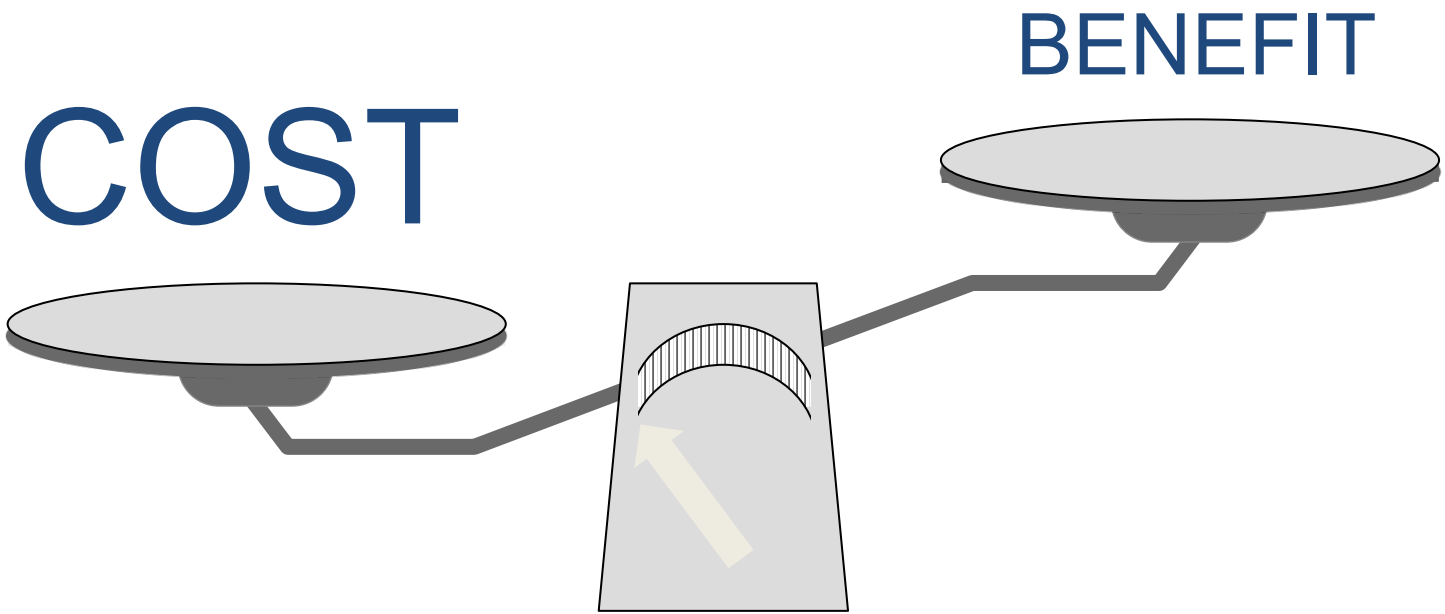
GLOBAL CYBER SECURITY CENTER

“The relevance to justify Information Security Capex and Opex”

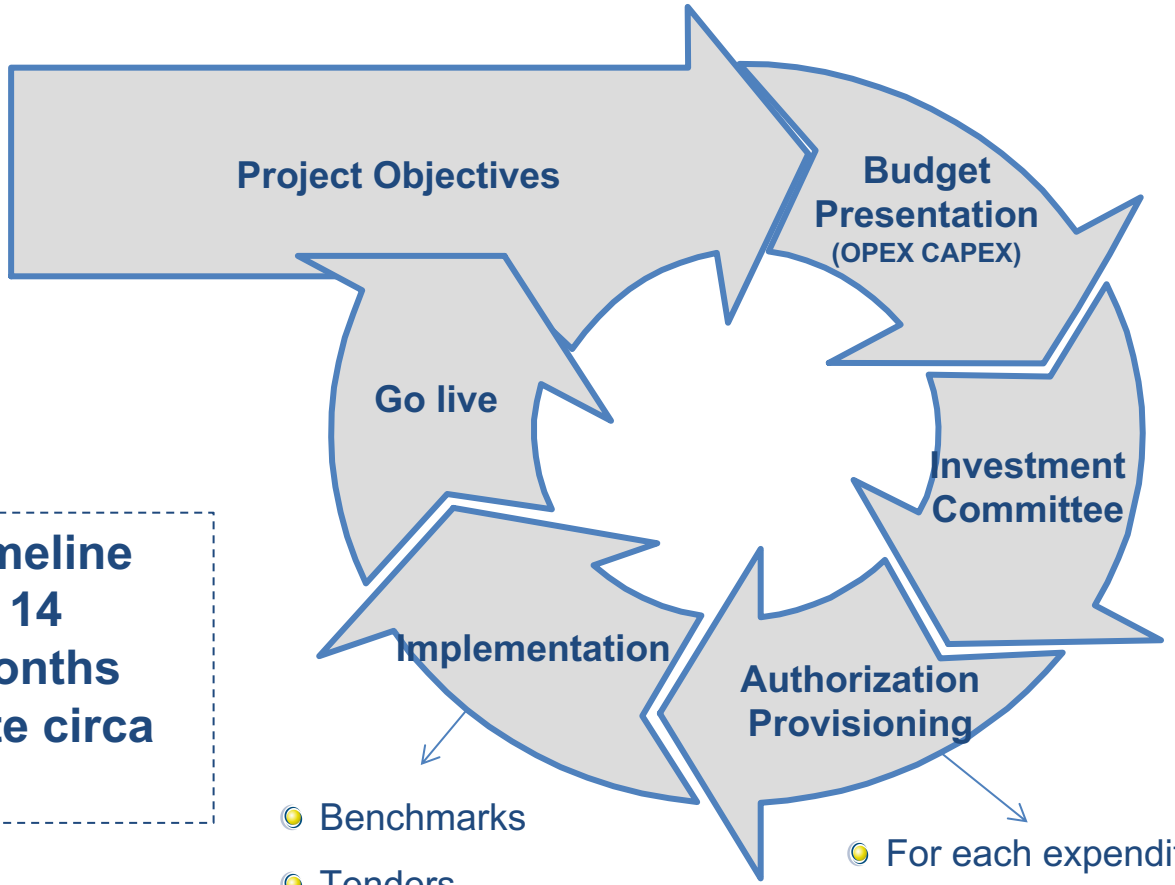
Bucarest, 4 June 2019

The Eternal Dilemma



Justify OPEX & CAPEX for Information Security

Opex and Capex Authorization procedures



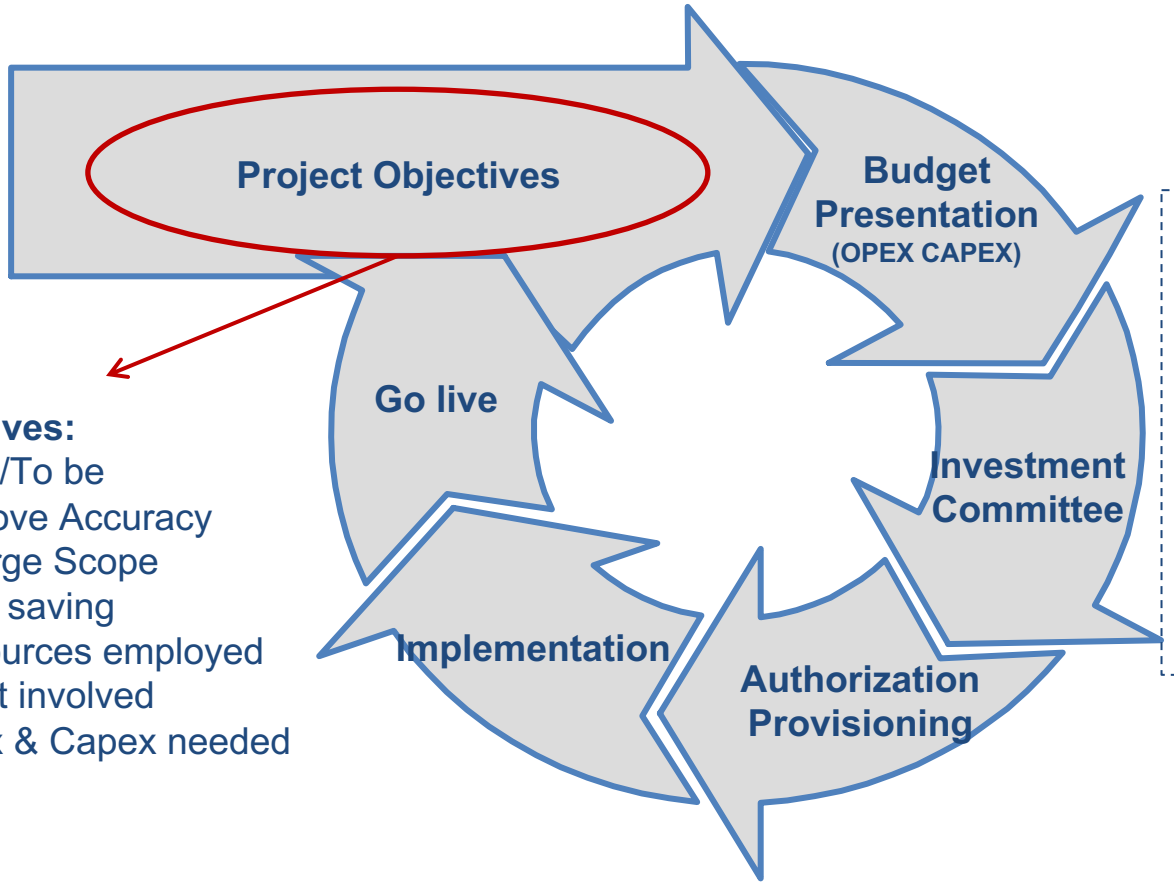
Every Year, a CISO should present a project of brief – medium or long period, including CAPEX and OPEX, needed to supply his/her services

Timeline
14 Months
4 Fte circa

- Benchmarks
- Tenders

- For each expenditure

Defining project objectives is the most relevant phase of the procedure



Objectives:

- As-Is/To be
- Improve Accuracy
- Enlarge Scope
- Time saving
- Resources employed
- Asset involved
- Opex & Capex needed

IS THAT ENOUGH ?

The Risk Reduction drives objectives:

$$R = T \times V_{Asset} \times I$$

Strategic Level	Motivation and Groups	Company exposure	Losses
Operational Level	Pattern of Attack	Chain of CVE and Asset exposed	Services Impacted
Tactical Level	Indicators of Compromise	Common Vulnerabilities and Exposure	Confidentiality, Integrity & Availability
	External Parameter	**Internal Parameter**	

GLOBAL CYBER SECURITY CENTER

The Risk Management past/present/future issues

$$R = T \times V_{Asset} \times I$$

- **Mitigate**
- **Transfer**
- **Accept**
- **Avoid**

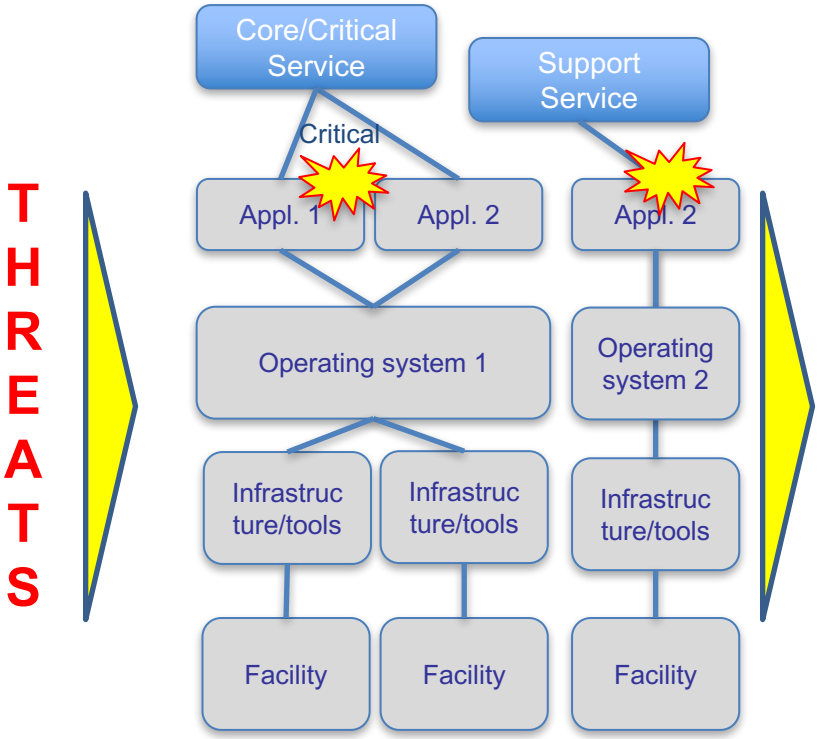
- Detailed data and trends for sectors
- Data quality certification to insert in the Risk Function
- Likelihood attribution

- Objective metrics and benchmark for global exposure
- Service vs Technology chain mapping including interdependencies
- Patch prioritization

- Value of Data (CIA) globally recognized
- Composition of Impact parameter
- Value of impact parameter (i.e. brand reputation)

GLOBAL CYBER SECURITY CENTER

Impact should be determined quantitatively & economically



Example Company impact matrix

IMPACT MATRIX

Company crisis

National Crisis

Parameter	Green	Yellow	Orange	Red
Health	No injuries	Light injuries	Heavy Injuries	Danger of life
Economics Loss	< 1% EBITDA	1%<EBITDA< 3%	3%<EBITDA< 5%	> 5% EBITDA
Service disruption	0 – 10 minutes	10 – 60 minutes	1 day	> 1 day
Reputation	Inside the company	Local level	National level	International level
Share value	…			
….				

TRANSFORM in an economic value

Return on Security Investment (ROSI)

Parameter	Green	Yellow	Orange	Red
Health	No injuries	Light injuries	Heavy Injuries	Danger of life
Economics Loss	< 1% EBITDA	1%<EBITDA< 3%	3%<EBITDA< 5%	> 5% EBITDA
Service disruption	0 – 10 minutes	10 – 60 minutes	1 day	> 1 day
Reputation	Inside the company	Local level	National level	International level
Share value	…			
….				

IMPACT MATRIX

THREATS & VULNERABILITIES

$$ROSI = \frac{ALE \times Mitigation\ ratio - Cost\ of\ solution}{Cost\ of\ solution}$$

Annual Loss Expectancy (ALE) = is the total annual financial loss to expect from security incidents. This is the control number that demonstrates how much money can be lost by maintaining business-as-usual.

https://www.csoonline.com/article/3229887/how-to-calculate-your-return-on-security-investments.html

Critical Issues of Annual Loss Expectancy

Annual Loss Expectancy (ALE) = is the total annual financial loss to expect from security incidents. This is the control number that demonstrates how much money can be lost by maintaining business-as-usual.

Some samples:

- The economic value of Data (CIA) should be the same for Companies and Insurances because it influences the Insurance Premium;
- The trends of security incidents per year worlwide can replace the absence of internal security statistics (IT NEVER HAPPENS TO US WHY IT SHOULD HAPPEN TOMORROW). Data source authoritativeness should be globally recognized
- The parameters composing each voice of impact should be shared between stakeholders to guarantee the transparency (direct, indirect cost)

Impact value samples to validate with Business Owner and CFO

Parameter	Samples
Health	Average value of reimbursement for typology of injuries (also psychological for personal information)
Economics Loss	Direct economic loss such as financial tefth (i.e. fraud reimbursement to client; Business Email Compromise financial theft; customer churn rate,…)
Service disruption	Time of disruption for average revenue of the same past period or historical trends, extra-salaries for work to be completed
Reputation	Cost of Communication campaigns for retention strategy or client support;…
Sanctions	GDPR Regulation; Service Level Agreement unsatisfied;…
Share value	Daily price fluctuation after the event

Share value fluctuation analysis after a cyber attack

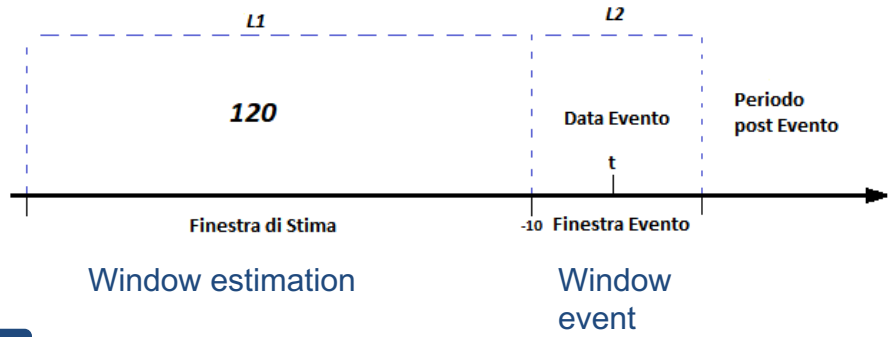
Work in progress

Premises:

- External attack for compromission/theft of CIA data;
- First analysis on 37 cyber attacks from 2016 to 2019 (UK, USA, NO, DE, CHI, CDN)
- Stock Exchange Market considered: New York Stock Exchange, NASDAQ, other markets (London, Tokyo, Oslo,…)
- Methodology: Event Study Financial Literature; Parameter estimation on Market Model

Methodology:

Share estimated performance, on the basis of the performance during the long period before the attack compared with the market index performance during the same period. The estimation is then ccompared with the Abnormal return (AR) and the Cumulative Average Abnormal Return (CAAR) realized.

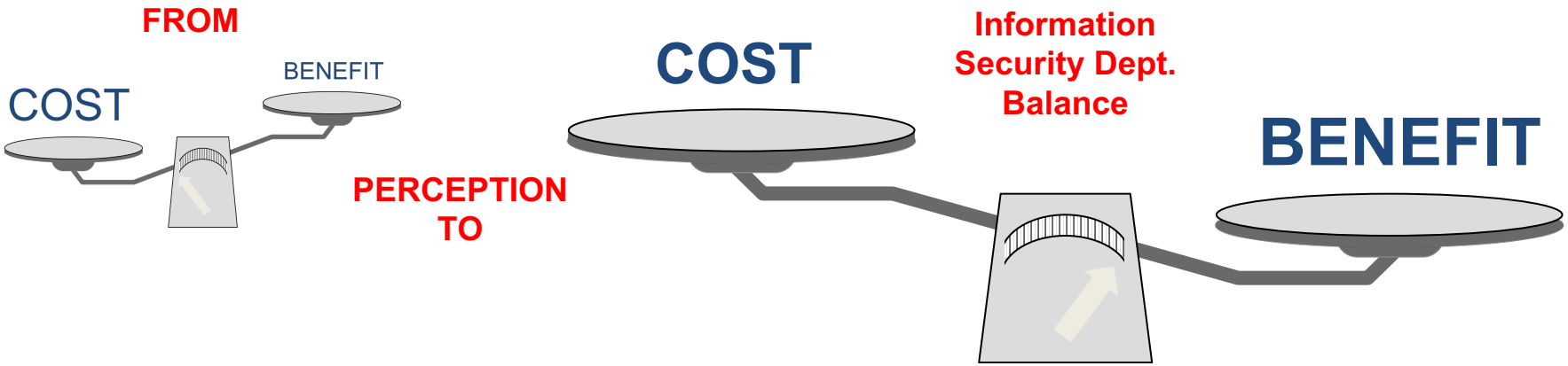


The fluctuation of CAAR is low. The average daily price fluctuation is -0,5/-1%. The adjustments come the day after the announcement. The event has no propagation. It is not possible to realize extra-performance because the market is fast to absorb the news.

Global Cyber Security Center

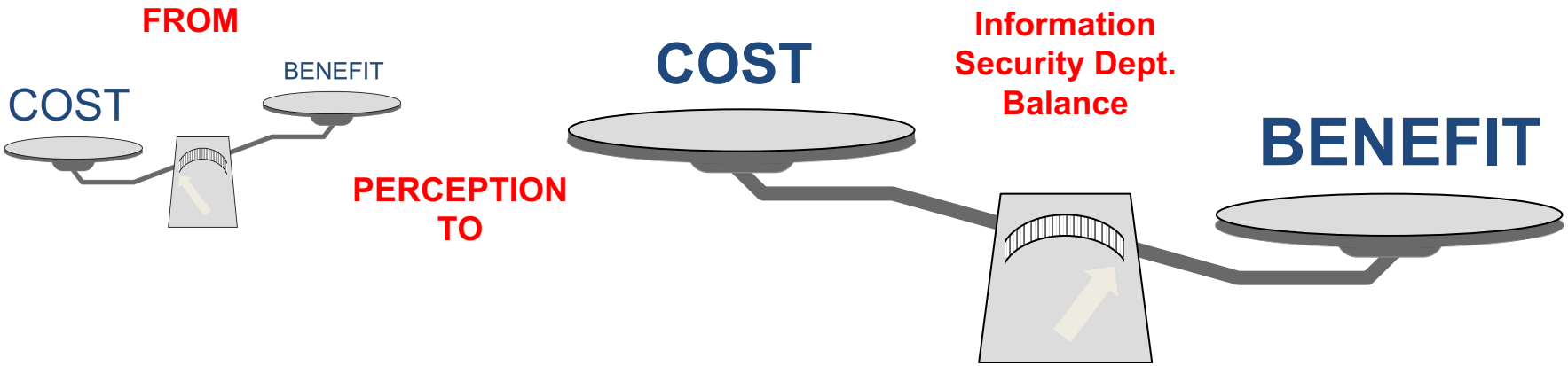
Source: Marika Mazza <m.mazza.marika@gmail.com>

Certified Data and methodology are vital for the Risk estimation that brings to a solid ROSI estimation



- Shared Certified Data between Stakeholders (Financial Institutions, Insurances, Authorities, Stakeholders,…)
- Shared components and estimation methodology of Impact voices by Stakeholders
- Detailed analytical data gathering to fullfill the analysis
- Create a cost/benefit behaviour inside Information Security Department to talk the same language of Chief Financial Officer and Business Owner

Certified Data and methodology are vital for the Risk estimation that brings to a solid ROSI estimation



- Shared Certified Data between Stakeholders (Financial Institutions, Insurances, Authorities, Stakeholders,…)
- Shared components and estimation methodology of Impact voices by Stakeholders
- Detailed analytical data gathering to fullfill the analysis
- Create a cost/benefit behaviour inside Information Security Department to talk the same language of Chief Financial Officer and Business Owner

Homework for everybody

"We built an algorithm to track bots during the European elections – what we found should scare you"

https://www.independent.co.uk/voices/european-elections-parliament-bots-social-media-matteo-salvini-far-right-a8924831.html?fbclid=IwAR3PFzzJEVjn6odAa_DZFqE23HKEf9WRwfCHCFO2NhYRTtcUjDNpoYWvfUE

"The impact of political risk on the volatility of stock returns: The case of Canada"

https://www.researchgate.net/publication/5223173_The_impact_of_political_risk_on_the_volatility_of_stock_returns_The_case_of_Canada

DISINFORMATION AND SOCIAL NETWORK "DOPING" COULD INFLUENCE COMPANY STOCK VALUES?

GLOBAL CYBER SECURITY CENTER

THANKS

Massimo Cappelli: massimo.cappelli@gcsec.org

For Share Value Fluctuation analysis: Marika Mazza

m.mazza.marika@gmail.com