PANACEA project and the EU-wide push for cybersecurity in hospital systems

Sabina Magalini

Surgeon of the Policlinico Gemelli of Rome
Aggregate Professor of the Catholic University School of Medicine
PANACEA Project coordinator

HIMSS 23

DISCLAIMER: The views and opinions expressed in this presentation are solely those of the author/presenter and do not necessarily represent any policy or position of HIMSS.

PANACEA project overview

- PANACEA H2020 project started in **Jan 2019**, ended **Feb 2022; 5 million €; 15 partners**
- It has developed and validated in **three Healthcare Organizations** (in Italy, Ireland and Greece) a **toolkit of nine tools**, acting holistically on all the components of a Healthcare Organization (HCO)

PANACEA Tools			HCO components		
			Technology	People	Organization
Solution Toolkit	DRMP	Dynamic Risk Management Platform	✓	✓	
	SbDF	Security by Design Framework	✓		✓
	SISP	Secure Information Sharing Platform	✓		
	IMP	Biometric Identification Management platform	✓	✓	
	SBNT	Secure Behaviours Nudging Tool		✓	
	TECT	Training & Education for Cybersecurity Tool		✓	
	RGT	Resilience Governance Tool			✓
Delivery Toolkit	C-ROI	Cybersecurity Return on Investment			✓
	IGT	Implementation Guidelines Tool			✓

To know more: see https://panacearesearch.eu/panacea-toolkit and read the White Paper https://www.panacearesearch.eu/sites/default/files/WhitePaperA4_December2021_final_0.pd f

PANACEA project: focus on people

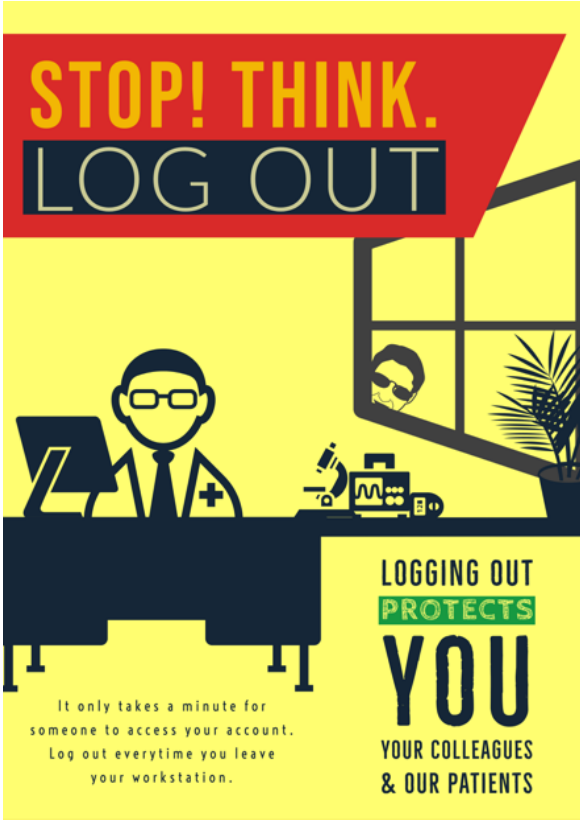
- Four of the 9 PANACEA tools aim at minimizing human error.
- Secure Behaviour Nudging Tool (SBNT) is one of them.
- It is a methodology to help staff responsible for encouraging cybersecure behaviours within a healthcare organisation.
- Designed by a team of behaviour change experts, the SBNT is a toolkit of evidence-driven techniques and methodologies built around established psychological theories.
- The SBNT includes a range of innovative tools to assist the user in:
    1. Identifying insecure behaviour in the workplace for each type of staff (e.g. nurses, residents, administrative staff)
    2. Identifying Factors driving this behaviour and barriers to secure behaviour
    3. Designing 'nudges' to overcome the barriers and encourage more secure behaviour

To learn more, watch the video https://panacearesearch.eu/secure-behaviour-nudging

PANACEA project: focus on people

From vulnerabilities to nudges (example)

Human Vulnerability List
• No 'logout' when leaving the workstation
• Disposal or reuse of storage media without proper erasure
• Sharing credential
• Unprotected credential
• Poor password management
• Insufficient security training on
• Incorrect use of software and hardware
• Lack of security awareness
• Unsupervised work by outside or cleaning staff
• E-mail misuse
• Non-compliance with procedures for introducing software into operational systems
• Non-compliance to policy on mobile computer usage
• Insufficient 'clear desk and clear screen' policy


STOP! THINK.
LOG OUT
It only takes a minute for someone to access your account. Log out everytime you leave your workstation.
LOGGING OUT
PROTECTS
YOU
YOUR COLLEAGUES
& OUR PATIENTS

PANACEA project exploitation by Gemelli Hospital/UCSC

- **PHCAS**-Launched in March 2022, the **PANACEA Healthcare Cybersecurity Advisory Service** is a business-oriented collaborative framework involving **13 of the 15 PANACEA partners.** Aims to support healthcare organisations in improving cybersecurity capabilities, adopting PANACEA toolkit, whether as standalones or integrated solution

  https://www.panacearesearch.eu

- **CYBERHIMPREX**-2023-2024, Digital Europe Programme (DIGITAL). The project is co-financed (50% of 2,7 million €) by DIGITAL programme. It has the objective of **improving the cybersecurity capabilities of three Healthcare providers** (Gemelli Hospital, 7th Health Region of Crete, Fundació Privada Hospital Asil de Granollers) implementing a portfolio of 11 initiatives. 7 of the 11 initiatives adopt solutions that have been developed by two H2020 projects: PANACEA and CUREX. **3 PANACEA partners are directly involved (as adopters) and 3 more will be involved as solution providers**. UCSC coordinates.

  https://cyberhimprex.policlinicogemelli.it/overview/

- **DYNAMO**, 2022-2025, Horizon Europe. The mission of DYNAMO is to **combine the two fields of Business Continuity Management (BCM) and Cyber Threat Intelligence (CTI)** to generate a situational awareness picture for decision support across all stages of the resilience cycle, developing both technical and people-oriented solutions. **2 PANACEA partners are involved.**

  https://horizon-dynamo.eu

- **TRUSTEE**, 2022-2025, Horizon Europe. The project aims to **deliver a trustworthy framework that will aggregate various interdisciplinary data repositories** from, e.g., Healthcare, Education, Energy, Space, Automotive using techniques such as homomorphic encryption. For healthcare, TRUSTEE platform will be used in areas such as Epidemiology & Bio statistics, Bioinformatics, Artificial Intelligence and Big Data processing to support clinical research and healthcare process improvement. **3 PANACEA partners are involved**.

  https://horizon-trustee.eu

The EU-wide push for cybersecurity in hospital systems

- Establishment of the EH-ISAC (Athens 25th May, 2023)
- NIS 2 (16th January, 2023, MS must transform it to law in October 2024)
- Horizon Europe calls
  - Cluster 1 (Health)→ nothing 2023
  - Cluster 2 (Cultural) → Deadline 2024: TRANSFORMATIONS-01-06; 01-11 (Cybersecurity is not present in these calls even though it would be necessary and useful)
  - Cluster 3 (Security)→ Deadline 23 Nov 2023: CS01-01, CS01-02, CS0-03
  - Cluster 4 (Digital, Industry and Space) → nothing 2023
- Digital Europe Programme (DIGITAL) calls

  → Deadline 6 July 2023: DIGITAL-ECCC-2022-CYBER-B-03-UPTAKE-CYBERSOLUTIONS, DIGITAL-ECCC-2022-CYBER-B-03-CYBER-RESILIENCE - EU Cybersecurity Resilience, Coordination and Cybersecurity Ranges, …

New Entry "Transforming Health Care Systems" (THCS) cybersecurity is in the Strategic Plan

Lessons learned

- Scope: research must
  - Adapt to «healthcare new normals» (telehealth, smart working)
  - consider that q great part of medical devices are still not ready to securely connect to HC information systems
  - Consider that health sector economies are «deficient», necessity to plan according to possibility of spending
- People empowerment
  - Workforce must not be pigeonholed as a threat, but must be leveraged to identify security challenges
  - Teaching health care students cybersecurity
- Limitations to successful research
- EU Research funding mechanism does not favour passage of tools developed to a TRL 9
- HCOs do not have "simulation environment, research environment" for cybersecurity.

Suggestions:

- Better European networking of Hospital cybersecurity practitioners (EU-ISAC)
- Better focused funding for Hospital Cybersecurity also considering the new «normals»
- Involving Healthcare Systems in major Cybersecurity Projects as Pilot testing sites due to their similarity/diversity compared to other Critical Infrastructures
- Enforcement of MDR regulation for new medical devices and closer contact with certification agencies
- Focusing better on the Human Aspects of Behaviour
- Empowering HC personnel in definition of behaviours
- Last but not least revision of GDPR issues.

Thank you

Contact:
Sabina.magalini@unicatt.it