A.I.S.I.S.
(Associazione Italiana Sistemi Informativi in Sanità)

X Conferenza Nazionale sui Dispositivi Medici
18 / 19 DICEMBRE 2017 ROMA
AUDITORIUM ANTONIANUM - VIALE MANZONI, 1

Cybersecurity nella sanità digitale e dell'IoT: la splendida opportunità di una tempesta perfetta

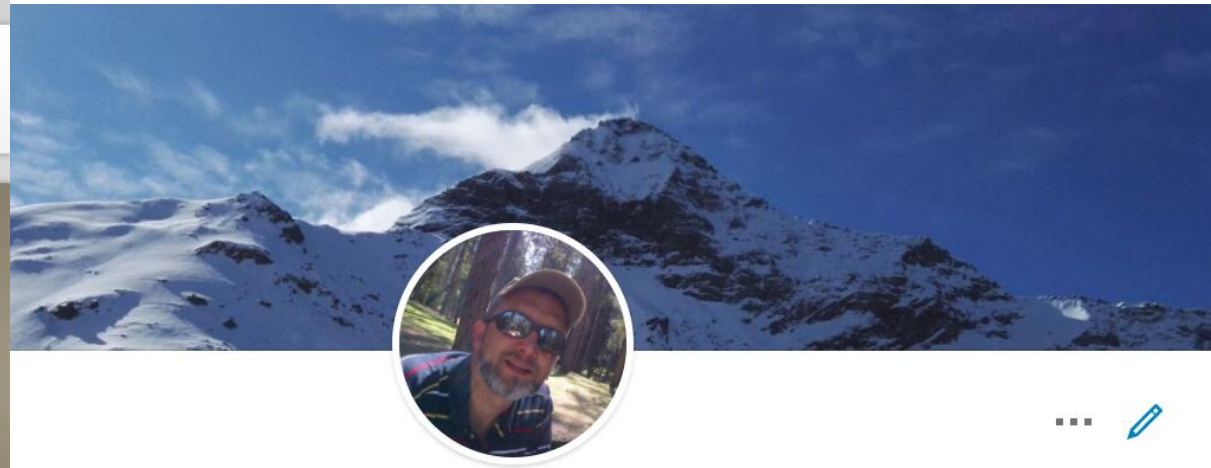
ovvero: La Battaglia delle 5 armate

(G. Pozza – Presidente di AISIS e C.I.O. IRCCS Ospedale S. Raffaele)

Agenda

- Presentazione
- Dove siamo (tempesta e opportunità perfetta)
- Tre paradossi
- Approccio olistico (no linea Maginot!)
- Una battaglia… e una proposta

Presentazione



Giuliano Pozza

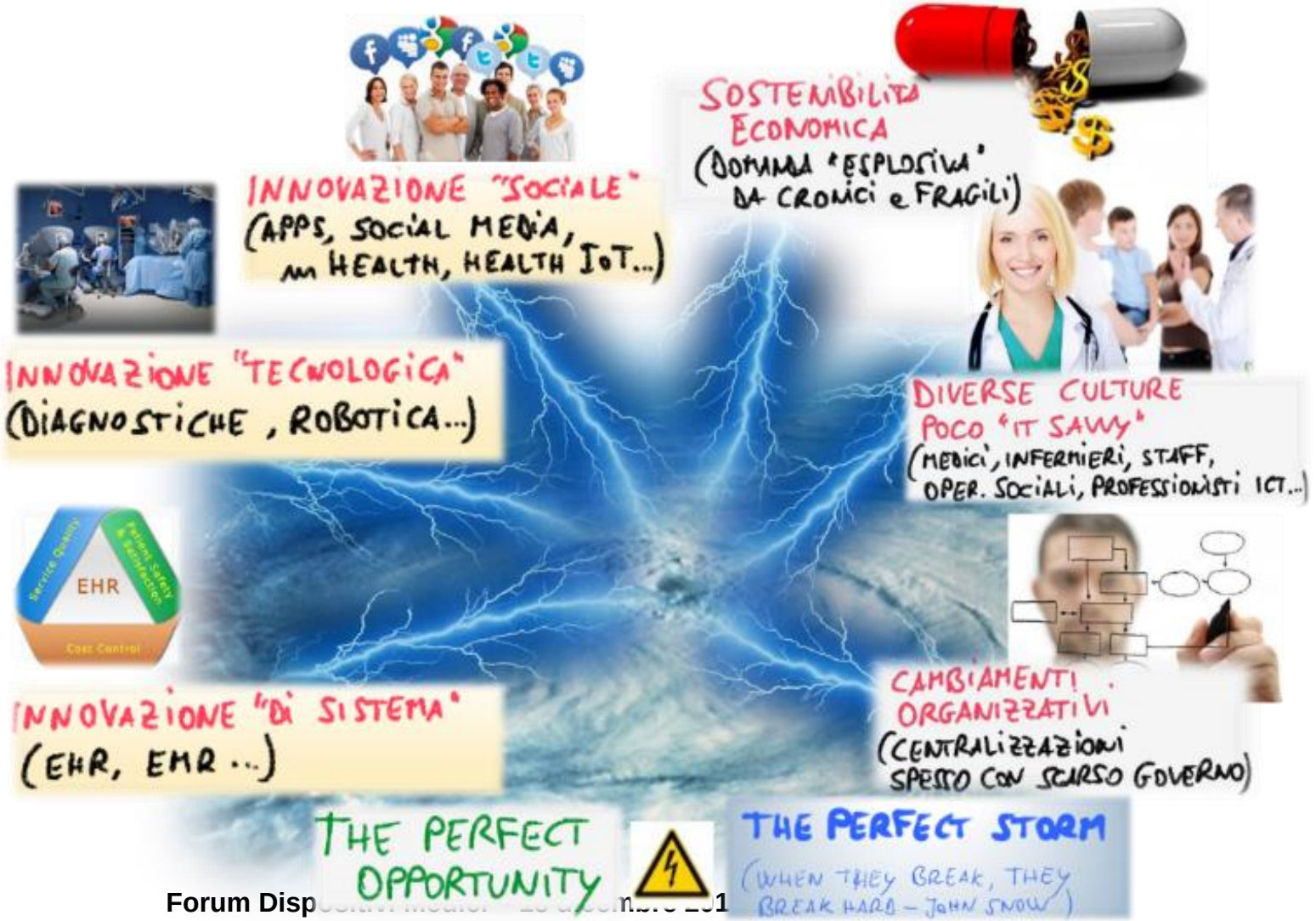
Chief Information Officer at Ospedale San Raffaele - Presidente di AISIS (Associazione Italiana S.I. in Sanità)

Ospedale San Raffaele • Politecnico di Milano

Milan Area, Italy • 500+

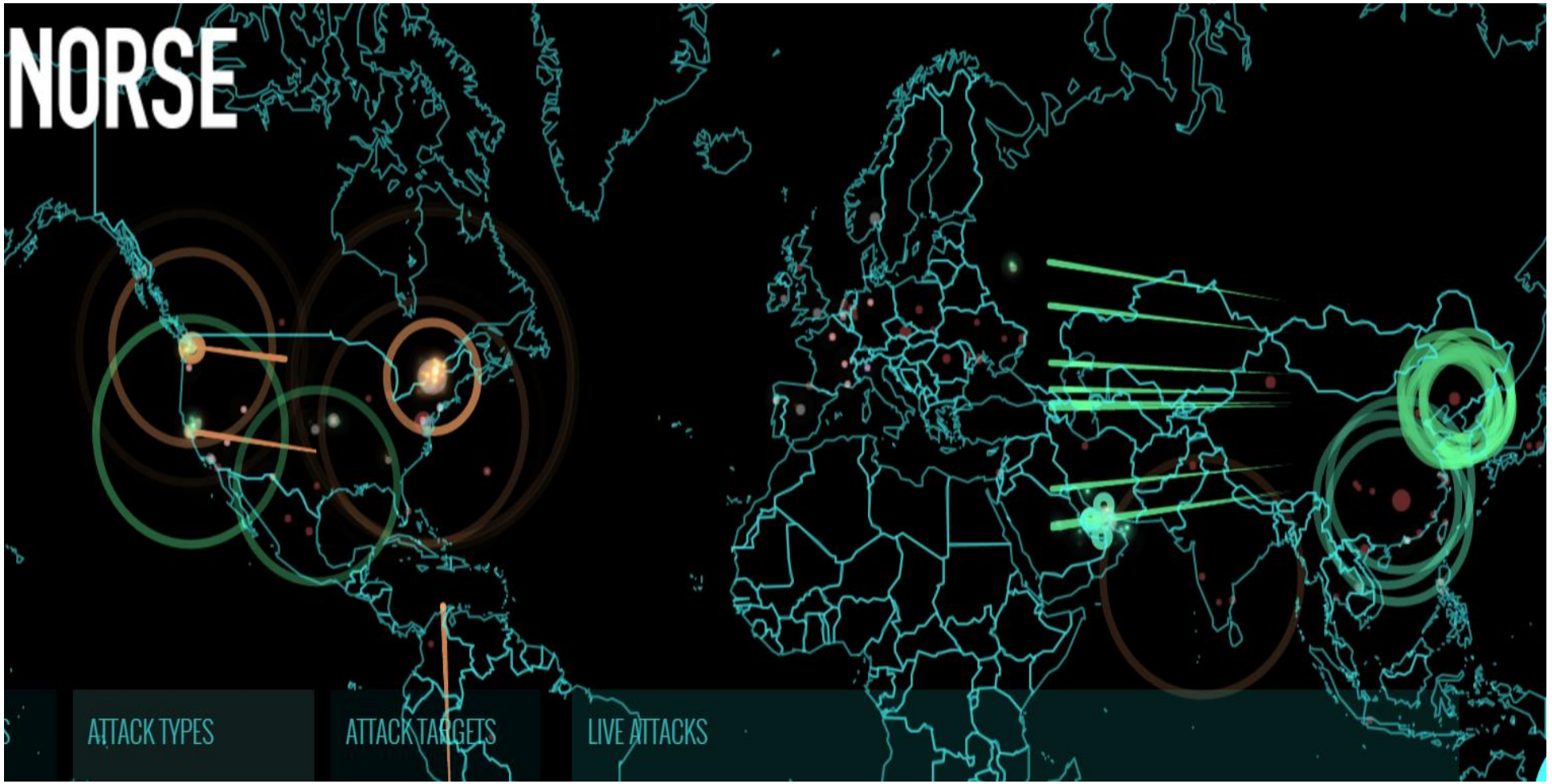
Chief Information Officer with experience in IT strategy definition and execution in complex and challenging environments.

Dove siamo: la **tempesta** (o l'opportunità) perfetta (1/5)



Fonte: L'insostenibile Leggerezza del C.I.O. (Bellini – Dalle Rive- Pozza – Squizzato ed: AICA /Mondo Digitale)

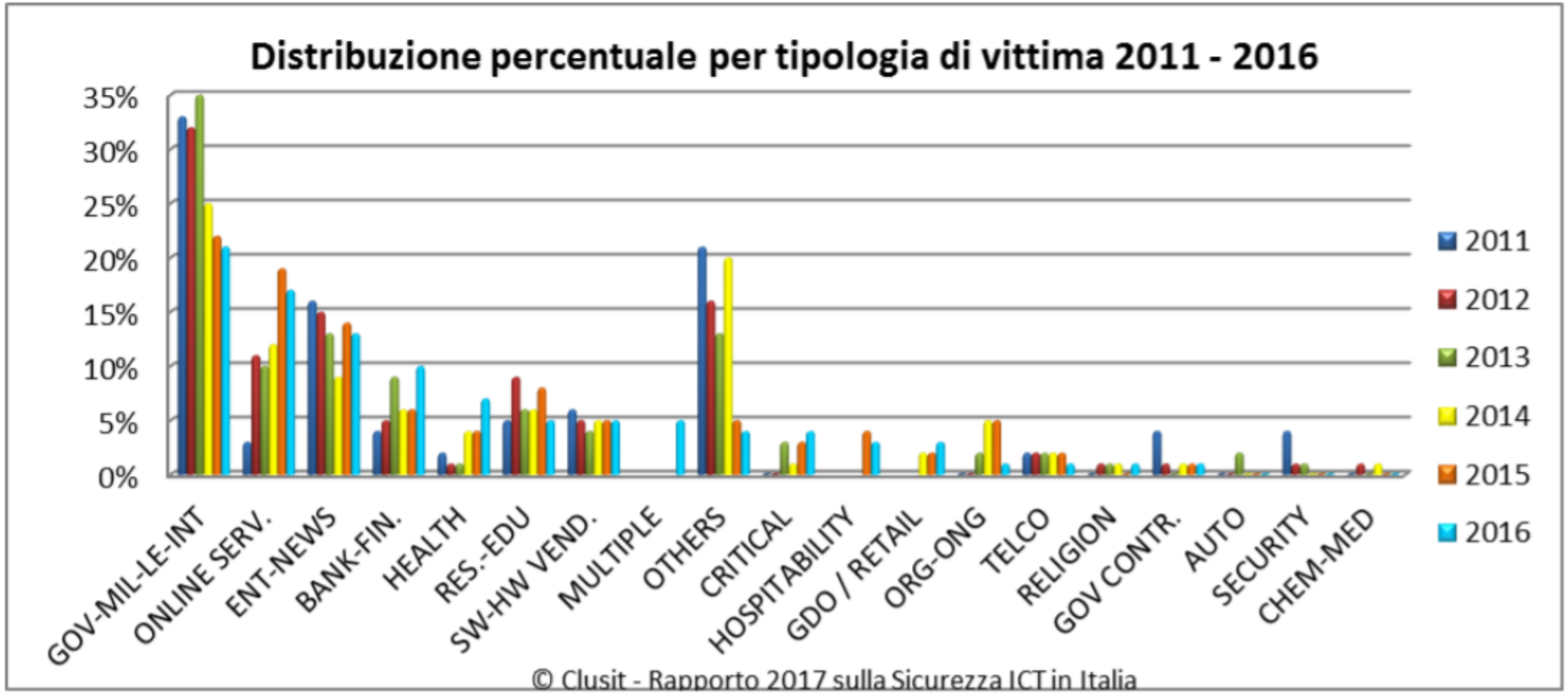
Dove siamo: la **tempesta** (o l'opportunità) perfetta (2/5)



(http://map.norsecorp.com)

Dove siamo: la **tempesta** (o l'opportunità) perfetta (3/5)

Rapporto CLUSIT 2017



Rispetto al 2015, nel 2016 la crescita percentuale maggiore di attacchi gravi si osserva verso le categorie "Health" (+102%), "GDO/Retail" (+70%) e "Banking / Finance" (+64%), seguite da "Critical Infrastructures" (+15%).

Dove siamo: la **tempesta** (o l'opportunità) perfetta (4/5)

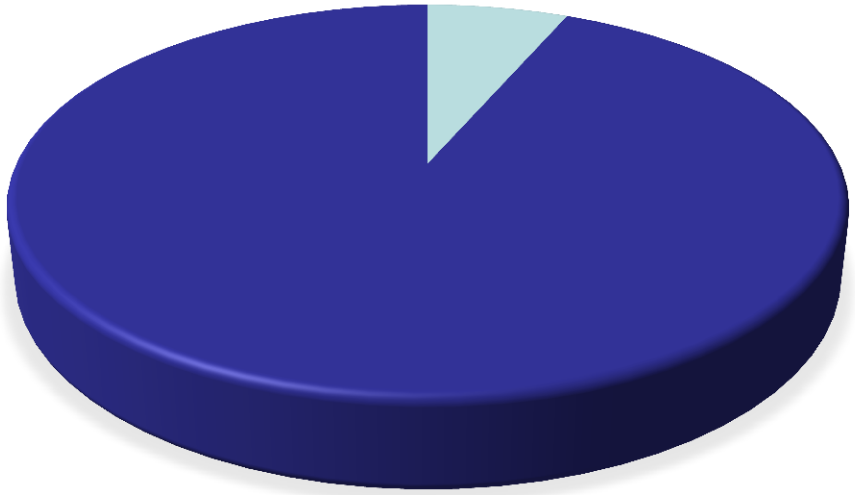
United States EMR Adoption Model SM			
Stage	Cumulative Capabilities	2015 Q3	2015 Q4
Stage 7	Complete EMR; CCD transactions to share data; Data warehousing; Data continuity with ED, ambulatory, OP	4.1%	4.2%
Stage 6	Physician documentation (structured templates), full CDSS (variance & compliance), full R-PACS	25.4%	27.1%
Stage 5	Closed loop medication administration	34.6%	35.9%
Stage 4	CPOE, Clinical Decision Support (clinical protocols)	10.3%	10.1%
Stage 3	Nursing/clinical documentation (flow sheets), CDSS (error checking), PACS available outside Radiology	17.3%	16.4%
Stage 2	CDR, Controlled Medical Vocabulary, CDS, may have Document Imaging; HIE capable	3.4%	2.6%
Stage 1	Ancillaries - Lab, Rad, Pharmacy - All Installed	1.8%	1.7%
Stage 0	All Three Ancillaries Not Installed	3.1%	2.1%
Data from HIMSS Analytics® Database ©2014		N = 5454	N = 5460

Dove siamo: la **tempesta** (o l'opportunità) perfetta (5/5)

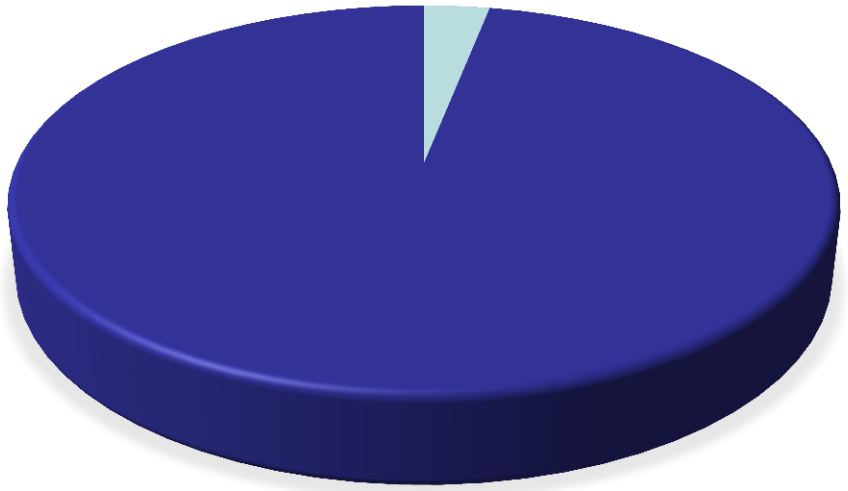
Tre paradossi

- PARADOSSO #1: «Ci son più cose in cielo e in terra, Orazio, che non sogni la tua filosofia» (Amleto). Ossia: ci sono più informazioni nello «shadow IT» che nell'IT Ufficiale. Due esempi (dati reali):

SERVIZI CLOUD (51 VS 730)



VOLUME IMMAGINI (20TB VS 631TB) [CASO REALE OSPEDALE]



Report CISCO 2015: Do You Know the Way to Ballylickey? Shadow IT and the CIO Dilemma – N. Earle

Tre paradossi

- PARADOSSO #2: In sanità, i sistemi più critici e i dati più sensibili dal punto di vista della sicurezza (sia come security che safety) sono in una «terra di nessuno»

(Download for free): http://mycourses.med.harvard.edu/ec_res/nt/880676B7-B74D-48B9-B6A3-0E91F7048E20/TheFifthDomain-Rel2.1-CC.pdf

NIST
Framework for Improving Critical Infrastructure Cybersecurity

FDA
Postmarket Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

ISACA Journal Volume 1, 2015

- Current Issue
- Practically Speaking Blog
- CPE Quizzes
- Submit an Article
- Advertise
- Editorial Calendar
- Read More on COBIT
- Archives
  - 2016
  - 2017
- Webinar Quiz Certificate

DOWNLOAD ARTICLE

Book Reviews

COMMENTS

The Fifth Domain: Wake Up Neo

Guiliano Pozza and John D. Halamka | Reviewed by Ibe Etea, CISA, CRISC, CA, CFE, CIA, CRMA

The Fifth Domain: Wake Up Neo, written by two chief information officers (CIOs), is an innovative experiment with the cybertechnology novel and is worth the attention of information security professionals. The two authors have tinkered with contemporary reality and plausible fiction to raise the stakes in knowledge transfer, using a leisurely but effective way of sharing information while piquing readers' interest in a highly technical field—the world of cybertechnology.

With the simplicity of a magazine article and a clearly defined purpose, the authors go about exploring key points about the scary, but real, nature of cyberthreats. These threats are most often overlooked in business, albeit actually lurking around every corner of this highly mechanized and computerized world.

The key characters are analyzed concisely in terms of their personalities and their professional lives in such a way that one empathizes with the characters and story, which develop further as the tale thickens. In this book, readers can connect with the characters they meet: their fears, routines, concerns and intrigues.

Tre paradossi

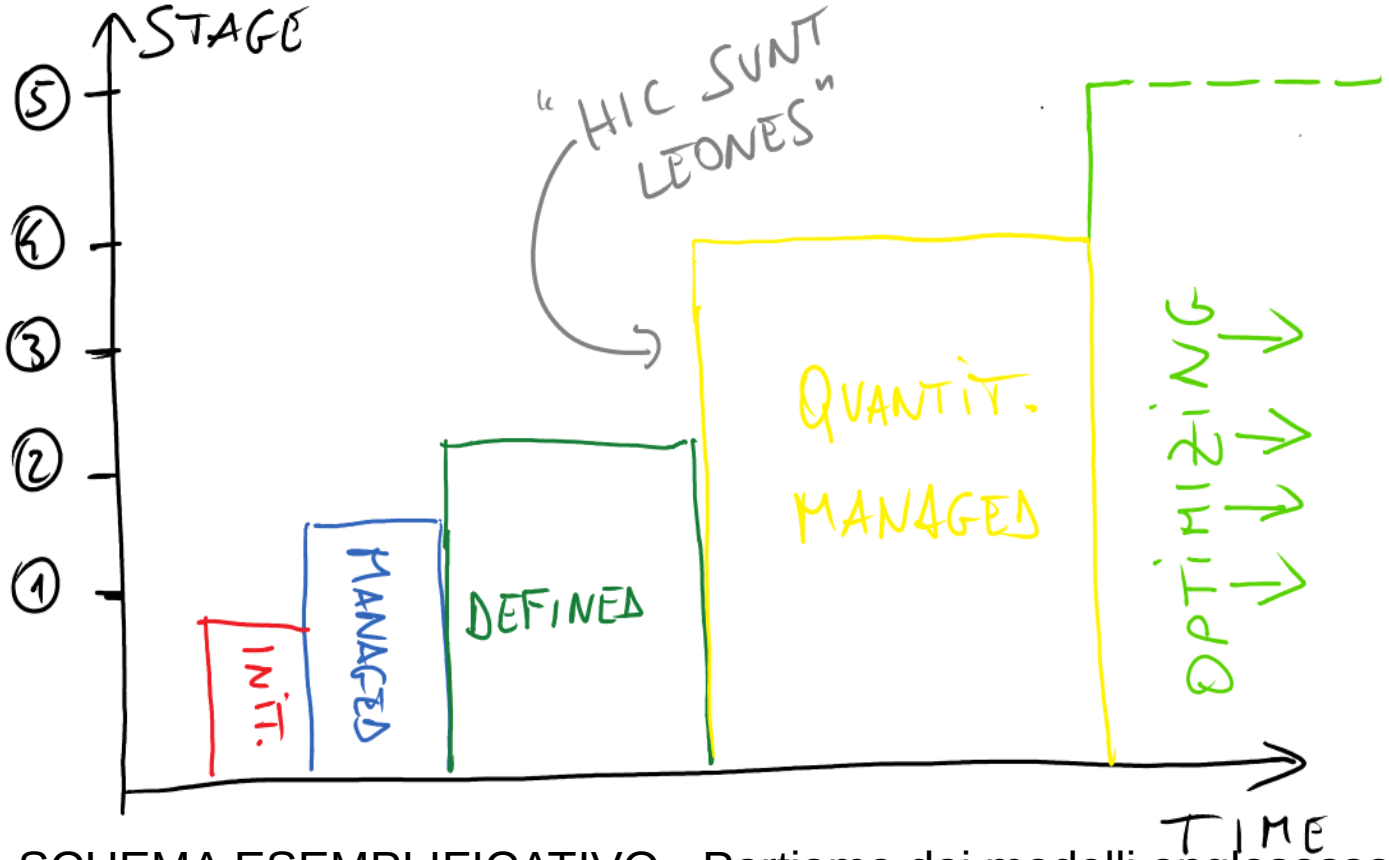
- PARADOSSO #3: I C.I.O. stanno lavorando febbrilmente (pro GDPR e non solo) per fortificare la cittadella… ma non c'è più alcuna cittadella da difendere!

Approccio olistico (NO LINEA MAGINOT)

Approccio olistico (poche e semplici regole tecniche)

- Esempi di interventi TECNICI (spunti):
  - **Patching** questo sconociuto (e.g. wanna cry - NHS)
  - **Cifratura** per comunicazione (sempre, non solo per gli impiantabili)
  - **AI e analisi dei pattern** per identificare pericoli in modo preventivo
  - **Gestione password** e identità digitali
  - **«Firma» del sw installato** per immodificabilità
  - In sintesi: **security «by design»** (altrimenti recall: rischio e costi)
- Ma il 90% della sicurezza è data da:
  - Organizzazione e Processi
  - Competenze e consapevolezza
  - Strategia e Governance

Un percorso possibile… (1/3): organizzazione e processi



Stage 1 (INITIAL): gestione locale non strutturata

Stage 2 (MANAGED): gestione sicurezza ICT strutturata, altre aree (e.g. Medical Devices, ricerca, building automation…) coperte in modo sporadico/non gestite

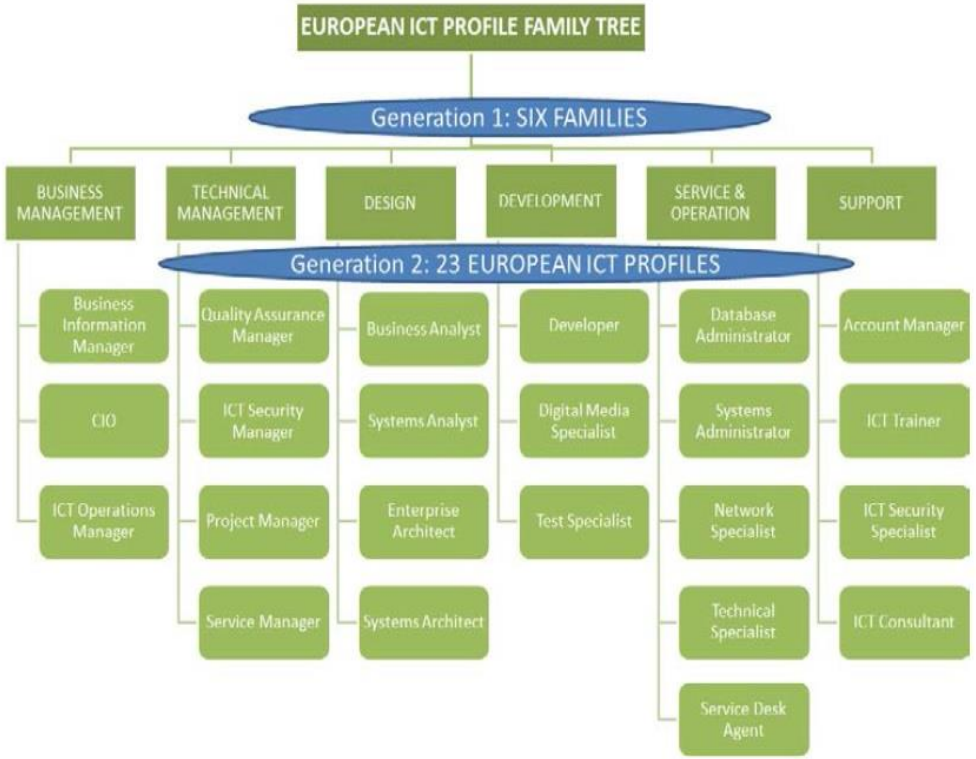
Stage 3 (DEFINED): azioni coordinate tra i diversi "gestori di tecnologie informatiche" (ICT, Area tecnica, Ingegneria Clinica). Nessuna organizzazione trasversale dedicate alla sicurezza

Stage 4 (QUANTITATIVELY MANGED): esiste un ruolo "cross" di responsabile della sicurezza (tipicamente un C.I.S.O. che risponde all'AD) a 360°

Stage 5 (OPTIMIZING): strategia di sicurezza convergente: i dipartimenti tech dell'ospedale sono sotto un'unica responsabilità e la sicurezza e la governance hanno approccio olistico

SCHEMA ESEMPLIFICATIVO - Partiamo dai modelli anglosassoni (NIST) ed elaboriamo Nostro percorso con modello di maturità

Un percorso possibile… (2/3): e-CF (con AICA) per certificare le COMPETENZE



BENEFICI per gli attori coinvolti:

- **ICT Professionals:** profili definiti che chiariscono le competenze
- **Ing. Clinici:** almeno una figura nella loro organizzazione deve avere competenze informatiche trasversali (e.g. sicurezza)
- **Fornitori:** mappare le competenze in ambito sicurezza e colmare i GAP permetterebbe di fare la «security by design» e «by default» del GDPR

Un percorso possibile… (3/3): eHealthAcademy (con SDA Bocconi): consapevolezza su strategia e governance

Giorno 1

(NASI/POZZA/CACCIA: 9:30-10:00)
Introduzione al corso

(CACCIA: 10:00 – 13:00)
Nuovi scenari di contesto, nuovi fabbisogni informativi

(LONGO: 14:30-17:30)
Dinamiche evolutive del settore della sanità

Giorno 2

(POZZA: 9:00-13:00)
Governare i Sistemi Informativi nell'era della sanità elettronica

(NEW - 2018)
Cybersecurity nella sanità digitale e dell'IoT

Giorno 3

(SALVIOTTI/FARACI: 9:00-17:00)
Digital transformation e digital innovation

DEVO Lab HIT Radar (con MIT)

Esercitazione: Digital Innovation in sanità

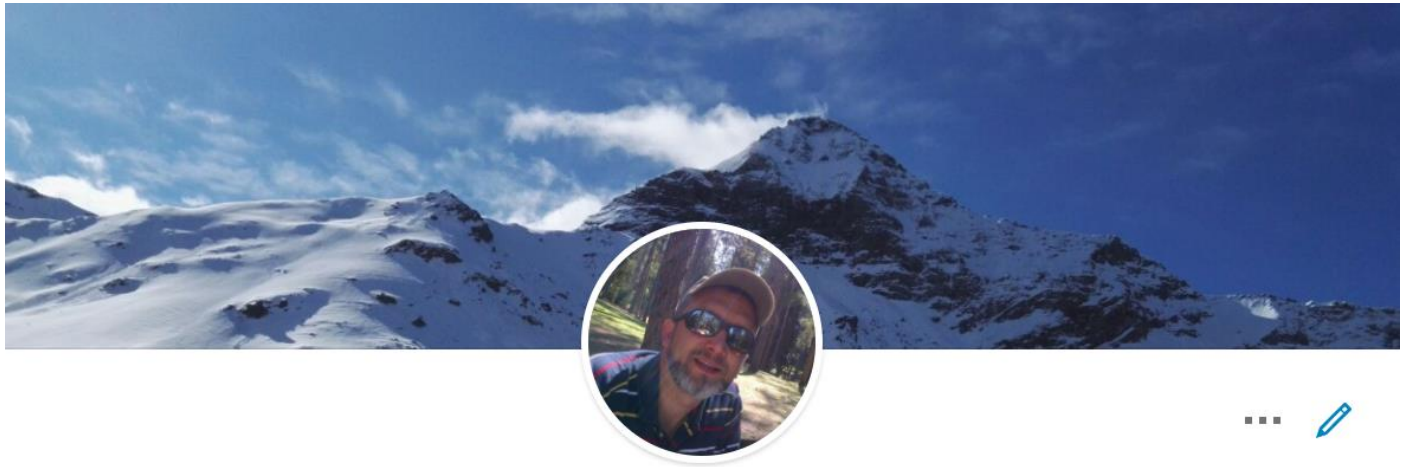
(NASI-CACCIA-POZZA: 17:00-17:30)
Chiusura del corso

Per affrontare la battaglia delle 5 armate…

…una proposta

- Tavolo di lavoro delle tre armate: Associazioni (AISIS, AIIC, associazioni in ambito sicurezza…), Istituzioni (Ministero, AGID…), Fornitori (di sistemi informativi, medical devices, sicurezza)
- Come AISIS mettiamo a disposizione percorsi di certificazione (e-CF con AICA) e di formazione (Governance con SDA Bocconi) sperimentati. L'esperienza insegna che percorsi di «ibridazione» che mettano insieme figure diverse hanno enorme valore.
- Documento congiunto su Cybersecurity & IoT in sanità con modello di maturità e framework (partendo da modelli anglosassoni)
- Osservatorio per il monitoraggio della «maturità», degli eventi avversi ma anche delle buone pratiche

Riferimenti



Giuliano Pozza

Chief Information Officer at Ospedale San Raffaele - Presidente di AISIS
(Associazione Italiana S.I. in Sanità)

Ospedale San Raffaele • Politecnico di Milano

Milan Area, Italy • 500+

Chief Information Officer with experience in IT strategy definition and execution in complex and challenging environments.

segreteria@aisis.it
Presidenza@aisis.it