Panacea

People-centric cybersecurity in healthcare

Cybersecurity from a healthcare professional perspective

Sabina Magalini, MD

Fondazione Policlinico Gemelli, Rome, Italy

Funded by the European Union’s Horizon 2020
Research and Innovation Programme, under Grant Agreement no 826293

MEDRAD
Ooops, your files have been encrypted!
ccurred
injection.
ystem to use.
nd contact Services
via VirtualCa
to the operations manual or the internet at
http://www.radiology.bayer.com

My worst nightmare today?

Hospitals at the moment can't handle Cyberattacks

- Healthcare operations nowadays are increasingly based and dependent from information systems
- Legacy connected devices represent a major risk (black boxes) designed when cybersecurity attacks were not envisaged
- The increase of connected devices both inside and outside the Hospital is putting the patient and the Hospital at even greater risk due to hackability
- Hospitals are like ”seaports” (fully open to relatives, suppliers, all)
- Constant appearance of new threats (e.i. possibility of adding a tumor directly to a radiography exam)
- Cyberthreats are on the rise (87 billion in 2018 on 3 million assisted patients)
- Hospital structures and administrations are focalizing mainly on protection of patient data (because of possible legal consequences)
- Unpreparedness of Hospitals due to many different causes

Cybersecurity of patient data

- Security of patient data is not guaranteed.
- EHR can be found on the dark web for very low prices
- PHI (patient health information) are more important than PII (personally identifiable information)
- Cyberattacks are not immediately identified: most of them are discovered after they have been active for 18 months
- How as a doctor, nurse, health practioner am I responsible for this? What can I do?

Main types of cyberthreats daily experienced in Hospitals

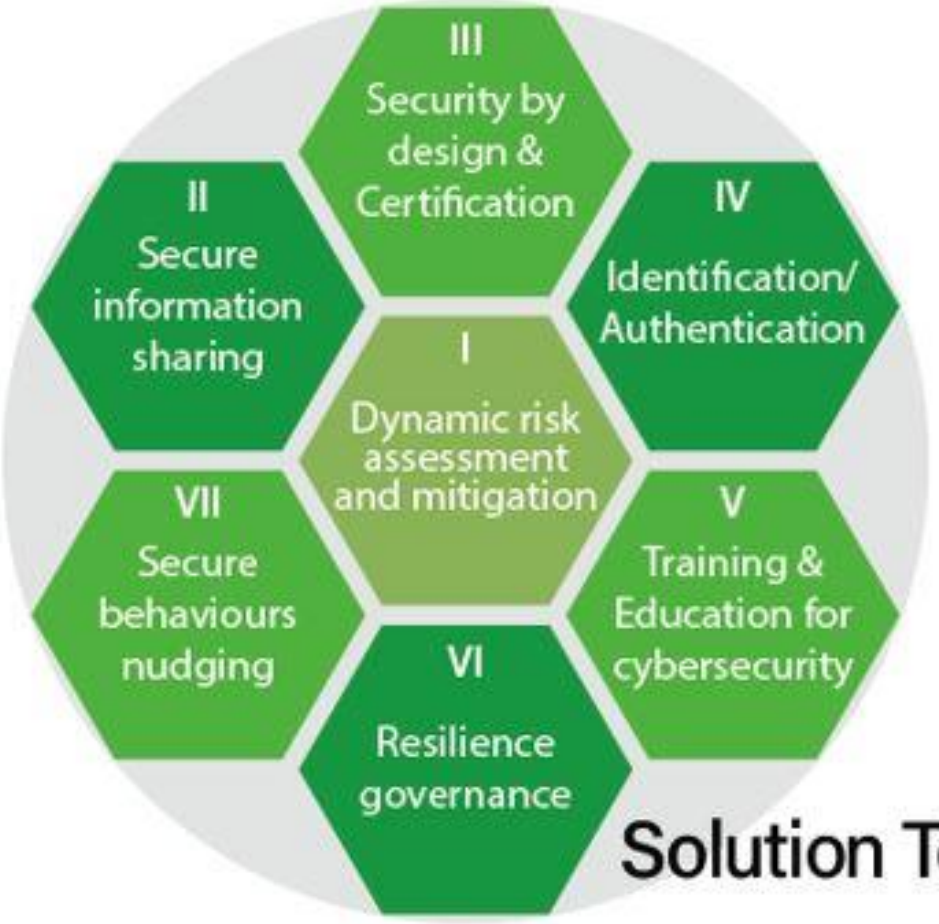
- Data Breaches
  - PHI and PII: over 15 million health records have been compromised by data breaches in the last year
- Ransomware:
  - phishing with attachments
  - clicking on malicious link
  - viewing advertisement
  - RaaS (Ransomware as a Service!)
- DDoS attacks
  - while most are opportunistic and accidental, many target victims (Hospitals) for social, political, ideological or financial causes related to a situation that angers cyberthreat actors. Medical operations may create conditions of anger/revenge
- Insider threats
  - insiders have legitimate access to the system so they do not have to face traditional cybersecurity defences, the best defence against these threats is by other insiders
- Business email compromise and frauds
  - scammers pretend to be a person of power (e.g. CEO, supervisor). Very effective because they are well targeted (These threats have risen by 1300% since 2015).

What to do?

- Very little help at the moment from Hospital administration and governace
- Scarse knowledge of the ICT technology underlying the systems and devices we utilize
- Present methods to guarantee cybersecurity in our systems are time consuming: nurses, technicians and doctors must daily identify on different terminals and devices much more often than employees working in other industries or roles

Panacea

Involvement of Healthcare staff together with ICT staff to identify risks, work methodology and possible solutions.


III
Security by design & Certification
II
Secure information sharing
IV
Identification/ Authentication
I
Dynamic risk assessment and mitigation
VII
Secure behaviours nudging
V
Training & Education for cybersecurity
VI
Resilience governance

Solution Toolkit

Partners

UNIVERSITÀ CATTOLICA del Sacro Cuore

Gemelli
Fondazione Policlinico Universitario A. Gemelli
Università Cattolica del Sacro Cuore

RINA
RINA. Excellence Behind Excellence.

FORTH

IDEMIA

RHEA GROUP

Northumbria University NEWCASTLE

security tech Stelar law research

AON Empower Results®

SAPIENZA UNIVERSITÀ DI ROMA

Trust-IT Services
Communicating ICT to markets

HSE
Seirbhís Sláinte Níos Fearr á Forbairt
Building a Better Health Service

ICEM

INNOVATION SPRINT