ASSOCIAZIONE ITALIANA
SISTEMI INFORMATIVI IN SANITÀ

Cybersecurity in Healthcare

ASSOCIAZIONE ITALIANA
SISTEMI INFORMATIVI IN SANITÀ

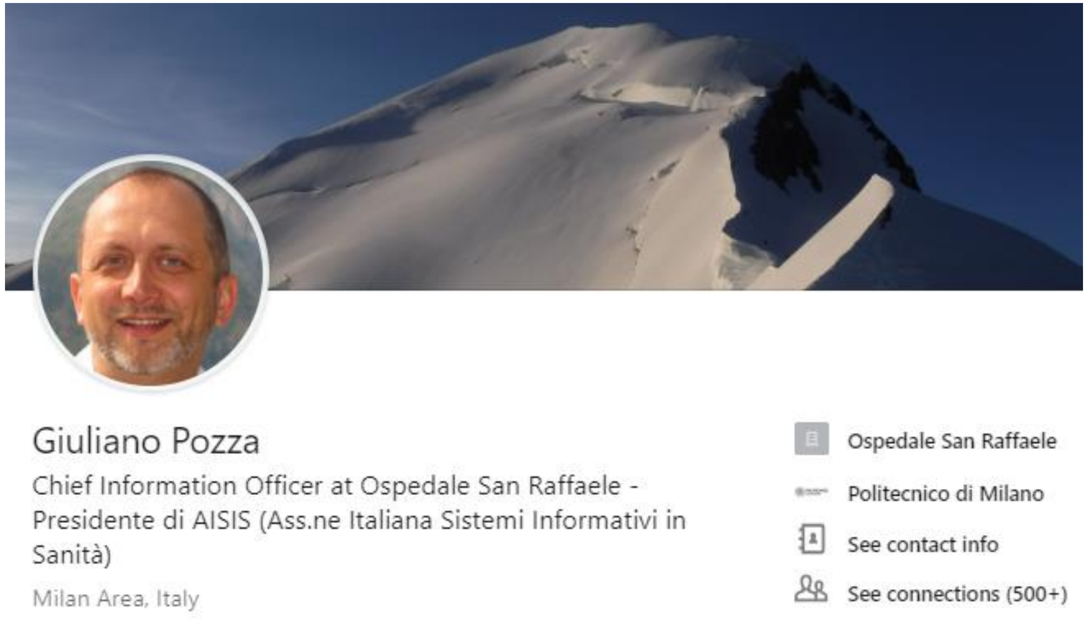
Three Paradoxes and the Need for a Paradigm Shift

XVIII International Symposium on Progress in Clinical Pacing – Rome Dec. 4 2018

Introducing myself…

Giuliano Pozza

- President of A.I.S.I.S. (Italian Association of Healthcare Information Systems Professionals– www.aisis.it)
- C.I.O. Ospedale S. Raffaele
- Biomedical Engineer



Giuliano Pozza

Chief Information Officer at Ospedale San Raffaele - Presidente di AISIS (Ass.ne Italiana Sistemi Informativi in Sanità)

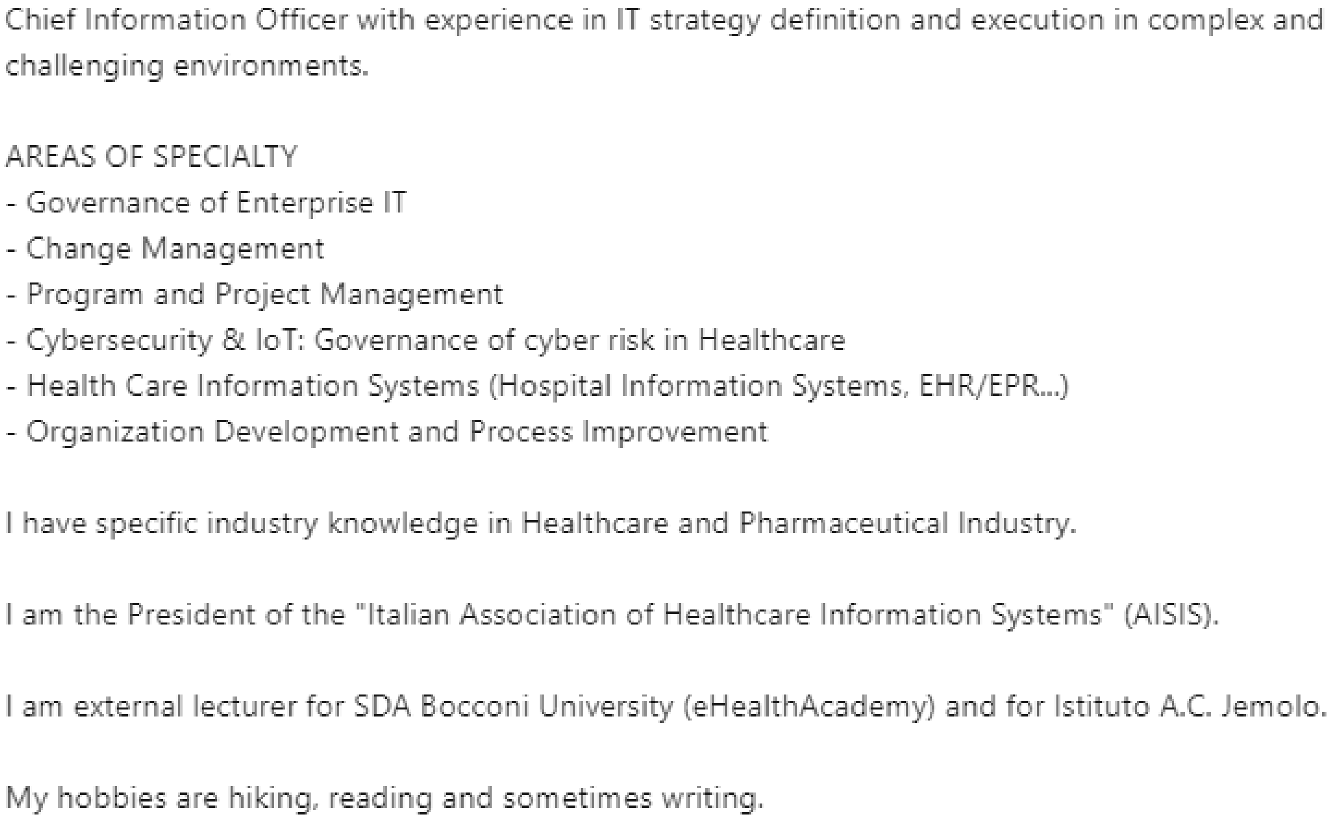
Milan Area, Italy

Ospedale San Raffaele

Politecnico di Milano

See contact info

See connections (500+)



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

AREAS OF SPECIALTY
- Governance of Enterprise IT
- Change Management
- Program and Project Management
- Cybersecurity & IoT: Governance of cyber risk in Healthcare
- Health Care Information Systems (Hospital Information Systems, EHR/EPR...)
- Organization Development and Process Improvement

I have specific industry knowledge in Healthcare and Pharmaceutical Industry.

I am the President of the "Italian Association of Healthcare Information Systems" (AISIS).

I am external lecturer for SDA Bocconi University (eHealthAcademy) and for Istituto A.C. Jemolo.

My hobbies are hiking, reading and sometimes writing.

www.linkedin.com/in/gpozza/

www.yottabronto.net

… and AISIS

About AISIS

The Italian organization of healthcare information systems managers (AISIS) was founded in 2003 to promote the development of IT professionals and the strategic role of Information Technology in healthcare. It currently has over 500 members ranging from CIOs to non-technical e-Leaders. AISIS organizes events, training courses (AISIS eHealth Academy), research programs (eHealthLab) and is also active in the promotion of a social and philanthropic approach to healthcare IT (AISIS4Social). AISIS operates in association with other national and international organizations. For more information, please visit www.aisis.it.

Annual event: Digital Health Summit with LifeTech Forum (www.digitalhealthsummit.it)

Main Partnerships:

- AICA
- AIIC
- AITASIT
- ASSD
- CHIME (https://chimecentral.org/chime-and-aisis-announce-plans-to-launch-chapter-in-italy/)
- Ethos.it
- FIASO
- GHT
- HIMSS
- Istituto Superiore Sanità
- LifeTech Forum
- Osservatorio Innovazione Digitale in Sanità del Politecnico di Milano
- SDA Bocconi School of Management
- …

Agenda

- The Context: Cybersecurity in Healthcare
- Three paradoxes
  - Are There More Things in Shadow IT Than in Official IT?
  - In Healthcare, a Large and Growing Amount of Sensitive Data and the Most Dangerous and Potentially Life-Threatening Systems Are, From the Security Perspective, in a “No Man’s Land”
  - CIOs Are Working Hard to Fortify the Walls of the Citadel, but There Is no Citadel to Defend
- Paradigm Shift Ahead!
  - The light and the dark side
  - We need a risk based approach
  - The human factor
  - A good start
- Q&A

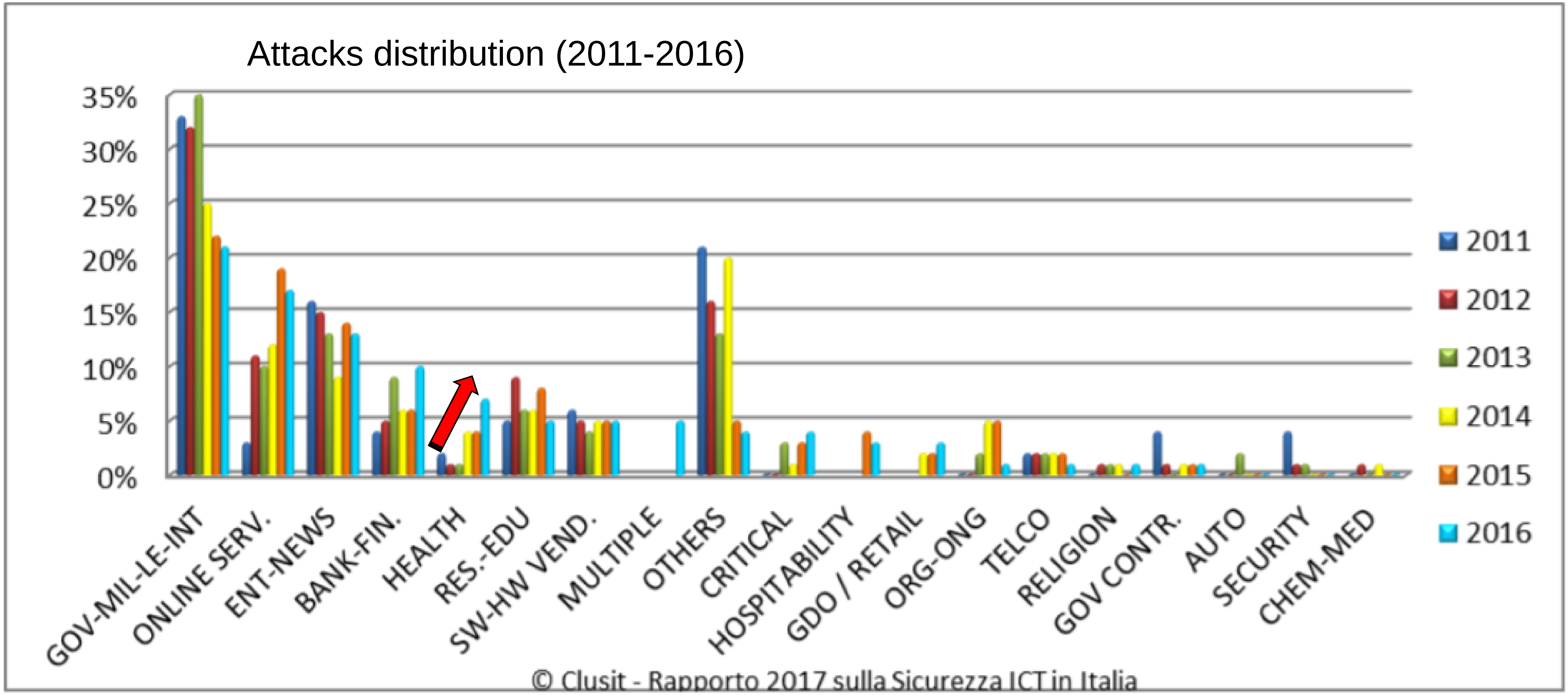
War games…

(The battle of the black gate)

(https://threatmap.fortiguard.com - http://www.norse-corp.com/map/ - www.digitalattackmap.com)

Healthcare under attack!

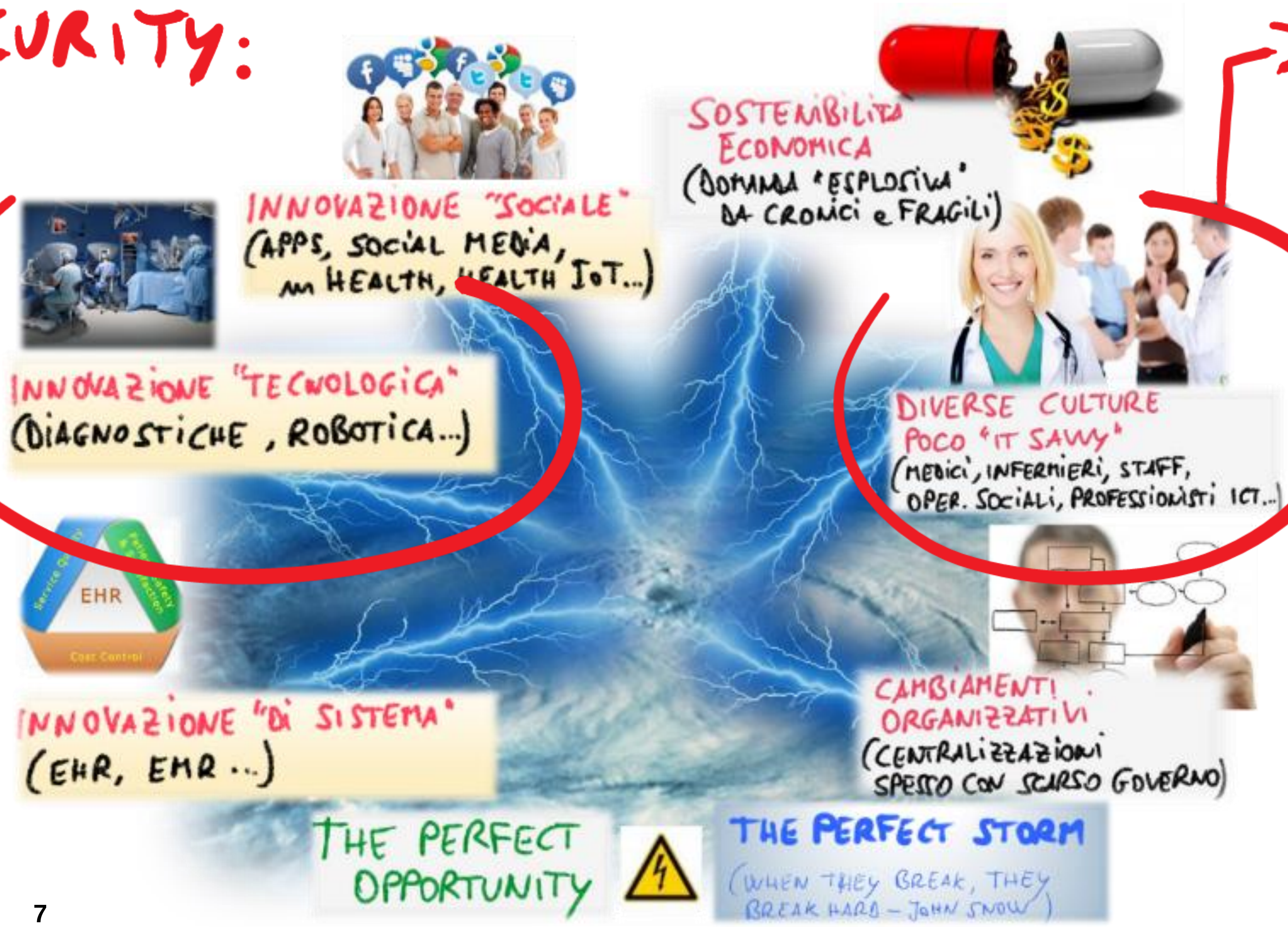
Source: Rapporto CLUSIT 2017



Healthcare: The perfect storm

IT SECURITY:

→ HEALTH CARE



INNOVAZIONE "SOCIALE"
(APPS, SOCIAL MEDIA, m HEALTH, HEALTH IoT...)

SOSTENIBILITÀ ECONOMICA
(DOMANDA 'ESPLOSIVA' DA CRONICI e FRAGILI)

INNOVAZIONE "TECNOLOGICA"
(DIAGNOSTICHE, ROBOTICA...)

DIVERSE CULTURE
POCO "IT SAVVY"
(MEDICI, INFERMIERI, STAFF, OPER. SOCIALI, PROFESSIONISTI ICT...)

INNOVAZIONE "DI SISTEMA"
(EHR, EMR...)

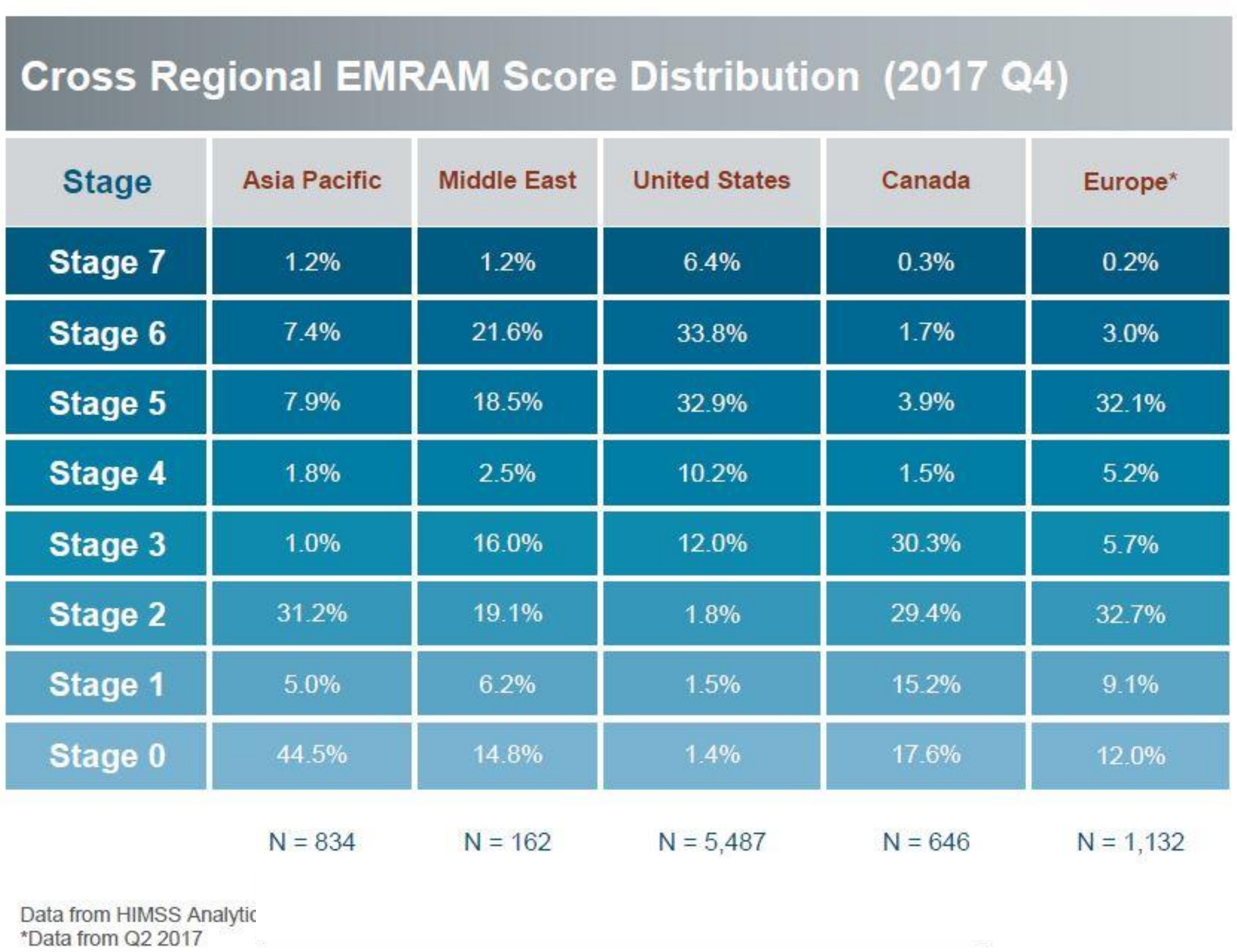
CAMBIAMENTI ORGANIZZATIVI
(CENTRALIZZAZIONI SPESSO CON SCARSO GOVERNO)

THE PERFECT OPPORTUNITY

THE PERFECT STORM
(WHEN THEY BREAK, THEY BREAK HARD – JOHN SNOW)

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

Healthcare: The perfect opportunity



Cross Regional EMRAM Score Distribution (2017 Q4)

Stage	Asia Pacific	Middle East	United States	Canada	Europe*
Stage 7	1.2%	1.2%	6.4%	0.3%	0.2%
Stage 6	7.4%	21.6%	33.8%	1.7%	3.0%
Stage 5	7.9%	18.5%	32.9%	3.9%	32.1%
Stage 4	1.8%	2.5%	10.2%	1.5%	5.2%
Stage 3	1.0%	16.0%	12.0%	30.3%	5.7%
Stage 2	31.2%	19.1%	1.8%	29.4%	32.7%
Stage 1	5.0%	6.2%	1.5%	15.2%	9.1%
Stage 0	44.5%	14.8%	1.4%	17.6%	12.0%
	N = 834	N = 162	N = 5,487	N = 646	N = 1,132

Data from HIMSS Analytic
*Data from Q2 2017

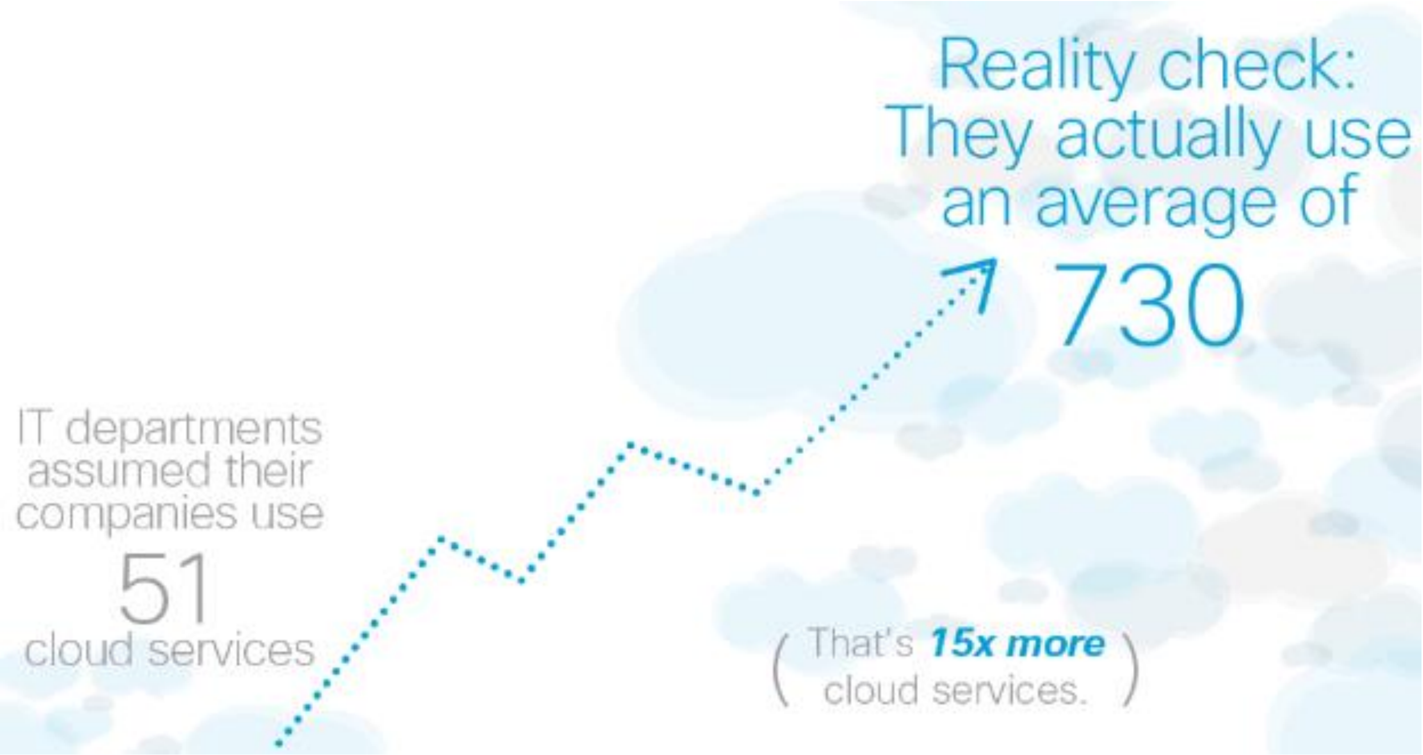
ITALY:
- 6 LEVEL 6 HOSPITALS
- ALMOST ALL BELOW LEVEL 3

Agenda

- The Context: Cybersecurity in Healthcare
- Three paradoxes
  - Are There More Things in Shadow IT Than in Official IT?
  - In Healthcare, a Large and Growing Amount of Sensitive Data and the Most Dangerous and Potentially Life-Threatening Systems Are, From the Security Perspective, in a “No Man’s Land”
  - CIOs Are Working Hard to Fortify the Walls of the Citadel, but There Is no Citadel to Defend
- Paradigm Shift Ahead!
  - The light and the dark side
  - We need a risk based approach
  - The human factor
  - A good start
- Q&A

Paradox #1

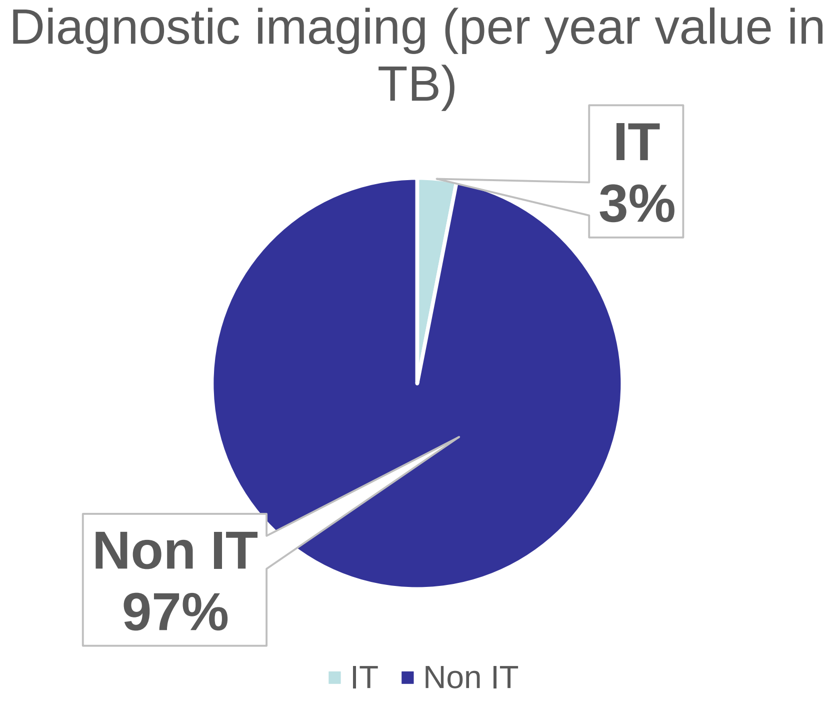
Are There More Things in Shadow IT Than in Official IT?



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

Real life example: diagnostic imaging in an hospital:

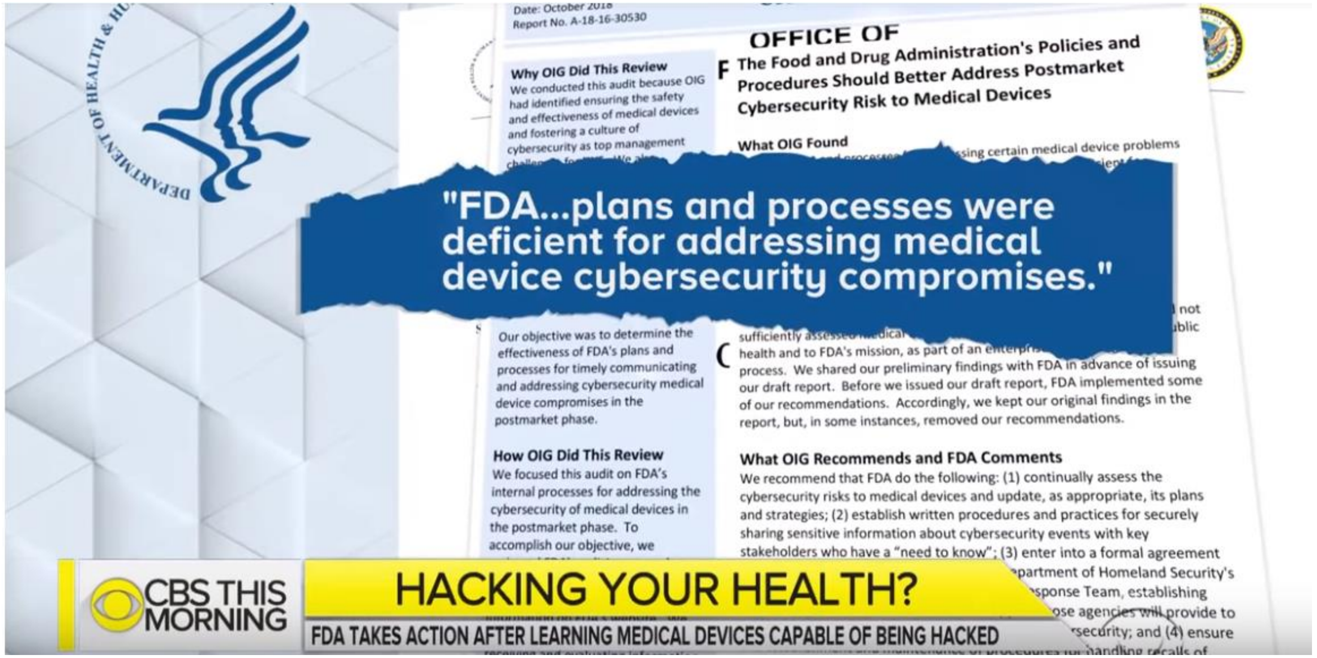
20TB Managed by IT (RIS-PACS), 631TB not managed by IT (or not managed?)



Paradox #2

In Healthcare, a Large and Growing Amount of Sensitive Data and the Most Dangerous and Potentially Life-Threatening Systems Are, From the Security Perspective, in a “No Man’s Land”

https://www.youtube.com/watch?v=smhPhmNsvVc



Date: October 2018
Report No. A-18-16-30530

OFFICE OF

The Food and Drug Administration's Policies and Procedures Should Better Address Postmarket Cybersecurity Risk to Medical Devices

Why OIG Did This Review
We conducted this audit because OIG had identified ensuring the safety and effectiveness of medical devices and fostering a culture of cybersecurity as top management

What OIG Found
sing certain medical device problems

"FDA...plans and processes were deficient for addressing medical device cybersecurity compromises."

Our objective was to determine the effectiveness of FDA's plans and processes for timely communicating and addressing cybersecurity medical device compromises in the postmarket phase.

not
sufficiently ablic
health and to FDA's mission, as part of an
process. We shared our preliminary findings with FDA in advance of issuing our draft report. Before we issued our draft report, FDA implemented some of our recommendations. Accordingly, we kept our original findings in the report, but, in some instances, removed our recommendations.

How OIG Did This Review
We focused this audit on FDA’s internal processes for addressing the cybersecurity of medical devices in the postmarket phase. To accomplish our objective, we

What OIG Recommends and FDA Comments
We recommend that FDA do the following: (1) continually assess the cybersecurity risks to medical devices and update, as appropriate, its plans and strategies; (2) establish written procedures and practices for securely sharing sensitive information about cybersecurity events with key stakeholders who have a “need to know”; (3) enter into a formal agreement
partment of Homeland Security's
sponse Team, establishing
ose agencies will provide to
security; and (4) ensure
handling recalls of

DEPARTMENT OF HEALTH & HU
CBS THIS MORNING
HACKING YOUR HEALTH?
FDA TAKES ACTION AFTER LEARNING MEDICAL DEVICES CAPABLE OF BEING HACKED

Top 10 Health Technology Hazards for 2018
health DEVICES
ECRI Institute

Top 10 Health Technology Hazards for 2018 ECRI Institute

1. **Ransomware and Other Cybersecurity Threats to Healthcare Delivery Can Endanger Patients**
2. Endoscope Reprocessing Failures Continue to Expose Patients to Infection Risk
3. Mattresses and Covers May Be Infected by Body Fluids and Microbiological Contaminants
4. Missed Alarms May Result from Inappropriately Con gured Secondary Noti cation Devices and Systems
5. Improper Cleaning May Cause Device Malfunctions, Equipment Failures, and Potential for Patient Injury
6. …

Paradox #3

CIOs Are Working Hard to Fortify the Walls of the Citadel, but There Is no Citadel to Defend

WE (C.I.O.s) THINK WE ARE HERE

BUT... → WE ARE HERE

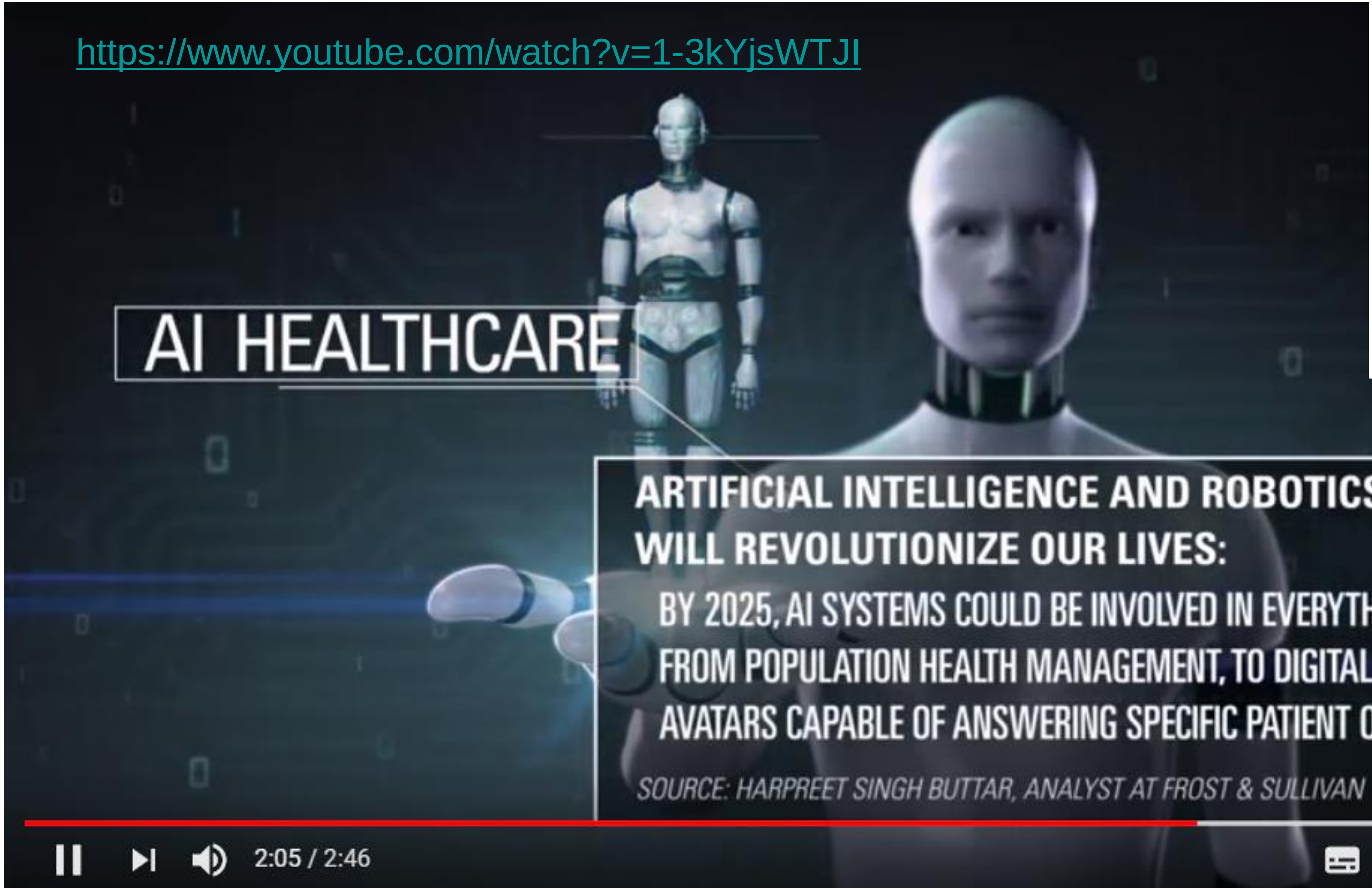
BEST ANALOGY: WWW.THREATSPROJECT.EU

Agenda

- The Context: Cybersecurity in Healthcare
- Three paradoxes
  - Are There More Things in Shadow IT Than in Official IT?
  - In Healthcare, a Large and Growing Amount of Sensitive Data and the Most Dangerous and Potentially Life-Threatening Systems Are, From the Security Perspective, in a "No Man's Land"
  - CIOs Are Working Hard to Fortify the Walls of the Citadel, but There Is no Citadel to Defend
- Paradigm Shift Ahead!
  - The light and the dark side
  - We need a risk based approach
  - The human factor
  - A good start
- Q&A

Technology will dramatically improve our lives…

https://www.youtube.com/watch?v=1-3kYjsWTJI



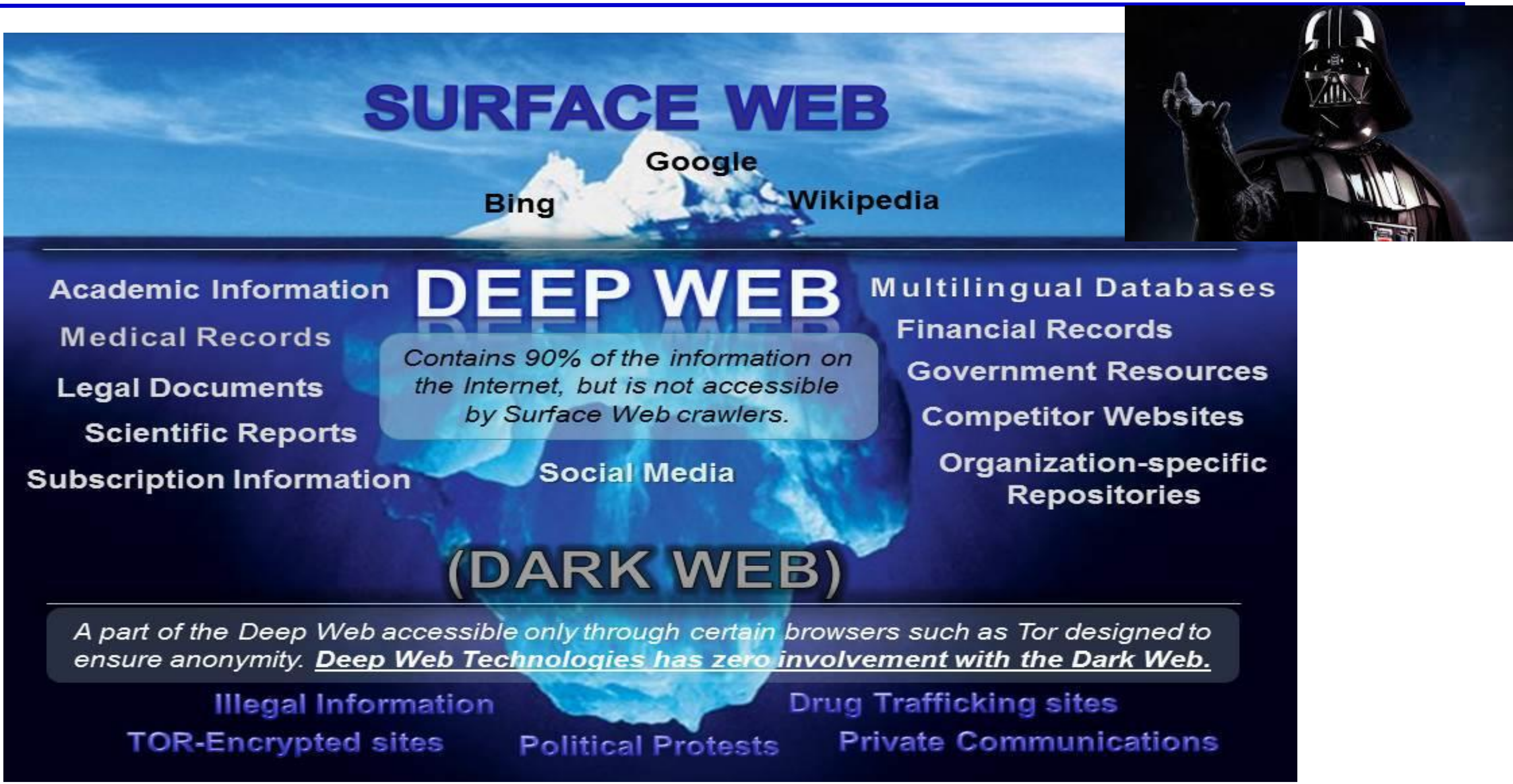
AI HEALTHCARE

ARTIFICIAL INTELLIGENCE AND ROBOTICS WILL REVOLUTIONIZE OUR LIVES:

BY 2025, AI SYSTEMS COULD BE INVOLVED IN EVERYTHING FROM POPULATION HEALTH MANAGEMENT, TO DIGITAL AVATARS CAPABLE OF ANSWERING SPECIFIC PATIENT QUERIES.

SOURCE: HARPREET SINGH BUTTAR, ANALYST AT FROST & SULLIVAN

…but there is a dark side!



SURFACE WEB

Google

Bing

Wikipedia

DEEP WEB

Academic Information

Medical Records

Legal Documents

Scientific Reports

Subscription Information

Contains 90% of the information on the Internet, but is not accessible by Surface Web crawlers.

Social Media

Multilingual Databases

Financial Records

Government Resources

Competitor Websites

Organization-specific Repositories

(DARK WEB)

A part of the Deep Web accessible only through certain browsers such as Tor designed to ensure anonymity. **Deep Web Technologies has zero involvement with the Dark Web.**

Illegal Information

TOR-Encrypted sites

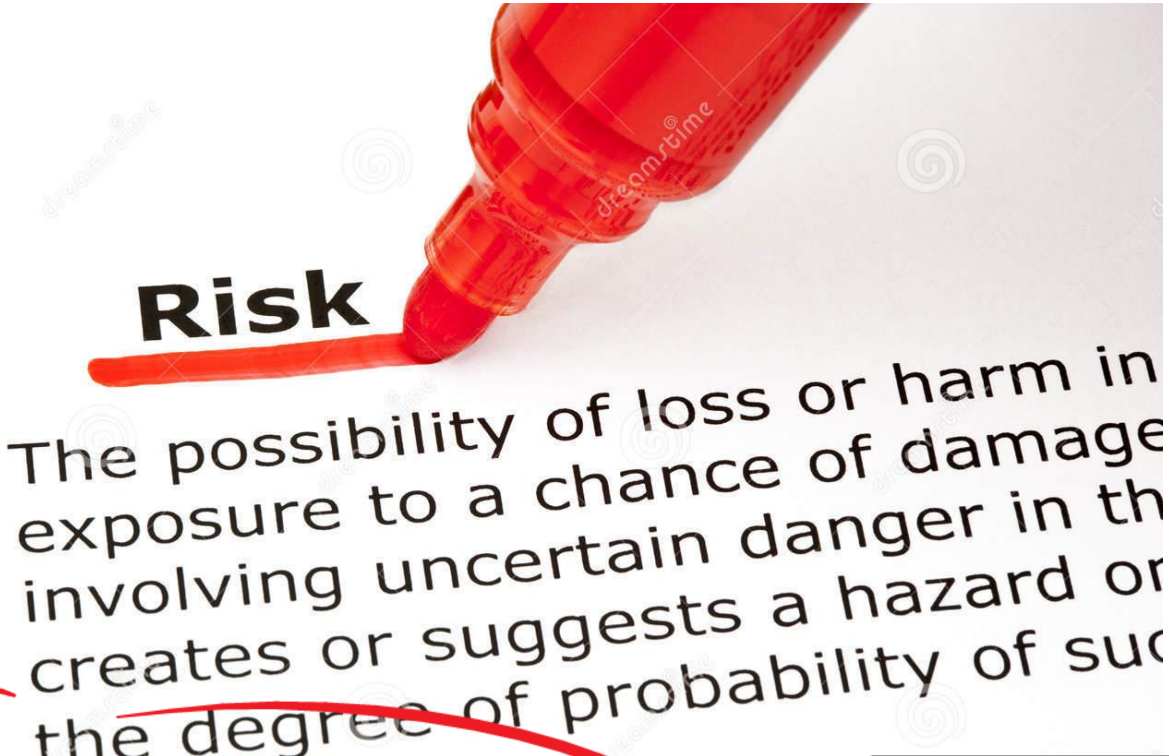
Political Protests

Drug Trafficking sites

Private Communications

We need a Risk based approach

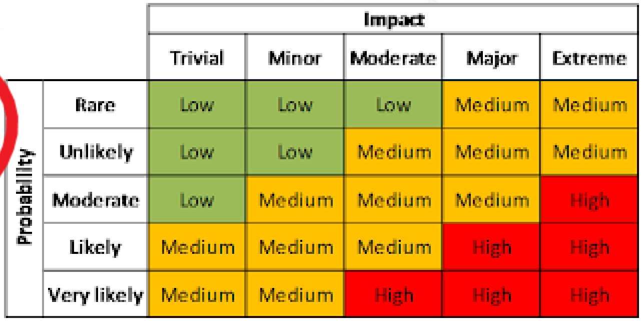
Definition



Risk

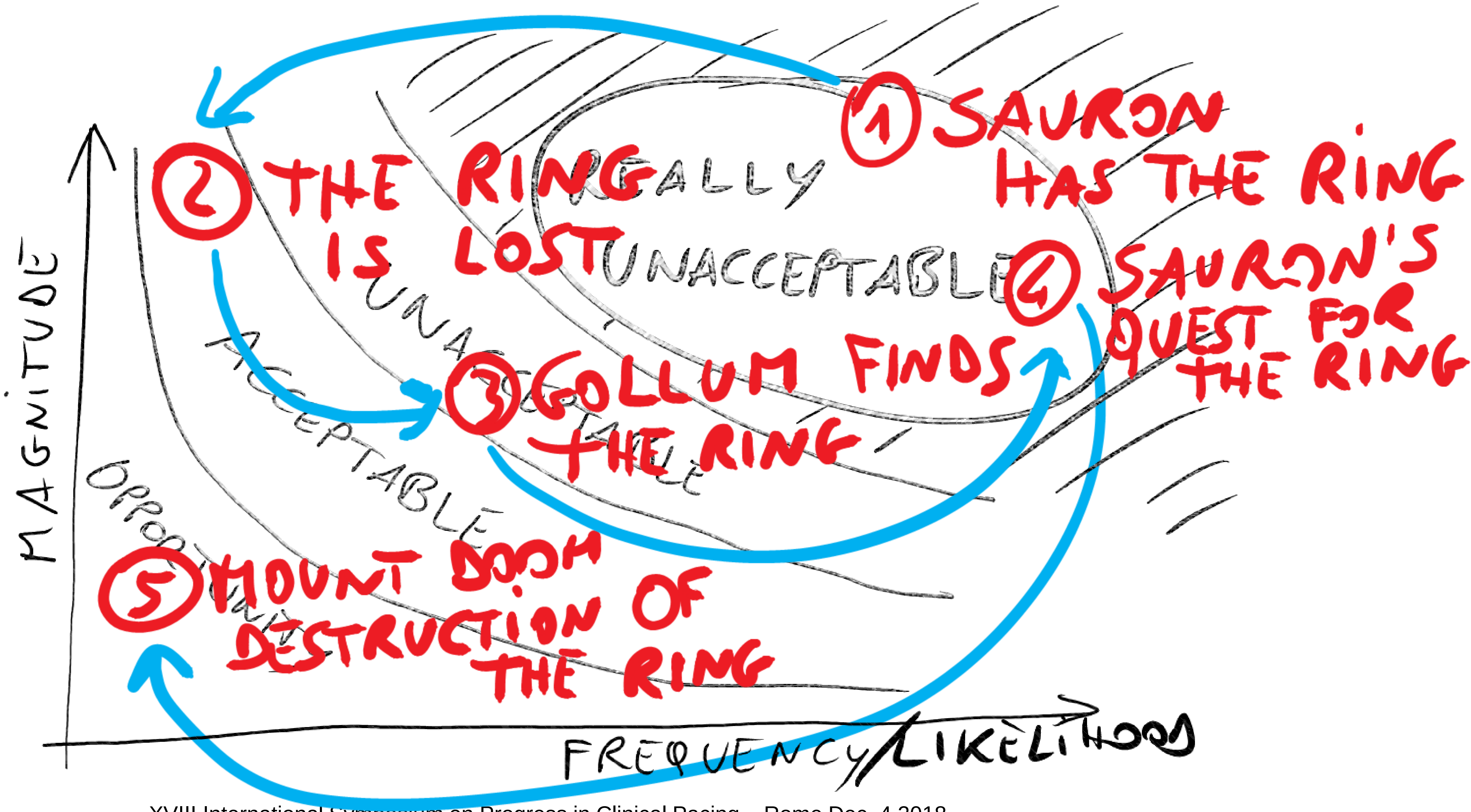
The possibility of loss or harm in exposure to a chance of damage involving uncertain danger in th creates or suggests a hazard or the degree of probability of suc

RISK = PROBABILITY x IMPACT



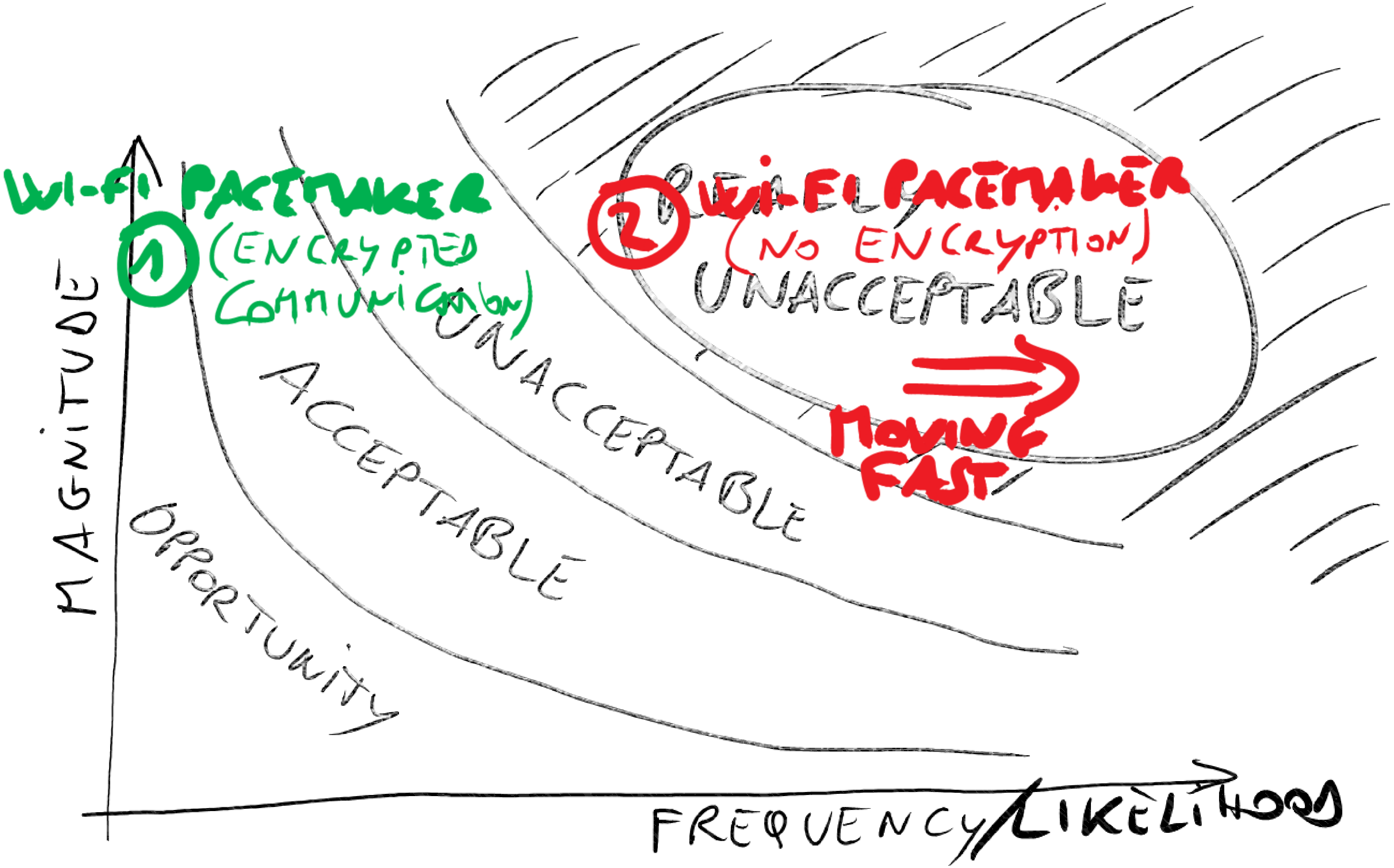
		Impact				
		Trivial	Minor	Moderate	Major	Extreme
Probability	Rare	Low	Low	Low	Medium	Medium
	Unlikely	Low	Low	Medium	Medium	Medium
	Moderate	Low	Medium	Medium	Medium	High
	Likely	Medium	Medium	Medium	High	High
	Very likely	Medium	Medium	High	High	High

Risk map – example (1/2)



Fonte: ISACA – CRISC review manual (www.isaca.org)

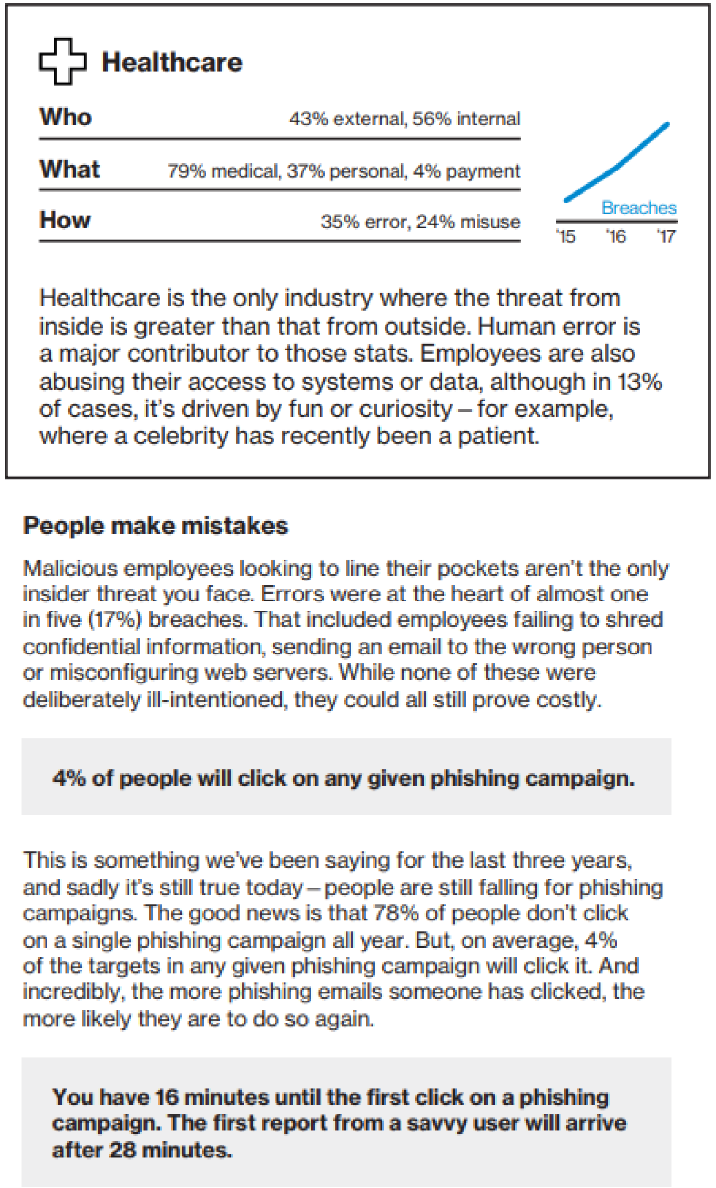
Risk map – example (2/2)



Fonte: ISACA – CRISC review manual (www.isaca.org)

The Human Factor

Source: 2018 Data Breach Investigations Report - Verizon



Healthcare

Who	43% external, 56% internal
What	79% medical, 37% personal, 4% payment
How	35% error, 24% misuse

Breaches
'15
'16
'17

Healthcare is the only industry where the threat from inside is greater than that from outside. Human error is a major contributor to those stats. Employees are also abusing their access to systems or data, although in 13% of cases, it's driven by fun or curiosity – for example, where a celebrity has recently been a patient.

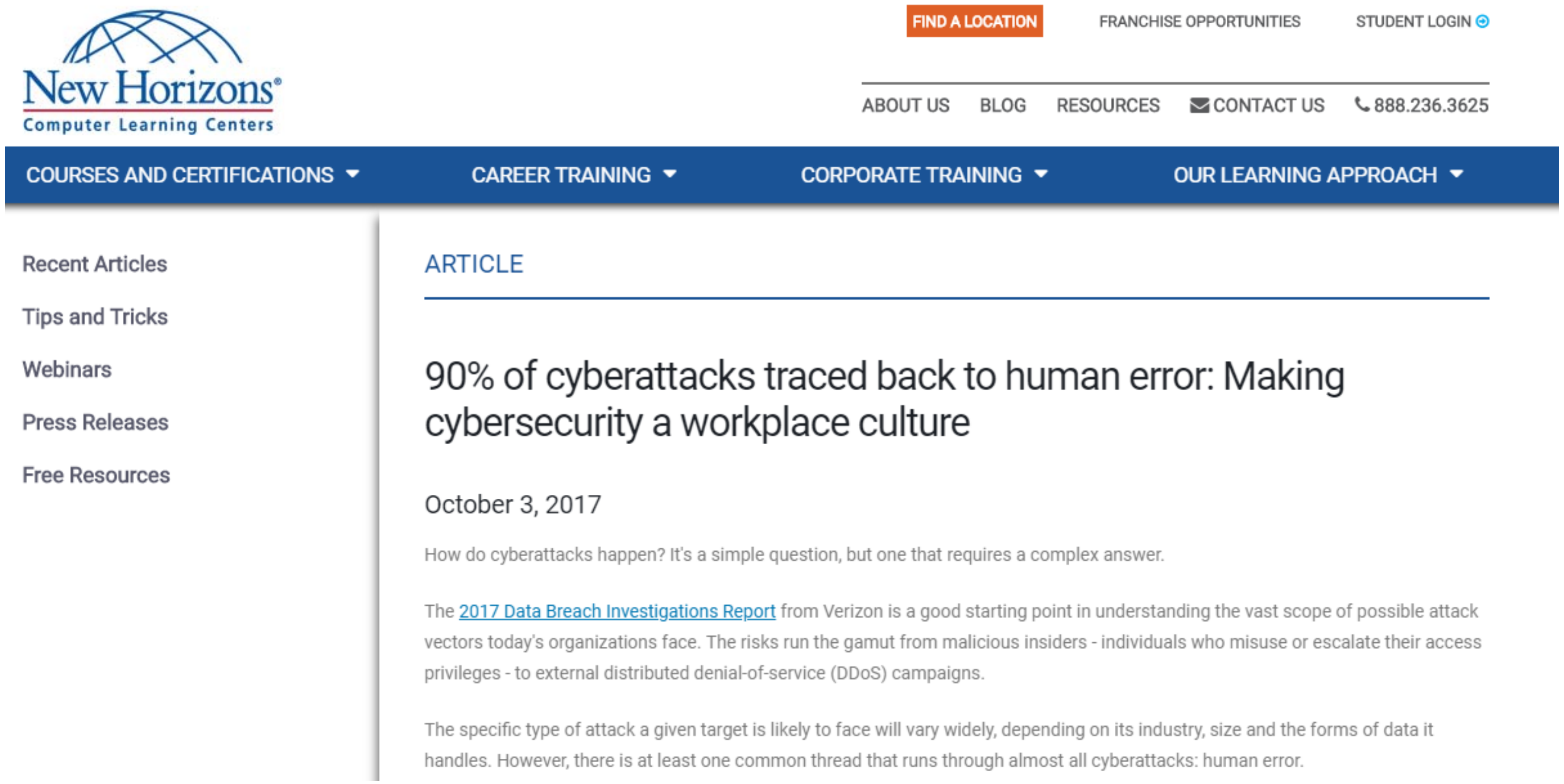
People make mistakes

Malicious employees looking to line their pockets aren't the only insider threat you face. Errors were at the heart of almost one in five (17%) breaches. That included employees failing to shred confidential information, sending an email to the wrong person or misconfiguring web servers. While none of these were deliberately ill-intentioned, they could all still prove costly.

4% of people will click on any given phishing campaign.

This is something we've been saying for the last three years, and sadly it's still true today – people are still falling for phishing campaigns. The good news is that 78% of people don't click on a single phishing campaign all year. But, on average, 4% of the targets in any given phishing campaign will click it. And incredibly, the more phishing emails someone has clicked, the more likely they are to do so again.

You have 16 minutes until the first click on a phishing campaign. The first report from a savvy user will arrive after 28 minutes.



ARTICLE

90% of cyberattacks traced back to human error: Making cybersecurity a workplace culture

October 3, 2017

How do cyberattacks happen? It's a simple question, but one that requires a complex answer.

The 2017 Data Breach Investigations Report from Verizon is a good starting point in understanding the vast scope of possible attack vectors today's organizations face. The risks run the gamut from malicious insiders - individuals who misuse or escalate their access privileges - to external distributed denial-of-service (DDoS) campaigns.

The specific type of attack a given target is likely to face will vary widely, depending on its industry, size and the forms of data it handles. However, there is at least one common thread that runs through almost all cyberattacks: human error.

If you want a good start… S.T.O.P.!

To address cybersecurity effectively in healthcare we need to address 3 areas:

STRATEGY:

- **No citadel to defend:** protection of an open city with a wide attack surface
- **Move from a siloes approach to an integrated and holistic approach to security**. All the information and automation technologies in and out the hospital must be addressed, regardless of who is responsible for what

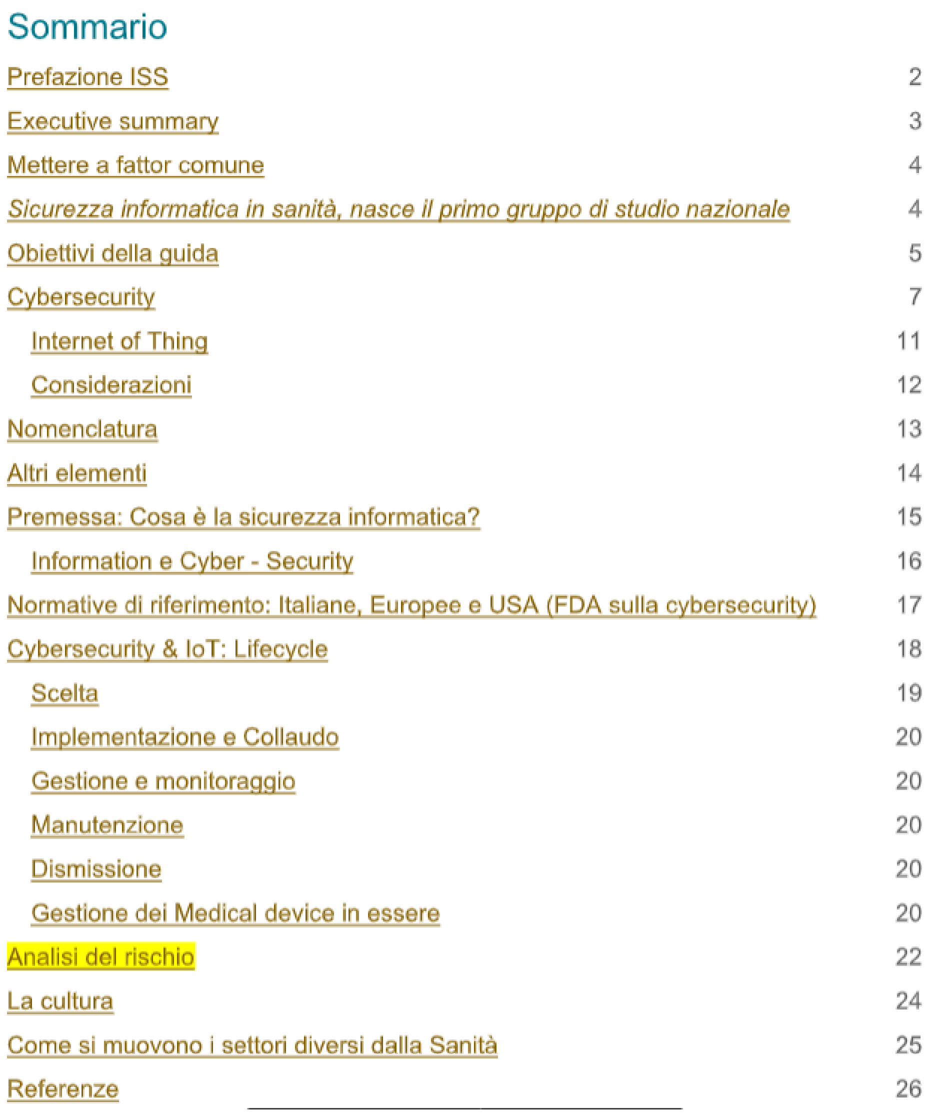
TECHNOLOGY:

- **In technology assessment and acquisition, it is important to ensure that security is one of the basic requirements**, included by design in the technology under evaluation (from applications to pacemaker)
- **In selecting the tools and services to support security, the IT department should incorporate an architectural vision and evaluation of the impact on the users (security vs. usability, data protection vs. data sharing…)**

ORGANIZATION & PROCESSES

- **Robust and «risk focused» process review needed**
- **Work on culture! (90% of defence!)**
- **Unification/coordination of different technology departments is a must!** E.g.: the three typical technology departments in a hospital (facility, clinical engineering and IT) were born when buildings were walls and bricks, medical devices were dumb machines, and IT managed a well-defined set of applications and data.
- **Cross-fertilization and hybridation is a value!**
- **The whole echosystem (supplier, providers, patients, clinicians, IT professionals, payors) must work together**

Example of a good stard: AISIS & AIIC

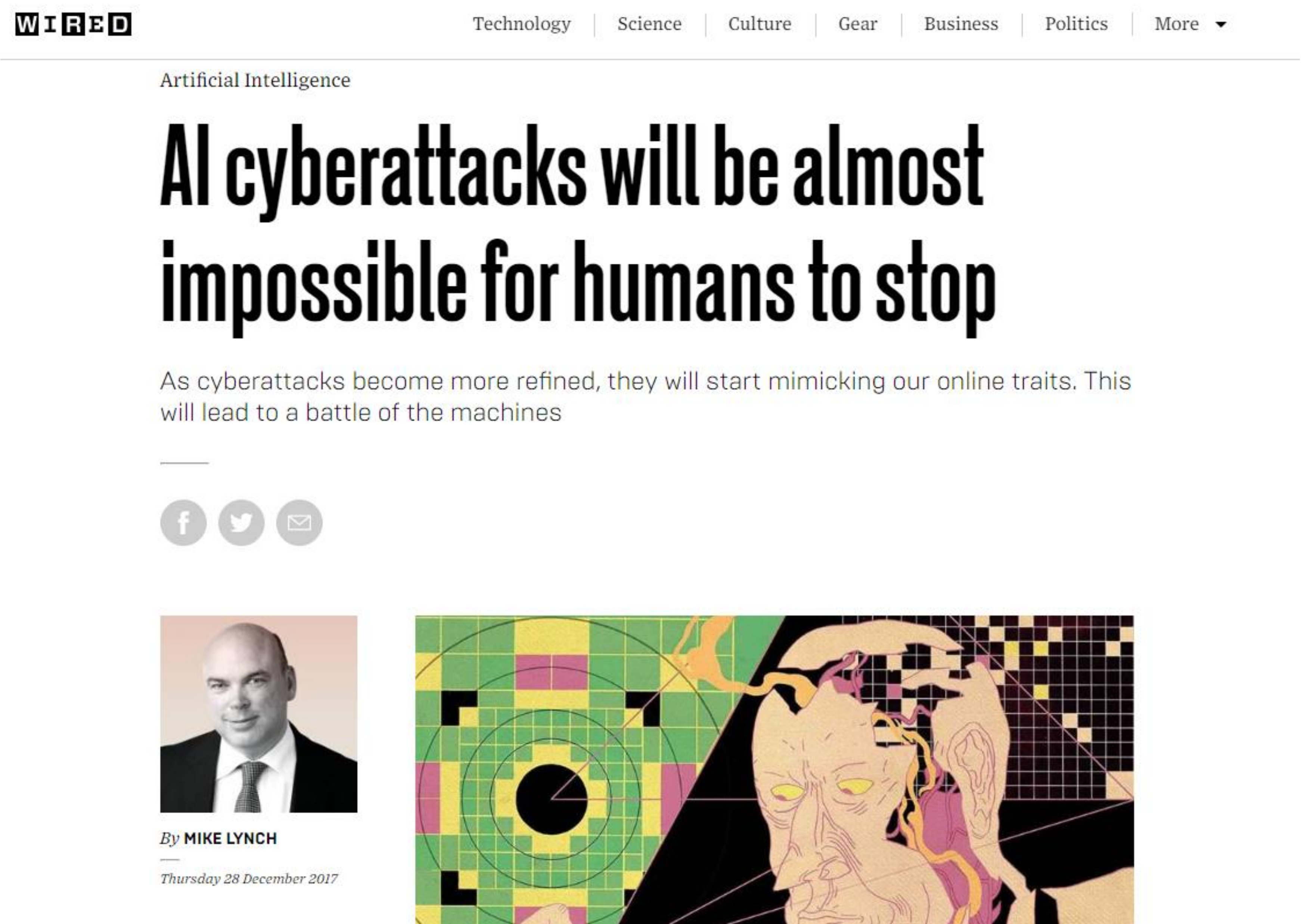


Sommario

The battle of the 5 armies:

The first joint document by C.I.O.s (AISIS) and Clinical Engineers (AIIC) on Cybersecurity & IoT in Healthcare!

What Next…



Artificial Intelligence

AI cyberattacks will be almost impossible for humans to stop

As cyberattacks become more refined, they will start mimicking our online traits. This will lead to a battle of the machines

By **MIKE LYNCH**

Thursday 28 December 2017

Final considerations: are we here…

…or here?

Q&A

Contact Info: giuliano.pozza@gmail.com or www.yottabronto.net