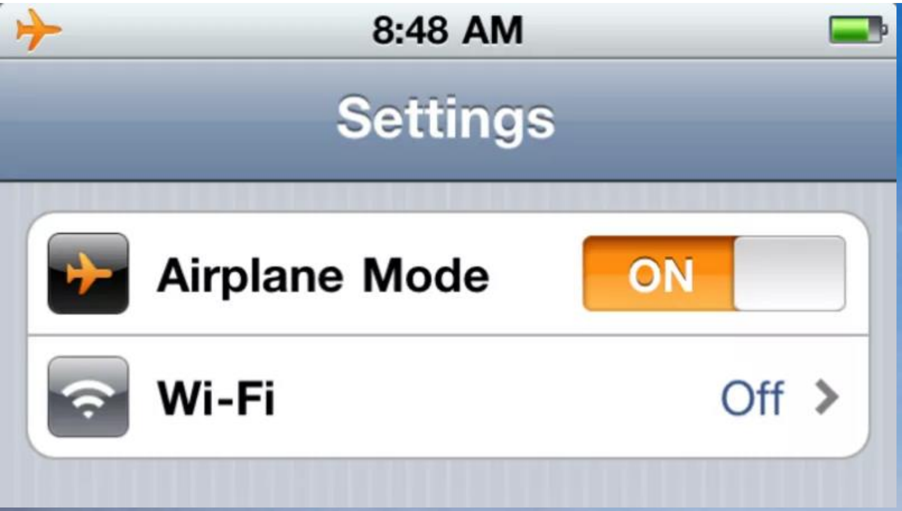
Three Paradoxes and the Need for a Paradigm Shift—A CIO Perspective

Pre-flight safety briefing


8:48 AM

Settings

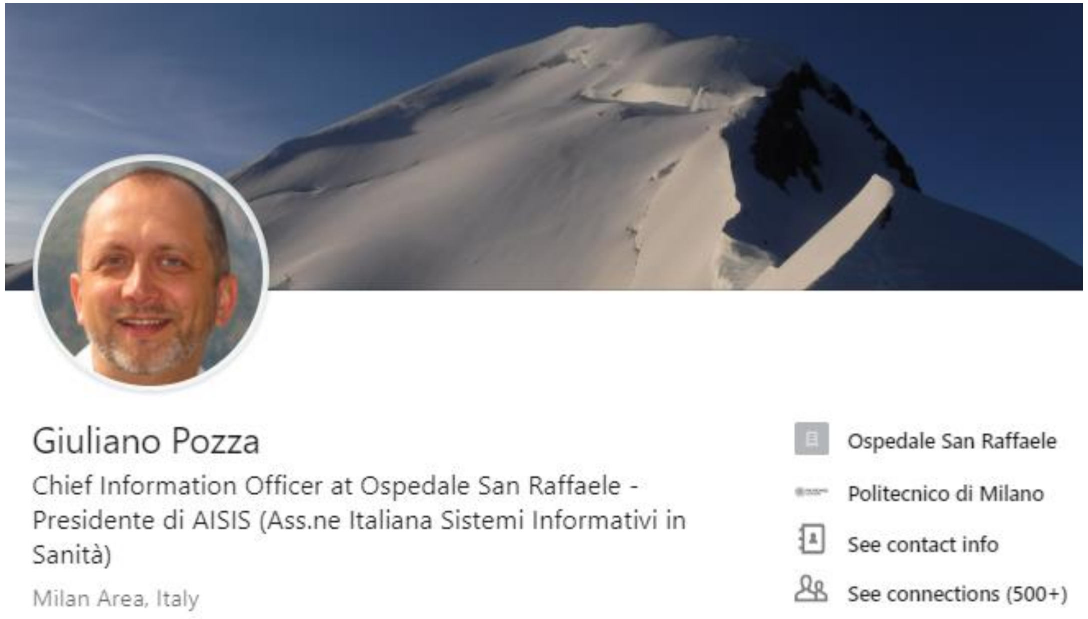
Airplane Mode ON

Wi-Fi Off

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

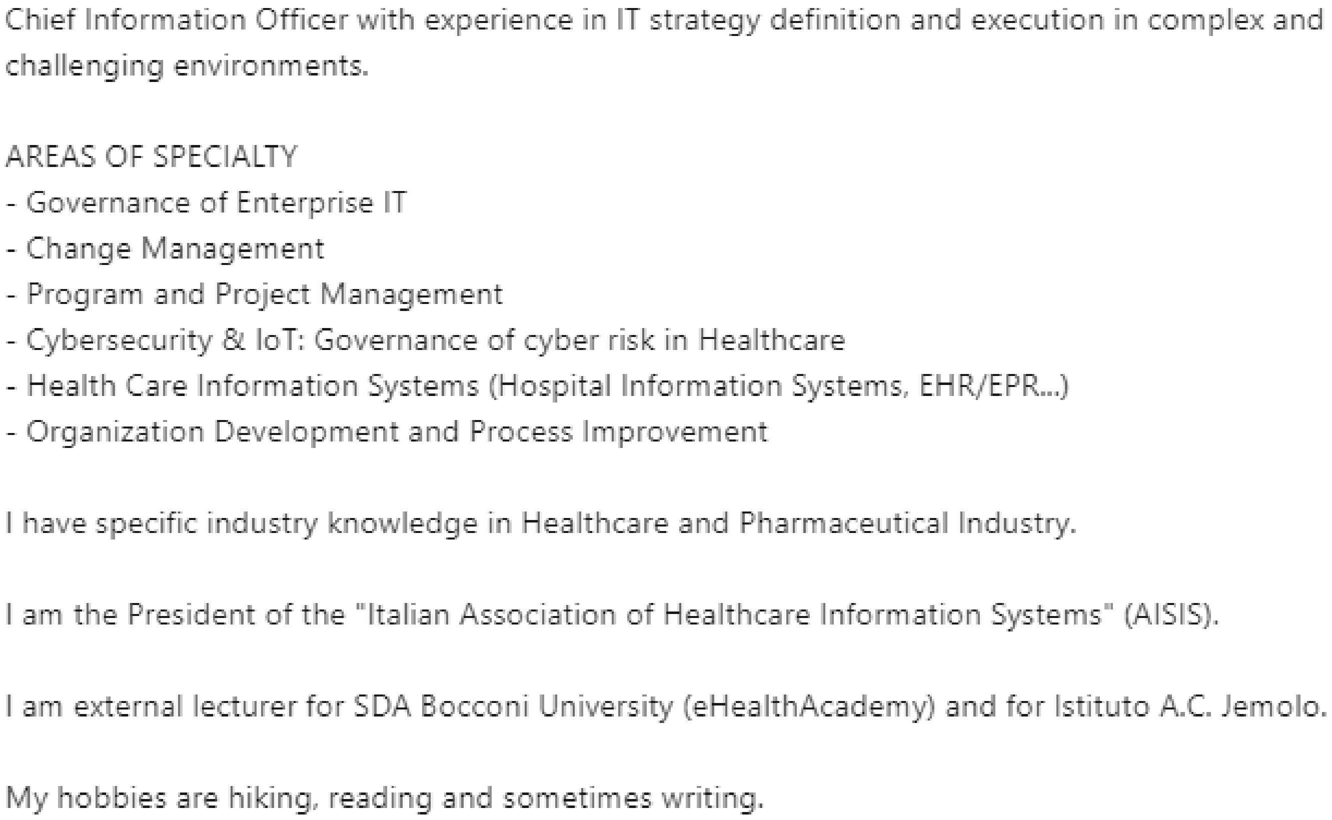
Politecnico di Milano

See contact info

See connections (500+)

www.linkedin.com/in/gpozza/

www.yottabronto.net



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.

… 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.

ACTIVE COLLABORATION with POLIMI:

AISIS4Social - www.aisis.it/aisis4social

(2019: 2 scholarships)

Main Partnerships:

- AICA
- AIIC
- 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
- …

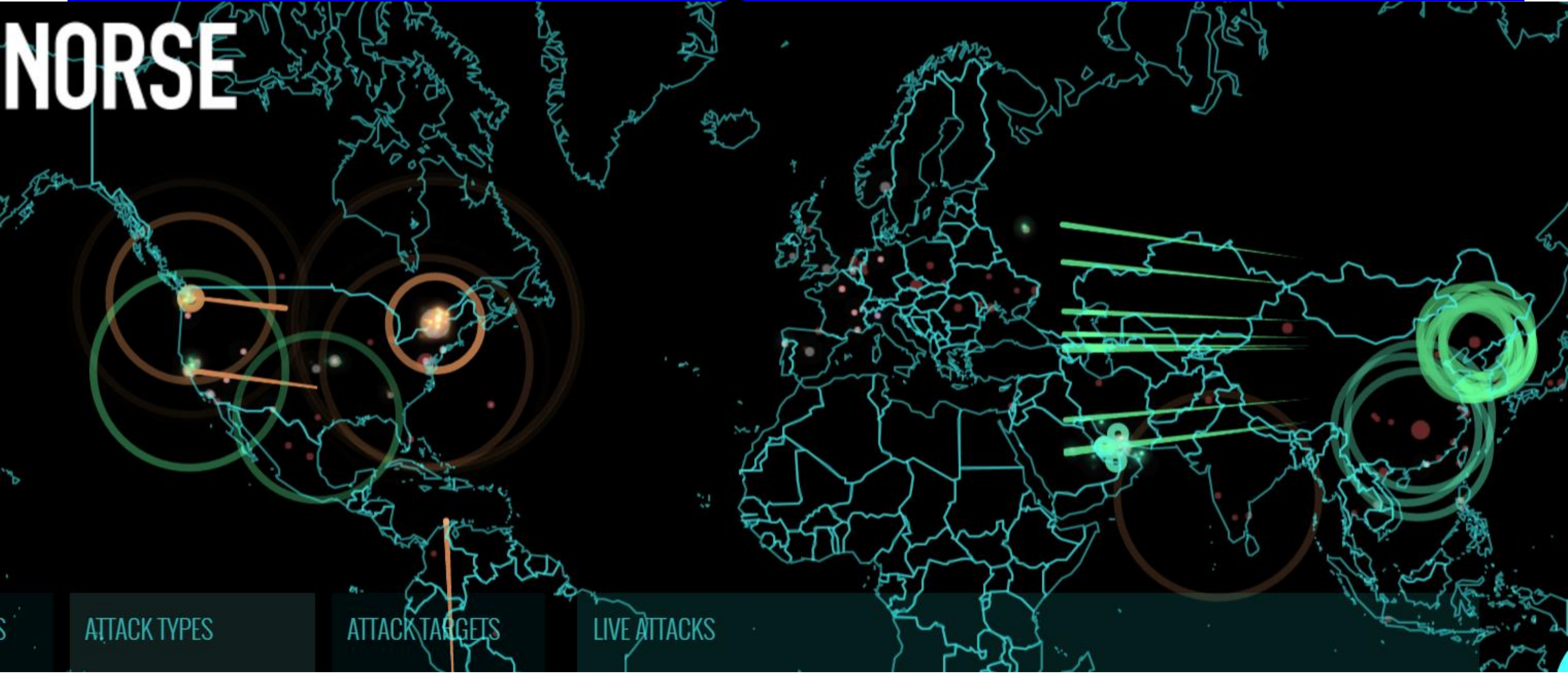
Course Objectives

- Understand the context of cybersecurity <u>in healthcare</u>
- Analyze from a risk management/accountability perspective (as required by GDPR) the most dangerous cyber threats
- Define mitigation scenarios

Agenda

- (15 min) Context: cybersecurity & IoT in Healthcare
- (15 min) 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
- (15 min) Paradigm Shift Ahead!
  - It’s all about data and information!
  - We need a Risk management perspective
  - Review of Strategy – Technology – Processes – People
  - Final considerations
- (Takeoff tracks: personal bibliography)
- (15 min) Q&A

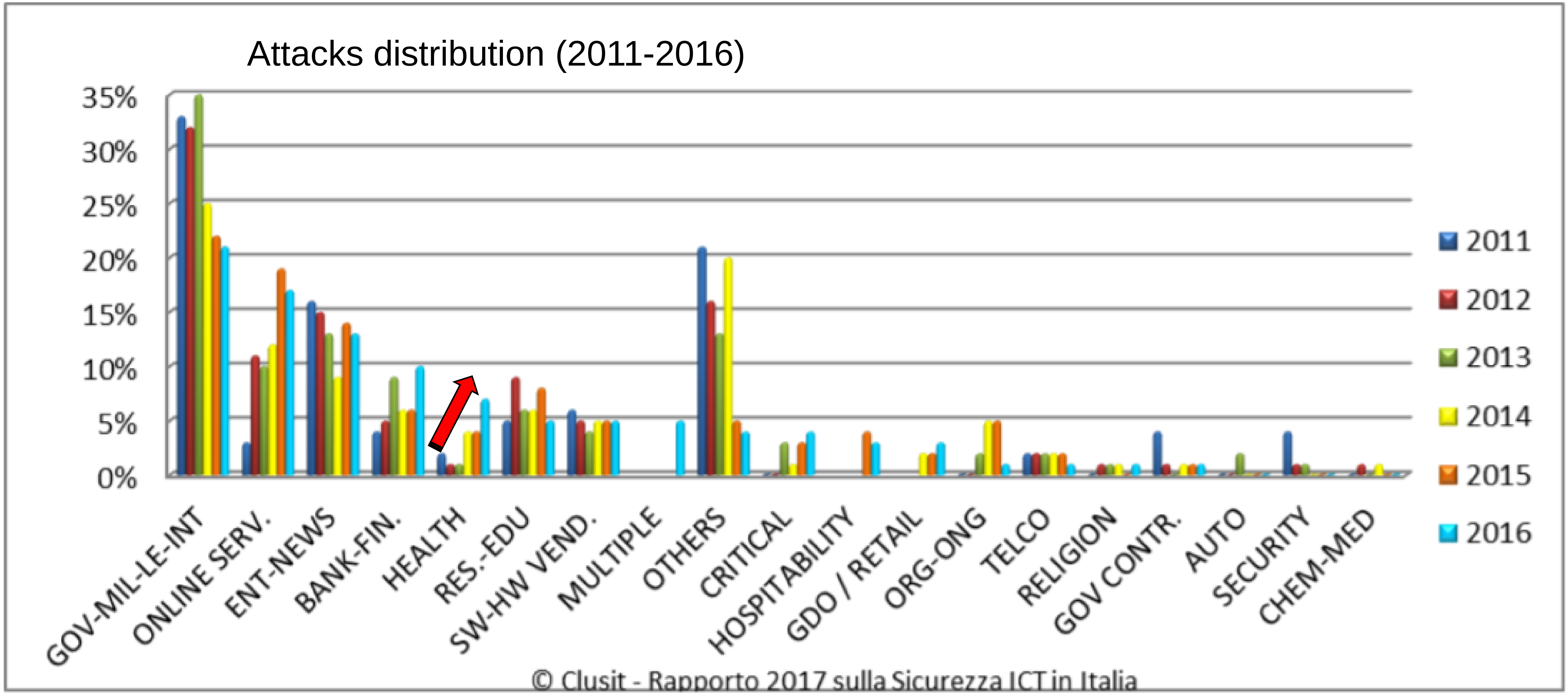
War games…



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

Healthcare under attack (1/2)

Source: Rapporto CLUSIT 2017



© Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia

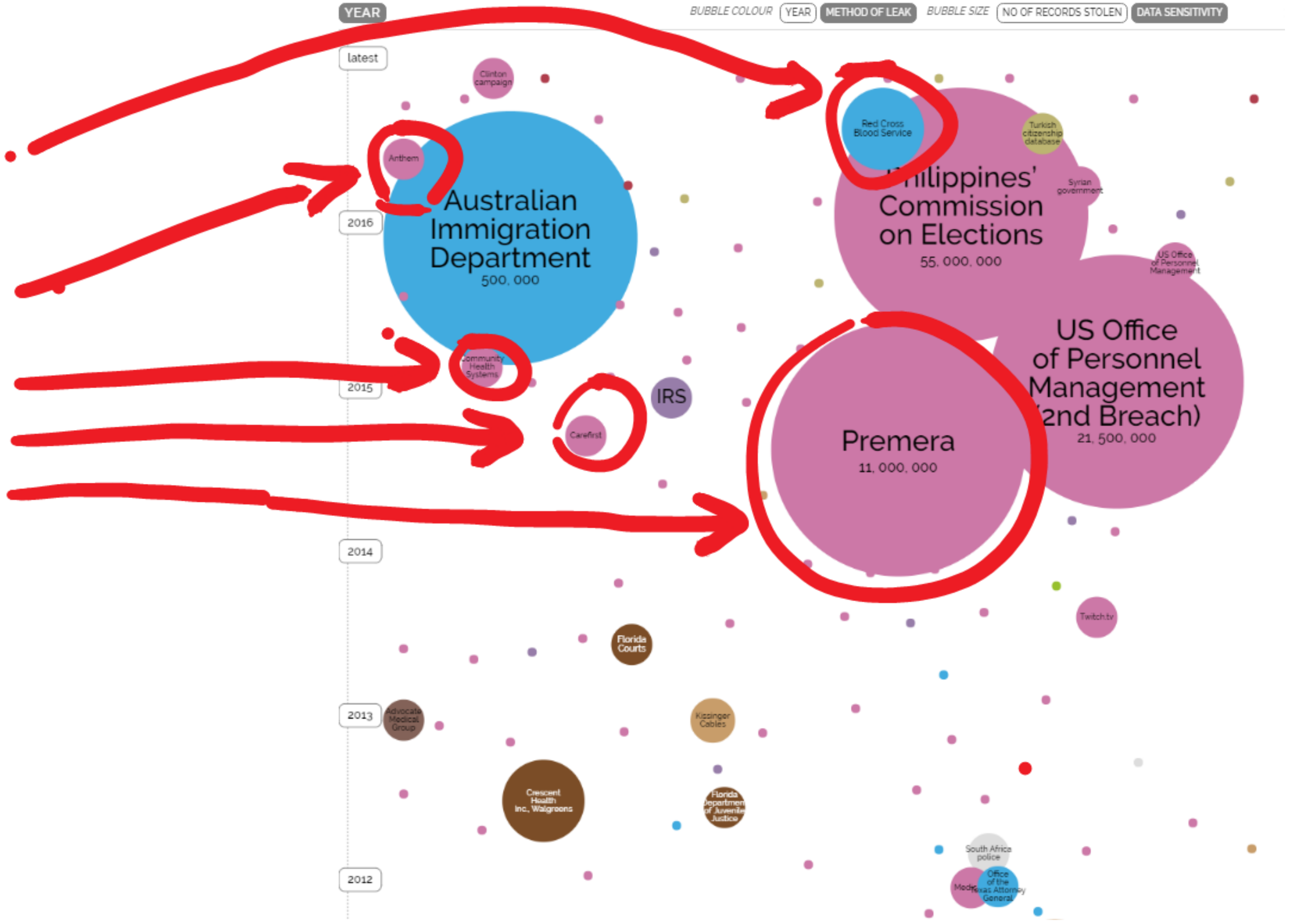
Healthcare under attack (2/2)

World's Biggest Data Breaches (Healthcare & Government)

Selected losses greater than 30,000 records

(updated 15th Oct 2016)

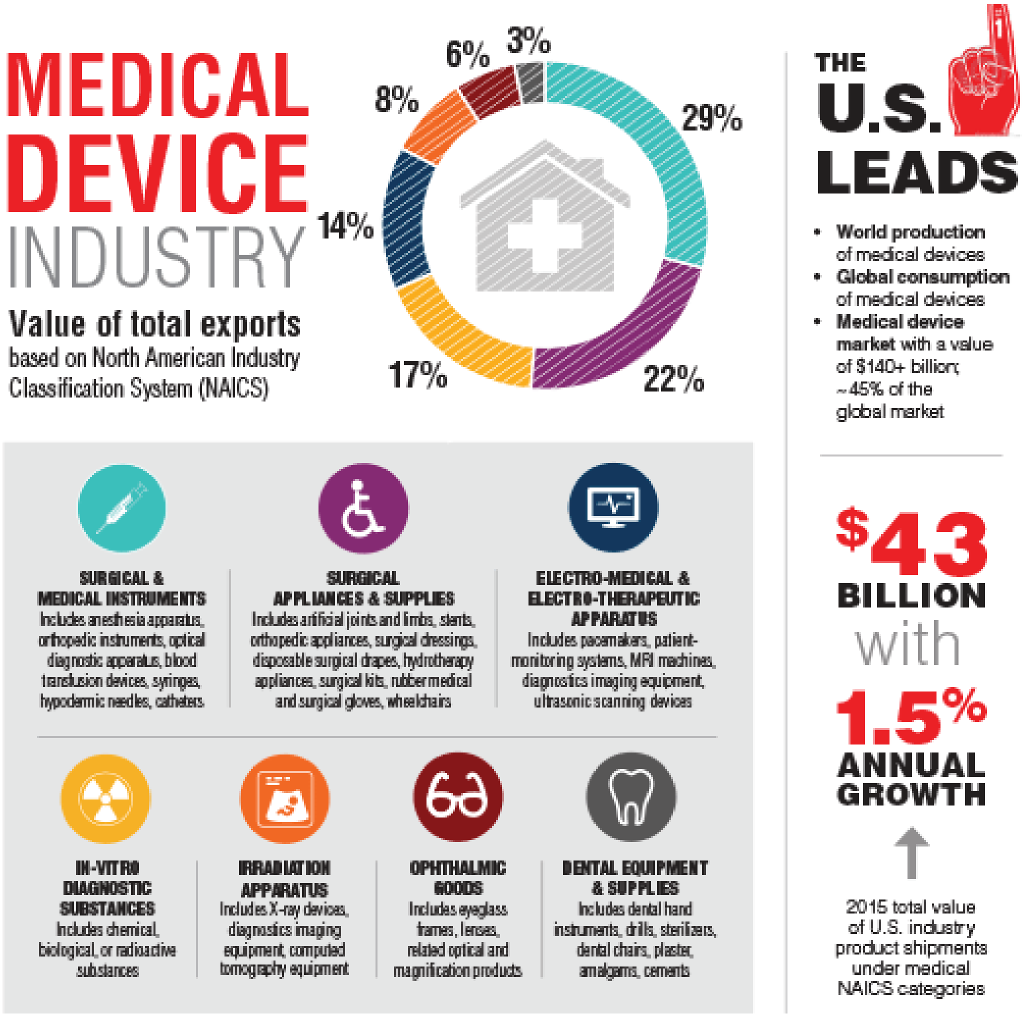
Health Data



Source: www.informationisbeautiful.net

Internet of Things (1/3)

Source: EvaluateMedTech® World Preview 2016, Outlook to 2022



MEDICAL DEVICE INDUSTRY

Value of total exports
based on North American Industry Classification System (NAICS)

THE U.S. LEADS

- **World production** of medical devices
- **Global consumption** of medical devices
- **Medical device market** with a value of $140+ billion; ~45% of the global market

$43 BILLION with 1.5% ANNUAL GROWTH

2015 total value of U.S. industry product shipments under medical NAICS categories

SURGICAL & MEDICAL INSTRUMENTS
Includes anesthesia apparatus, orthopedic instruments, optical diagnostic apparatus, blood transfusion devices, syringes, hypodermic needles, catheters

SURGICAL APPLIANCES & SUPPLIES
Includes artificial joints and limbs, stents, orthopedic appliances, surgical dressings, disposable surgical drapes, hydrotherapy appliances, surgical kits, rubber medical and surgical gloves, wheelchairs

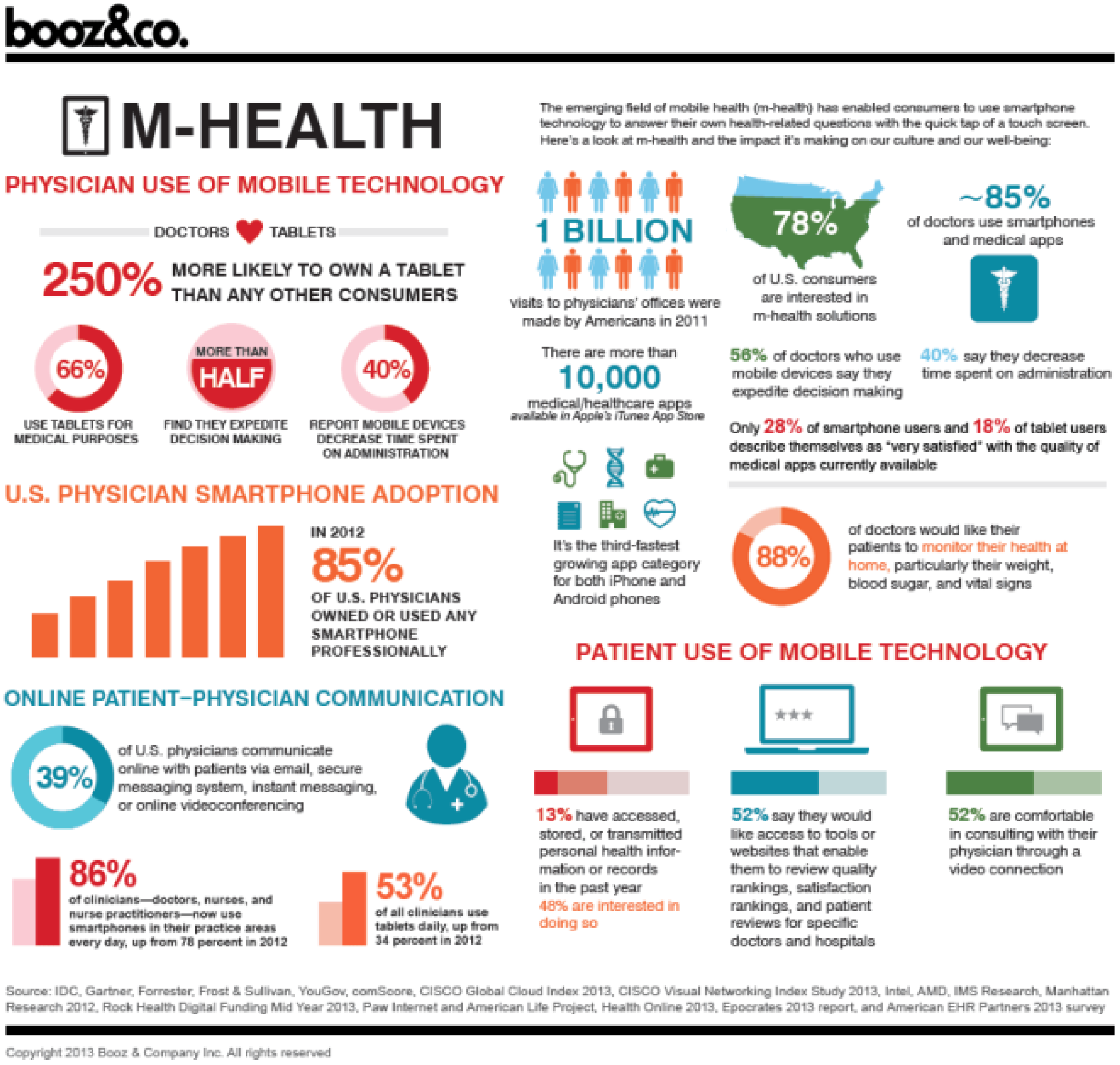
ELECTRO-MEDICAL & ELECTRO-THERAPEUTIC APPARATUS
Includes pacemakers, patient-monitoring systems, MRI machines, diagnostics imaging equipment, ultrasonic scanning devices

IN-VITRO DIAGNOSTIC SUBSTANCES
Includes chemical, biological, or radioactive substances

IRRADIATION APPARATUS
Includes X-ray devices, diagnostics imaging equipment, computed tomography equipment

OPHTHALMIC GOODS
Includes eyeglass frames, lenses, related optical and magnification products

DENTAL EQUIPMENT & SUPPLIES
Includes dental hand instruments, drills, sterilizers, dental chairs, plaster, amalgams, cements



booz&co.

M-HEALTH

The emerging field of mobile health (m-health) has enabled consumers to use smartphone technology to answer their own health-related questions with the quick tap of a touch screen. Here's a look at m-health and the impact it's making on our culture and our well-being:

PHYSICIAN USE OF MOBILE TECHNOLOGY

DOCTORS ♥ TABLETS

250% MORE LIKELY TO OWN A TABLET THAN ANY OTHER CONSUMERS

66% USE TABLETS FOR MEDICAL PURPOSES

MORE THAN HALF FIND THEY EXPEDITE DECISION MAKING

40% REPORT MOBILE DEVICES DECREASE TIME SPENT ON ADMINISTRATION

1 BILLION visits to physicians' offices were made by Americans in 2011

78% of U.S. consumers are interested in m-health solutions

~85% of doctors use smartphones and medical apps

There are more than **10,000** medical/healthcare apps *available in Apple's iTunes App Store*

56% of doctors who use mobile devices say they expedite decision making

40% say they decrease time spent on administration

Only **28%** of smartphone users and **18%** of tablet users describe themselves as "very satisfied" with the quality of medical apps currently available

It's the third-fastest growing app category for both iPhone and Android phones

88% of doctors would like their patients to monitor their health at home, particularly their weight, blood sugar, and vital signs

U.S. PHYSICIAN SMARTPHONE ADOPTION

IN 2012 **85%** OF U.S. PHYSICIANS OWNED OR USED ANY SMARTPHONE PROFESSIONALLY

ONLINE PATIENT–PHYSICIAN COMMUNICATION

39% of U.S. physicians communicate online with patients via email, secure messaging system, instant messaging, or online videoconferencing

86% of clinicians—doctors, nurses, and nurse practitioners—now use smartphones in their practice areas every day, up from 78 percent in 2012

53% of all clinicians use tablets daily, up from 34 percent in 2012

PATIENT USE OF MOBILE TECHNOLOGY

13% have accessed, stored, or transmitted personal health information or records in the past year
48% are interested in doing so

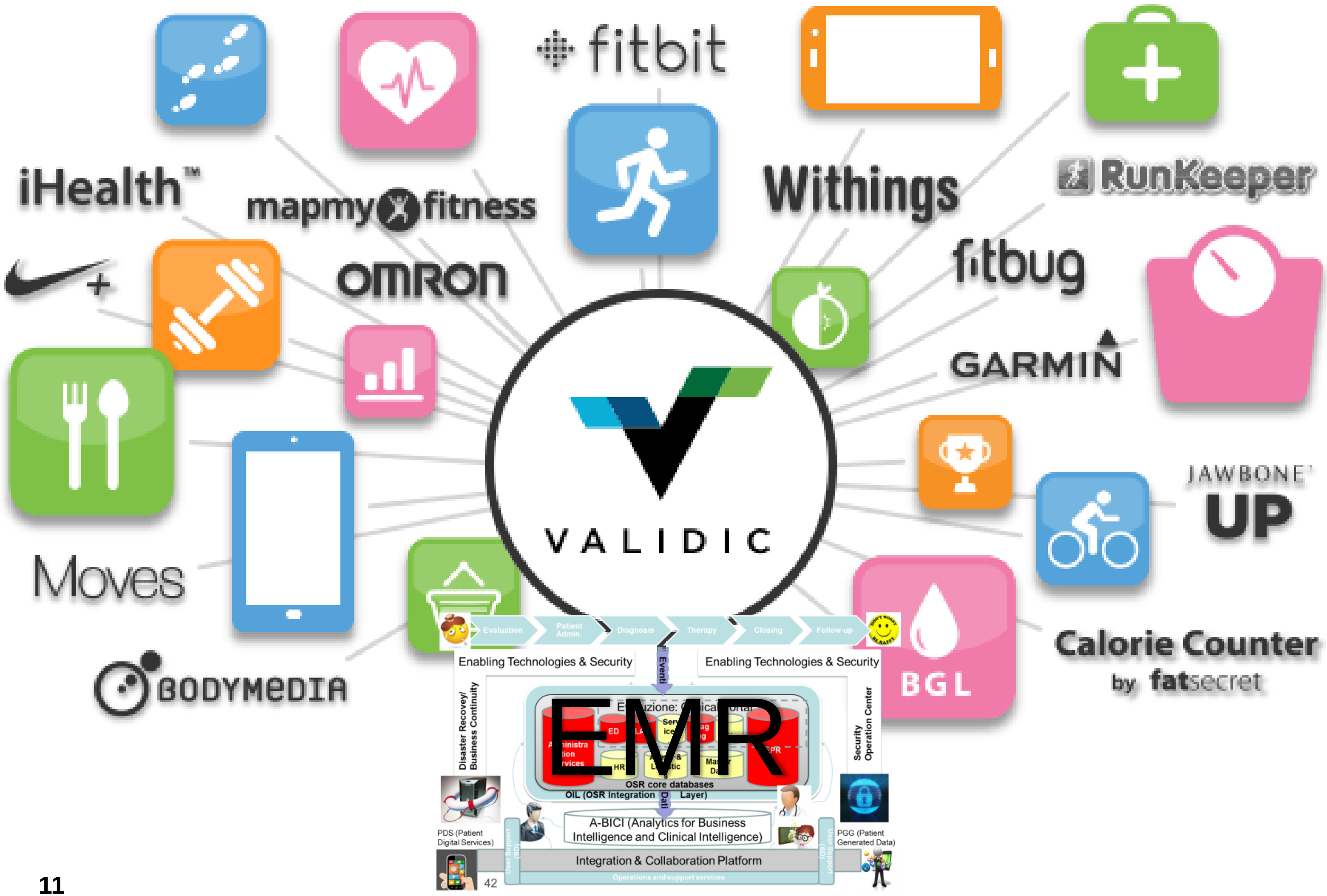
52% say they would like access to tools or websites that enable them to review quality rankings, satisfaction rankings, and patient reviews for specific doctors and hospitals

52% are comfortable in consulting with their physician through a video connection

Source: IDC, Gartner, Forrester, Frost & Sullivan, YouGov, comScore, CISCO Global Cloud Index 2013, CISCO Visual Networking Index Study 2013, Intel, AMD, IMS Research, Manhattan Research 2012, Rock Health Digital Funding Mid Year 2013, Paw Internet and American Life Project, Health Online 2013, Epocrates 2013 report, and American EHR Partners 2013 survey

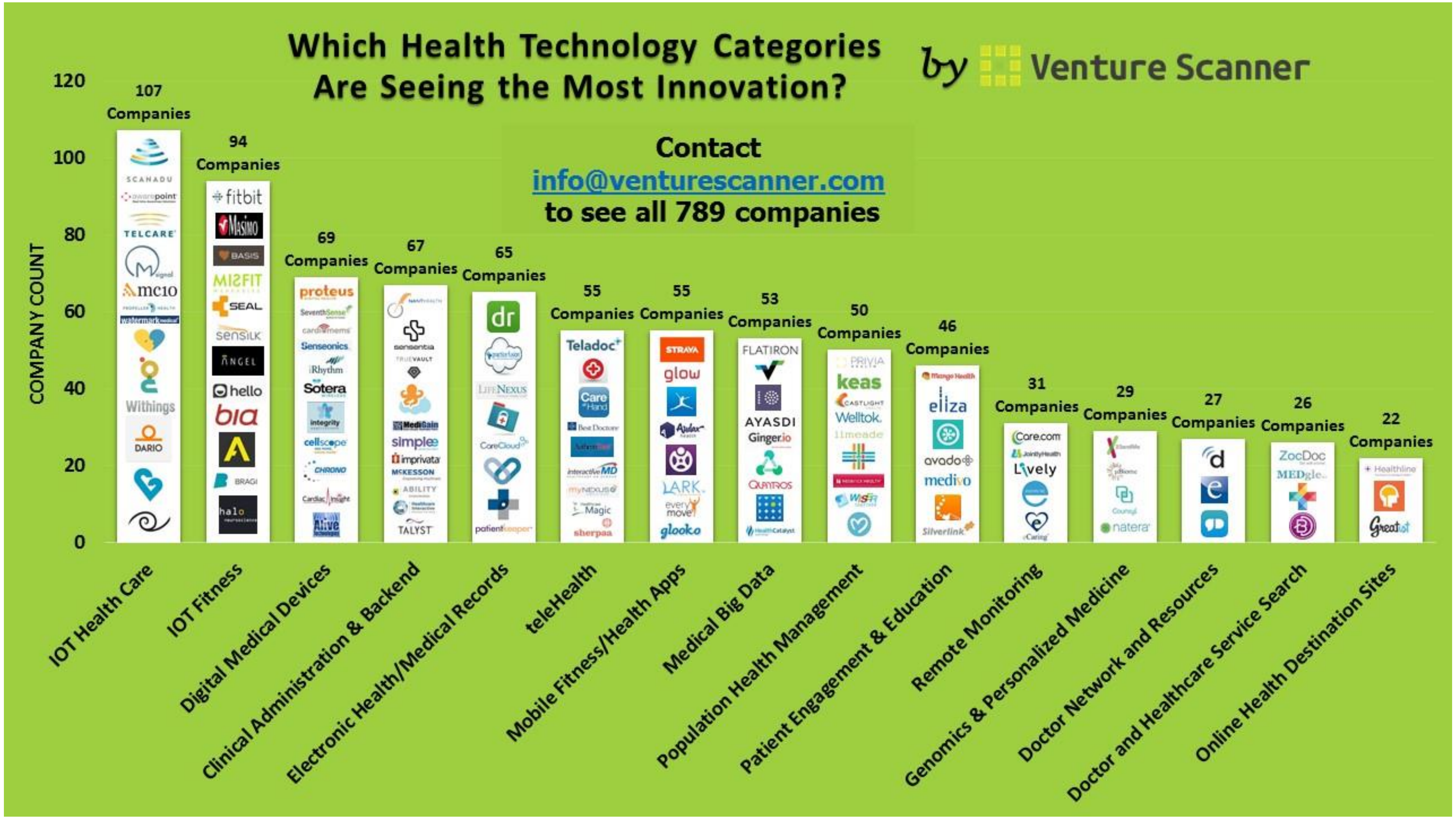
Internet of Things: wearable (2/3)

Patient Generated Data
(PGD)


fitbit
iHealth™
mapmy fitness
Withings
RunKeeper
OMRON
fitbug
GARMIN
VALIDIC
JAWBONE UP
Moves
BODYMEDIA
BGL
Calorie Counter by fatsecret
EMR
Evaluation
Patient Admin.
Diagnosis
Therapy
Closing
Follow-up
Enabling Technologies & Security
Enabling Technologies & Security
Eventi
Disaster Recovey/ Business Continuity
Security Operation Center
OSR core databases
OIL (OSR Integration Layer)
Dati
A-BICI (Analytics for Business Intelligence and Clinical Intelligence)
PDS (Patient Digital Services)
PGG (Patient Generated Data)
User Support (SD)
User Support (SD)
Integration & Collaboration Platform
Operations and support services
42

Patient Generated Data
(PGD)

Internet of Things & wearable (3/3)

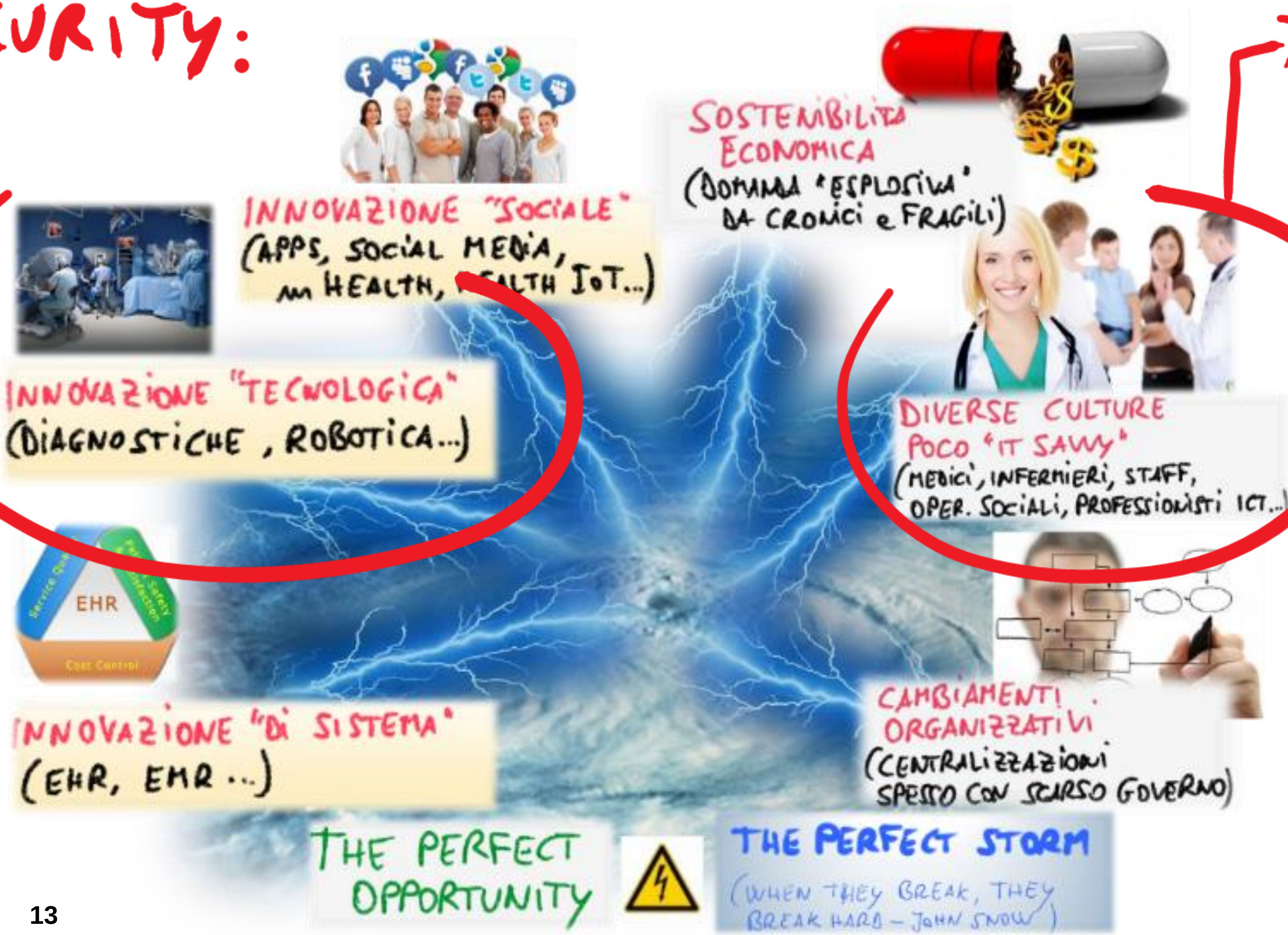


Contact info@venturescanner.com to see all 789 companies

Healthcare: The perfect storm

IT SECURITY:

→ HEALTH CARE



INNOVAZIONE "SOCIALE"
(APPS, SOCIAL MEDIA, mHEALTH, 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 ...)

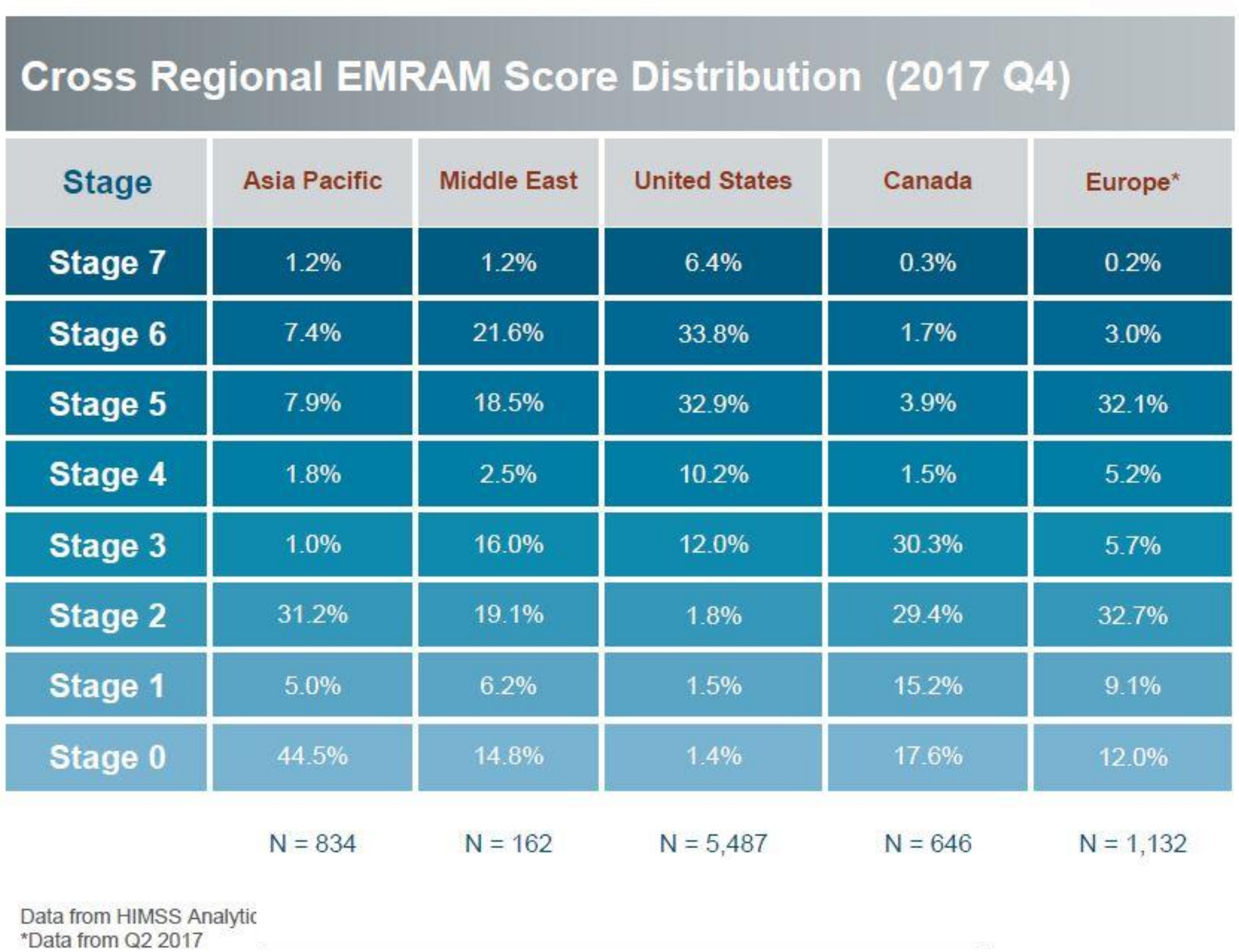
CAMBIAMENTI ORGANIZZATIVI
(CENTRALIZZAZIONI SPESSO CON SCARSO GOVERNO)

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

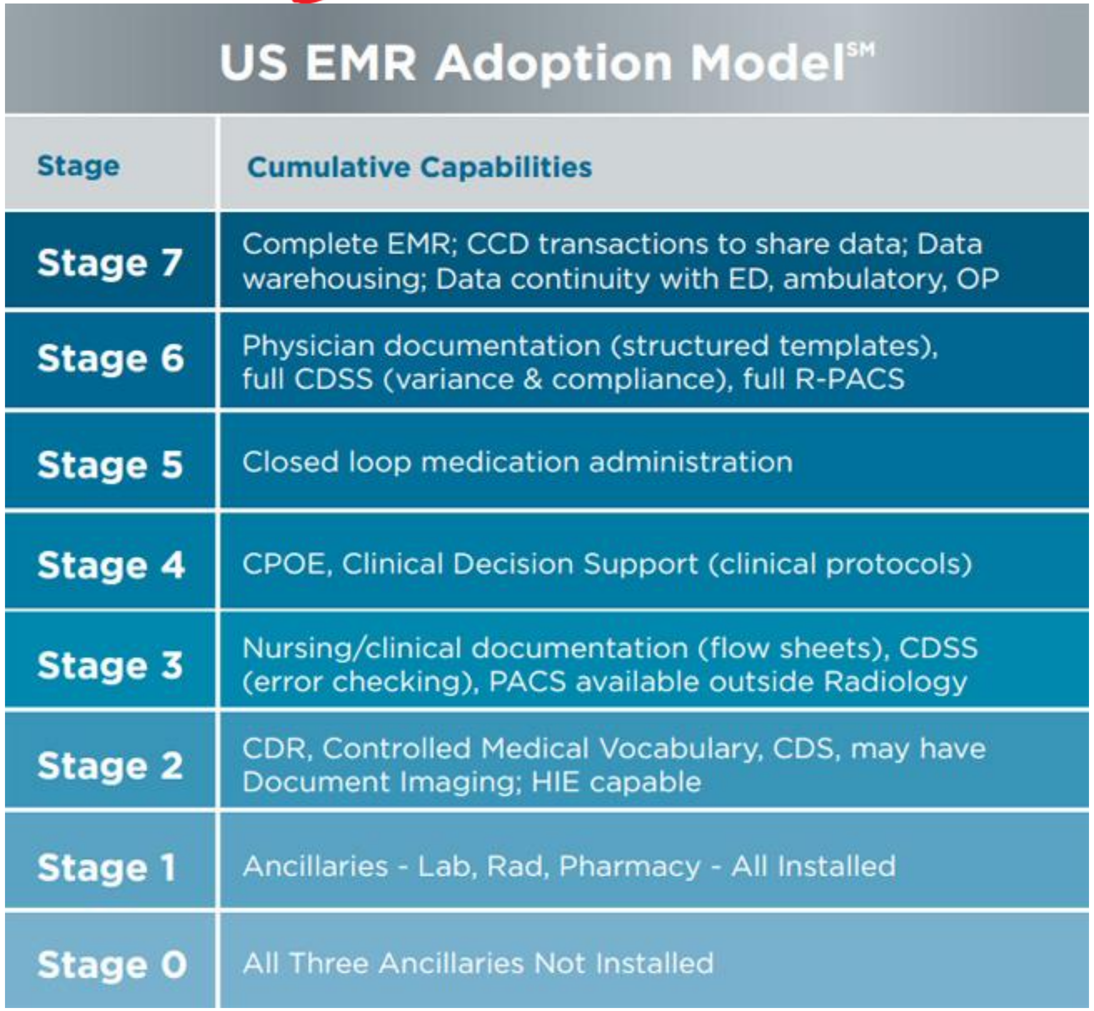
Data from HIMSS Analytic
*Data from Q2 2017

ITALY:

- 6 LEVEL 6 HOSPITALS
- ALMOST ALL BELOW LEVEL 3

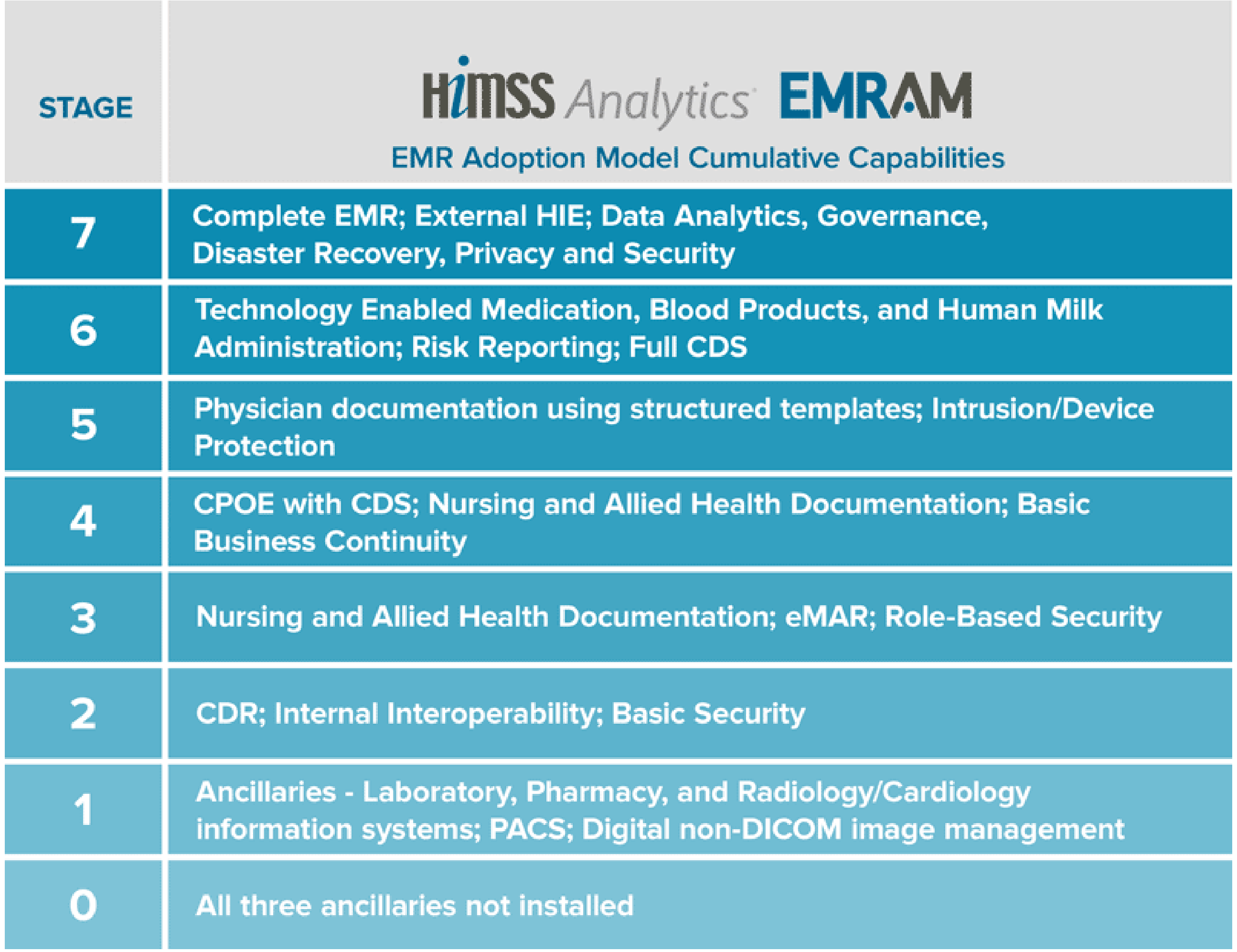
PS: EMRAM Scale

BEFORE 2018 → AFTER 2018



US EMR Adoption Model℠

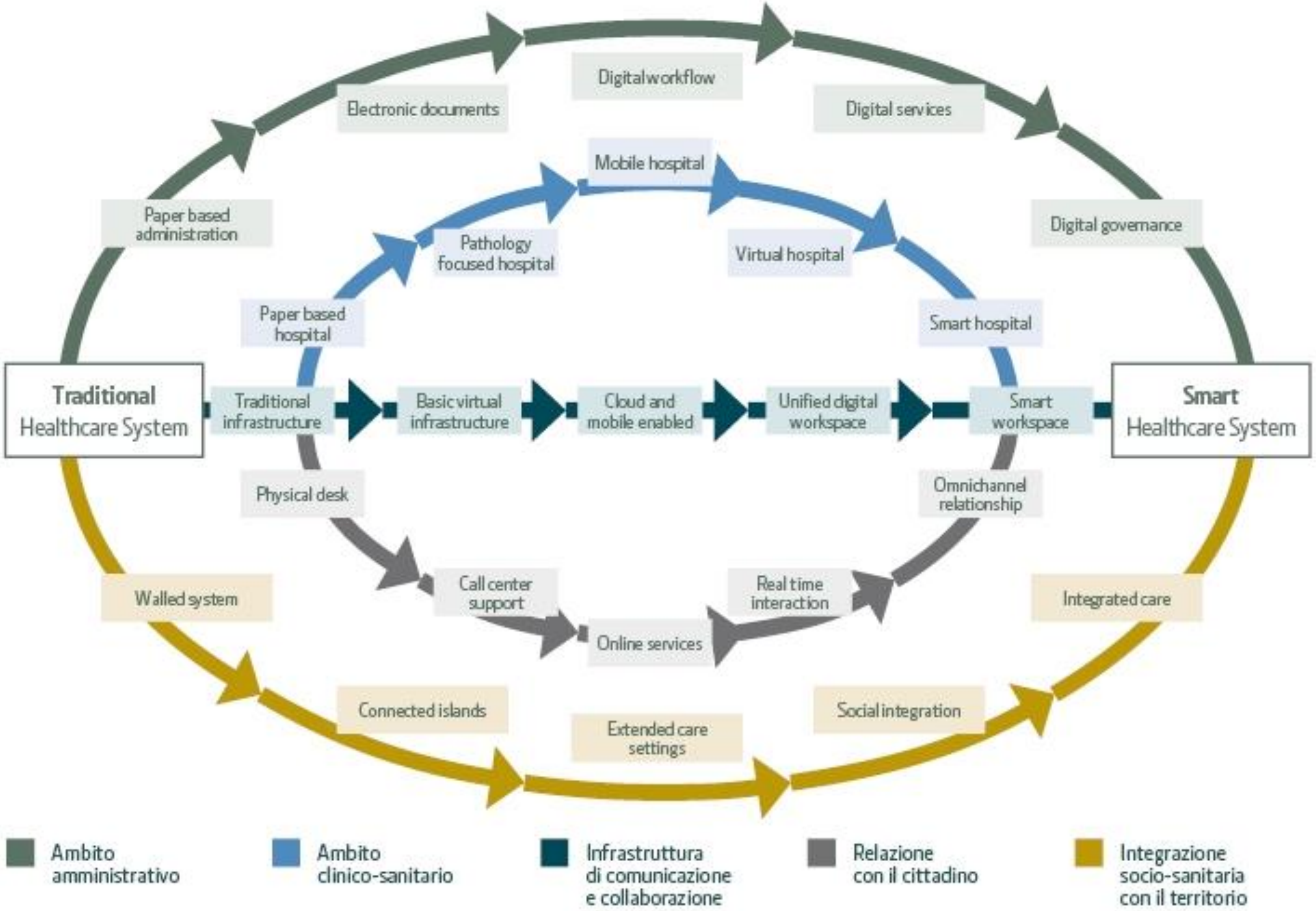
Stage	Cumulative Capabilities
Stage 7	Complete EMR; CCD transactions to share data; Data warehousing; Data continuity with ED, ambulatory, OP
Stage 6	Physician documentation (structured templates), full CDSS (variance & compliance), full R-PACS
Stage 5	Closed loop medication administration
Stage 4	CPOE, Clinical Decision Support (clinical protocols)
Stage 3	Nursing/clinical documentation (flow sheets), CDSS (error checking), PACS available outside Radiology
Stage 2	CDR, Controlled Medical Vocabulary, CDS, may have Document Imaging; HIE capable
Stage 1	Ancillaries - Lab, Rad, Pharmacy - All Installed
Stage 0	All Three Ancillaries Not Installed



STAGE	HIMSS Analytics EMRAM EMR Adoption Model Cumulative Capabilities
7	Complete EMR; External HIE; Data Analytics, Governance, Disaster Recovery, Privacy and Security
6	Technology Enabled Medication, Blood Products, and Human Milk Administration; Risk Reporting; Full CDS
5	Physician documentation using structured templates; Intrusion/Device Protection
4	CPOE with CDS; Nursing and Allied Health Documentation; Basic Business Continuity
3	Nursing and Allied Health Documentation; eMAR; Role-Based Security
2	CDR; Internal Interoperability; Basic Security
1	Ancillaries - Laboratory, Pharmacy, and Radiology/Cardiology information systems; PACS; Digital non-DICOM image management
0	All three ancillaries not installed

+ DIFFUSION

Other maturity models…



Traditional Healthcare System

Paper based administration

Electronic documents

Digital workflow

Digital services

Digital governance

Paper based hospital

Pathology focused hospital

Mobile hospital

Virtual hospital

Smart hospital

Traditional infrastructure

Basic virtual infrastructure

Cloud and mobile enabled

Unified digital workspace

Smart workspace

Physical desk

Call center support

Online services

Real time interaction

Omnichannel relationship

Walled system

Connected islands

Extended care settings

Social integration

Integrated care

Smart Healthcare System

■ Ambito amministrativo

■ Ambito clinico-sanitario

■ Infrastruttura di comunicazione e collaborazione

■ Relazione con il cittadino

■ Integrazione socio-sanitaria con il territorio

Fonte: Osservatorio Innovazione in Sanità del Politecnico di Milano

Agenda

- (15 min) Context: cybersecurity & IoT in Healthcare
- (15 min) 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
- (15 min) Paradigm Shift Ahead!
  - It’s all about data and information!
  - We need a Risk management perspective
  - Review of Strategy – Technology – Processes – People
  - Final considerations
- (Takeoff tracks: personal bibliography)
- (15 min) 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

IT departments assumed their companies use 51 cloud services

Reality check: They actually use an average of 730

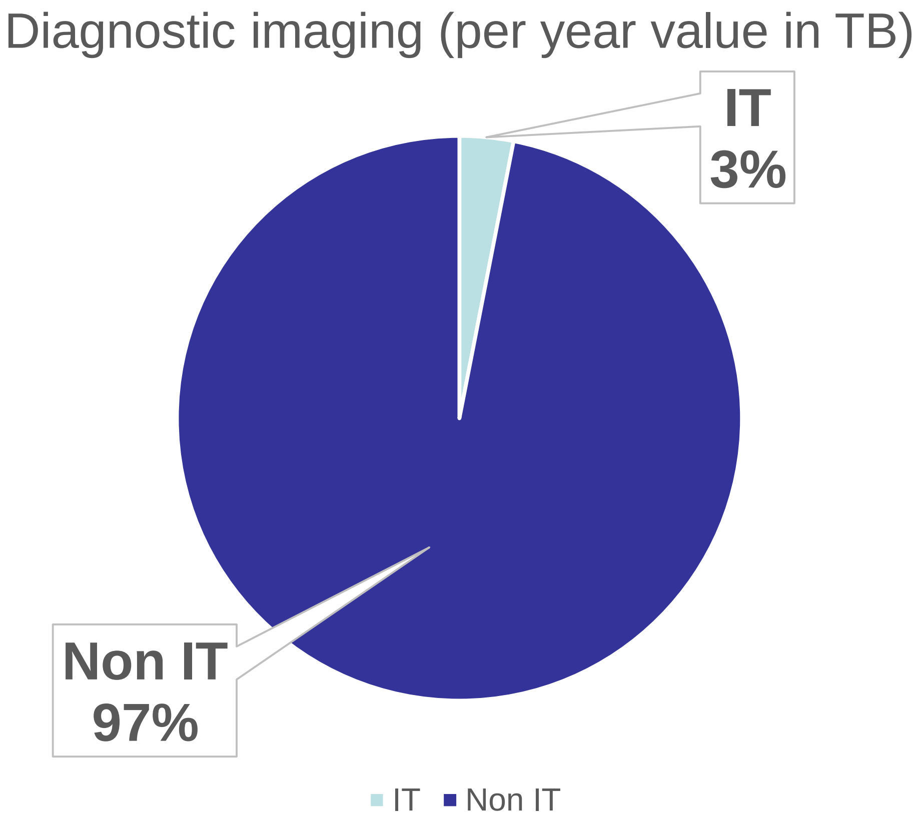
(That's ***15x more*** cloud services.)

Paradox #1

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

Real life example: diagnostic imaging in an hospital:

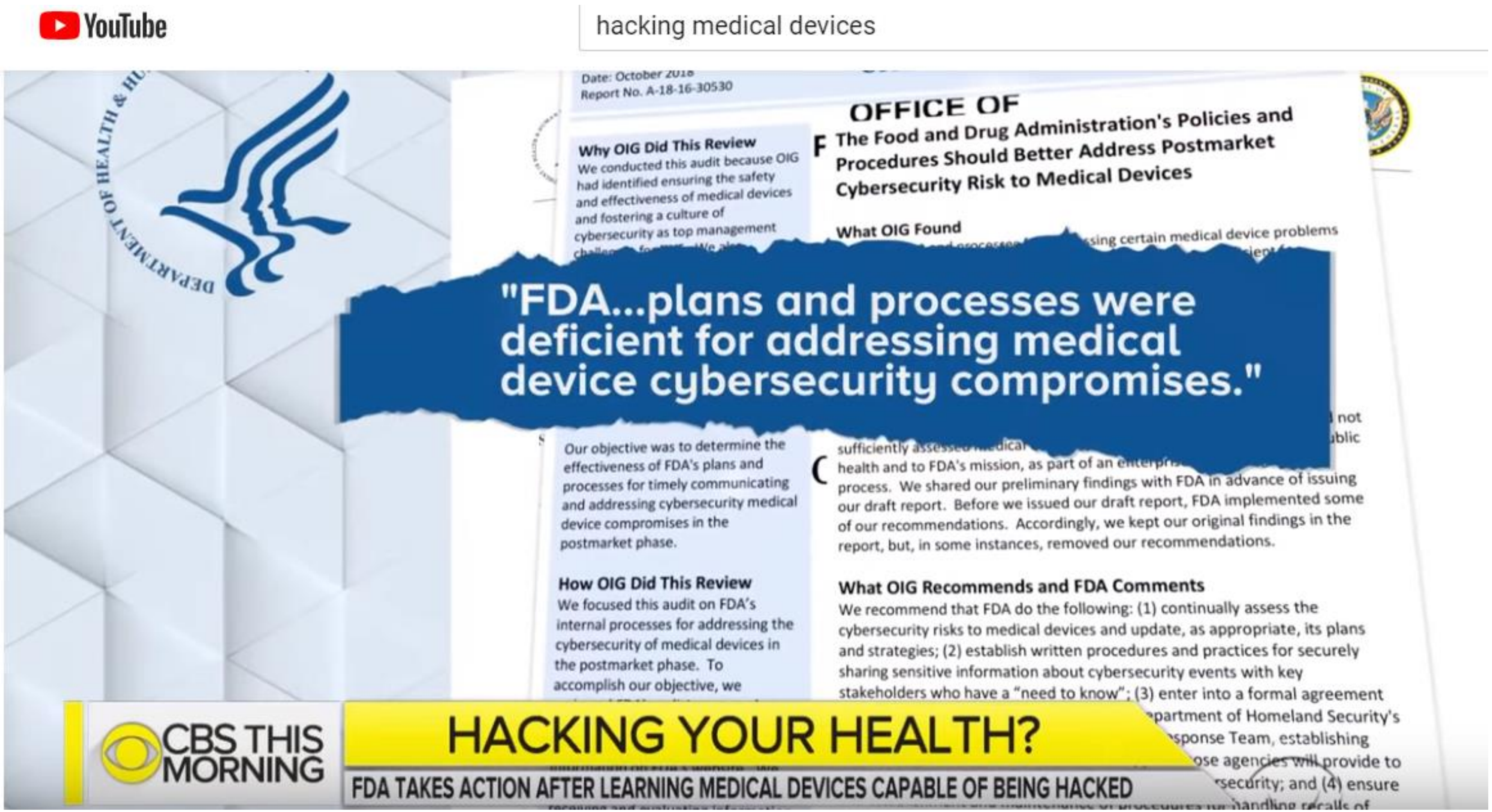
20TB Managed by IT (RIS-PACS), 631TB not managed by IT (or not managed?)



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”

Paradox #2: Hacking a medical Device



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

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.

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 Found
sing certain medical device problems

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

not
ublic
sufficiently assessed medical
health and to FDA's mission, as part of an enterpri
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.

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

CBS THIS MORNING

HACKING YOUR HEALTH?

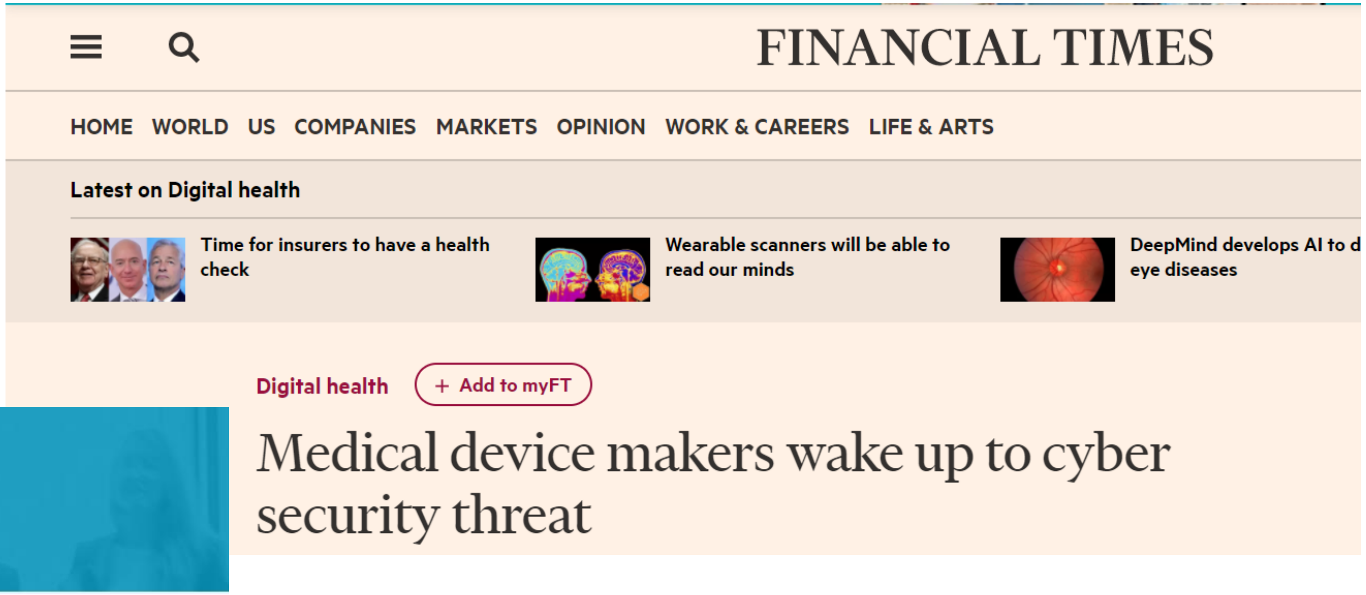
FDA TAKES ACTION AFTER LEARNING MEDICAL DEVICES CAPABLE OF BEING HACKED

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

Paradox #2

FROM THE BUYER SIDE:

Clinical Engineers evaluate and manage medical devices but…lack competencies in cybersecurity (and sometimes awareness of the risk level)



FINANCIAL TIMES

HOME WORLD US COMPANIES MARKETS OPINION WORK & CAREERS LIFE & ARTS

Latest on Digital health

Time for insurers to have a health check

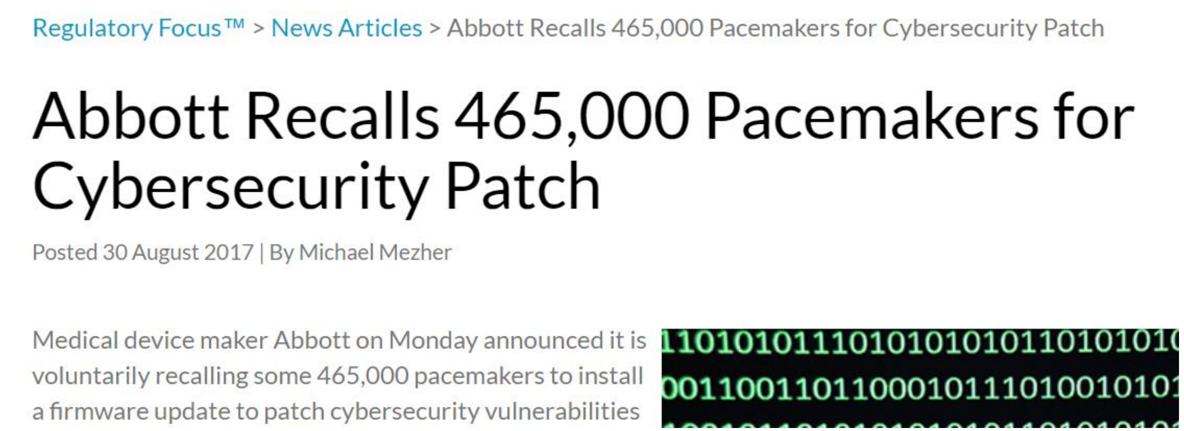
Wearable scanners will be able to read our minds

DeepMind develops AI to d eye diseases

Digital health

Medical device makers wake up to cyber security threat

RF Regulatory Focus™



Regulatory Focus™ > News Articles > Abbott Recalls 465,000 Pacemakers for Cybersecurity Patch

Abbott Recalls 465,000 Pacemakers for Cybersecurity Patch

Posted 30 August 2017 | By Michael Mezher

Medical device maker Abbott on Monday announced it is voluntarily recalling some 465,000 pacemakers to install a firmware update to patch cybersecurity vulnerabilities

FROM THE SUPPLIER SIDE:

Historically Engineering department of medical device manufacturers did not embed cyber security measure in device design process (security by design). Everything OK for “closed” devices. Then… wi-fi and remote control were so tempting…
(PS: PHASE OUT on Implanted devices is a problem!)

Paradox #2

- Clinial Engineering and ICT cannot be considere separate fields anymore
- Almost every equipment/medical device has a software component
- Clinical Engineering is the first buyer of IT Systems in many hospitals

Top 10 Health Technology Hazards for 2018

A Report from Health Devices

health DEVICES

ECRI Institute

The Discipline of Science. The Integrity of Independence.

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 Configured Secondary Notification 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

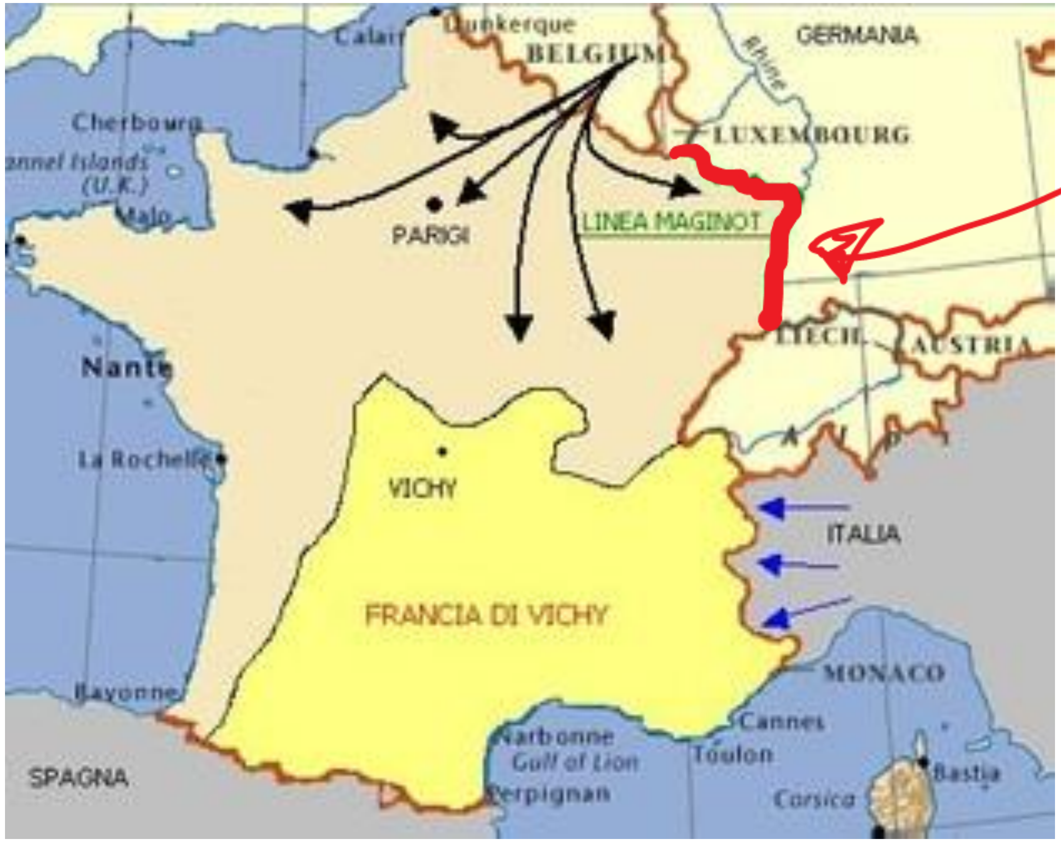
WE (C.I.O.s) THINK
WE ARE HERE

BUT... → WE ARE HERE

BEST ANALOGY: WWW.THREATSPROJECT.EU

Paradox #3

Holistic Approach (local hyper-security is dangerous)

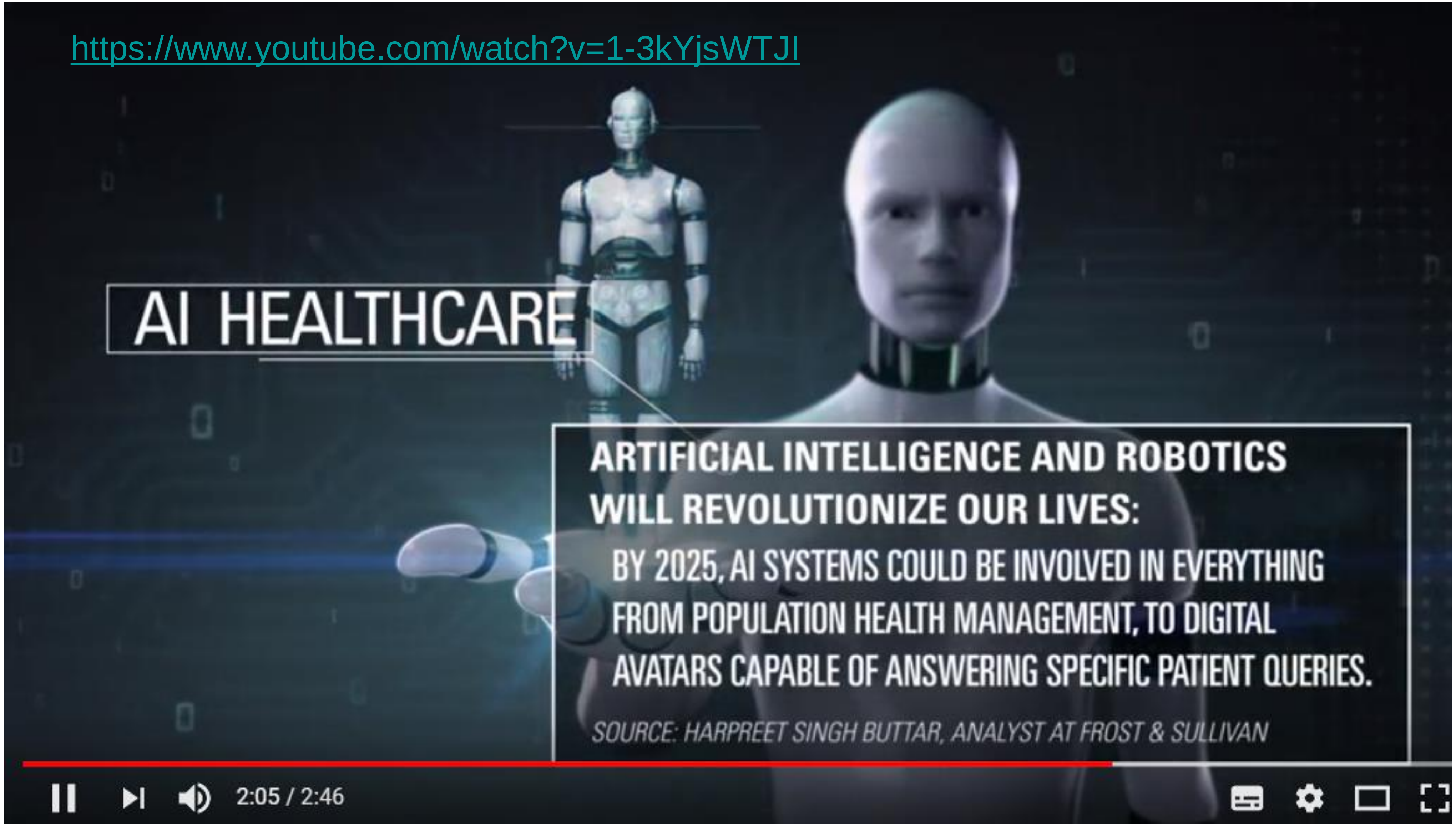


- Maginot line was not crazy: it was ment to be part of a global (holistic) strategy
- Local Hyper security (what IT Department are doing now) is a problem because absorbs most of the resources without mitigating risk (se next slides…)

Agenda

- (15 min) Context: cybersecurity & IoT in Healthcare
- (15 min) 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
- (15 min) Paradigm Shift Ahead!
  - It’s all about data and information!
  - We need a Risk management perspective
  - Review of Strategy – Technology – Processes – People
  - Final considerations
- (Takeoff tracks: personal bibliography)
- (15 min) Q&A

It’s all about data and information! (1/4)



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

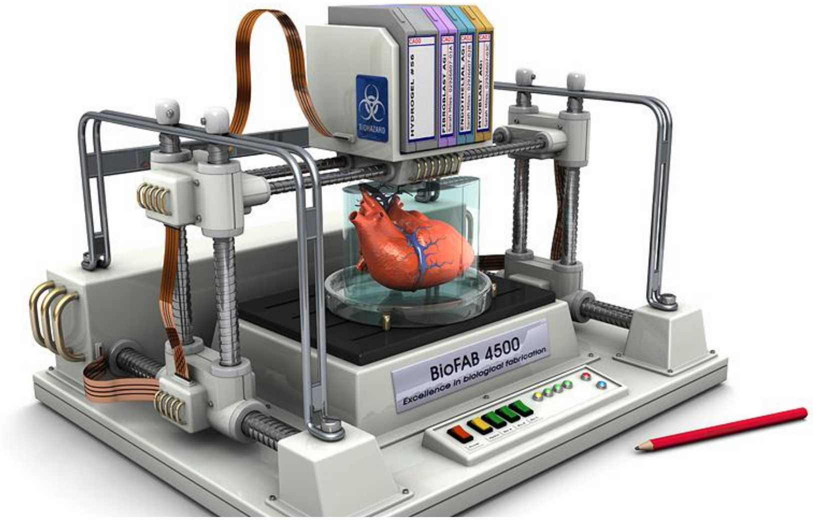
AI HEALTHCARE

ARTIFICIAL INTELLIGENCE AND ROBOTICS WILL REVOLUTIONIZE OUR LIVES:

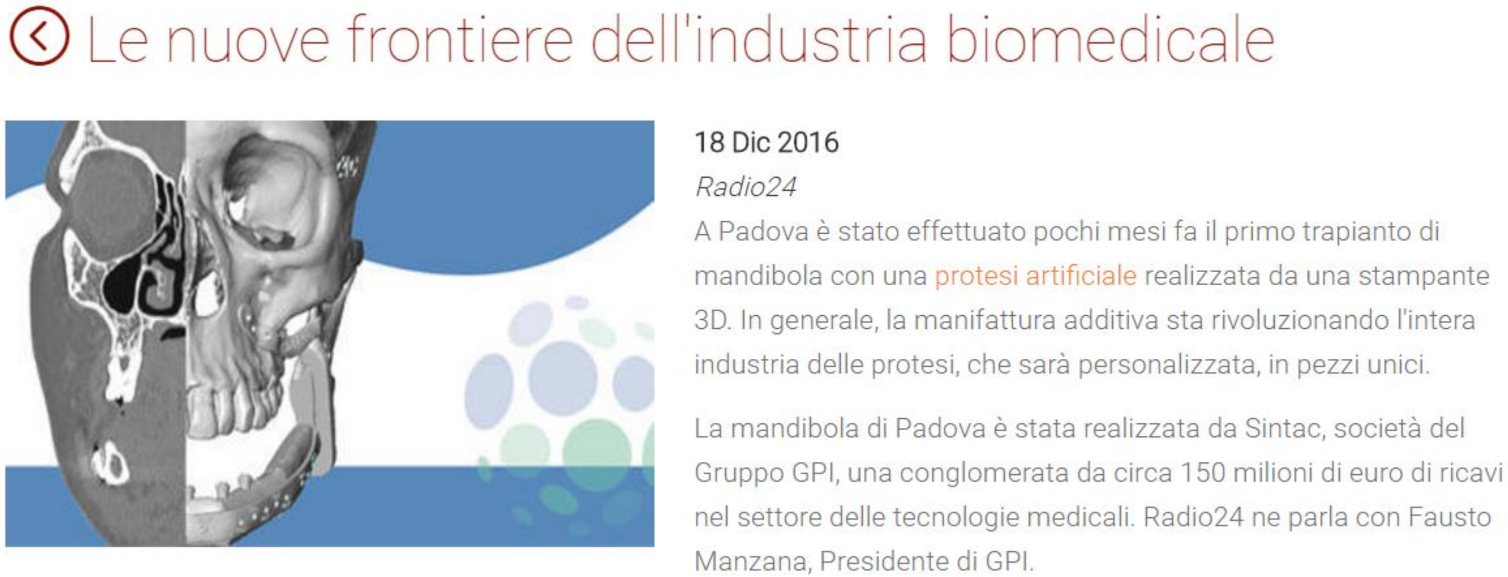
BY 2025, AI SYSTEMS COULD BE INVOLVED IN EVERYTHING FROM POPULATION HEALTH MANAGEMENT, TO DIGITAL AVATARS CAPABLE OF ANSWERING SPECIFIC PATIENT QUERIES.

SOURCE: HARPREET SINGH BUTTAR, ANALYST AT FROST & SULLIVAN

It’s all about data and information! (2/4)



Credit: Getty.com



Le nuove frontiere dell'industria biomedicale

18 Dic 2016

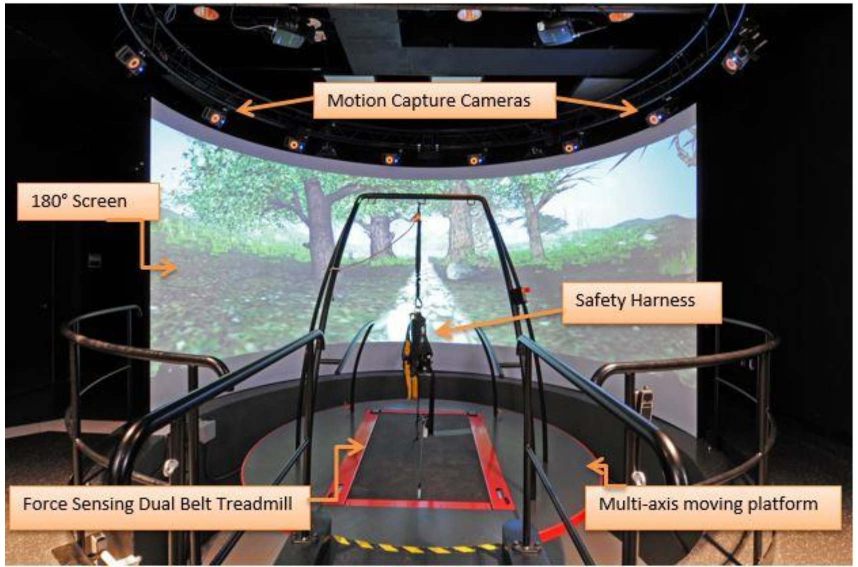
Radio24

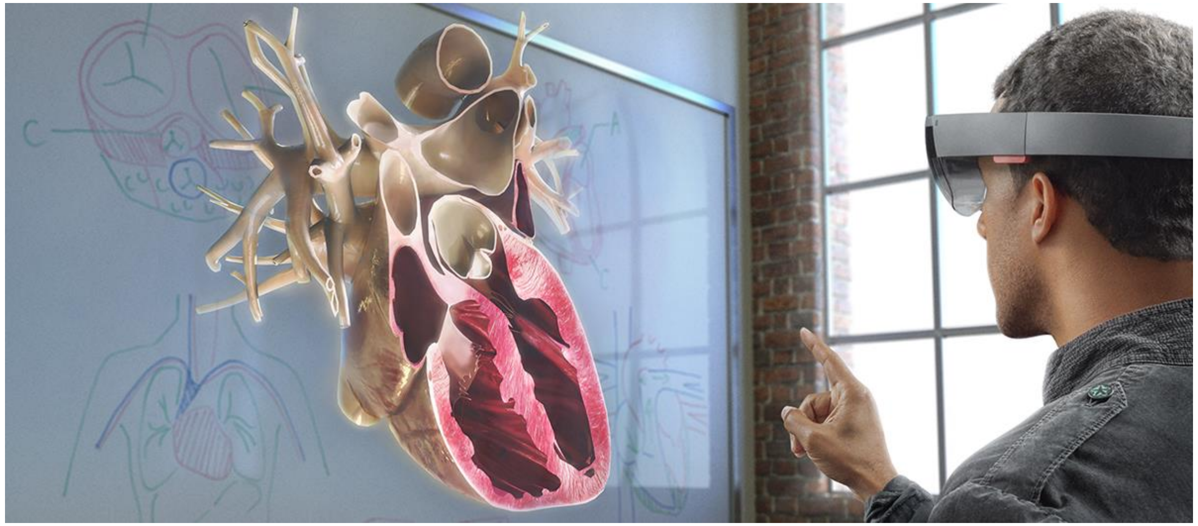
A Padova è stato effettuato pochi mesi fa il primo trapianto di mandibola con una protesi artificiale realizzata da una stampante 3D. In generale, la manifattura additiva sta rivoluzionando l'intera industria delle protesi, che sarà personalizzata, in pezzi unici.

La mandibola di Padova è stata realizzata da Sintac, società del Gruppo GPI, una conglomerata da circa 150 milioni di euro di ricavi nel settore delle tecnologie medicali. Radio24 ne parla con Fausto Manzana, Presidente di GPI.

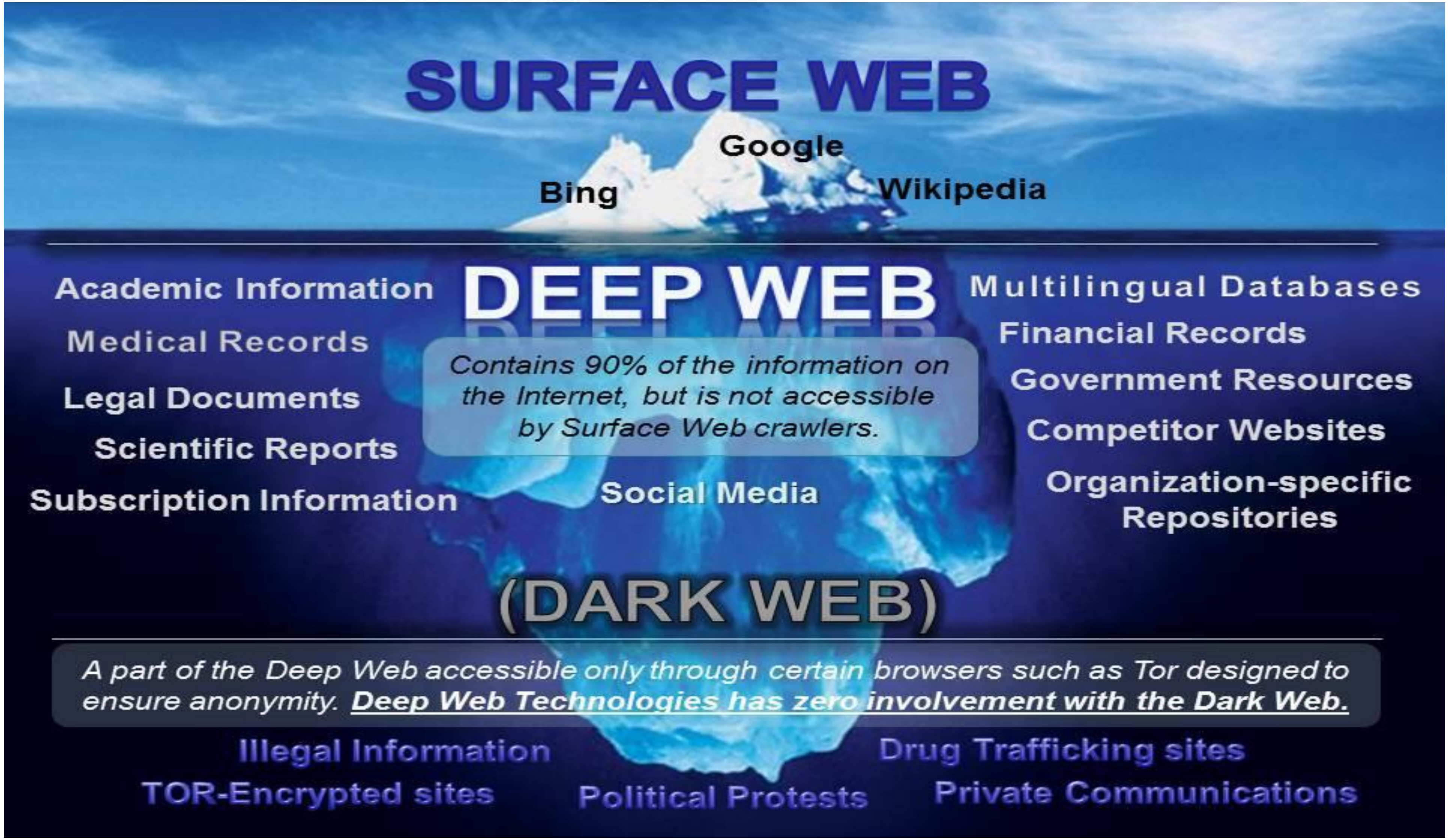
It’s all about data and information! (3/4)

- Healthcare applications
  - Education (Hololens)
  - «Flight simulators» for surgeons
  - Rehabilitation (The Ottawa Hospital)





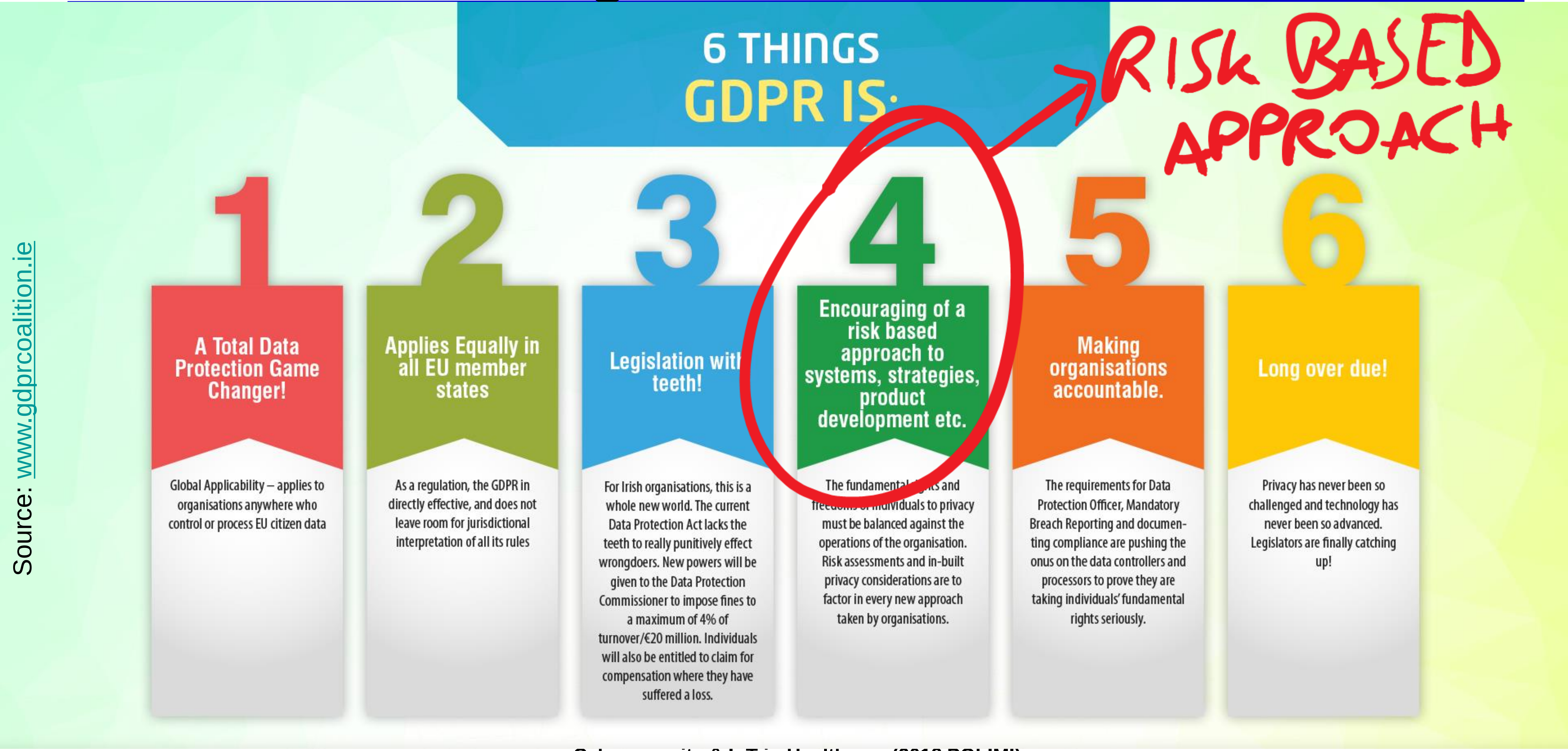
It’s all about data and information! (4/4)



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

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.***

Protecting data: GDPR & Risk



6 THINGS GDPR IS:

RISK BASED APPROACH

1 A Total Data Protection Game Changer!

Global Applicability – applies to organisations anywhere who control or process EU citizen data

2 Applies Equally in all EU member states

As a regulation, the GDPR in directly effective, and does not leave room for jurisdictional interpretation of all its rules

3 Legislation with teeth!

For Irish organisations, this is a whole new world. The current Data Protection Act lacks the teeth to really punitively effect wrongdoers. New powers will be given to the Data Protection Commissioner to impose fines to a maximum of 4% of turnover/€20 million. Individuals will also be entitled to claim for compensation where they have suffered a loss.

4 Encouraging of a risk based approach to systems, strategies, product development etc.

The fundamental rights and freedoms of individuals to privacy must be balanced against the operations of the organisation. Risk assessments and in-built privacy considerations are to factor in every new approach taken by organisations.

5 Making organisations accountable.

The requirements for Data Protection Officer, Mandatory Breach Reporting and documenting compliance are pushing the onus on the data controllers and processors to prove they are taking individuals' fundamental rights seriously.

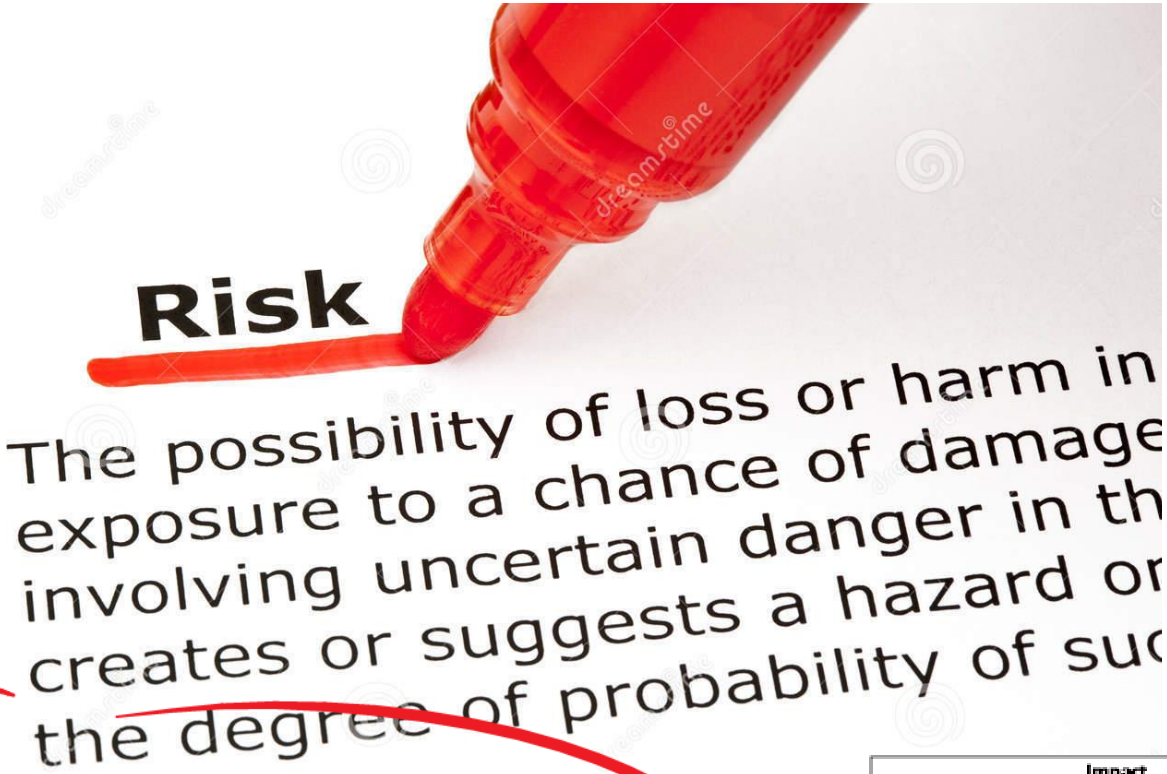
6 Long over due!

Privacy has never been so challenged and technology has never been so advanced. Legislators are finally catching up!

Source: www.gdprcoalition.ie

Risk

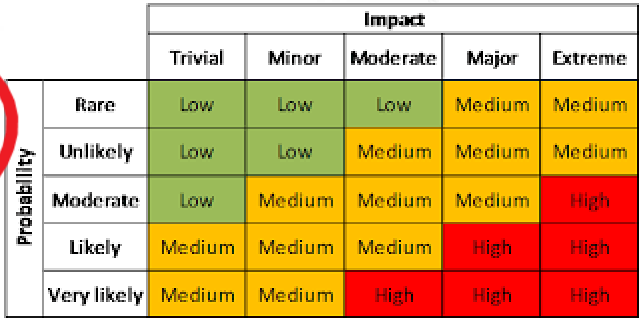
Definition



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

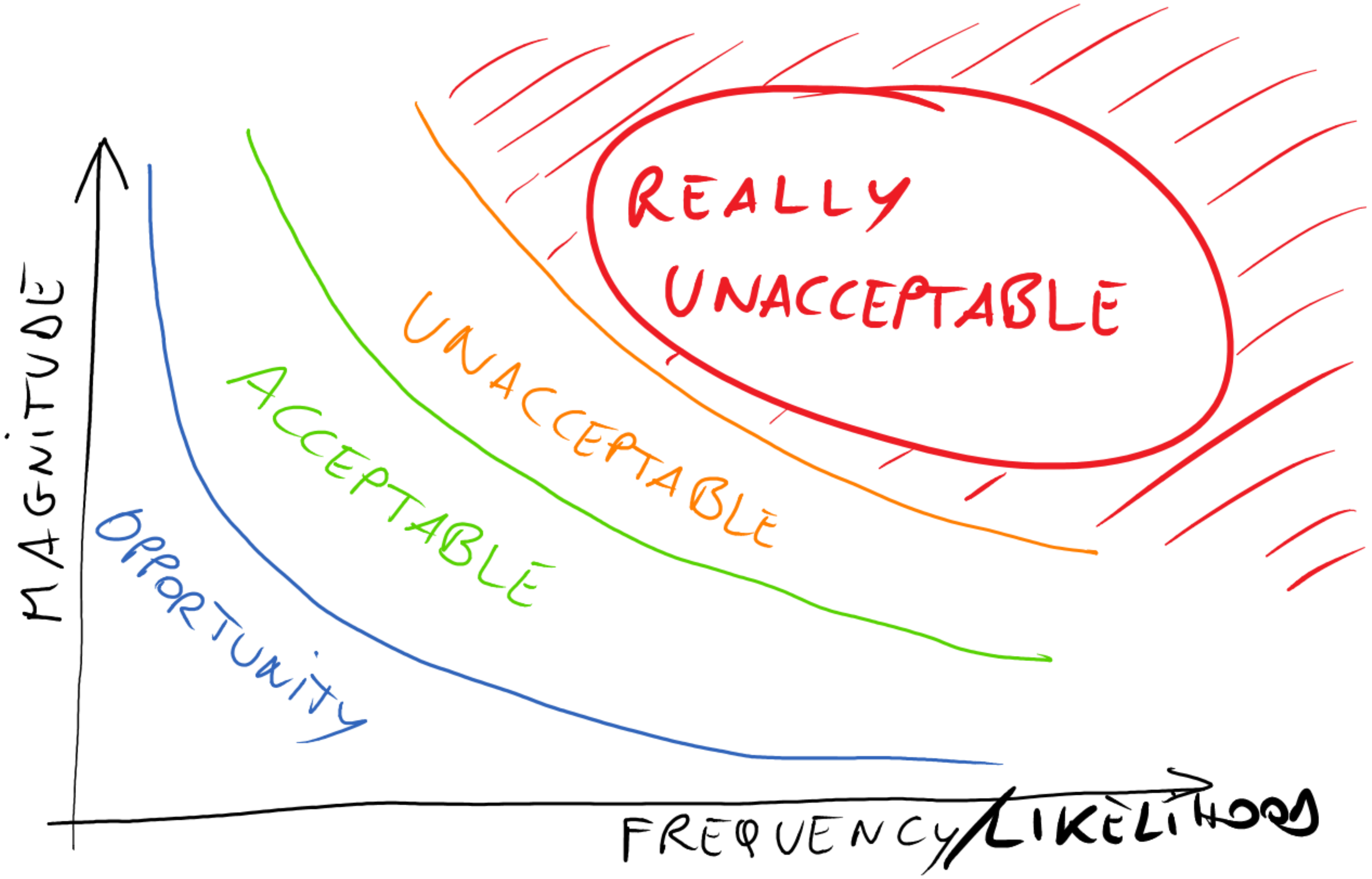
RISK =
PROBABILITY x IMPACT



		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

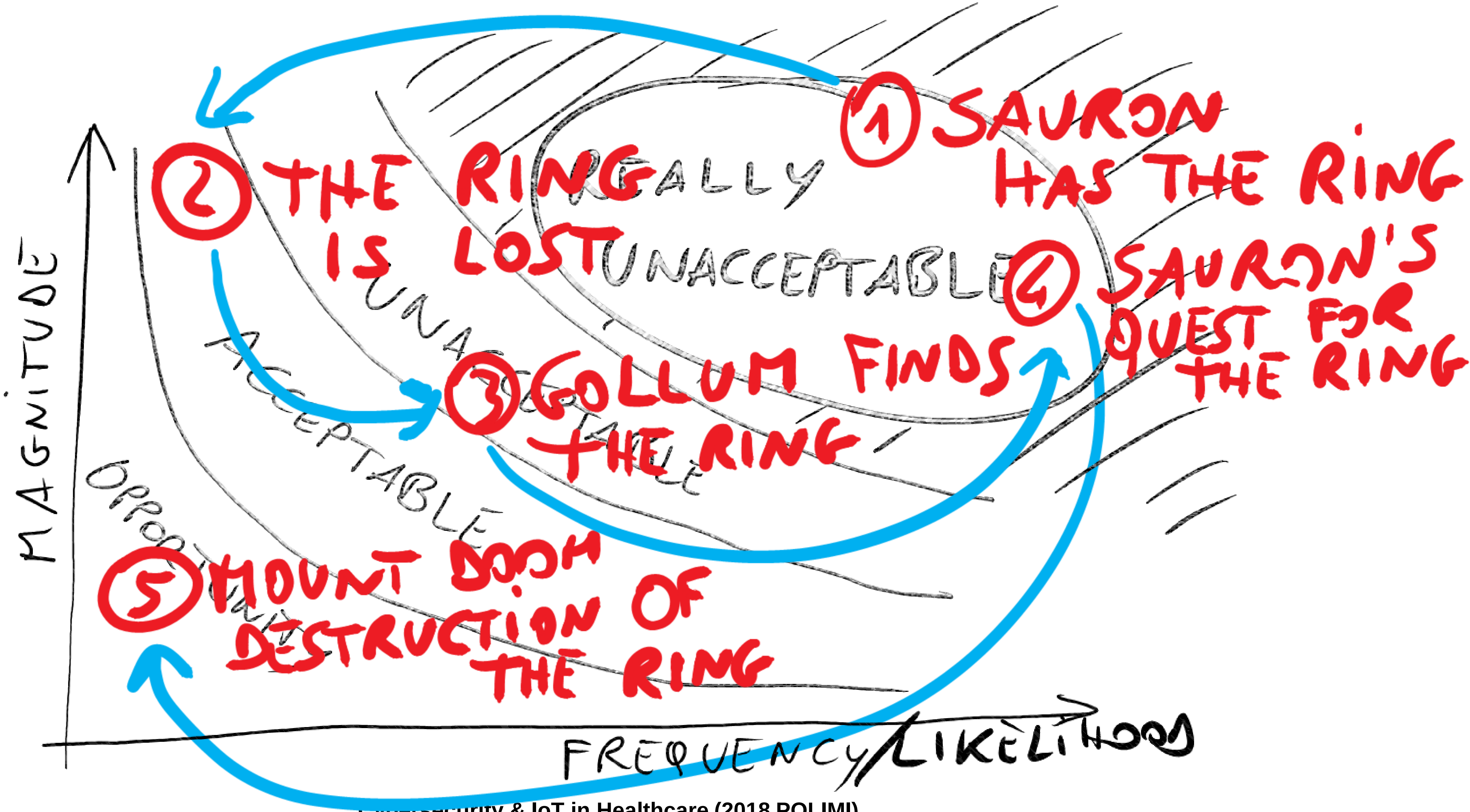
Risk map

Risk Optimization



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

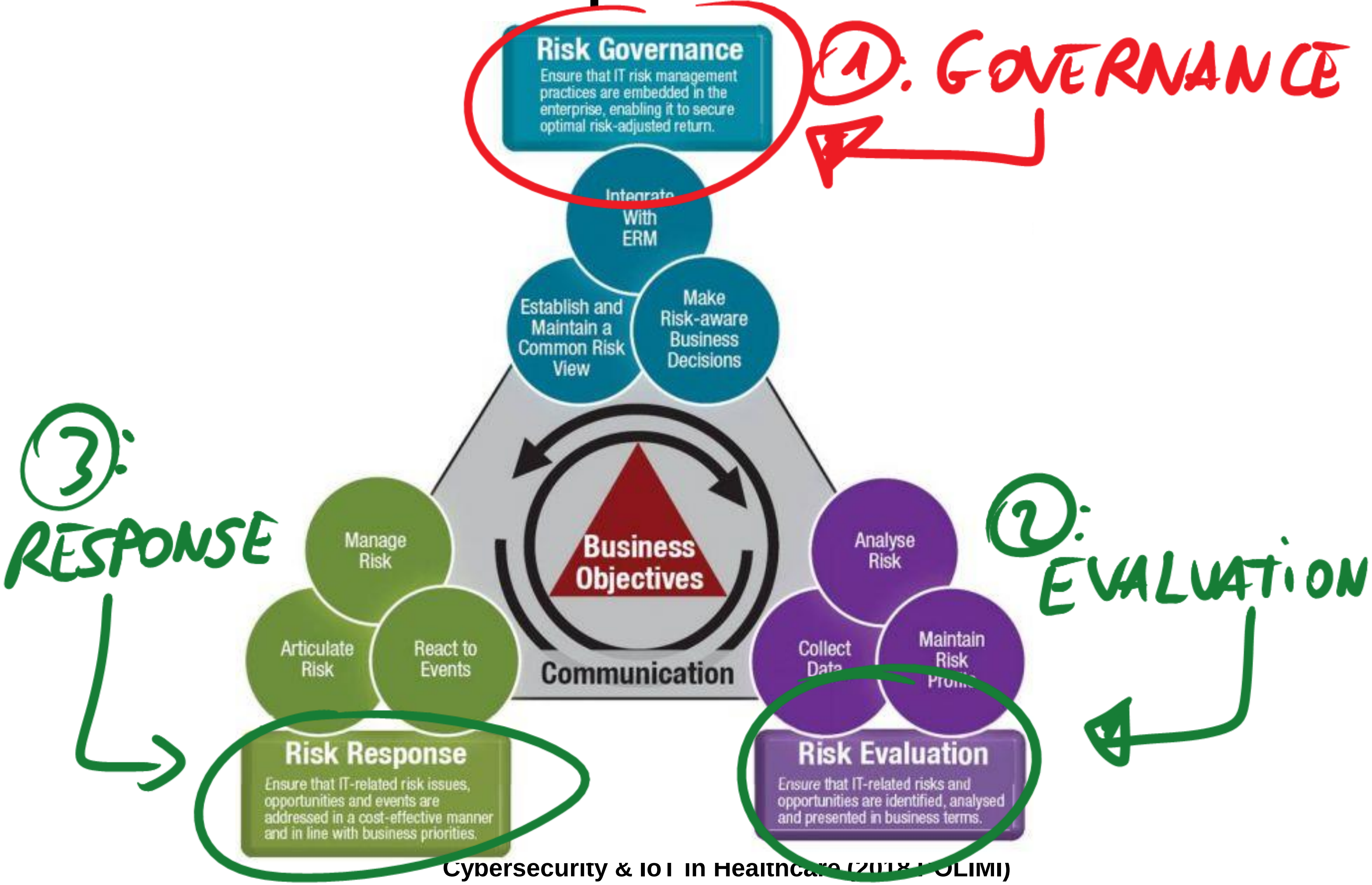
Risk map - example



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

Enterprise Risk Management

Risk Optimization



Risk Governance

Ensure that IT risk management practices are embedded in the enterprise, enabling it to secure optimal risk-adjusted return.

Risk Evaluation

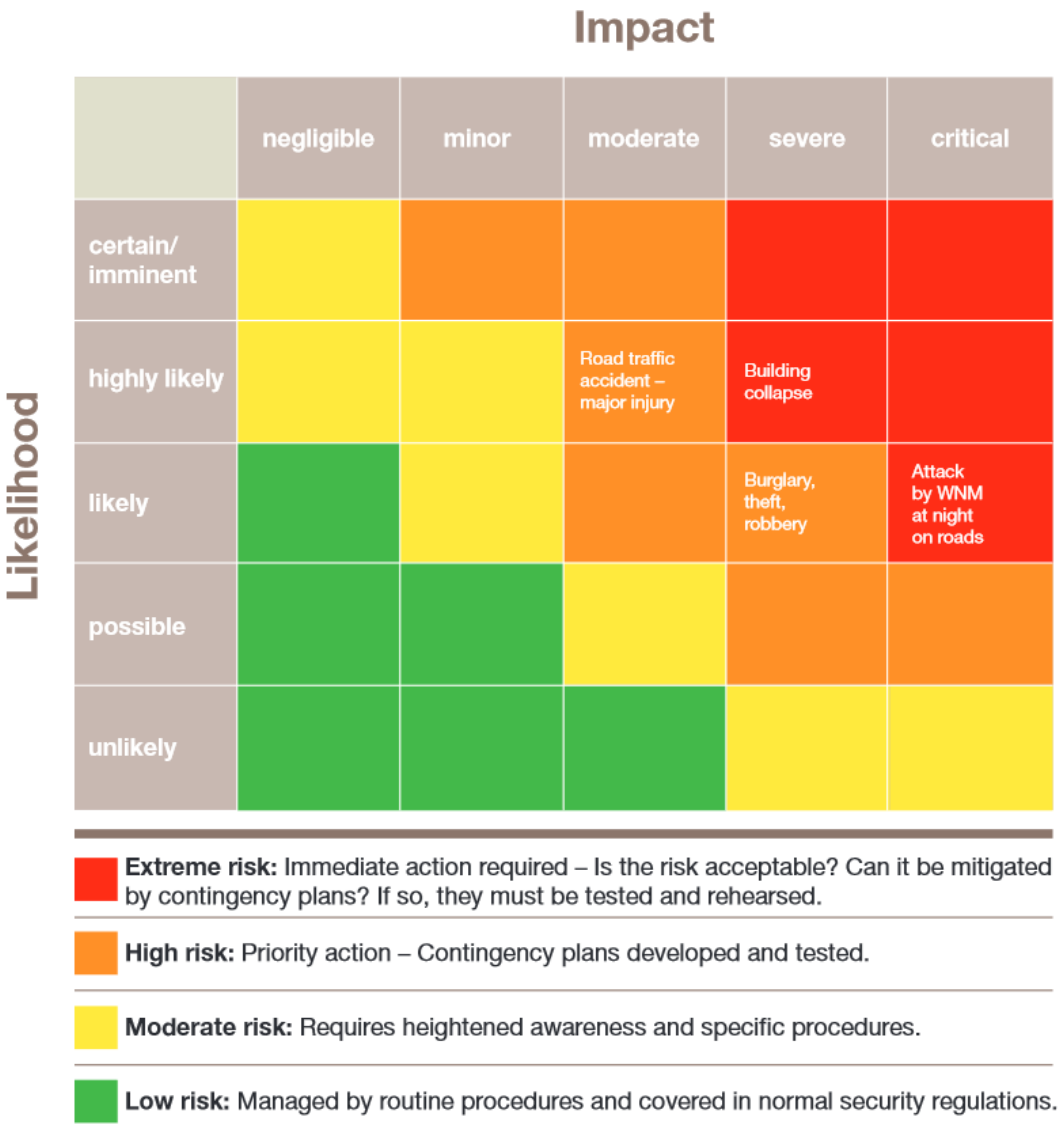
Ensure that IT-related risks and opportunities are identified, analysed and presented in business terms.

Risk Response

Ensure that IT-related risk issues, opportunities and events are addressed in a cost-effective manner and in line with business priorities.

Fonte: ISACA (www.isaca.org) – The RISK IT Framework

Risk evaluation – Heat map



Impact

Likelihood

	negligible	minor	moderate	severe	critical
certain/ imminent	🟨	🟧	🟧	🟥	🟥
highly likely	🟨	🟨	🟧 Road traffic accident – major injury	🟥 Building collapse	🟥
likely	🟩	🟨	🟧	🟧 Burglary, theft, robbery	🟥 Attack by WNM at night on roads
possible	🟩	🟩	🟨	🟧	🟧
unlikely	🟩	🟩	🟩	🟨	🟨

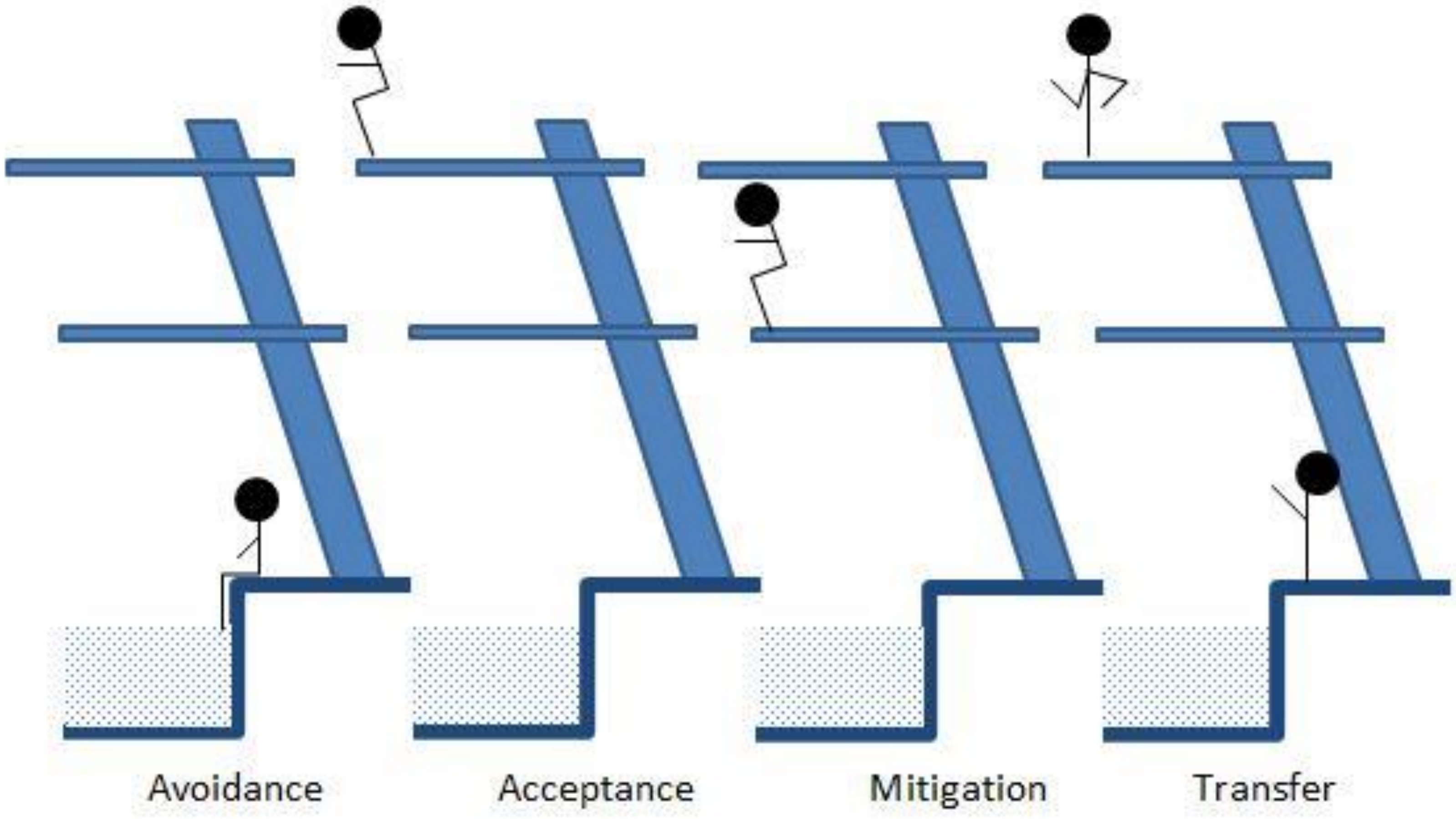
🟥 **Extreme risk:** Immediate action required – Is the risk acceptable? Can it be mitigated by contingency plans? If so, they must be tested and rehearsed.

🟧 **High risk:** Priority action – Contingency plans developed and tested.

🟨 **Moderate risk:** Requires heightened awareness and specific procedures.

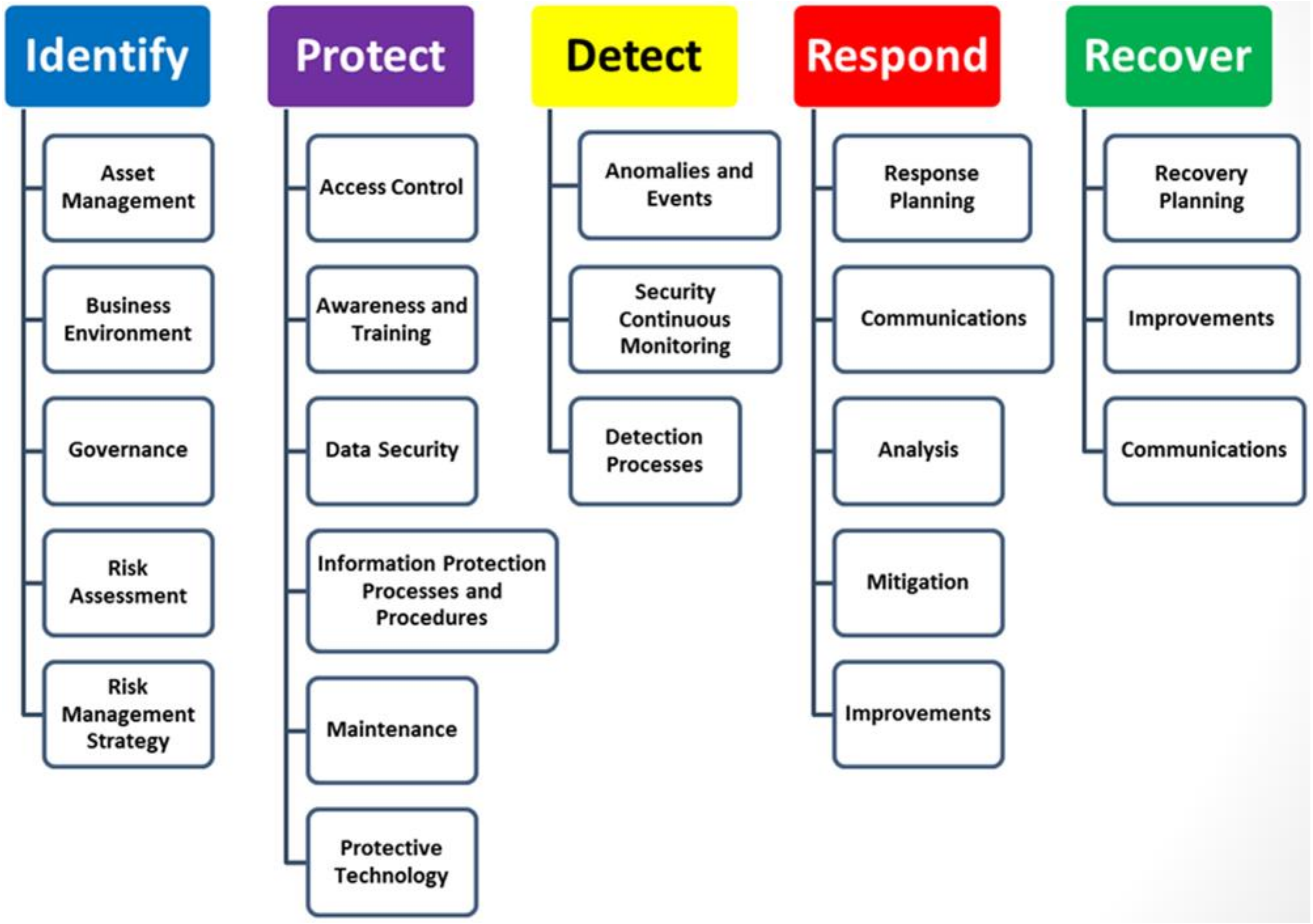
🟩 **Low risk:** Managed by routine procedures and covered in normal security regulations.

Risk response strategies



Strategies for dealing with risk

NIST CSF & Risk



Identify
- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

Protect
- Access Control
- Awareness and Training
- Data Security
- Information Protection Processes and Procedures
- Maintenance
- Protective Technology

Detect
- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes

Respond
- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

Recover
- Recovery Planning
- Improvements
- Communications

Source: www.nist.gov/cyberframework

Other frameworks

This table shows the most popular cyber security frameworks in healthcare, according to the 2018 HIMSS Cybersecurity Survey.

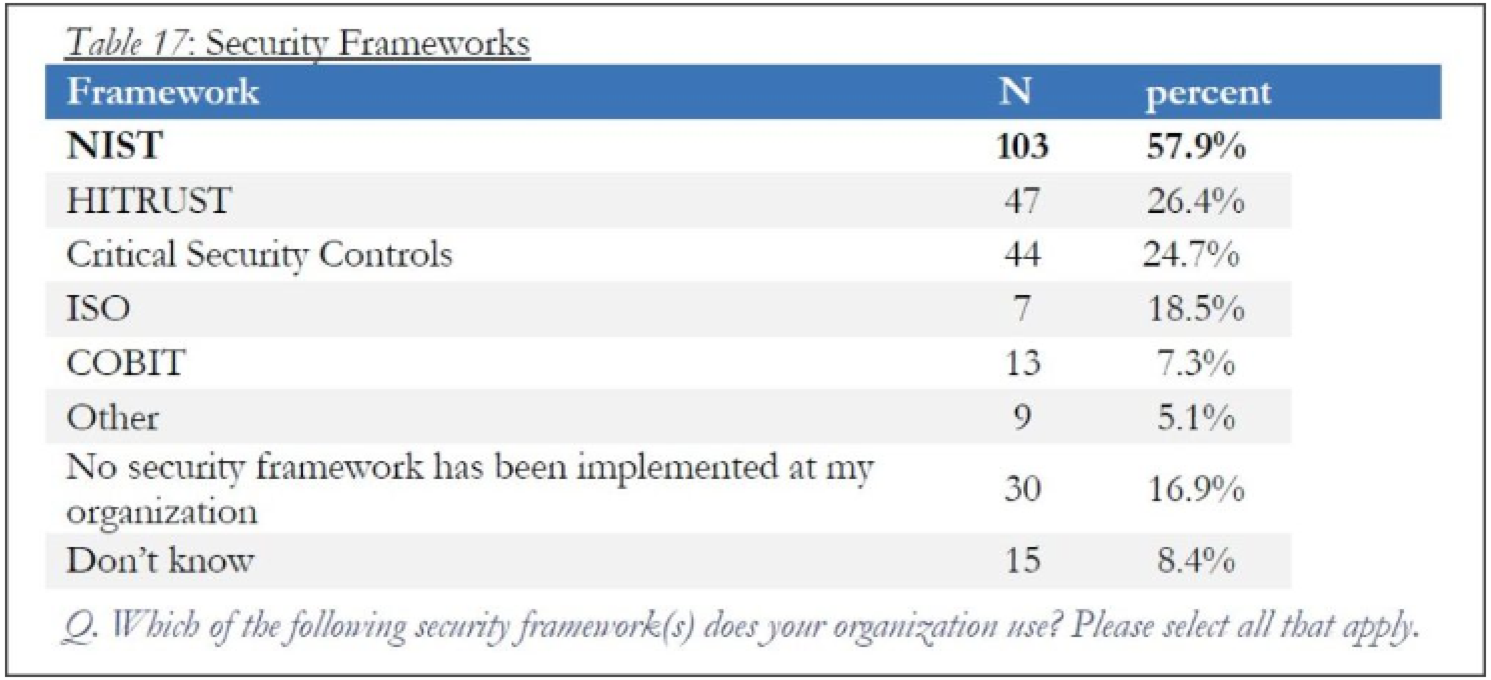


Table 17: Security Frameworks

Framework	N	percent
NIST	**103**	**57.9%**
HITRUST	47	26.4%
Critical Security Controls	44	24.7%
ISO	7	18.5%
COBIT	13	7.3%
Other	9	5.1%
No security framework has been implemented at my organization	30	16.9%
Don't know	15	8.4%

Q. Which of the following security framework(s) does your organization use? Please select all that apply.

HIMSS surveyed 239 healthcare information security professionals from Dec. 2017 through Jan. 2018 for the report. When asked to list the network security frameworks used at their organizations, respondents could select multiple answers.

Source: https://www.calyptix.com/hipaa/top-5-cyber-security-frameworks-in-healthcare/

Beyond the frameworks: S.T.O.P.

To address cybersecurity in healthcare we need to review:

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 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
- **In selecting the tools and services to support security, the IT department should incorporate an architectural vision** more than a mere evaluation of a single product in a traditional best-of-breed approach

PROCESSES:

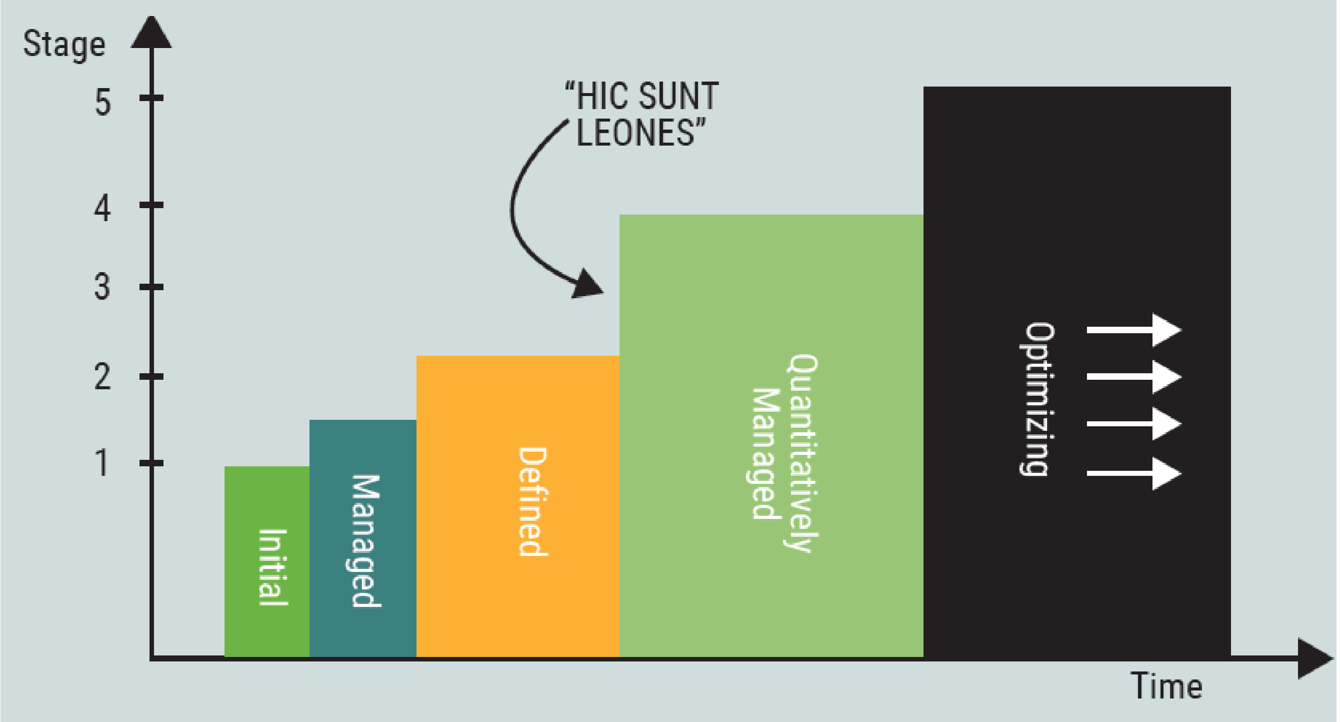
- **New methodology needed!** Beyond IT methodologies **(**IT Infrastructure Library [ITIL], COBIT® 5, International Organization for Standardization [ISO]/International Electrotechnical Commission [IEC] 27001) and Clinical Engineering Methodologies (health technology assessment [HTA])

ORGANIZATION:

- **Unification/coordination of different technology departments is a must!** 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!**

Source: G. Pozza - Healthcare Security—Three Paradoxes and the Need for a Paradigm Shift (ISACA Journal – Vol. 3 2018)

Final considerations: a proposal

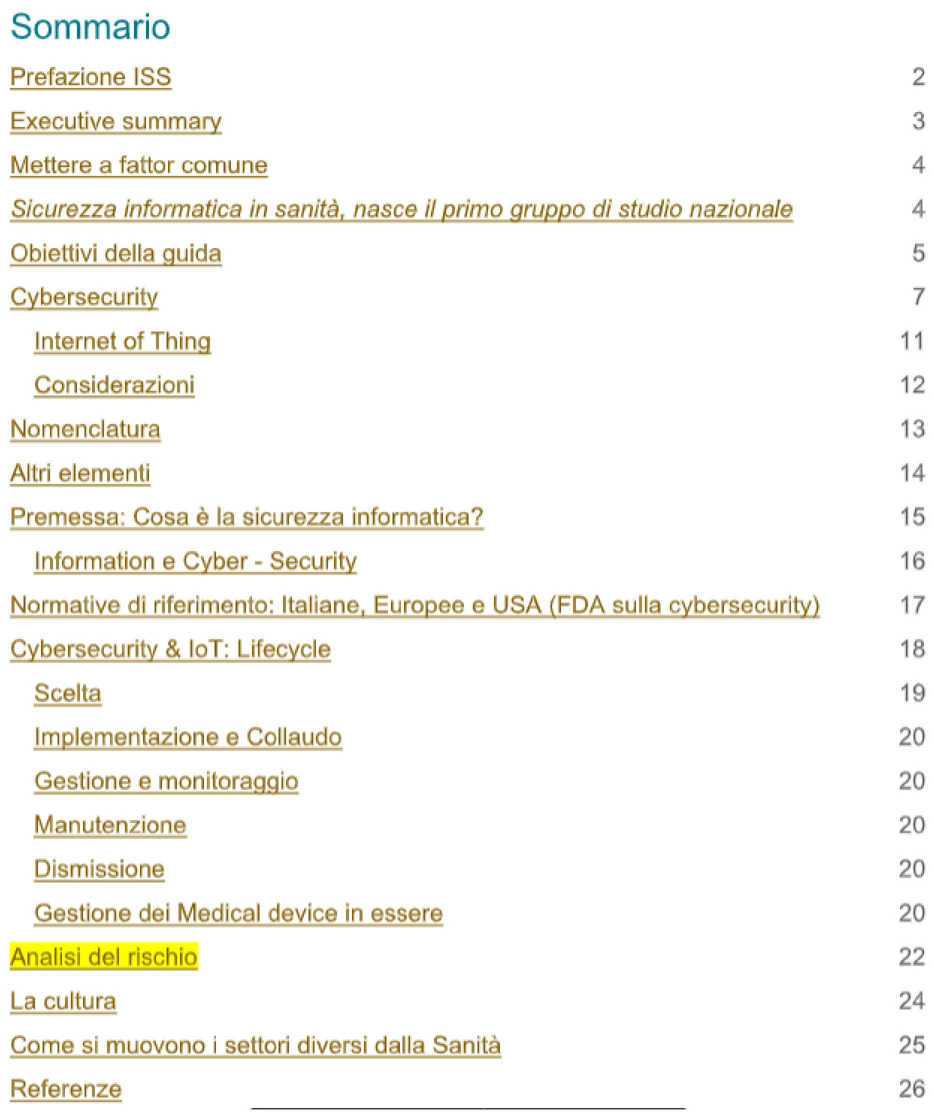


The stages can be defined as follows:

- **Stage 1 (Initial)**—"Local," not structured, security management exists.
- **Stage 2 (Managed)**—Structured security management for ICT is in place. There is general awareness about security in other technical areas (using the ICT department as the internal expert on call). Risk assessment present.
- **Stage 3 (Defined)**—Coordination efforts and policies on security are in place among different technology areas (ICT, facility, clinical engineering), but no dedicated cross-border organization on security exists. A structured framework is used.
- **Stage 4 (Quantitatively Managed)**—A cross-border role on security (e.g., the CISO reporting to the CEO) oversees security strategy and policies with a 360-degree approach. At the departmental level, security is well managed, with key performance indicators (KPIs) and monitoring processes.
- **Stage 5 (Optimizing)**—Converged security strategy and the organization. The technology departments in the hospital are under a unified responsibility. Security and governance are managed with a holistic approach.

Source: G. Pozza - Healthcare Security—Three Paradoxes and the Need for a Paradigm Shift (ISACA Journal – Vol. 3 2018)

Final consideraations: AISIS & AIIC



Sommario

That's one small step for a man, one giant leap for mankind!

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

Agenda

- (15 min) Context: cybersecurity & IoT in Healthcare
- (15 min) 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
- (15 min) Paradigm Shift Ahead!
  - It’s all about data and information!
  - We need a Risk management perspective
  - Review of Strategy – Technology – Processes – People
  - Final considerations
- (Takeoff tracks: personal bibliography)
- (15 min) Q&A

Takeoff tracks (personal bibliography)

Security in healthcare:

Pozza, G. Healthcare Security—Three Paradoxes and the Need for a Paradigm Shift (ISACA Journal – Vol. 3 2018)

HIPAA Journal, "Major 2016 Healthcare Data Breaches: Mid Year Summary," *HIPAA Journal*, 11 July 2016, *https://www.hipaajournal.com/major-2016-healthcare-data-breaches-mid-year-summary-3499/*

Clusit, Rapporto Clusit 2018 sulla sicurezza ICT in Italia, CLUSIT, Italy, 2018

Houlding, D.; "6 Most Common Types of Healthcare Data Security Breaches*,"* IT Peer Network, 18 February 2016, *https://itpeernetwork.intel.com/6-most-common-types-of-healthcare-data-security-breaches/*

DeGaspari, J.; "Managing the Data Explosion," Healthcare Informatics, 1 October 2013, www.healthcare-informatics.com/article/managing-data-explosion

Earle, N.; "Do You Know the Way to Ballylickey? Shadow IT and the CIO Dilemma," Cisco Blogs, 6 August 2015, *https://blogs.cisco.com/cloud/shadow-it-and-the-cio-dilemma*

Pozza, G. (2014, June). Healthcare SCACA Systems and Medical Devices Data Systems Governance and Security: A No Man's Land? - Journal of Clinical Engineering: July/September 2014 - Volume 39 - Issue 3 - p 136-141;

Rogers, M.; "The Shadow IT Phenomenon*,"* Logicalis, *https://www.us.logicalis.com/globalassets/united-states/whitepapers/cio-survey-2015-shadow-it-phenomenon.pdf*

Babbar, P.; A. Hemal; "Robot-Assisted Urologic Surgery in 2010—Advancements and Future Outlook," *Urology Annals*, 2011, vol. 3, no. 1, *www.urologyannals.com/article.asp?issn=0974-7796;year=2011;volume=3;issue=1;spage=1;epage=7;aulast=Babbar*

Food and Drug Administration, "Is The Product A Medical Device?" USA, *www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/ucm051512.htm*

Security in healthcare:

Lemke, H.; M. Vannier; “The Operating Room and the Need for an IT Infrastructure and Standards,” *International Journal of Computer Assisted Radiology and Surgery*, November 2006, vol. 1, no. 3, p. 117-121

Food and Drug Administration, Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (Formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication, USA, 29 August 2017, https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm

Sholten, B.; C. S. Filho; E. Smits; “Who Owns Information Systems in the Plant?” Accenture, 2012, https://www.accenture.com/t20150624T211125__w__/in-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Industries_10/Accenture-MES-Who-Owns-Information-Systems-Plant.pdf

US Department of Health and Human Safety, Office of Civil Rights, “Cases Currently Under Investigation,” https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Pozza, G.; J. D. Halamka; *The Fifth Domain: > Wake Up, Neo*, CreateSpace Independent Publishing Platform, 19 January 2014

Pozza, G. (2014, October). Beyond BYOD: Can I Connect My Body to Your Network? - ISACA Journal Vol. 5, 2014;

THREATS, www.threatsproject.eu/index.html

Grimes, S. L.; “Convergence of Clinical Engineering and Information Technology,” 24 August 2006, http://accenet.org/publications/Downloads/Presentations/chime.pdf

ECRI Institute, *Top 10 Health Technology Hazards*, ECRI, 2018

Ridley, E. L. (2012, 4 6). Imaging devices present hidden security risks. Retrieved from AuntMinnie: https://www.auntminnie.com/index.aspx?sec=ser&sub=def&pag=dis&ItemID=98957

The C.I.O.'s role

Broadbend, M; Kitzis, E (2004). The New CIO Leader: Setting the Agenda and Delivering Results. Harvard Business School Press.

Aron, D; Graha, W (2014). Taming the Digital Dragon: The 2014 CIO Agenda. Retrieved from https://www.gartner.com/imagesrv/cio/pdf/cio_agenda_insights2014.pdf

Heller, M (2012). The CIO Paradox: Battling the Contradictions of IT Leadership. Bibliomotion Inc.

De Marco, M; Occhini, G; Bellini, R. The Evolving Role of CIOs in Changing Business Settings from 1980 to 2010: Literature Review and Emerging Trends. IFIP Congress – Shenzen 2011

Governance:

ISO. (2008). ISO 38500. Retrieved from 38500: http://www.38500.org/

ISACA. (2014). IT Governance Institute. Retrieved from ITGI: http://www.isaca.org/About-ISACA/IT-Governance-Institute/Pages/default.aspx

ISACA. (2014). CGEIT Review Manual 2014. ISACA.

Carr, N. G. (2003, May). IT Doesn't Matter. Harvard Business Review.

Holt, A. L. (2013). Governance of IT: An Executive Guide to ISO/Iec 38500. BCS.

McFarlan, F. W., & Nolan, R. L. (2003, August 25). Why IT Does Matter. Retrieved December 2, 2013, from Harvard Business School Working Knowledge: http://hbswk.hbs.edu/item/3637.html

Parkinson, M. J., & Baker, N. J. (2005). IT and Enterprise Governance. Information Systems Control Journal, 3.

Plant, R. (2013, August 15). IT Doesn't Matter (to CEOs). Retrieved December 5, 2013, from http://blogs.hbr.org/2013/08/it-doesnt-matter-to-ceos/

Porter, M. (2001). Strategy and the Internet. Harward Business Review.

Ross, J. W., & Weill, P. (2006). Enterprise Architecture As Strategy. Harvard Business School Press.

Ross, J. W., & Weill, P. (2009). IT Savvy. Harvard Business School Press.

United Kingdom's Cabinet Office. (n.d.). Retrieved 01 24, 2014, from ITIL official web site: http://www.itil-officialsite.com/

Weill, P., & Ross, J. W. (2004). IT Governance: How Top Performers Manage IT Decision Rights for Superior Results. Harvard Business School Press.

The future of IT:
Hunter, R. (2013). The Future of Global Information Security. Gartner.

Rifkin, J (2014). The Zero Marginal Cost Society. Palgrave Macmillan

ICSPA. (2013). Project 2020: Scenarios for the Future of Cybercrime - White Paper for Decision Makers. Retrieved from 2020: http://2020.trendmicro.com

Kurzweil, R. (2005). The Singularity Is Near: When Humans Transcend Biology. Viking.

TrendLabs. (2013). BLURRING BOUNDARIES - Trend Micro Security Predictions for 2014 and Beyond.Trend Micro.

Leadership and competencies:

CEN. (2012). CWA 16458. Brusselles: European Committee for Standardization. Retrieved from CEN WORKSHOP AGREEMENT.

CEN. (2014). e-CF. Retrieved from http://www.ecompetences.eu/

e-CF. (2014). e-CF: ICT Professional Profiles. Retrieved December 6, 2013, from European e-Competences Framework: http://www.ecompetences.eu/

Gareis, K., Husing, T., Birov, S., Bludova, I., Shultz, C., & Korte, W. (2014). e-Skills for jobs in Europe: measuring progress and moving ahead - Final Report . Brusselles: Empirica.

Goleman, D. (2013, December). The Focused Leader. Harvard Business Review.

Grimes, S. L. (2006, August 24). Convergence of Clinical Engineering and Information Technology. Retrieved from ACCE (American College of Clinical Engineering): http://www.accenet.org/downloads/chime.pdf

ISA. (2008, 5). MES ownership up in air. Retrieved from ISA: http://www.isa.org/InTechTemplate.cfm?Section=Communities&template=/TaggedPage/DetailDisplay.cfm&ContentID=69056

Sholten, B., Filho, C. S., & Smits, E. (2012). Who Owns Information Systems in the Plant? Retrieved from Accenture: http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture-MES-Who-Owns-Information-Systems-plant.pdf

Austin, R. D., Nolan, R. L., & S., O. (2009). Adventures of an IT Leader. Harvard Business Press.

Kotter, J., & Rathgeber, H. (2006). Our Iceberg Is Melting. Macmillan.

Kotter, J. (2012). Leading Change.

Waller, G., Hallenbeck, G., & Rubenstrunk, K. (2010). The CIO Edge: 7 Leadership Skills You Need to Drive Results. Harvard Business School Press.

Healthcare:
Christensen, C. (2009). The Innovator's Prescription. McGraw-Hill Professional.

Giunco, F. (2014). Abitare Leggero. Verso una nuova generazione di Servizi per gli anziani. Quaderni dell'osservatorio della Fondazione Cariplo.

Halamka, J. D. (n.d.). Retrieved 1 25, 2014, from Life as a Healthcare CIO: http://geekdoctor.blogspot.com/

Halamka, J. D. (2014). Geekdoctor: Life as a Healthcare CIO. HIMSS.

M. E. Porter, E. O. Teisberg (2006). Redefining Health Care. Harvard Business School Press

… and more:

Turkle, S. (2012). Alone Together: Why We Expect More from Technology and Less from Each Other.

Boyd, D (2015). It's Complicated. (http://www.danah.org/books/ItsComplicated.pdf)

Varanini, F. (2016). Macchine per pensare: l'informatica come prosecuzione della filosofia con altri mezzi (Guerini)

Lindstrom, M. (2016). Small Data (Hoeply)

Watzlawick, P. (1976). How Real Is Real?

Watzlawick, P; Weakland, J; Fisch, R.. (1978). Change.

Turing, A. (1950). Computing machinery and intelligence (http://www.loebner.net/Prizef/TuringArticle.html)

Gotterbarn (et Al.). ACM Code of Ethics (https://www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct)

G. Mulgan (2018). Big Mind (Ed. Codice)

L. Keeley. Ten Types of Innovation: The Discipline of Building Breakthroughs (2018). Ed. John Wiley & Sons

Renée Mauborgne, W. Chan Kim. Blue Ocean Strategy (2015). Ed. Harvard Business Review

C. Accoto. Il mondo dato (2018). Ed. Egea

Kaplan, R. S., & Norton, D. P. (2008). The Execution Premium: Linking Strategy to Operations for Competitive Advantage. Harvard Business Review Press.

Agenda

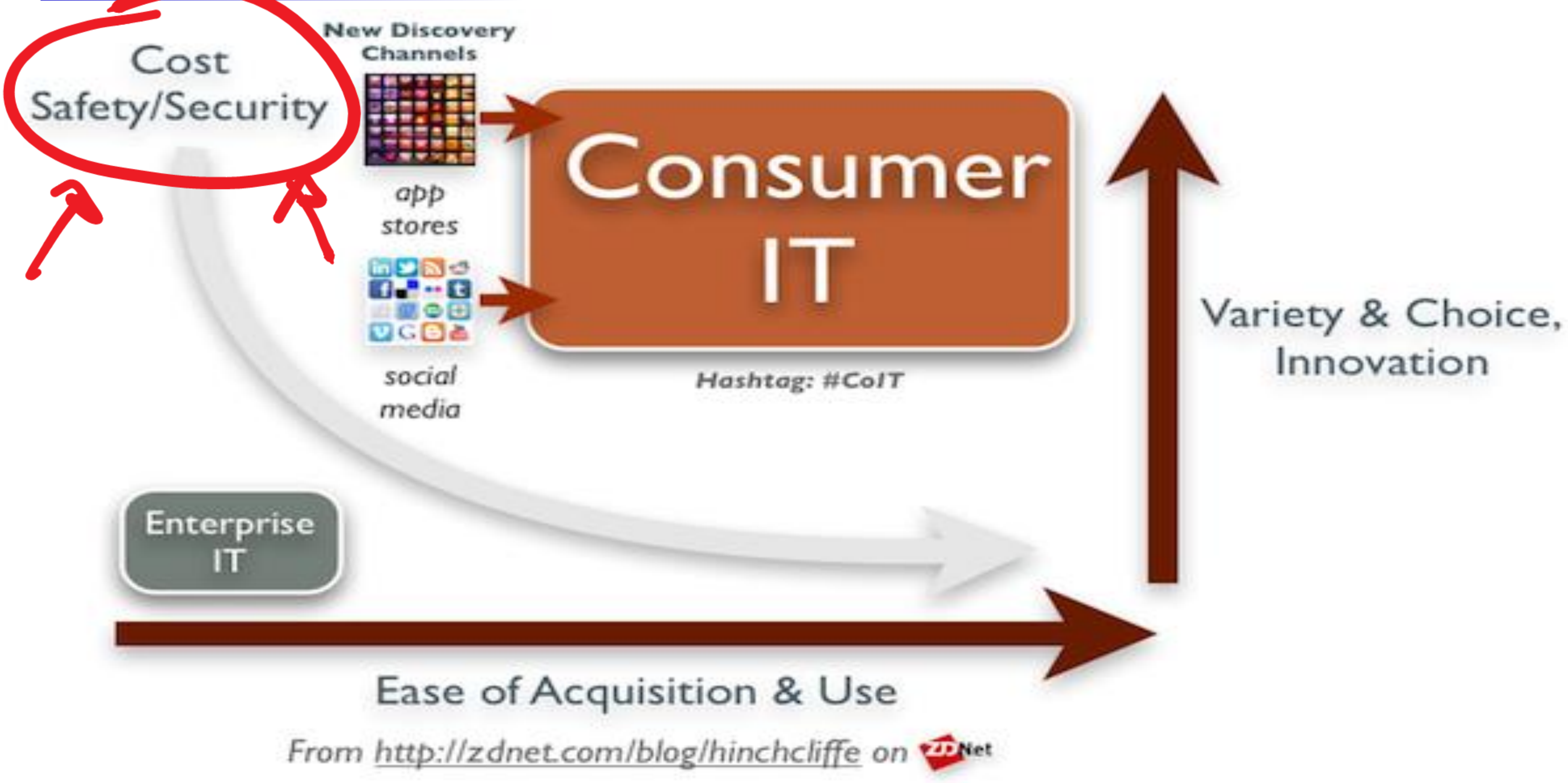
- (15 min) Context: cybersecurity & IoT in Healthcare
- (15 min) Three paradoxes
  - Are There More Things in Shadow IT Than in Official IT?
  - In Healthcare, a Large and Growing Amount of Sensitive Data and the Most Dangerous and Potentially Life-Threatening Systems Are, From the Security Perspective, in a “No Man’s Land”
  - CIOs Are Working Hard to Fortify the Walls of the Citadel, but There Is no Citadel to Defend
- (15 min) Paradigm Shift Ahead!
  - It’s all about data and information!
  - We need a Risk management perspective
  - Review of Strategy – Technology – Processes – People
  - Final considerations
- (Takeoff tracks: personal bibliography)
- (15 min) Q&A

Q&A

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

Back-up slides

IT Consumerization



Cost
Safety/Security

New Discovery Channels

app stores

social media

Consumer IT

Hashtag: #CoIT

Variety & Choice, Innovation

Enterprise IT

Ease of Acquisition & Use

From http://zdnet.com/blog/hinchcliffe on ZDNet

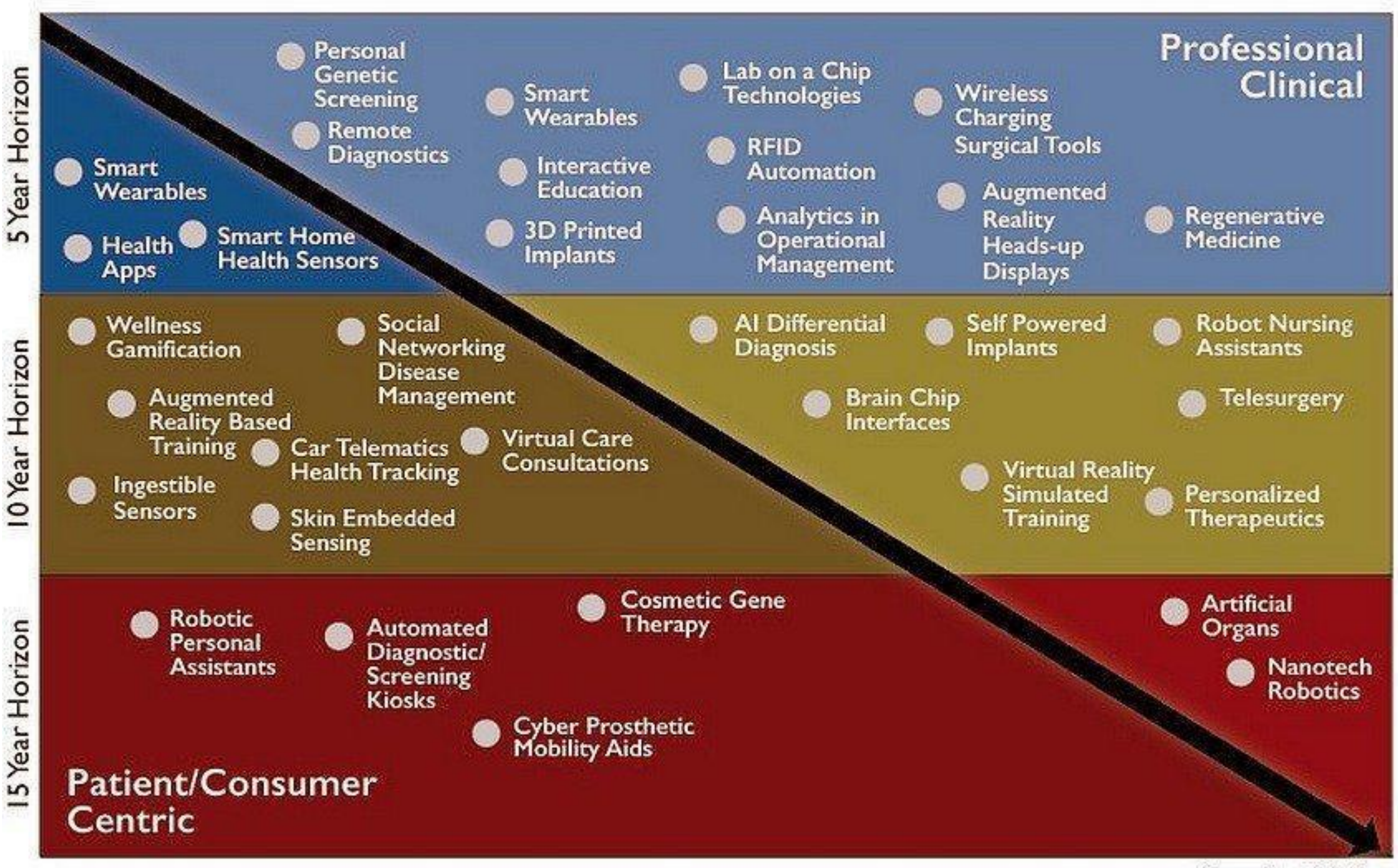
Video-break: IBM Vision

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

Video-break: Microsoft Vision

https://www.youtube.com/watch?v=-HWJ4sIzpXE

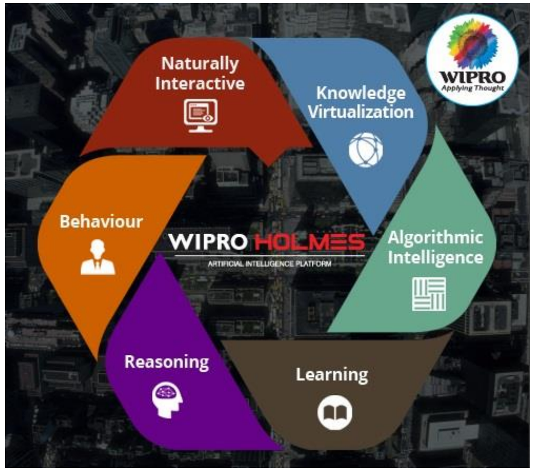
Appendice: Future of eHealth

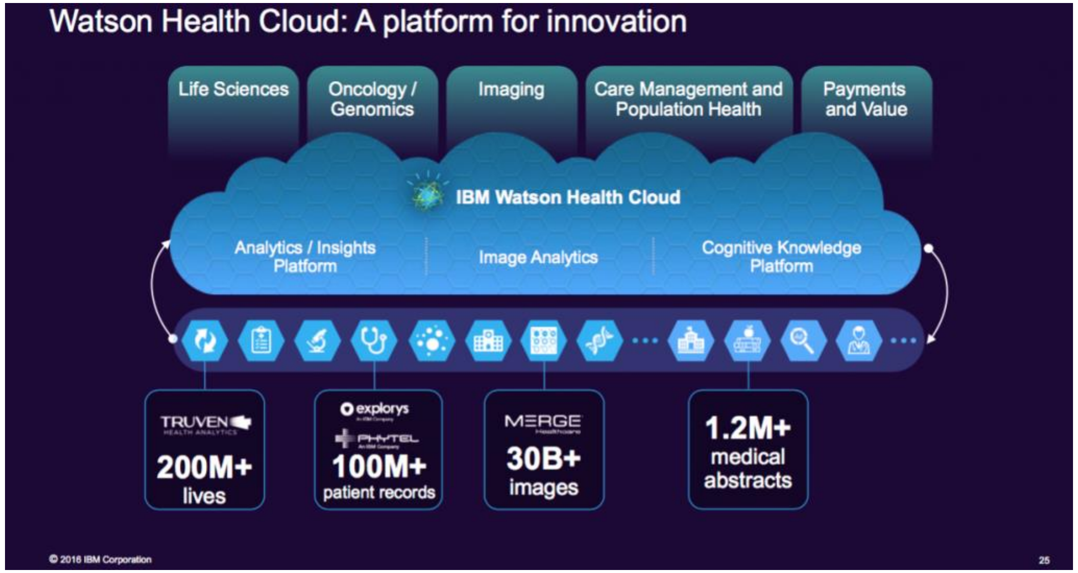

Professional Clinical
5 Year Horizon
Personal Genetic Screening
Remote Diagnostics
Smart Wearables
Lab on a Chip Technologies
Wireless Charging Surgical Tools
Smart Wearables
Interactive Education
RFID Automation
Augmented Reality Heads-up Displays
Health Apps
Smart Home Health Sensors
3D Printed Implants
Analytics in Operational Management
Regenerative Medicine
10 Year Horizon
Wellness Gamification
Social Networking Disease Management
AI Differential Diagnosis
Self Powered Implants
Robot Nursing Assistants
Augmented Reality Based Training
Brain Chip Interfaces
Telesurgery
Car Telematics Health Tracking
Virtual Care Consultations
Ingestible Sensors
Skin Embedded Sensing
Virtual Reality Simulated Training
Personalized Therapeutics
15 Year Horizon
Robotic Personal Assistants
Automated Diagnostic/ Screening Kiosks
Cosmetic Gene Therapy
Artificial Organs
Nanotech Robotics
Cyber Prosthetic Mobility Aids
Patient/Consumer Centric

Source: Frost & Sullivan

Artificial/Augmented Intelligence

- Keywords (buzzwords):
  - AI weak or strong
  - Cognitive Computing
  - Machine Learning





Watson Health Cloud: A platform for innovation

Life Sciences | Oncology / Genomics | Imaging | Care Management and Population Health | Payments and Value

IBM Watson Health Cloud

Analytics / Insights Platform | Image Analytics | Cognitive Knowledge Platform

TRUVEN HEALTH ANALYTICS — 200M+ lives

explorys, PHYTEL — 100M+ patient records

MERGE Healthcare — 30B+ images

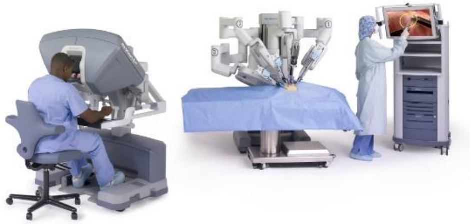
1.2M+ medical abstracts

© 2016 IBM Corporation

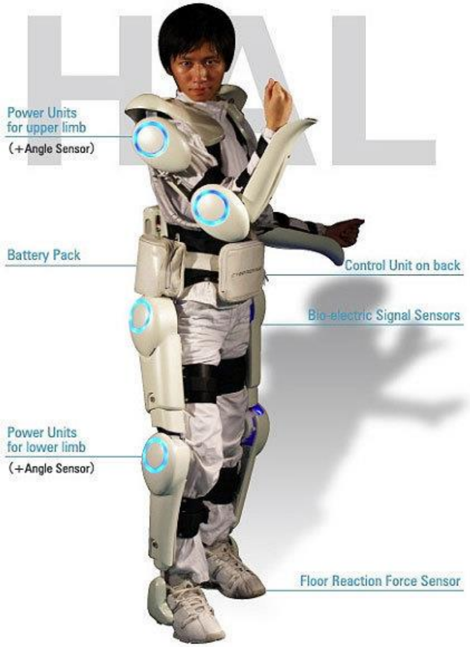
25

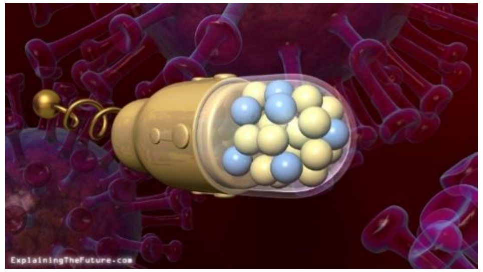
Robotics

- Not new:
  - «Da Vinci»

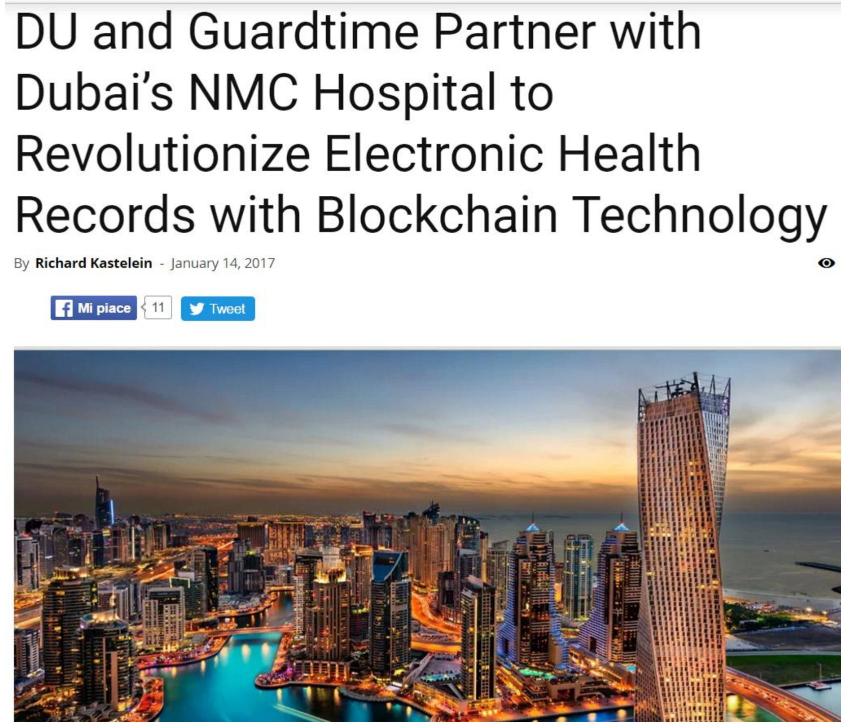


- New:
  - Medical emergency drones
  - HAL (Hybrid Assistive Limb)
  - Nanorobots (drugs targeted dispatching)
  - Tele-presence robots


HAL
Power Units for upper limb
(+Angle Sensor)
Battery Pack
Control Unit on back
Bio-electric Signal Sensors
Power Units for lower limb
(+Angle Sensor)
Floor Reaction Force Sensor

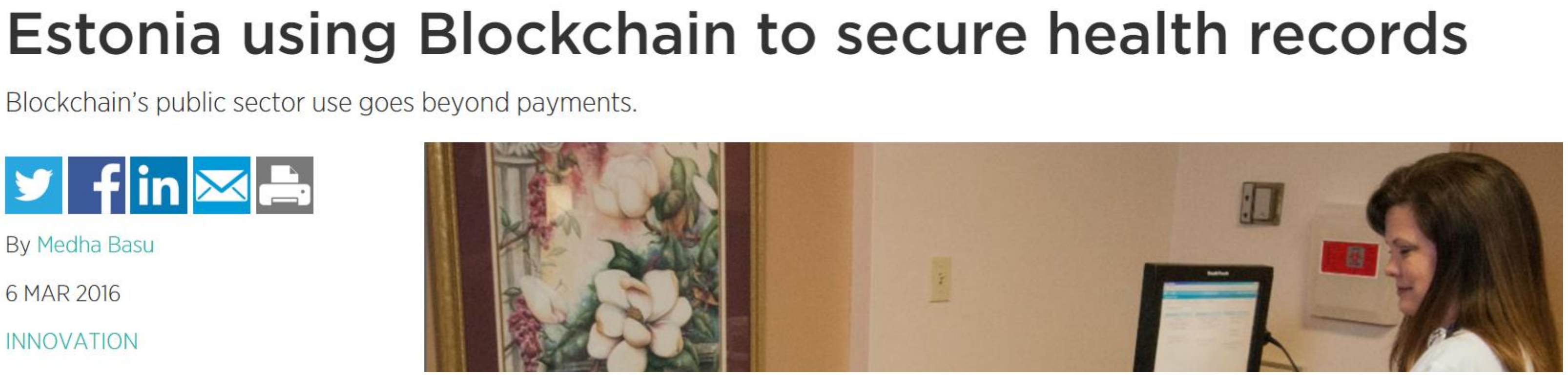


Bitcoin



DU and Guardtime Partner with Dubai's NMC Hospital to Revolutionize Electronic Health Records with Blockchain Technology

By **Richard Kastelein** - January 14, 2017



Estonia using Blockchain to secure health records

Blockchain's public sector use goes beyond payments.

By Medha Basu

6 MAR 2016

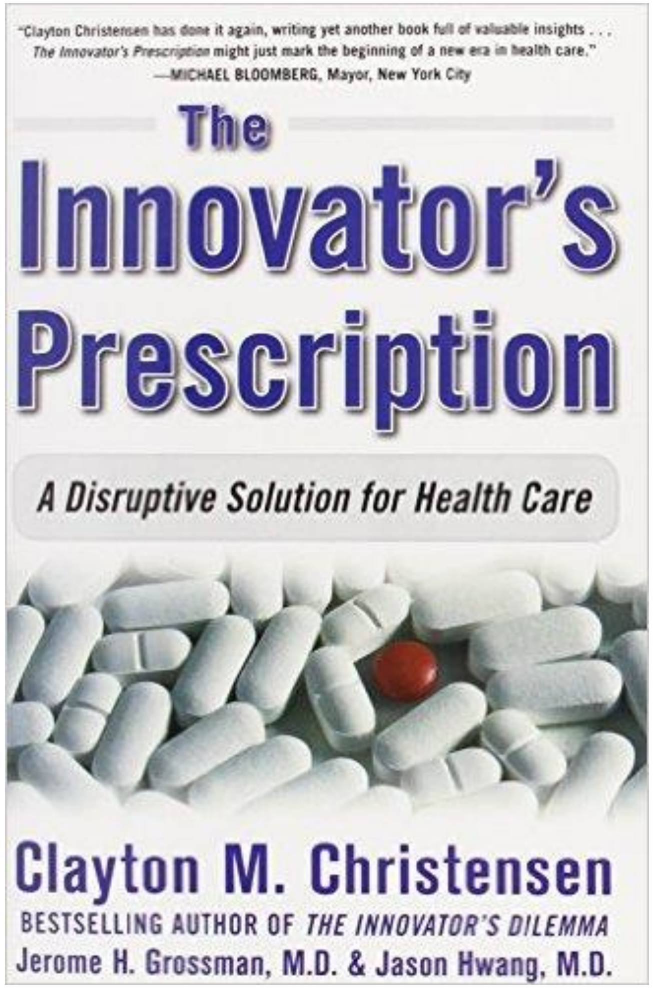
INNOVATION

Video-break: Healthcare 2020

Oltre le tecnologie dell’informazione, medical devices, genomica, nanotecnologie…

https://www.youtube.com/watch?v=totMfYaq8O8

Nota: Innovator’s Prescription



“Clayton Christensen has done it again, writing yet another book full of valuable insights . . . *The Innovator's Prescription* might just mark the beginning of a new era in health care.”
—MICHAEL BLOOMBERG, Mayor, New York City

The
Innovator’s
Prescription

A Disruptive Solution for Health Care

Clayton M. Christensen
BESTSELLING AUTHOR OF *THE INNOVATOR'S DILEMMA*
Jerome H. Grossman, M.D. & Jason Hwang, M.D.

https://www.youtube.com/watch?v=tmKqt6jf_H0