Complex Systems & Security Laboratory
www.coseritylab.it

STATI GENERALI DELLA SICUREZZA

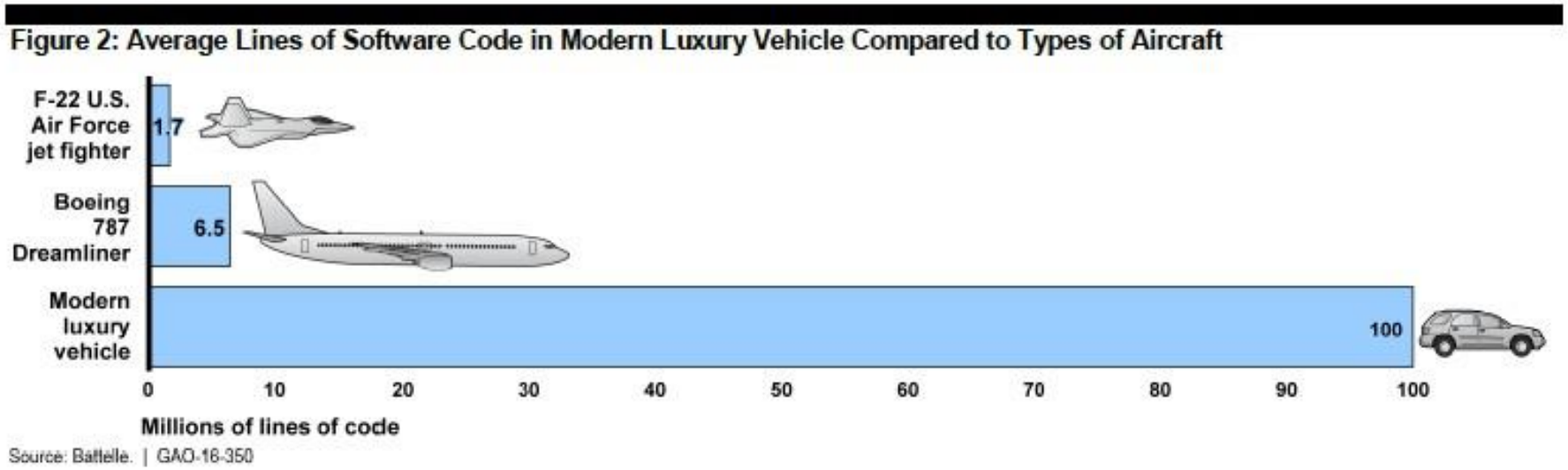
Digital Trasformation. Quali competenze per gli operatori della sicurezza?

Prof. Roberto Setola
r.setola@unicampus.it

Università Campus Bio-Medico di Roma
Via Alvaro del Portillo, 21
00128 Roma
Italy

Roma, 21 Marzo 2019

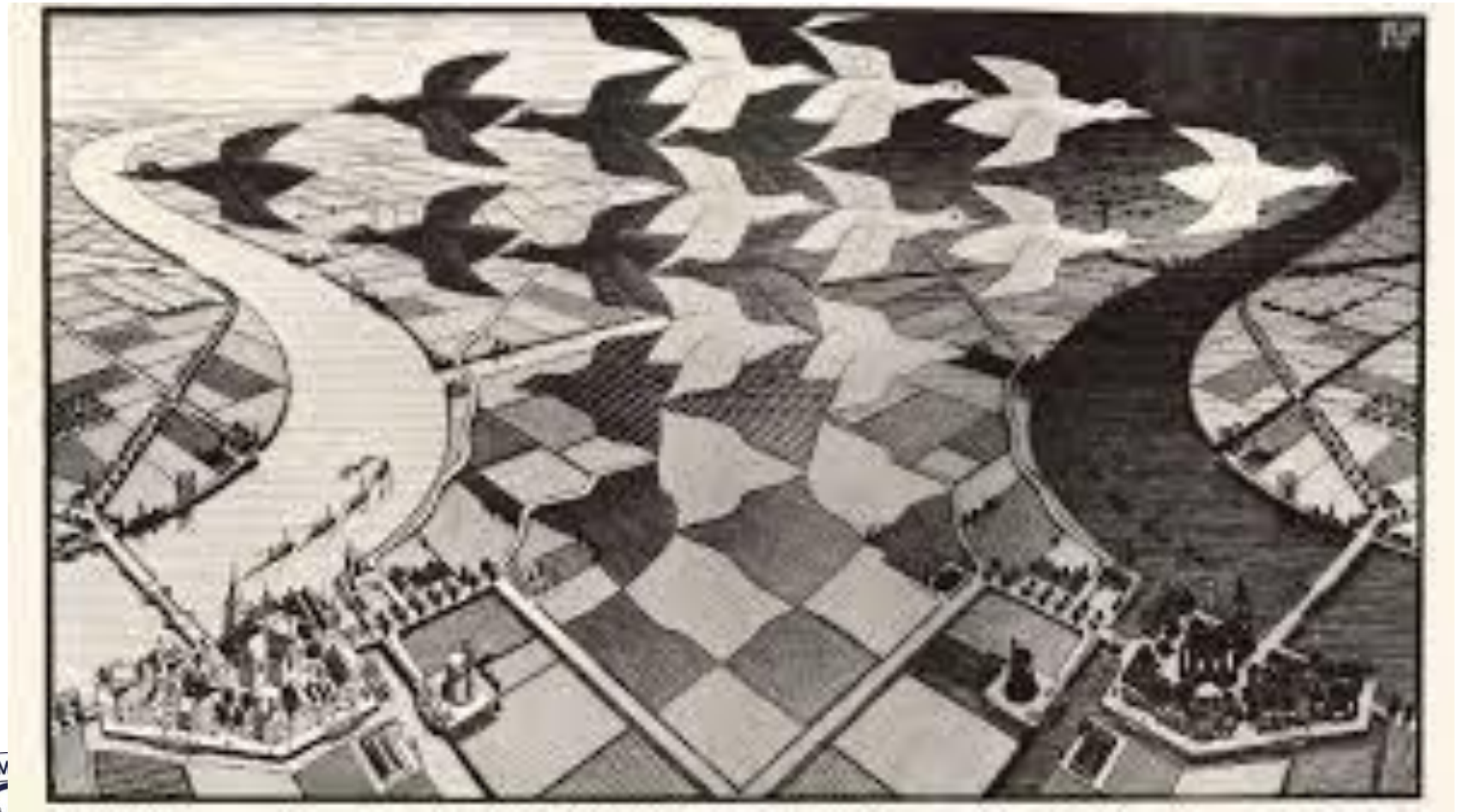
Cyber diffusion



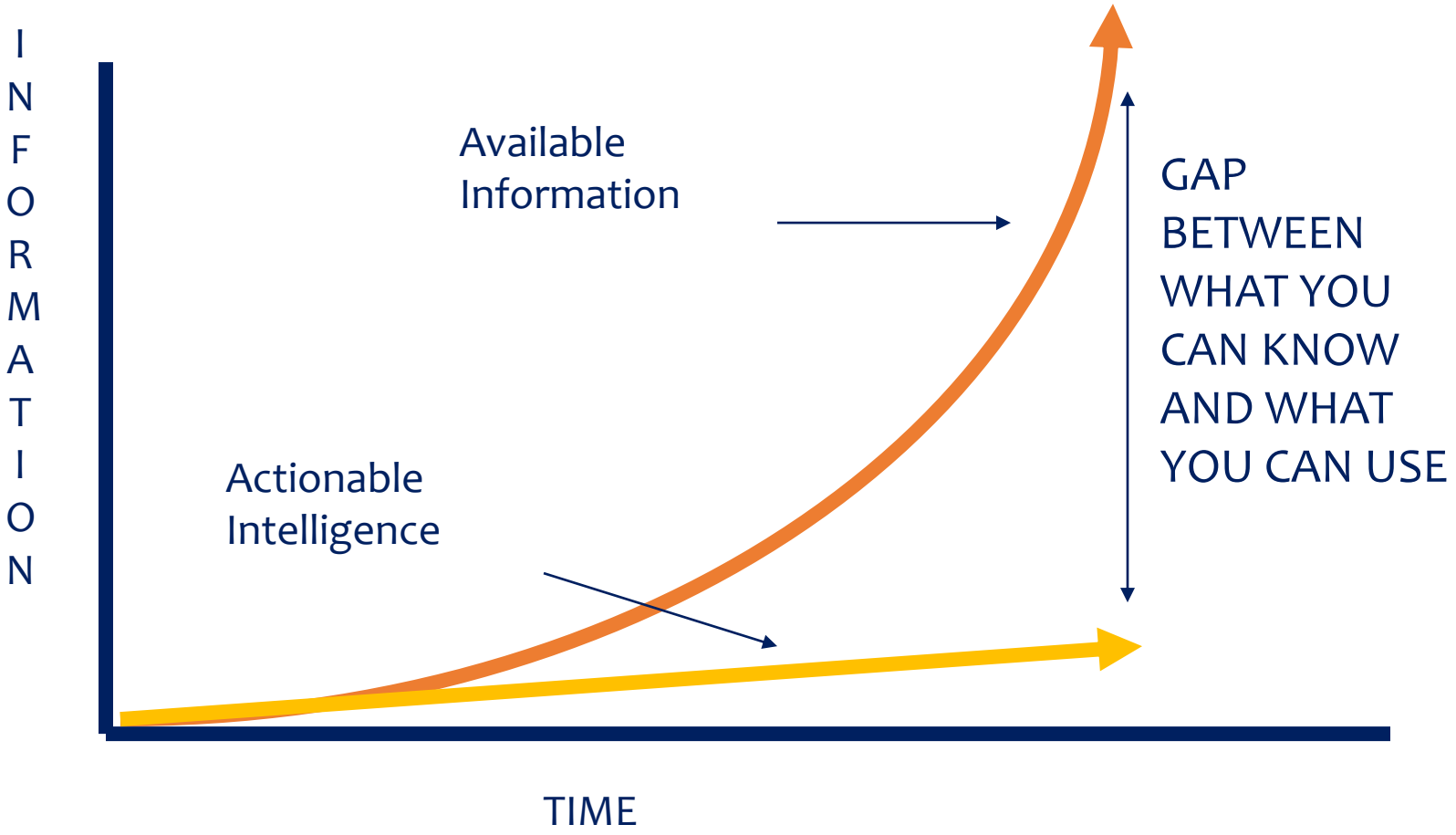
With the best Software Engineering techniques actually there is a bug rate of about 0,1 defects per KLOC

https://www.mayerdan.com/ruby/2012/11/11/bugs-per-line-of-code-ratio

Fluid border



NEW GAP


INFORMATION
Available Information
Actionable Intelligence
GAP BETWEEN WHAT YOU CAN KNOW AND WHAT YOU CAN USE
TIME

Fattore umano

Secondo lo studio di Proffpoint “the Human factor 2016” la tecnica di attacco più usata nel 2015 è stato il Social Engineering.

95%

Delle compromissioni a livello aziendale deriva da errore umano non intenzionale

Approccio "ALL HAZARD"

Si rende allora quanto mai necessario un approccio

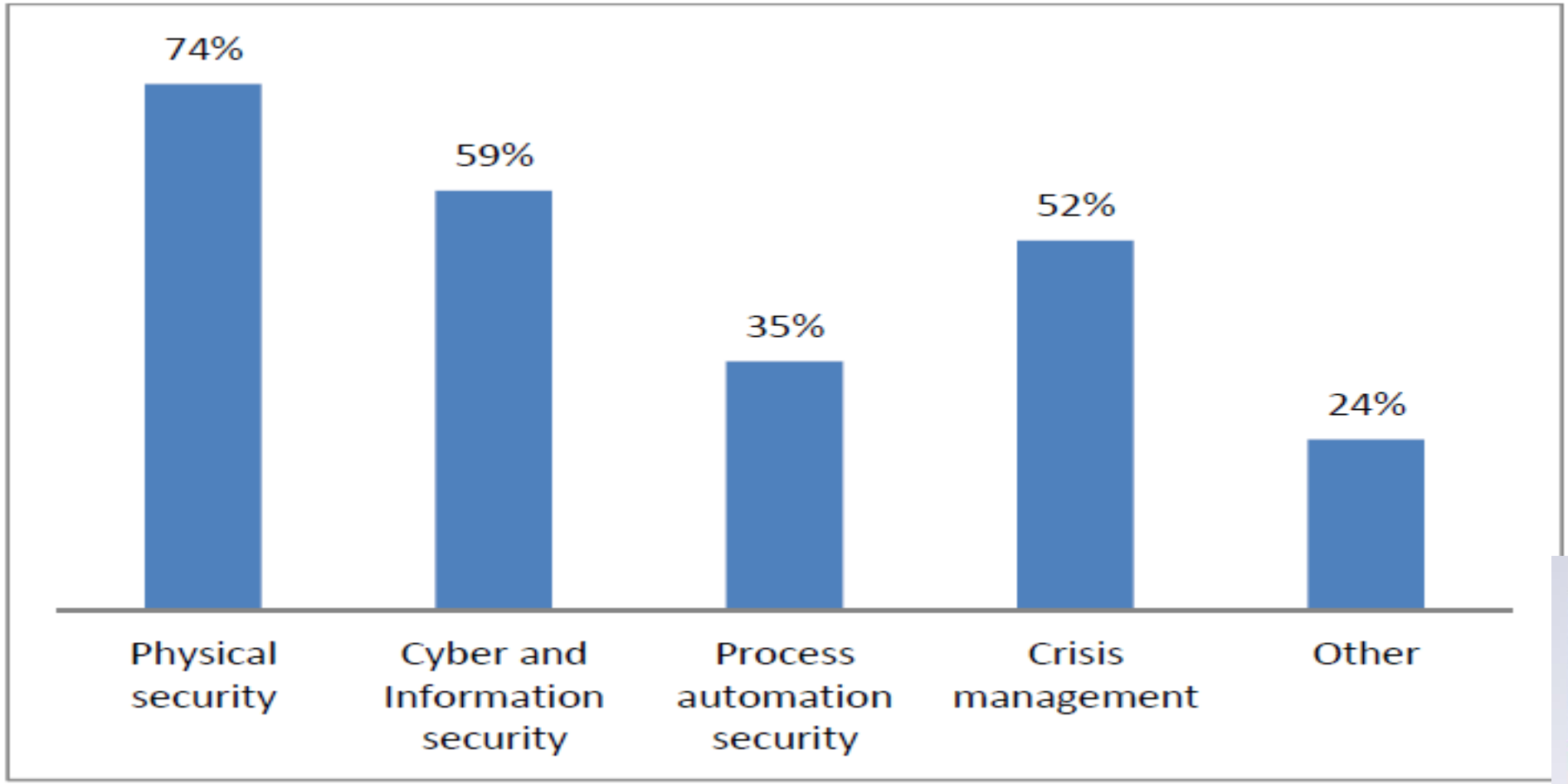
ALL HAZARD

focalizzato maggiormente sulle misure di riduzione delle **Conseguenze** e delle **Vulnerabilità**.

All-hazard : naturally occurring event, human induced events (both intentional and non-intentional) and technology caused events with potential impact on organization, community or society and environment on which it depends

Incident: any act or circumstance that produce consequences [ISO/CD 22300]

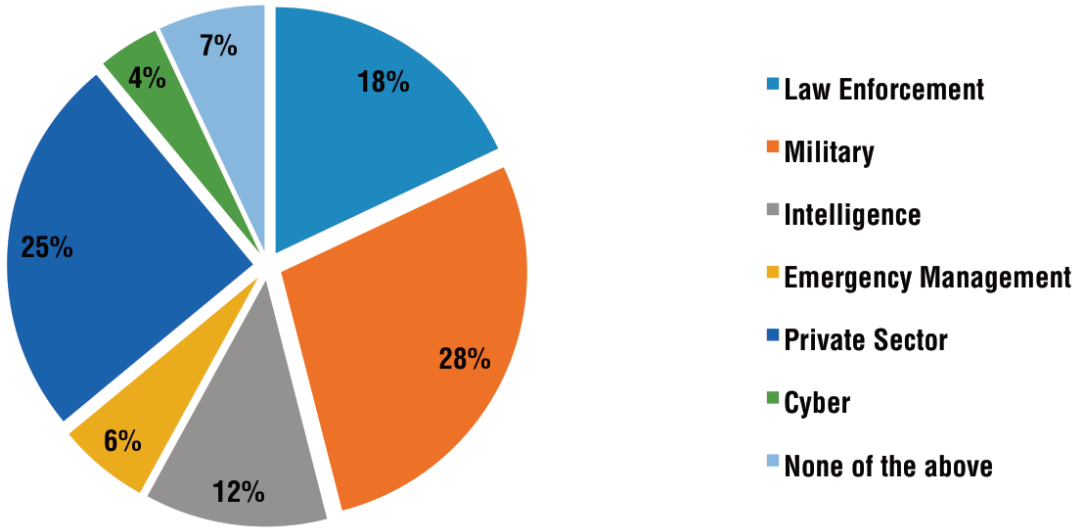
Topics managed by the security department



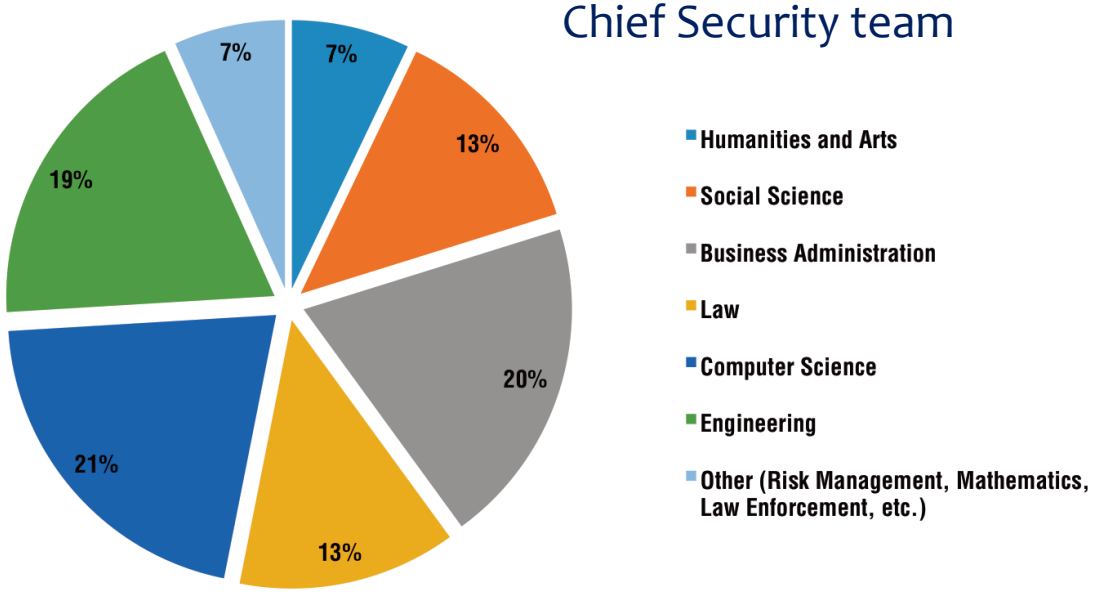
De Maggio, M. C., Mastrapasqua, M., Tesei, M., Chittaro, A., & Setola, R. (2019). How to Improve the Security Awareness in Complex Organizations. European Journal for Security Research, 4(1), 33-49..

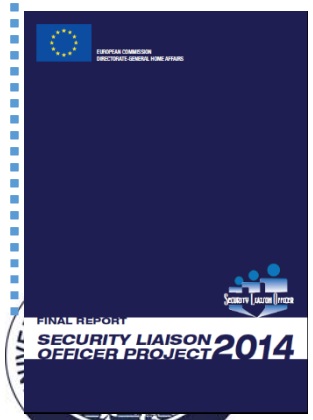
Background of people involved in the security division

Chief Security Officer



Chief Security team





De Maggio, M. C., Mastrapasqua, M., & Setola, R. (2015, October). The Professional Figure of the Security Liaison Officer in the Council Directive 2008/114/EC. In *International Conference on Critical Information Infrastructures Security* (pp. 211-222). Springer, Cham.

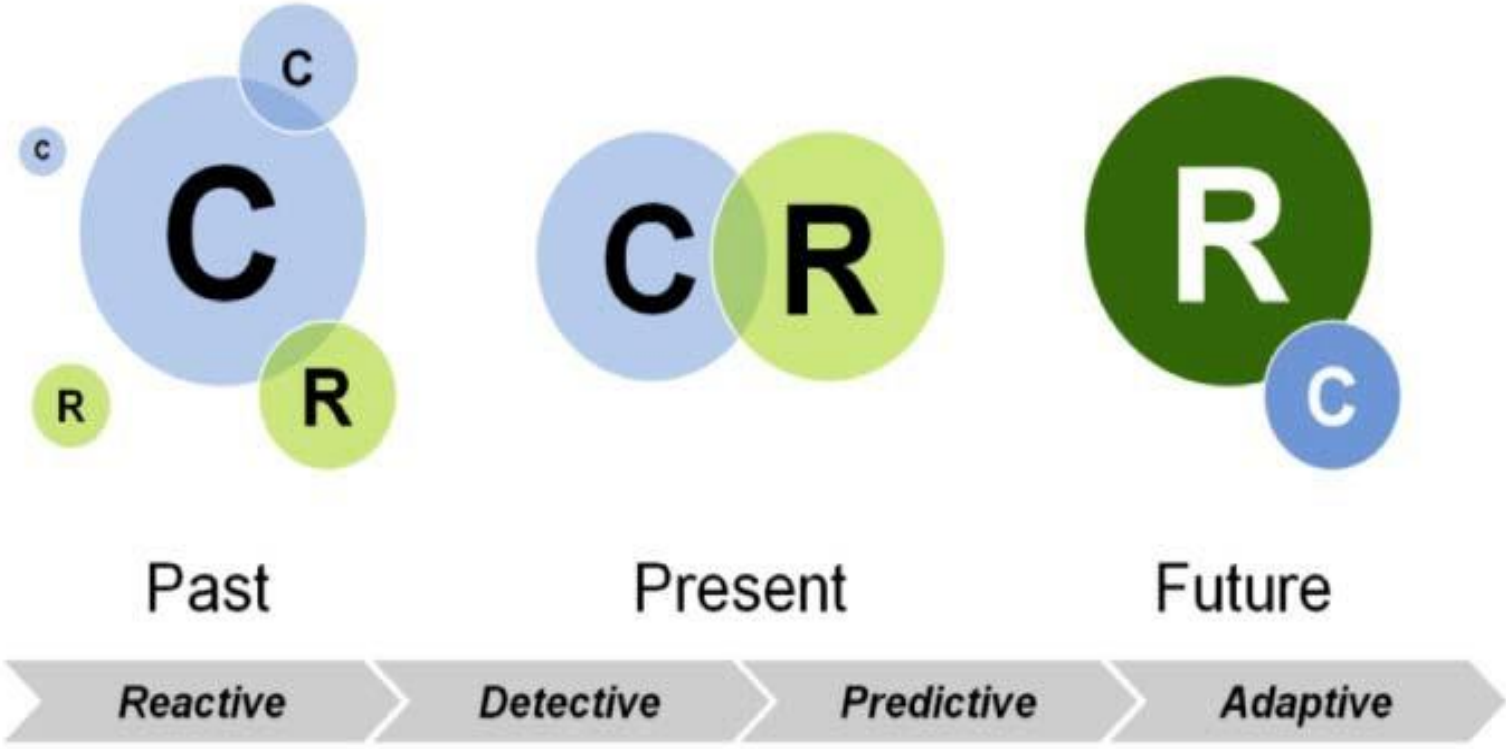
OdG 24 ottobre 2019 [p.f. Aresta]

[…] la *security*, **in una visione di sistema**, rappresenta una delle modalità con cui si attua un principio di rilevanza costituzionale, contenuto nell'articolo 41 della Carta fondamentale [...]

impegna il Governo

[…] stabilisca **un Sistema di gestione della sicurezza** (*security*) che preservi l'organizzazione da eventi pregiudizievoli – inclusi quelli che attengono alla sicurezza delle informazioni – assicurando il sostegno agli obiettivi delle politiche di sicurezza e la relativa conformità agli obblighi di legge, promuovendo la **cultura della *security*** e garantendo il presidio […] e designando un dirigente (***Security Manager***) incaricato di stabilire, mantenere, aggiornare un effettivo sistema di gestione della security assicurandogli i necessari poteri, le risorse umane e materiali per la gestione effettiva della sicurezza.

Compliance Is No Longer the Driver



Master in Homeland Security

Sistemi, metodi e strumenti per la security e il crisis management

XII edizione

Marzo 2020

HOMELAND SECURITY MASTER

Obiettivo finale

Fornire strumenti, metodologie e competenze per poter **valutare**, **pianificare**, **definire strategie** per gestire in modo *efficace* ed *efficiente* eventi anomali e/o di security (*all hazard*) e per poter essere in grado, in presenza di un tale evento, di gestirlo ……

… con improvvisazione (intelligenza, fantasia e creatività)

r.setola@unicampus.it