholders

Reduces project and implementation risks

Ensures vendor neutrality and unbiased technology

Avoids conflict of interests and independently manages cybersecurity objectives

Empowers business and offering
Develop cybersecurity talent with real world exercises and training to empower your people, and attract others.
Passion
Thank You

Samuel Linares
Samuel.Linares@Gmail.com
Tel +34 639656519
Twitter: @infosecmanblog