Abbiamo investito tanto nel GDPR: e la sicurezza?

Luca Bechelli

Luca Bechelli

- Practice Leader Information & Cyber Security Advisory Team @ P4I
- Membro del Comitato Direttivo e del Comitato Tecnico Scientifico Clusit Associazione Italiana per la Sicurezza Informatica
- Coordinatore GdL «La valutazione degli impatti del GDPR nelle clausole contrattuali dei fornitori» presso l'Osservatorio «Privacy & Security» del Politecnico di Milano OSSERVATORI.NET digital innovation
- Direttore Didattico Academy Experis per Master in Cybersecurity Experis ManpowerGroup
- Community Clusit - Oracle4Security Oracle Community For Security

Insurance studies suggest cyber risks are amongst the top concerns of large companies

(=) 2018: 1 (46%)

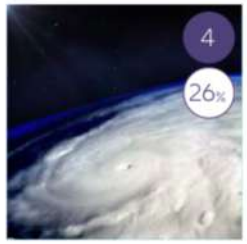
Business interruption
(incl. supply chain disruption)

(=) 2018: 2 (45%)

Cyber incidents[1]
(e.g. cyber crime, IT failure/ outage, data breaches, fines and penalties)

(=) 2018: 3 (27%)

Changes in legislation and regulation
(e.g. trade wars and tariffs, economic sanctions, protectionism, Brexit, Euro-zone disintegration)



(▼) 2018: 3 (27%)

Natural catastrophes
(e.g. storm, flood, earthquake)

(=) 2018: 5 (22%)

Market developments
(e.g. volatility, intensified competition/ new entrants, M&A, market stagnation, market fluctuation)

(=) 2018: 6 (19%)

Fire, explosion

(=) 2018: 7 (15%)

New technologies
(e.g. impact of increasing interconnectivity, nanotechnology, artificial intelligence, 3D printing, autonomous vehicles, blockchain)

(=) 2018: 8 (15%)

Loss of reputation or brand value

(▲) 2018: 10 (10%)

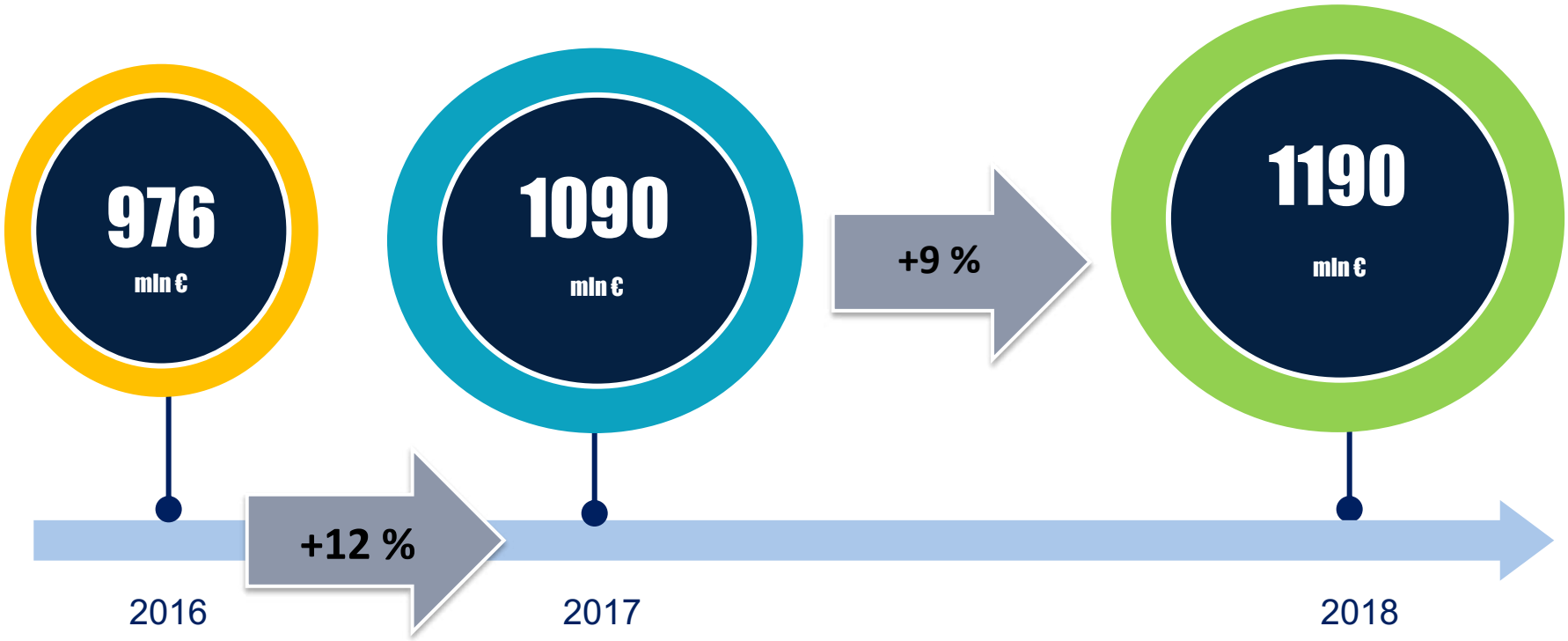
Macroeconomic developments[2]
(e.g. austerity programs, commodity price increase, deflation, inflation)

(▲) NEW

Climate change/ increasing volatility of weather

Source: Allianz Risk Barometer 2019 report

Il mercato dell'Information Security

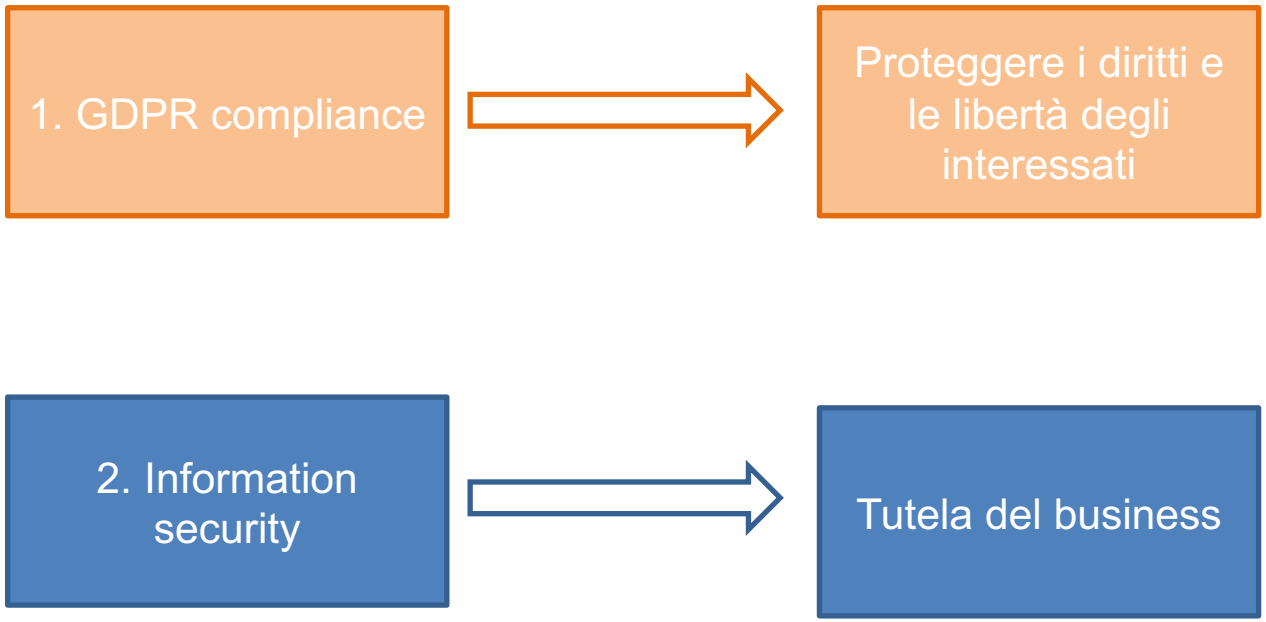


Findings of research by the Observatory of Politecnico University of Milan

Sample: 667 Italian organisations

Compliance e Cyber Risk

Due approcci differenti



1. GDPR Compliance: privacy frameworks

Risk assessment

c) implements **appropriate technical and organisational measures** to ensure a level of security appropriate to the risk pursuant to art. 32

L	Security policy and procedures for the protection of personal data	A.1	The organization should document its policy with regards to personal data processing as part of its information security policy.	A.5 Security policy
M	Security policy and procedures for the protection of personal data	A.3	The organization should document a separate dedicated security policy with regard to the processing of personal data. The policy should be approved by management and communicated to all employees and relevant external parties	A.5 Security policy
H	Security policy and procedures for the protection of personal data	A.6	The security policy should be reviewed and revised, if necessary, on a semestral basis.	A.5 Security policy

enisa «Handbook on Security of Personal Data Processing"

ISO
- ISO/IEC 29100:2017
- ISO/IEC 29101:2013
- ISO/IEC 29134:2017
- ISO/IEC 29151:2017
- ISO/IEC 29190:2015
- ISO/IEC 29191:2012

UNI Practice UNI/PdR 43:2018 «Linee guida per la gestione dei dati personali in ambito ICT secondo il Regolamento UE 679/2016 (GDPR) - Gestione e monitoraggio dei dati personali in ambito ICT»

2. Information security: che framework scegliere?

ISO 20000-1:2011 (Delivery of IT service)	ISO 22301:2012 (Business Continuity)
ISO:IEC 27000 series (Information Security Management)	NIST Cyber Security Framework
ANSI/ISA 62443 (Security for industrial automation and control systems)	PCI-DSS 3.2 (Electronic payments)
EBA / Bank of Italy Circulars	Technical Assessment (e.g. Critical Security Controls, OWASP Testing Guide, NIST 800-53A, etc.)
Customised models based on the Client's business	Other applicable standards (e.g. Cobit, CSA, HIPAA, etc.)

3. Un modello integrato

3.A Definire la libreria delle minacce e classificarle (senza i controlli)

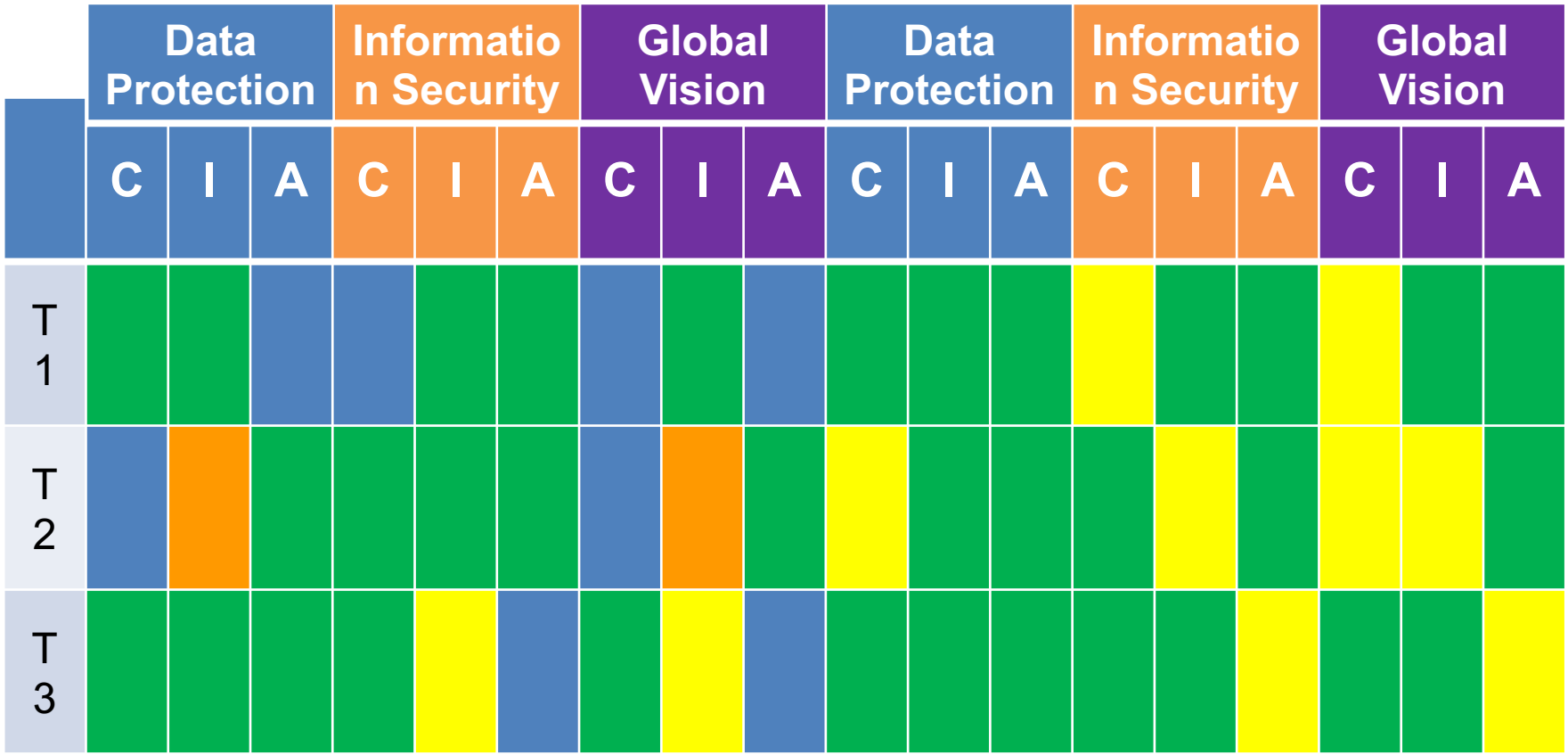
	Data Protection			Information Security			Global Vision		
	C	I	A	C	I	A	C	I	A
Threat 1									
Threat 2									
Threat 3									

3.B Definire i controlli

	Kind	Source	R	I	D
C1	ORG	GDPR art. 32 ISO 27002 A.8.3.3 NIST AC-2 CSA IAM-04	X		
C2	TECH			X	X
C3	TECH			X	

- Scegliere uno o più framework di riferimento
- Scegliere i controlli necessary
- Creare il proprio control-set

3.C Calcolare il rischio residuo grazie ai controlli



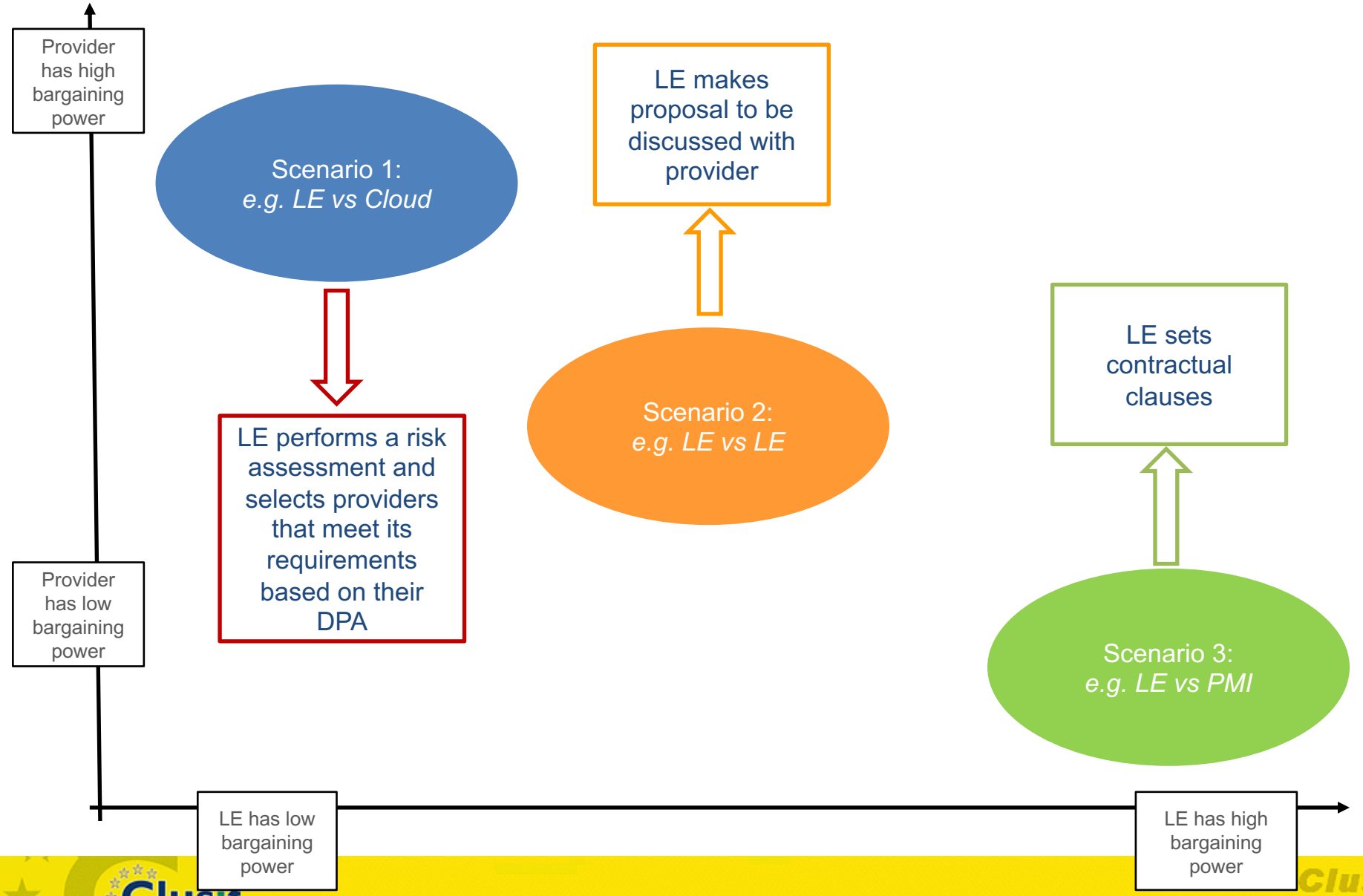
Is it “satisfying”?

Risk appetite e scenari what-If

- Definire il risk appetite
  - “accettabile” significa essere pronti ad accettare quel rischio, dopo aver valutato “pros and cons”
- E se il rischio residuo non è in linea con il risk appetite?
  - Modificare l’implementazione dei controlli, lavorando per ipotesi, fino a che il rischio non è trattato correttamente
  - Creare scenario differenti fino a trovare il corretto bilanciamento “pro-cons”
- Come essere più precisi?
  - Provare a categorizzare non per fasce qualitative (High, medium, low) ma quantitative (si, euro)

- Implementare il remediation plan, avendo ottenuto la libreria di controlli adatti (probabilmente per quello scenario), o chiedere al fornitore di farlo

Relazioni con i fornitori: 3 possibili scenari



Data Governance per i diritti degli interessati

- Soddisfare le richieste di esercizio dei diritti degli interessati rischia di essere una sfida nelle organizzazioni complesse
  - Diritto di cancellazione, limitazione, opposizione, portabilità
  - Gestione della retention
- Avere politiche di asset management, CMDB, data catalog, registro dei trattamenti etc etc permette di sapere quanti e quali dati sono conservati dove ed a che scopo
- Le relazioni di dipendenza tra i dati sono una informazione fondamentale da considerare in relazione alle finalità del trattamento ed alla coerenza dei trattamenti
- La relazione con la politica di classificazione delle informazioni può essere molto fortre e creare una ulteriore sinergia tra security e compliance

Conclusioni

- La soddisfazione delle necessità di compliance è parte della strategia di information security aziendali
- Non sempre gli obiettivi di compliance e tutela aziendale coincidono ma possono essere armonizzati
- Un approccio integrato per obiettivi, organizzazione e competenze garantisce l'eliminazione delle tipiche inefficienze dell'approccio per silos

GRAZIE!

Luca Bechelli
Comitato Scientifico Clusit
luca@bechelli.net
www.bechelli.net
https://twitter.com/luca_bechelli
https://www.facebook.com/bechelli.luca
http://www.linkedin.com/in/lucabechelli