A multi-layer Criticality Assessment methodology based on interdependencies

- Authors:
  - Marianthi Theoharidou, Panayiotis Kotzanikolaou, and Dimitris Gritzalis

- Journal:
  - Computers & Security
- Article history:
  - Received 10 January 2010
  - Received in revised form 18 February 2010
  - Accepted 28 February 2010

Outline

- Introduction
- A multi-layer design
- A Multi-layer Criticality Assessment methodology: modeling interdependencies and calculating risk
- Conclusions

Introduction

- Business, industry, government and society in general rely on critical information infrastructures in order to function.
- Such infrastructures (Critical Infrastructure, CI) are vital for several sectors, like banking, finance, government services, information and communication technologies (ICT), energy, health, food, water, transportation.
- **Criticality**
  - Contribution level of the infrastructure to the society in maintaining a minimum quality level of vital societal functions, health, *safety*, *security*, economic or social well-being of people.
  - Impact level to the society from the disruption or destruction of the CI.

Introduction (cont'd)

- This paper proposes a holistic Criticality Assessment methodology.
- The proposed methodology aims to integrate existing security plans and risk assessments performed in organizations (Critical Infrastructure Operators, CIOs).
- This paper defines three different layers of security assessments with different requirements and goals; the *operator layer*, the *sector layer* and the *intra-sector* or *national layer*.

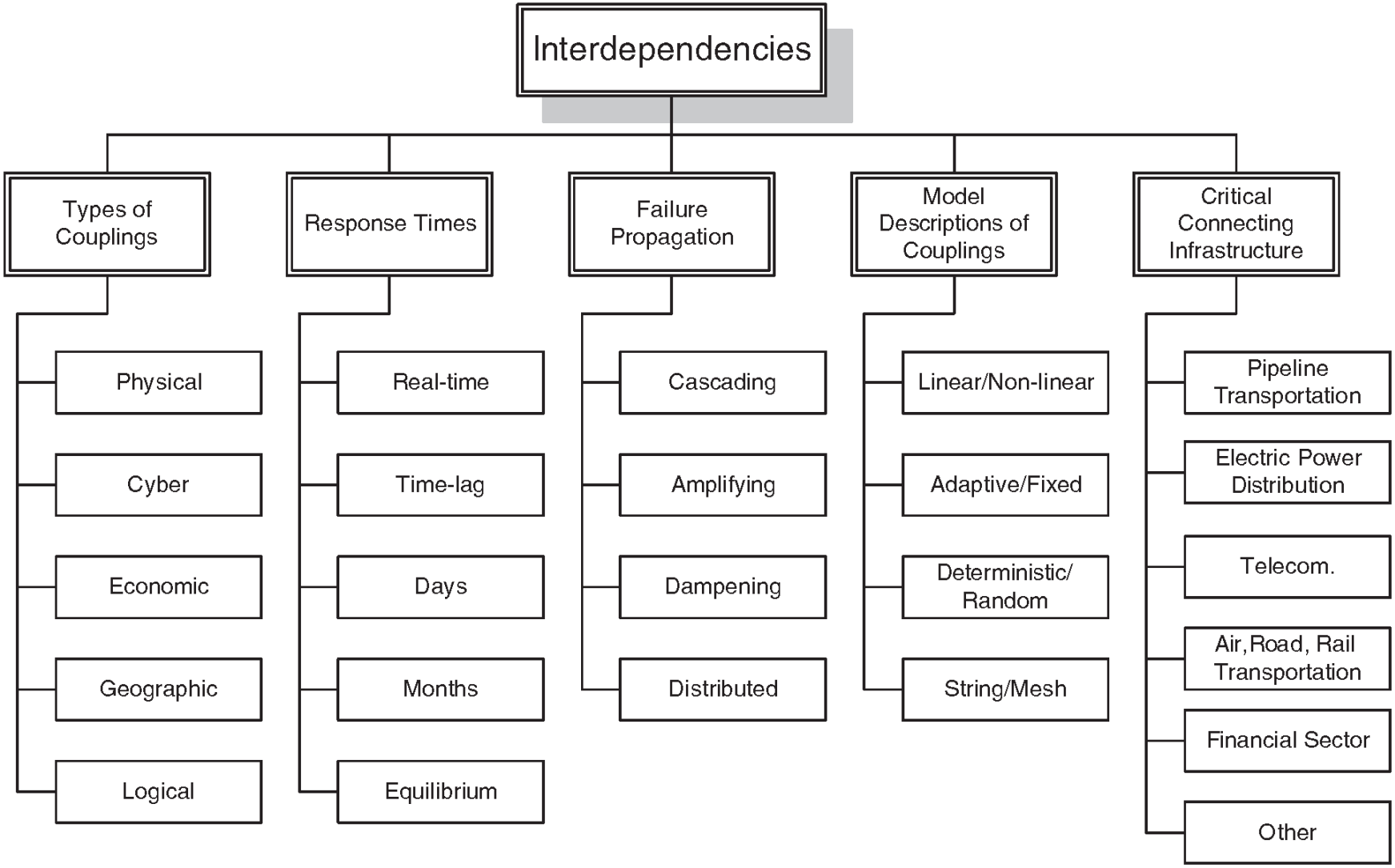
Introduction (cont'd)

- A key element is the formal definition of *interdependencies* between different infrastructures and their respective sectors.
- Interdependencies between infrastructures belonging to the same or to a different sector, as well as interdependencies between different sectors, act as interfaces through which threats and their impacts occurring on different layers or different sectors, are conveyed to others.
- Current risk assessment methodologies fail to address effectively this issue.

Interdependency

- The interdependency between CIOs can be categorized as *physical*, *cyber*, *geographic*, or *logical*.
- *Physical* interdependencies arise from physical linkages or connections among elements of the infrastructures.
- A CIO has *cyber* interdependency with another CIO if its state depends on information transmitted through the information infrastructure of the second CIO.

Introductory taxonomy for interdependency analysis

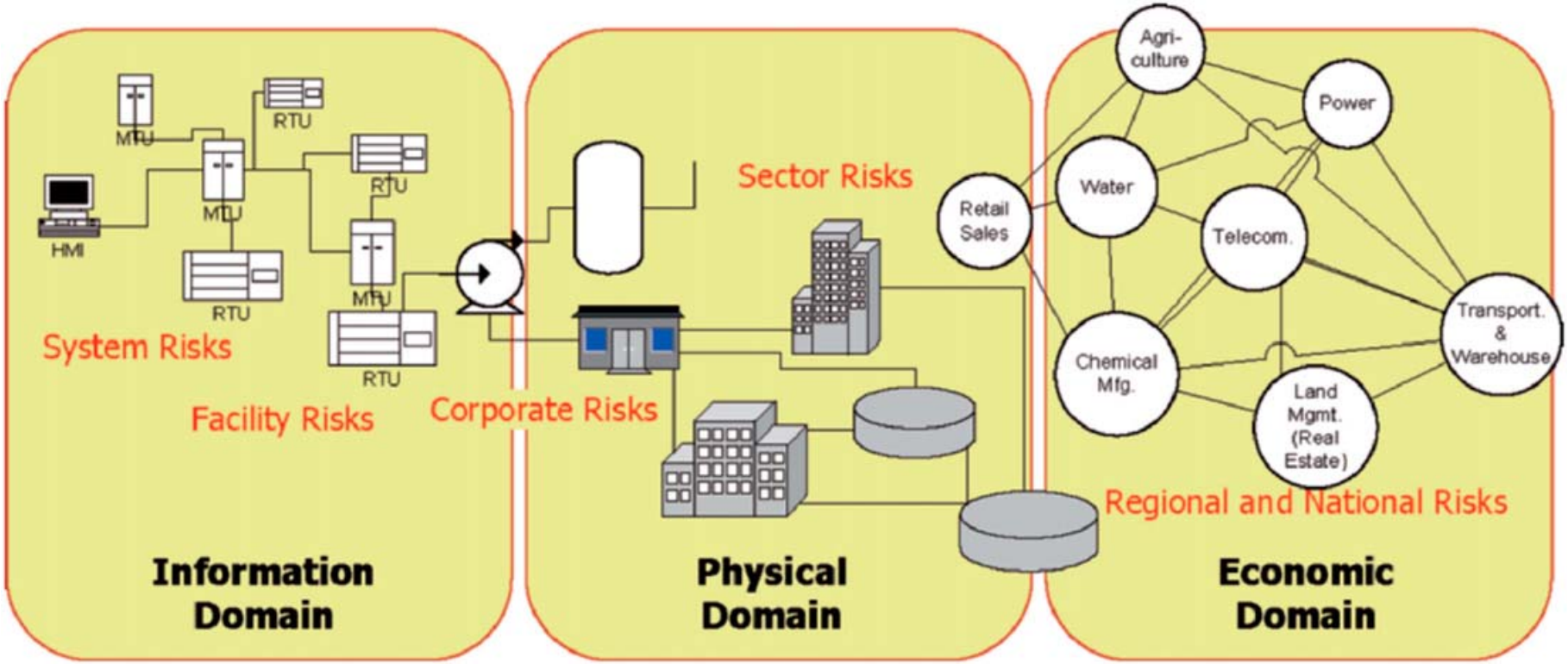


(Haimes et al., 2007)

Requirements for criticality assessment: a multi-layer design

- In order to develop a holistic Criticality Assessment methodology that takes into consideration existing security plans and risk assessments of CIOs.
- This paper proposes a structured approach which takes into consideration three layers of entities with different security need.
- This idea of interdependency layers is also supported by Haimes et al. (2007).

Layers of interdependencies

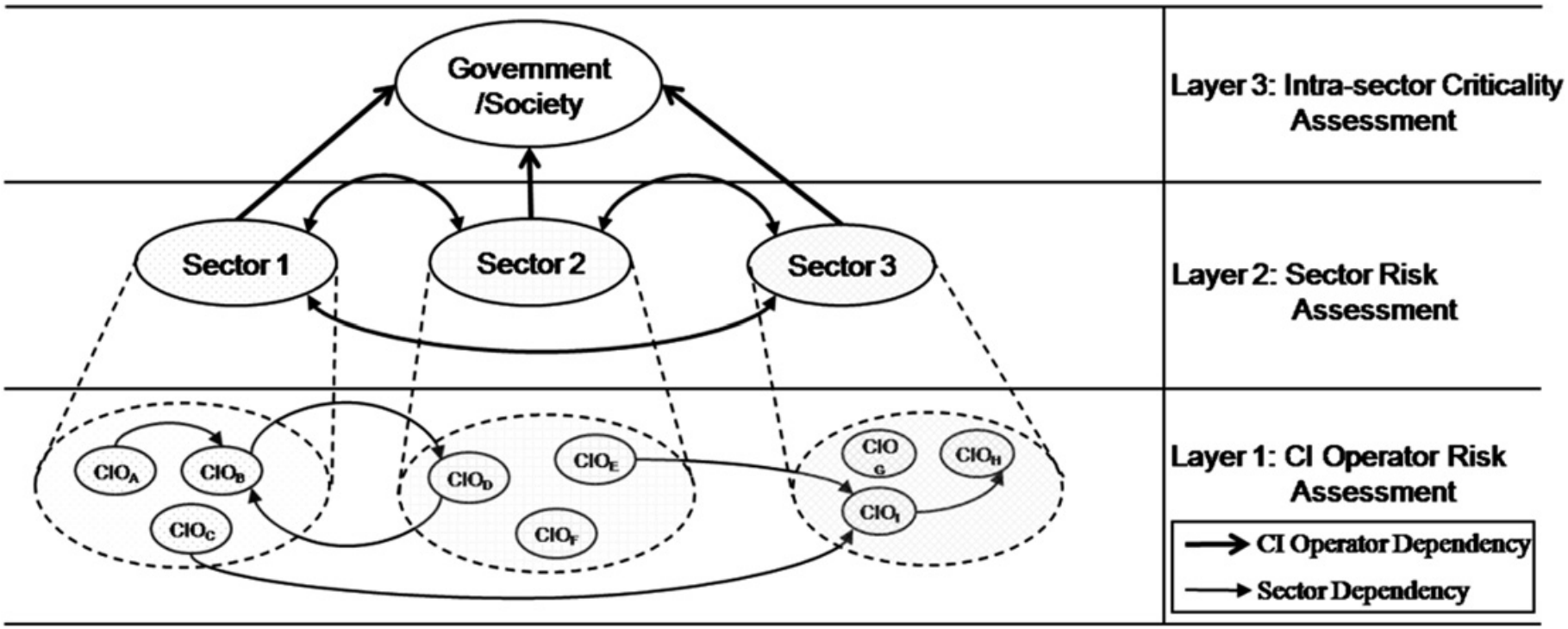


(Haimes et al., 2007)

Requirements for criticality assessment: a multi-layer design (cont'd)

- In order to model the needs and requirements for criticality assessment, this study adopt the layered approach and we examine risk and criticality in three respective layers, namely the *Operator layer*, the *Sector layer* and the *Intra-Sector/National layer*.
- This is a *bottom-up approach* during which the output of the analysis of a layer provides input to the layer above it.

A three-layer criticality analysis approach



Layer 1: operator risk assessment

- **Scope**: The basic concern of any CIO (private company, public body or any other entity) is to protect its own business operations, ICT assets and systems, from security threats.
- **Impact type and scale**: service loss, legal etc.
- **Dependencies**: During a risk assessment a CIO may consider both inside and outside threats.

Layer 2: sector risk assessment

- **Scope**: The scope of a sector-wide criticality analysis involves all the organizations that are members of the sector.
- **Impact type and scale**: societal impact.
  - A risk assessment for the banking sector may need to estimate the possible *social impacts* from an incident that affects the sector as a whole.
- **Dependencies**: During a sector-wide criticality analysis, dependencies with other sectors are examined.

Layer 3: intra-sector/national criticality assessment

- **Scope**: A national body (e.g. a government) is interested in protecting all the infrastructures.
- **Impact type and scale**: A national-wide criticality assessment needs to analyze security threats that are outside the scope of a single sector, but which pose an impact to the *whole society*.
- **Dependencies**: During this layer of analysis needs to examine how the realization of a threat in one sector may affect another sector.

Telecom Italia, 2004

- The failure of a service plant for an important Telecom Italia node in Rome shut down fixed and mobile telecommunications services for several hours.
- The outage affected the financial infrastructure and air transportation.
  - 5,000 bank branches and 3,000 post offices lost connectivity
  - 70% of the check-in desks at Rome's Fiumicino airport were forced to use manual procedures, resulting in numerous flight delays.

A Multi-layer Criticality Assessment methodology: modeling interdependencies and calculating risk

- With the proposed multi-layer criticality analysis methodology, the output of the lower layers is provided as input to the higher layers.
- For each sector, the body assigned as the sector coordinator, will perform the initial identification of the candidate CIOs.

Sector	Abbreviation
Banking & Finance	Finance
Central Government/Government Services	Gov.
(Tele-)Communication/Information & Communication Technologies	ICT
Emergency/Rescue Services	Emergency
Energy/electricity	Energy
Health Services	Health
Food	Food
Transportation/logistics/distribution	Transport
Water (supply)	Water

A Multi-layer Criticality Assessment methodology: modeling interdependencies and calculating risk (cont'd)

- This study assume that every CIO has already conducted an organization-wide risk assessment and has designed and adopted a security plan.
- This implies that the operator has documented all its *important assets*, the *possible impacts*, the *internal and external security threats* and has evaluated the security risks against its assets.

Layer 1: operator layer

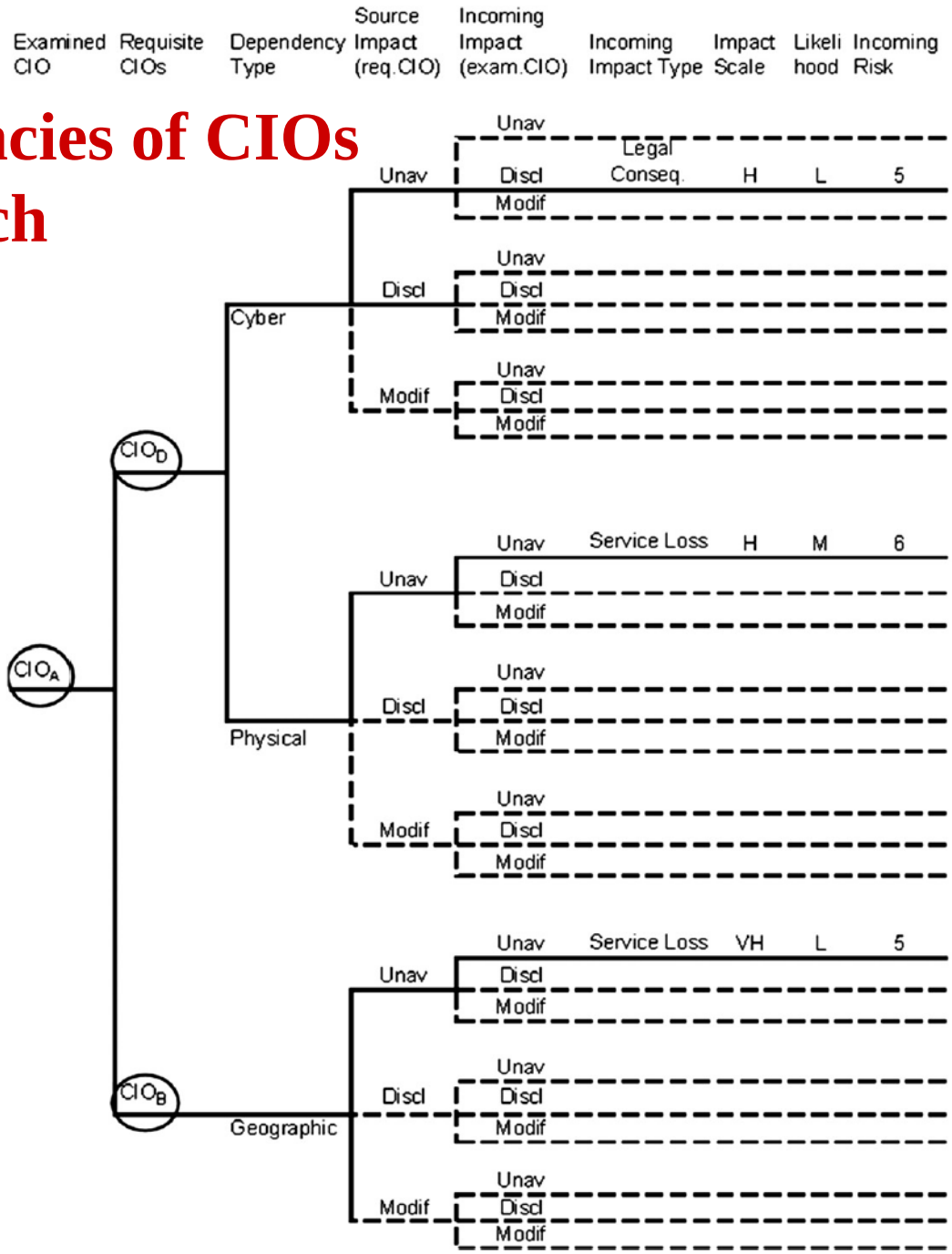
- In order to assess all the organization-wide security risks and also provide input to the next layer (sector-wide criticality analysis), each CIO needs to document its dependencies to third parties, by applying a unified method.
- The method should be simple and close enough to common practice, so that the information is extracted by existing risk analyses with minimum effort.
- In order to model the interdependencies between CIOs, each CIO formulates a *dependency tree*.

Modeling the dependencies of CIOs in a tree-based approach

Example:
the dependencies of CIO_A

Dependency Type:
- Physical
- Cyber (informational)
- Geographic
- Logical
- Social

Impacts:
- Confidentiality
- Integrity
- Availability



Examples of examined impact types and scales for incoming impacts

Incoming Impact Type: economic losses, safety, competitive disadvantage, service loss, legal consequences, etc.

Impact type	Impact scale
Violation of legislation and/or regulation Impairment of business performance Loss of goodwill/negative effect on reputation Breach associated with personal information Endangerment of personal safety Adverse effects on law enforcement Breach of confidentiality Breach of public order Financial loss Disruption to business activities Endangerment of environmental safety	(VL) Very Low (L)ow (M)edium (H)igh (VH) Very High

A risk matrix for the calculation of incoming risks

		Likelihood				
		Very low (very unlikely)	Low (unlikely)	Medium (possible)	High (likely)	Very high (frequent)
Impact	Very low	1	2	3	4	5
	Low	2	3	4	5	6
	Medium	3	4	5	6	7
	High	4	5	6	7	8
	Very high	5	6	7	8	9

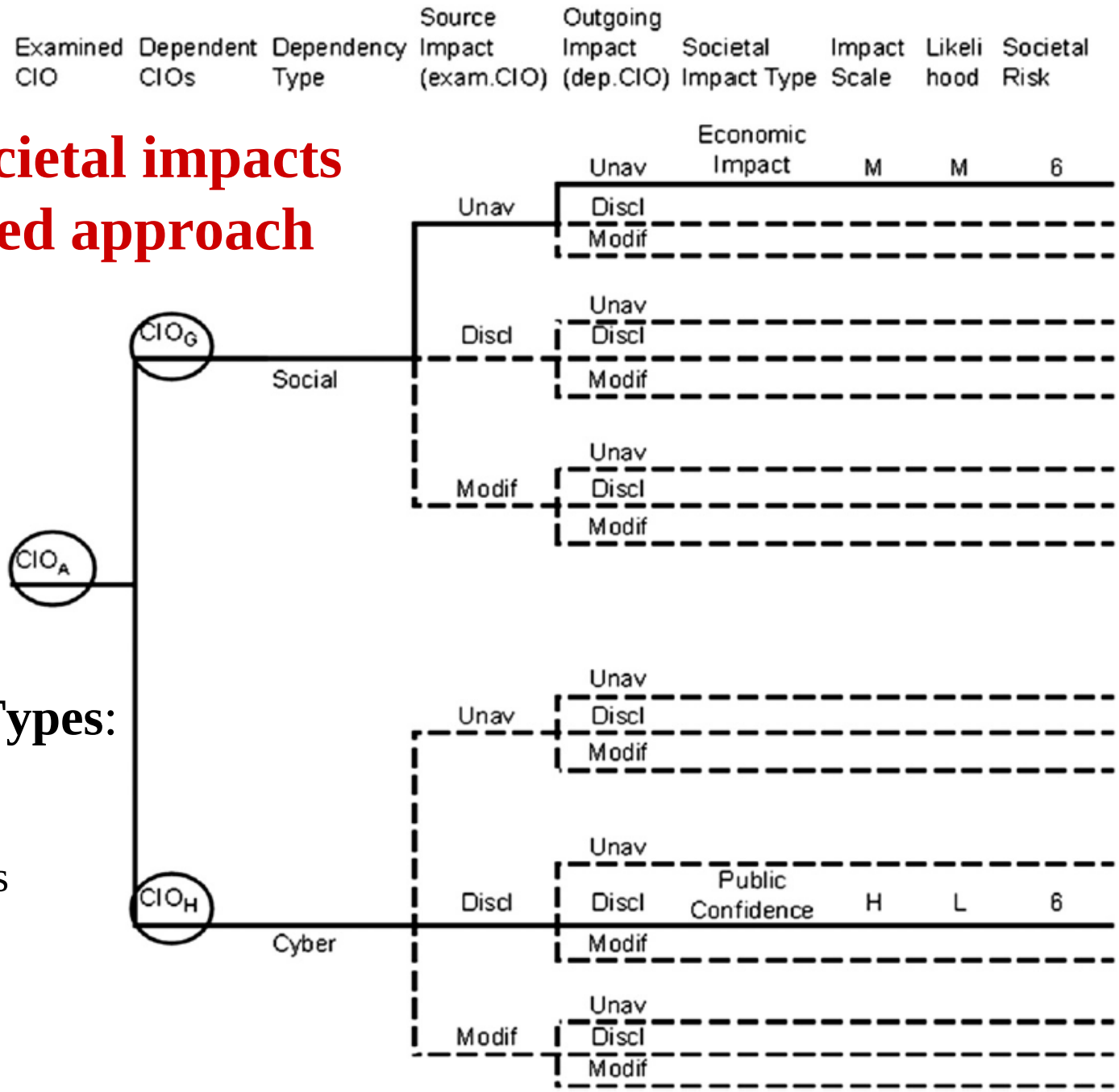
Incoming risks of the operator CIO_A deriving from other CIOs

Requisite CIOs	CIO_A (finance)								
	Dependency type	Description	Source impact	Incoming impact	Impact type	Impact scale	Likelihood	Incoming risk	
CIO_D (ICT)	Cyber	Depends for VPN services	Unavailability	Disclosure	Legal/regulatory Consequence	High	Low	5	4
	Physical	Depends for network connectivity	Unavailability	Unavailability	Service Loss	High	Medium	6	5
CIO_B (finance)	Geographic	Co-location of disaster recovery sites	Unavailability	Unavailability	Service loss	Very high	Low	5	6

Layer 2: sector layer

- The operator layer analysis is performed in a microscopic level, the CIO may fail to identify all the risks.
- Indeed, each CIO will ONLY examine the incoming risks deriving from its dependencies and it will NOT examine impacts on other CIOs or possible sector impacts and societal impacts and risks.
- In order to model the societal impacts that may derive from each CIO, the *sector coordinator* will formulate for each examined CIO a *social impact dependency tree*.

Modeling societal impacts in a tree-based approach



Societal Impact Types:

- Economic impact
- Public confidence
- International relations
- Public order
- Safety
- Defense

A risk matrix for the calculation of societal risks

		Likelihood				
		Very low (very unlikely)	Low (unlikely)	Medium (possible)	High (likely)	Very high (frequent)
Impact	Very low	2	3	4	5	6
	Low	3	4	5	6	7
	Medium	4	5	6	7	8
	High	5	6	7	8	9
	Very high	6	7	8	9	9

Societal risks deriving from the operator CIO_A of the Finance Sector

Dependent CIOs	CIO_A (finance)							
	Type	Description	Source effect	Incoming effect outgoing	Impact type	Impact scale	Likelihood	Societal risk
CIO_G (Gov.)	Social	Provides payment services for public insurance body	Unavailability	Unavailability	Economic impact	Medium	Medium	6
CIO_H (Gov.)	Cyber	Supports supply management	Disclosure	Disclosure	Public confidence	High	Low	6

CIO_D (ICT)					
Description	Effect	Impact type	Impact scale	Likelihood	Societal risk
Provides landline telecommunication services to 60% of the citizens in city X.	Unavailability for 3 h	Public confidence	Medium	Very low	4

Layer 3: intra-sector/national layer

- The results need to be combined so as to create a complete view of the dependencies between the various CIOs.
- During this layer, the sector coordinators will reexamine all the results of the previous layers in order to identify and confirm the dependencies between CIOs and form a more macroscopic view in a sector level.

Global view of risks between CIOs

Sectors		Finance			ICT			Gov.		IDR
		CIO_A	CIO_B	CIO_C	CIO_D	CIO_E	CIO_F	CIO_G	CIO_H	
Finance	CIO_A		6		**5**		2			0,206
	CIO_B				4		2	1		0,111
	CIO_C	3								0,048
ICT	CIO_D	2	9			8	6	4	8	0,587
	CIO_E			6	7		8		6	0,429
	CIO_F		3	6				4		0,206
Gov.	CIO_G									0,000
	CIO_H	1		5		6	4			0,254
ODR		0,095	0,286	0,270	0,254	0,222	0,349	0,143	0,222	

Dependency Risk: $DR_{i,j}$ of CIO_i from CIO_j $$DR_{i,j} = \max_{\forall (i,j)} \{r_{i,j}\}$$

Incoming Dependency Risk: IDR_i $$IDR_i = \frac{1}{(n-1) \times r_{\max}} \sum_{\forall i \neq j}^{n} DR_{i,j}$$

Outgoing Dependency Risk: ODR_j $$ODR_j = \frac{1}{(n-1) \times r_{\max}} \sum_{\forall j \neq i}^{n} DR_{i,j}$$

Global view of societal risks between CIOs

Sectors		Finance			ICT			Gov.		ISR
		CIO_A	CIO_B	CIO_C	CIO_D	CIO_E	CIO_F	CIO_G	CIO_H	
Finance	CIO_A		5					**6**	**6**	0,270
	CIO_B	7		3		7		7		0,381
	CIO_C							8		0,127
ICT	CIO_D								5	0,079
	CIO_E	5								0,079
	CIO_F				8					0,127
Gov.	CIO_G	1	3							0,063
	CIO_H			4			9			0,206
OSR		0,206	0,127	0,111	0,127	0,111	0,143	0,333	0,175	

Societal Risk: $SR_{i,j}$

$$SR_{i,j} = \max_{\forall (i,j)} \{sr_{i,j}\}$$

Incoming Societal Risk: ISR_i

$$ISR_i = \frac{1}{(n-1) \times r_{\max}} \sum_{\forall i \neq j}^{n} SR_{i,j}$$

Outgoing Societal Risk: OSR_j

$$OSR_j = \frac{1}{(n-1) \times r_{\max}} \sum_{\forall j \neq i}^{n} SR_{i,j}$$

Measuring potential societal risk

CIO_D (ICT)					
Description	Effect	Impact type	Impact scale	Likelihood	Societal risk
Provides landline telecommunication services to 60% of the citizens in city X.	Unavailability for 3 h	Public confidence	Medium	Very low	4

Societal Risk: SR_i for a CIO_i

$$SR_i = \frac{1}{r_{max}} \max\{sr_i\}$$

Criticality levels for various CIOs

	Finance			ICT			Gov.	
	CIO_A	CIO_B	CIO_C	CIO_D	CIO_E	CIO_F	CIO_G	CIO_H
ODR_i	0.095	0.286	0.270	0.254	0.222	0.349	0.143	0.222
OSR_i	0.206	0.127	0.111	0.127	0.111	0.143	0.333	0.175
SR_i	0.667	0.556	0.444	0.222	0.333	0.111	0.889	0.444
C_i	0.968	0.969	0.825	0.603	0.666	0.603	1.365	0.841

Criticality level C_i of an operator CIO_i

$$C_i = ODR_i + OSR_i + SR_i$$

If n_i is the number of operators included in the sector S_i then, the criticality level of the sector S_i can be computed as the *average* of the criticality levels C_j of all its members j.

$$C_{S_i} = \frac{1}{n_i} \sum_{\forall j \in S_i} C_j$$

Global view of risks between sectors

	Finance CIO_A, CIO_B, CIO_C	**ICT** CIO_D, CIO_E, CIO_F	**Gov.** CIO_G, CIO_H	**IDR**
Finance CIO_A, CIO_B, CIO_C		5	1	0,333
ICT CIO_D, CIO_E, CIO_F	9		8	0,944
Gov. CIO_G, CIO_H	5	6		0,611
ODR	0,778	0,611	0,500	

$$DR_{S_i,S_j} = \max_{\forall k \in S_i, \forall l \in S_j, S_i \neq S_j} \{DR_{k,l}\}$$

$$IDR_{S_i} = \frac{1}{(m-1) \times r_{\max}} \sum_{S_i \neq S_j} DR_{S_i,S_j}$$

$$ODR_{S_i} = \frac{1}{(m-1) \times r_{\max}} \sum_{S_i \neq S_j} DR_{S_j,S_i}$$

Global view of societal risks between sectors

	Finance CIO_A, CIO_B, CIO_C	**ICT** CIO_D, CIO_E, CIO_F	**Gov.** CIO_G, CIO_H	**ISR**
Finance CIO_A, CIO_B, CIO_C		7	8	0,833
ICT CIO_D, CIO_E, CIO_F	5		5	0,556
Gov. CIO_G, CIO_H	4	9		0,722
OSR	0,500	0,889	0,722	

$$SR_{S_i,S_j} = \max_{\forall k \in S_i, \forall l \in S_j, S_i \neq S_j} \{SR_{k,l}\}$$

$$ISR_{S_i} = \frac{1}{(m-1) \times r_{\max}} \sum_{S_i \neq S_j} SR_{S_i,S_j}$$

$$OSR_{S_i} = \frac{1}{(m-1) \times r_{\max}} \sum_{S_i \neq S_j} SR_{S_j,S_i}$$

Conclusions

- This paper proposes a structured, multi-layer Criticality Assessment methodology that takes into consideration the operator, the sector and the intra-sector layer.
- The proposed methodology builds upon well known risk analysis concepts, in order to assist operators and sector coordinators in the implementation of the methodology.