Panacea

People-centric cybersecurity in healthcare

White Paper

Lessons learnt from PANACEA on the cyber-protection of hospitals and care centres

Date: December 2021

Authors

- Claude Bauzou, IDEMIA
- Silvia Bonomi, University of Rome, La Sapienza
- Martina Bossini Baroggi, RINA
- Lynne Coventry, Northumbria University at Newcastle
- Peter Daly, Health Executive Service
- Fabrizio De Vecchis, RHEA
- Federica Foti, RINA
- Sabina Magalini, Sacred Heart Catholic University
- Pasquale Mari, Gemelli University Hospital
- Fabio Rizzoni, Gemelli University Hospital
- Raniero Rapone, AON
- Don Slyne, Irish Centre for Emergency Management
- Ivan Tesfai, RINA

Editorial Team

- Kallia Anastasopoulou, 7th Health Region of Crete
- Lynne Coventry, Northumbria University at Newcastle
- Peter Daly, Health Executive Service
- Sabina Magalini, Sacred Heart Catholic University
- Stephanie Parker, TRUST-IT
- Emmanouil Spanakis, FORTH

Graphic Design

- Gianluca Savini, Trust-IT

Disclaimer

PANACEA has received funding from the European Commission's Horizon 2020 research and innovation programme under the Grant Agreement no 826293. The content of this white paper does not represent the opinion of the European Commission, and the European Commission is not responsible for any use that might be made of such content.

Contents

Executive Summary

Cybersecurity in Healthcare Organisations is a complex issue, due to the convergence of many structural and regulatory challenges.

The attack surface is wide and dynamic because of the multiplicity of connected endpoints, increasing digitalisation, many non-secure legacy medical devices and increasing levels of inter-organisational data sharing. Staff working in the healthcare sector mostly consider cybersecurity as a burden and distraction from treating patients effectively. This leads to risky behaviours when interacting with people, devices and data online. The COVID-19 pandemic has amplified and made manifest risky situations for healthcare organisations (such as smart-working and telemedicine), bringing also new risks, such as the fast onboarding of new staff, and the need to quickly turn non-healthcare sites, e.g., hotels, into structures for healthcare operations.

However, the mission of the healthcare sector, more than for any other industry, implies that cybersecurity is not only financially, but also socially relevant in that successful cyber-attacks have a high impact on quality of care, patient safety and on data privacy.

Cybersecurity is thus an essential part of a high-quality healthcare service and not an obstacle limiting the performance of healthcare operations, with HCO compliance also top of mind, spanning regulations and guidelines such as the Directive on Security of Network and Information Systems (NIS), General Data Protection Regulation (GDPR), Medical Device Regulations (MDR) and the related MDCG-16-Guidance on Cybersecurity for medical devices, and the ENISA Procurement Guidelines for Cybersecurity in Hospitals, must all be taken into consideration.

The H2020 PANACEA project has implemented a holistic and customisable approach, including Tools for an automatic, dynamic and multi-dimensional risk assessment, secure by design deployment of medical devices and systems, easy and manageable information sharing, user-friendly clinical staff identity management, security behaviour assessment with ways to improve it through nudges alongside universally understandable education video-clips to influence correct behaviours, and implementing distributed governance.

Validation with three European HCOs and four medical device/system developers has shown the usability and the added value brought by the PANACEA Toolkit as an integrated solution to build cybersecurity capability and resilience in HCOs. The analysis of a recent ransomware attack on the Health Service Executive of Ireland highlights the potential of the PANACEA Toolkit in strengthening cybersecurity capabilities during both the preparation and the recovery phases.

Healthcare organisations willing to adopt PANACEA Tools can count on the support of PANACEA's partners along a roadmap that starts with a regulatory, organisational and technical assessment designed to prioritise cybersecurity investments, and then deploys the PANACEA tools and solutions.

With many cybersecurity solutions already existing in healthcare, PANACEA uniquely offers a robust portfolio of Tools and expertise that combine technological and risk governance measures with measures on human behavioural aspects into an integrated solution.

Scope and Definitions

This white paper focuses on critical cybersecurity challenges that are specific to healthcare organisations, showing how PANACEA offers a holistic approach to coping with them. This approach is based on a set of technical and organisational Tools developed by the PANACEA Project[1] to contrast cyber threats and data breaches by strengthening cybersecurity within healthcare organisations.

It draws extensively on the lessons learned by the PANACEA Consortium Partners over a 3-year period (2019-2021), during which partners have worked on five interconnected pillars:

1. Research, and the analysis of relevant standards and regulations, performed when implementing the Tools.
2. "On the ground" activities for their validation.
3. Active participation in a wide range of relevant conferences and workshops including panel and interactive discussions.
4. Feedback received from end-users and policy makers as part of the stakeholder engagement strategy, organised by PANACEA or through clustering activities with peer initiatives.
5. The impacts of a recent (May 2021) and significant cyber-attack on a national healthcare system and the necessary response management.

To guide readers through this complex landscape, the white paper opens with a core set of definitions.

Healthcare Organisations (HCOs): organisations providing healthcare services. They include single Hospitals, single Outpatient Clinics, a Group of Hospitals operating with some inter-hospital processes (e.g. procurement managed as a shared service, medical consultations among the hospitals of the Group), and Health Regions (which include headquarter, hospitals, territorial health services delivery via general practitioners and local healthcare units).

Cybersecurity: the set of activities necessary to protect network and information systems, users of such systems, and others affected by cyber threats (see [EU Act])

Cyber threat: any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems, and other persons (see [EU Act])

Data breach: an event in which an individual's name and a medical record and/or a financial record or debit card is potentially put at risk, either in electronic or paper format.

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

Cybersecurity Challenges in Healthcare and Impacts of Cyber-attacks

There are many reasons for the vulnerability of healthcare organisations, from routine to COVID-like situations and regulatory challenges.

Structural challenges: Routine situations

Wide, dynamic and vulnerable attack surface

- A multiplicity of connected endpoints (including devices and mobile consumer devices whose number and type can change on a day-by-day basis), many different interconnected systems, including no longer supported legacy systems and the digitalisation of patient data.
- Healthcare is increasingly evolving towards digitalisation. Electronic Health Records (EHRs) have been developed and widely adopted. Teleconsultation and tele-expertise are thriving, and enabling technologies emerging, such as big data analytics, IoT, AI, high-performance, cloud, mobile Computing, Blockchain) alongside the increasing use of connected medical devices.
- However, there are still many legacy medical devices. Many manufacturers have historically not designed their products with security in mind [1] and their lifespans are typically long [2][2].
- While many healthcare organisations are defining or rolling out their digital transformation roadmaps, the COVID-19 pandemic in Europe and elsewhere has exposed the weaknesses of national health services. With IT investments forecast to grow [3], there is a clear need to invest not just in e-health and tele-health but also cybersecurity.
- Inter-organisational data sharing in the healthcare domain is an additional challenge arising as a consequence of the stronger integration along the patient journey for increased patient safety[3], the interoperability issues and the attractiveness of the shared information.
- As an example, a hospital with 1500 beds and 5800 staff members (including 1300 medical doctors, 2200 nurses) has 3000 networked medical devices (for the most part portable, e.g. electrocardiograph) and 4400 access devices (workstations, laptops, etc.).

Human vulnerability

- Work culture can lead to security being overlooked or being perceived as a burden, particularly if it is seen to detract from patient care.
- The working environment is also prone to regular changes to team structures through staff rotation and new employees being hired.
- In many cases, staff involvement with information systems and medical devices follows a many-to-one scheme: many staff members in clinical wards and laboratories access the same workstation (or interface) many times during the working day. This increases the risk of poor attention to password management and unlocked workstations. Healthcare operators may have to log in and off more than 80 times a day in clinical wards.
- Other risky behaviours include using USB devices and sharing patient information (e.g., using instant messaging applications, like WhatsApp, rather than official systems to avoid leaving the patient's bedside and emailing patients documents if they cannot access them via official systems).

2 The lifespan of medical devices and clinical assets depends on several of factors, including frequency of use, maintenance and servicing, how the device is used, among others. However, under normal operating conditions, most connected medical devices have an estimated useful lifecycle of 7-10 years.

3 WHO, 2021, *Global patient safety action plan 2021–2030: towards eliminating avoidable harm in health care.*

- According to ENISA, 84% of cyber-attacks rely on social engineering, including phishing [5], while threats based on human errors are perceived to have the highest likelihood of occurrence (4.2 on a scale from 1 to 5) and are rated as the second most "critical" threat in terms of impact on Hospital operations, with 70% of the respondents saying that it is critical [6]. Insider threat, including unintentional abuse or error, is among the most frequent types of threats/ attacks in the healthcare sector [7].

Structural Challenges: COVID-like Situations

On 11 March 2020, after a global outbreak of infections, WHO declared COVID-19 as a pandemic.

The pandemic has worsened risks in certain situations:

- **Telemedicine**: The policy to keep non-severe COVID-19 patients at home plus the need for telemonitoring, has extended the use of telemedicine, which has a low-security level.
- **Smart working**: Risks may come from technology illiteracy of staff working from home through connections from home devices not sufficiently protected or carelessness in exchanging credentials with colleagues to VPN or shared folders.
- **Inter-organisational data flows**: Major requests for data flows to monitor infections and for epidemiological reporting, among other similar activities. These data flows occur between many entities (hospitals, primary care services, regional and national authorities, also located in different countries); information sharing is often performed insecurely.

The pandemic has also given rise to new risks:

- **Quick onboarding of new staff**: Newly hired healthcare personnel have no experience of organisational cybersecurity policies or of the work environment (colleagues, superiors, acceptable behaviours). Many are "Digital-natives, Generation Z" and take cybersecurity for granted, even if this is not true. The sudden arrival of a lot of new members of staff can weaken the provisioning, de-provisioning and profiling processes, leading to security issues.
- **Fast design of ad-hoc IT solutions**: The healthcare sector needs to design and deploy Apps and back-end systems rapidly. Fast design increases the risks of delivering solutions that are not secure.
- **Non-healthcare sites used for healthcare operations**: Temporary hospitals, churches, nearby hotels, and other empty but usable spaces have been upgraded to "hospital level". The WiFi systems of these structures are not always secure and hackers can monitor traffic over airways to steal access credentials.
- **Specific types of cyber-threats** have been enacted, such as:
  - Phishing: Coronavirus-themed phishing emails, where clicking on a link lets the fraudster steal personal data, email logins or banking details.
  - Malware, spyware and trojans: these have been found embedded in interactive coronavirus maps and websites on the coronavirus; domains on the internet include terms like "coronavirus", "corona-virus", "covid19" and "covid-19". These maps are visited frequently by healthcare operators.
  - Fraud: Hospitals and healthcare agencies are making frequent orders for fear of running out of equipment and medicines. There have been cases of paid orders for equipment, from face masks to hand sanitisers, that have never arrived.
  - Scammers: Have been seen mimic groups such as the Centre for Disease Control and Prevention (CDC) or the World Health Organization (WHO), with links redirecting to a page where data can be stolen.

Regulatory Challenges

More than in other industries, the mission of the healthcare sector implies that cybersecurity is not only financially, but also socially relevant in that cyber-attacks put patient safety and health personal data at risk while also threatening the operational continuity of a service for millions of people as a critical infrastructure. Therefore, compliance with relevant guidelines and EU regulatory frameworks is vital.

GDPR (EU) 2016/679

The General Data Protection Regulation (GDPR) came into force on 25 May 2018, setting out the rules for the processing and the free movement of personal data [8]. The GDPR applies to all domains of the public and private sectors. It treats health data as a "special category" of personal data that is sensitive by its very nature and imposes a higher standard of protection for data processing [9].

In particular:

- Organisations processing health data have the obligation (among others) to implement appropriate technical and organisational measures to ensure the security of the processing systems, services and personal data [9].
- Art. 25 *Data protection by design and by default* of [GDPR] states that: *... the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, ... designed to implement data-protection principles.*

DIRECTIVE (EU) 2016/1148 (NIS)

The Directive on Security of Network and Information Systems (NIS Directive, [10]) was adopted by the European Parliament on the 6 July 2016 and entered into force in August 2016. All 27 Member States have transposed the Directive into their national legislation[4].

The Directive concerns measures for a high common level of security of network and information systems across the Union. The goal of the NIS Directive is to ensure a culture of network and information systems security across sectors (i.e. energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure), vital for our society and economy and heavily dependent on ICT. In particular, it regards the Operators of Essential Services (OES) in these sectors, with healthcare settings (including hospitals and private clinics) falling under the OES category.

- Whereas 50 of [10] "Manufacturers and software developers ... play an important role in enabling operators of essential services and digital service providers to secure their network and information systems".
- Art. 14 §1 of [10] "OES should take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems used for operations".
- The Directive goes beyond the implementation of security requirements, as it gives power to the regulatory bodies to audit the OES to ensure the level of cybersecurity in the organisation is acceptable and as per the provisions of the Directive [9].
- The NIS Cooperation Group has provided a substantial and comprehensive mapping of the security requirements for the OES category [11]. For healthcare organisations, they specifically include the fulfilment of the European ISO 27799:2016 and of the USA Health Insurance Portability and Accountability Act of 1996 (HIPAA)[5].

MEDICAL DEVICE REGULATION (EU) 2017/745.

The Medical Device Regulation (MDR) [12] includes specific provisions related to the IT security (hardware, software etc.) for all medical devices. In particular:

- It states that for devices that incorporate software or for software that are devices in themselves, the software shall be developed and manufactured in accordance with the state of the art considering the principles of development

4 https://digital-strategy.ec.europa.eu/en/policies/nis-transposition.

5 https://www.hhs.gov/hipaa/index.html.

life cycle, risk management, including information security, verification and validation[6].

- The General Safety and Performance Requirements defined within the MDR include, among others, IT security measures, including protection against unauthorised access.

The MDR also requires the establishment of the Medical Device Coordination Group (MDCG)[7]. Published in December 2019, the MDCG-16-Guidance on Cybersecurity for medical devices to provide manufacturers with guidance on how to fulfil all the relevant essential requirements of the MDR. They deal with both pre-market and post-market aspects, such as:

- Requirements for the devices.
- Requirements for the processes accompanying the device lifecycle.
- A description of other EU and global guidance and pieces of legislation that are relevant to the domain of cybersecurity for medical devices.

PROCUREMENT GUIDELINES FOR CYBERSECURITY IN HOSPITALS

Published by ENISA in February 2020, the Procurement Guidelines [9] aim to provide hospital procurement officers and CISOs/CIOs with a comprehensive set of tools and good practices that can be adapted to the hospital procurement process to ensure that cybersecurity objectives are met. In this context, the report maps good practices in three distinct phases within the procurement lifecycle, namely "plan, source and manage". The leading assumption is that one vulnerable device/system/service can cause significant cybersecurity impacts for a hospital as an operator of essential services. In particular, guidelines make recommendations for:

- Conducting risk assessment in the "plan" phase: Before launching a new procurement process, healthcare organisations should assess the impact of their new acquisition on their IT security risk (e.g., new risk, increase/decrease in likelihood or impact of existing risk).
- Providing cybersecurity training in the "source" phase: Ensure that internal staff or external contractors/consultants working on-premise are adequately trained in the healthcare organisation's security practices.
- Raising cybersecurity awareness in the "management" phase: Ensure staff is aware of the cybersecurity risks associated with newly acquired products or services.

Ensuring dedicated access control mechanisms for medical device facilities: Medical devices such as PET/ CT scanners, surgical robots etc. should also be physically protected. Access should be allowed only for specialised personnel and each one should have a dedicated account. The IT department should monitor the access control policy of each device. When procuring devices these provisions should be considered by the supplier.

Impacts of Cyber-attacks

The impacts of successful cyberthreats in healthcare are high:

- Impact on quality of care and patient safety. Across industries, the average time to contain a data breach is 75 days[8] [14]. System downtime is a direct threat to the quality of service and patient safety/lives, due to the delay in receiving medical care and treatment [15]. Life is endangered through redirection to other facilities or inaccessibility of medical records and tests results, errors related to manual data processing. In September 2020, German Authorities reported a death directly due to a cybersecurity attack: the hospital could not accept emergency patients because of the attack so the woman was sent to another healthcare facility around 20 miles away. Doctors were not able to start treating her for an hour and she died [16].
- Financial impacts. In 2021, HCOs experienced, for the eleventh year in a row, the highest average cost of a data breach

6 This is reinforced by the [13], which establishes the need to develop and apply an EU-wide cybersecurity certification framework for digital products, services and processes.

7 The MDCG is composed of representatives of Member States, the Commission, and the ENISA to facilitate strategic cooperation between the Member States regarding the security of network and information systems.

8 The time it takes for an organisation to resolve a situation once it has been detected and ultimately restore service.

compared with other industries. Healthcare data breach costs (excluding the cost of the ransom) increased from an average total cost of $7.13 million in 2020 to $9.23 million in 2021, a 29.5% increase[9] [14].

- Impact on data privacy. A Sophos survey [17][10] found that in 2020, 74% of the organisations whose data had been encrypted did not pay the ransom to retrieve it. In fact, ransom payments may not stop ransomware groups from leaking the exfiltrated data [18]. Patients are therefore victims of theft and the unlawful disclosure of their personal health information following a data breach, the indirect impacts of which are often long-lasting [15].

9 Data refer to hospitals and clinics and to detection and escalation, notification, post breach response, lost business cost.

10 The survey cohort included 5,400 IT decision makers across 30 countries. The survey was conducted in January and February 2021.

PANACEA: A Holistic Approach to Cybersecurity in Healthcare

PANACEA is a Research & Innovation action funded under the European Commission's Horizon 2020 programme, running from January 2019 to December 2021. It has delivered a *Solution Toolkit* of seven Tools, to assess and improve cybersecurity readiness of healthcare socio-technical systems (ICT, networked devices, staff, organisation) and of medical device/systems lifecycle, and a *Delivery Toolkit* of two Tools to support the adoption of the Solution Toolkit. They make up a **holistic set of solutions**, because they act on the structural components of a healthcare organisation across **Technology**, **People** and **Organisation**[11], as illustrated in Table 1: PANACEA Toolkit and targeted Healthcare Organisation's components on which they act.

PANACEA Tools have been validated in terms of usability and usefulness in 22 use cases performed with seven end-user organisations: three healthcare organisations[12] and four medical device/system developers[13]. In general, IT managers, clinical managers and staff have reported that compared with current practices, the PANACEA Tools allow a more structured and complete approach to the risk assessment and risk reduction and, if extensively used, can achieve key targets in terms of human behaviour and organisational accountability for cybersecurity.

Table 1: PANACEA Tools and targeted Healthcare Organisation's components

PANACEA Tools			HCO components		
			Technology	People	Organisation
Solution Toolkit	**DRMP**	Dynamic Risk Management Platform	🔒	🔒	
	SbDF	Security by Design Framework	🔒		🔒
	SISP	Secure Information Sharing Platform	🔒		
	IMP	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			🔒

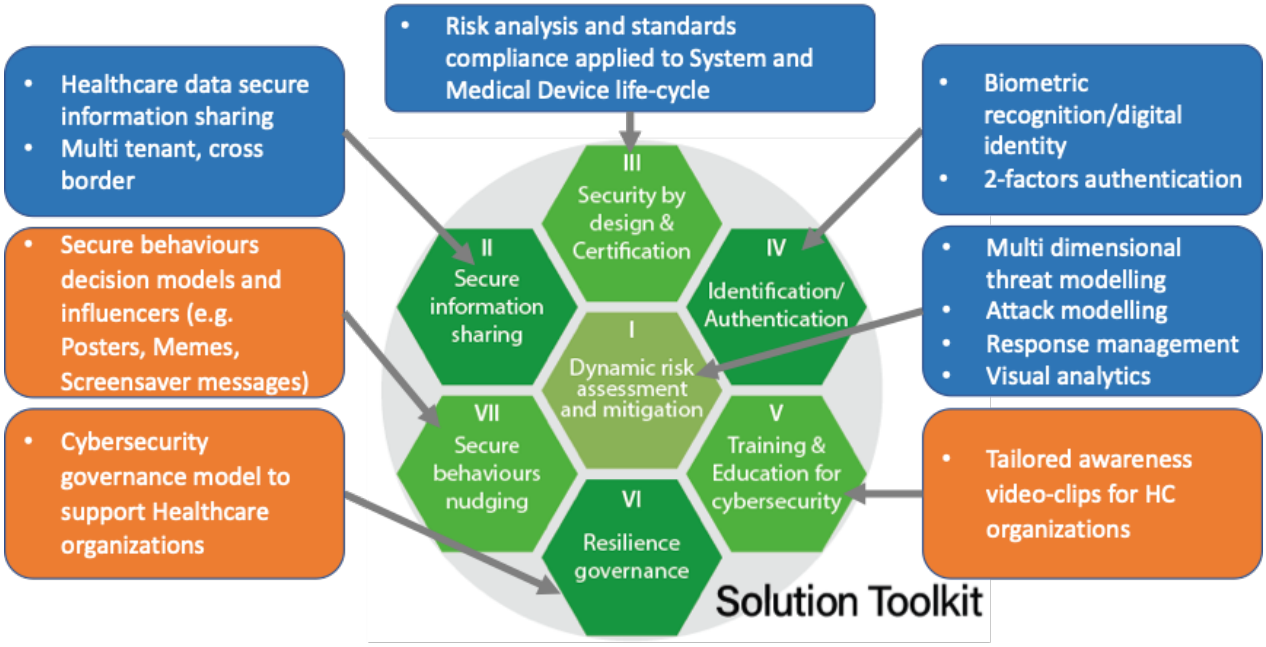
11 These are the key components of socio-technical systems like healthcare organisations. For more details on how the socio-technical perspective has been applied in PANACEA, see [19] and [20].

12 Fondazione Policlinico Universitario Agostino Gemelli, Rome, Italy; 7th HealthCare Region of Crete, Heraklion, Greece; HSE-South/Southwest Hospital Group, Cork, Ireland are all partners in the PANACEA Consortium.

13 RINICOM (a UK based company) has used SbDF in developing one of its new medical devices; FORTH (a PANACEA partner) has implemented the integration of IMP H2M within their Clinical Information System (ICS), iSPRINT (a PANACEA partner) has used SbDF in developing the integration of its Clinical Studies System (Healthentia) with an assistive robot (QTrobot) of LuxAI (a Luxembourg based company).

Walkthrough of the Solution Toolkit

The Solution Toolkit covers Dynamic Risk Assessment and Mitigation, Security by Design and Certification, Secure Information Sharing Platform, Identification and Authentication, Secure Behaviour Nudging Tool, a package for the Training and Education for Cybersecurity Tool and the Resilience Governance Tool.



Videos on the Tools

Dynamic Risk Management Platform		https://www.youtube.com/watch?v=dnRxQuwtJaQ&t=3s
DRMP in HSE		https://www.youtube.com/watch?v=m4fsG-z1QsM
Security by Design Framework		https://www.youtube.com/watch?v=qY6HMs6psDU&t=2s
Compliance Support Tool		https://www.youtube.com/watch?v=X20yVWGG5As&t=4s
Secure Information Sharing		https://www.youtube.com/watch?v=2e4hrP_fAmk
Identity Management Platform for Human to Machine Authentication		https://www.youtube.com/watch?v=_3og9nMY7U0&t=39s

Videos on the Tools		
Secure Behaviour Nudging Tool		https://www.youtube.com/watch?v=DFzUqldtCf0&t=33s
Training and Education for Cybersecurity		https://www.youtube.com/watch?v=-B9gSEt1mq4&t=29s
Resilience Governance and Cyber Return on Investment		https://www.youtube.com/watch?v=Vkv2WGCeRjA&t=23s

Dynamic Risk Assessment and Mitigation

The **Dynamic Risk Management Platform** (DRMP) is designed to protect a complex IT infrastructure by quantitatively assessing the current level of risk through a multi-dimensional threat analysis and ensuing business impact. This tool constantly monitors the network topology for the timely detection of changes within it and its configuration, as well as new risks and vulnerabilities affecting the system both at the technical and non-technical level, that is, human interactions with IT and medical systems. The risk analysis is fed by the dynamically computed potential attack paths, which help establish their impact on the business.

The DRMP instantiates the **multi-dimensional attack model**[14], reflecting the role played by human behaviours in the unfolding of a cyber-attack. The model is aimed at capturing how human users access ICT systems and medical devices, detecting human vulnerabilities as the most commonly exploited threats in healthcare organisations, as illustrated in Table 2[15].

Table 2: Attributes for assessing human vulnerabilities

Attribute	Description
Individual Security Attitude	Allows users to evaluate and measure the priority given to cybersecurity practices by an individual.
Security Behaviour	Allows users to estimate and measure the individual level of cybersecurity based on the analysis of past behaviours.
Security Culture at Work	Allows users to estimate and measure whether deviation from security practices is the norm in the workplace
Security Training Level	Allows users to estimate and quantify the overall level of training received by the individual.
Trust in Colleagues	Allows users to estimate and quantify the level of trust that the individual feels about her/his colleagues.
Trust of Physical Security of the Building	Allows users to estimate and quantify the level of trust that the individual feels about the security of the environment's security.

14 For more details, see [21].

15 For more details, see PANACEA [22].

The risk computation triggers the identification of technical and non-technical mitigation actions to reduce the risk level alongside the business impact that such actions may cause. DRMP considers 'human' vulnerabilities, due to improper behaviour of medical personnel using the assets of the network (i.e. medical devices).

- The DRMP adopts a generally different approach from SOAR (Security Orchestration, Automation and Response) solutions, network management systems and vulnerability assessment Tools as it focuses on the computation of possible attack paths traversing multiple layers (network, access and human: see Fig. 2) and on the evaluation of related risks. The resulting risk assessment output then takes into consideration different, combined layers and gives a more comprehensive risk estimation.

The Dynamic Risk Management Platform captures diverse layers, from human to business, access to network, as illustrated below.

Security-by-Design Framework

- The **Security-by-Design Framework (SbDF)** is a methodological tool to help overcome design limitations of medical devices and information systems, which often do not specifically include **security-engineering aspects** about **cyber risks**.
- The tool is designed for a typical assessment and system monitoring audit workflow. It is supported by specific technical solutions for conformity assessment, through compliance schemes, and risk assessment by focusing on cybersecurity and engineering aspects.
- SbDF supports medical device **manufacturers** and **health system providers** in deciding possible security controls that need to be implemented during software and system development and engineering phases. It also supports healthcare organisations when deploying medical devices and systems in their IT environment. It comprises two components: **Compliance Support Tool (CST) and Secure Design Support Platform (SDSP).**
- The **Compliance Support Tool is for conformity assessment. It guides the assessor through a standardised programme** for assessing the conformance of the target object (i.e. medical device, information system, network medical device) with a series of standards relevant for the user and application context, e.g. GDPR, ISO 27001, EN ISO 13485, ISO IEC 80001. It supports users in assessing the medical system development process during all the phases of its lifecycle, following a wizard procedure that enables a conformity assessment by answering up to 560 questions based on the use case in scope and with a real application by a medical device manufacturer.
- The **Secure Design Support Platform focuses on risk assessment. It guides the risk analyst** through the risk assessment process of a network or of a system "network + medical devices". It links business processes/activities to their malfunctions and their assets, links assets to their potential vulnerabilities and to threats that can exploit these vulnerabilities. Based on these variables, it calculates the risk associated with each asset, showing the most critical ones and recommends measures to reduce the risk(s). This tool fully supports analysts, not only through a guided workflow and the calculation algorithm, but also by listing malfunctions, vulnerabilities, threats and measures specific to healthcare. The lists can be enriched based on the knowledge and skills of the analyst and team members.

Secure Information Sharing Platform

The Secure Information Sharing Platform (SISP) is designed to deliver a secure sharing support tool enabling healthcare personnel to share information in near real-time within their own organisation and with external organisations.

- The tool enables healthcare professionals to **exchange healthcare information** more efficiently and more securely than the current baseline, by promoting interoperable file formats, cryptographic methods and a mutual trust model. Information sharing can be performed between different healthcare organisations, across borders and between organisations within a single country.

- Distributed and centralised deployment models are available in the Secure Information Sharing Platform, which can support the sharing of customisable types of data, including large datasets, such as hi-res images, in full compliance with the GDPR. Security is also taken into consideration, with the full support of certificates and encrypted communications[16].

Identification Management Platform for Human to Machine Authentication

The **Identification Management Platform for Human to Machine Authentication** (IMP H2M**)** is designed to make sure that users of a medical system or medical device are known to the hospital system and are really who they claim to be. As an alternative to passwords, it removes the usual threats of passwords that may be shared, unprotected, too short or too simple, hard to remember or poorly managed, etc. It makes login faster and simpler than using passwords. It is GDPR compliant, suitable for use in a healthcare working environment and does not require the storage of biometric data in a central place.

The IMP is suitable for Windows workstations (either connected to large medical devices like radiology equipment, or laboratory management systems, or directly to the IT network) as well as medical devices running Windows Embedded and including a webcam and a minimal user interface.

- The Tool allows user authentication based on two authentication factors, which are the **biometry** (who you are), and a **smartphone** (what you have), through the following steps:

a) User downloads the PANACEA IMP application and installs it on her or his smartphone.

b) User opens the PANACEA IMP application, registers and takes her/his photo.

c) User goes to work, keeping her/his smartphone in her/his pocket, with Bluetooth LE switched ON

d) User authenticates into the workstation using his or her biometry.

- The workstation detects smartphones closed to it, accessible via Bluetooth LE, and accesses the encrypted face image template, the login name, and a hash of the user's password from the user's smartphone[17].
- The workstation displays a login screen, and the user clicks the OK button to accept biometric authentication.
- The workstation takes the real-time image of the user via its camera and computes a biometric template from the face image.
- The IMP identification software compares the biometrics template computed on the workstation to the biometric template deciphered from the smartphone. If the comparison concludes that this is the same person, known to the hospital's authorised persons repository.
- The access is authorised using the user's login name and the hash of the password, while the image and its associated template are removed from the computer memory for GDPR compliance.

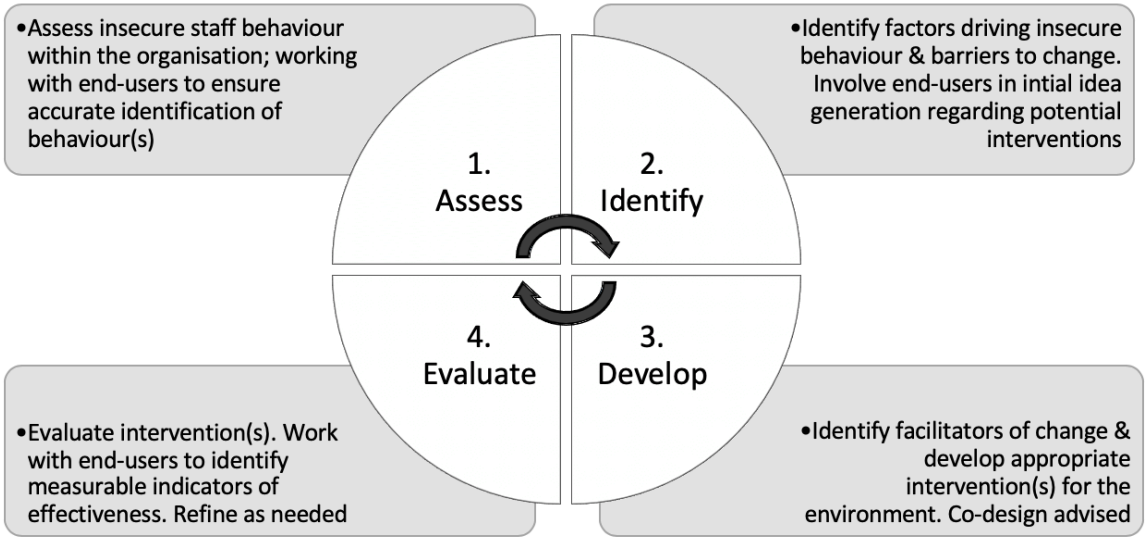
e) With the same enrolment application, users can remove their consent to use biometrics at any point in time and delete their biometric template from their smartphone.

16 For more details, see [23].

17 A biometrics template is a code extracted from some biometric data, irreversible (you cannot go back to the original data from the code), and that can be used to compare two biometric data samples.

Secure Behaviour Nudging Tool

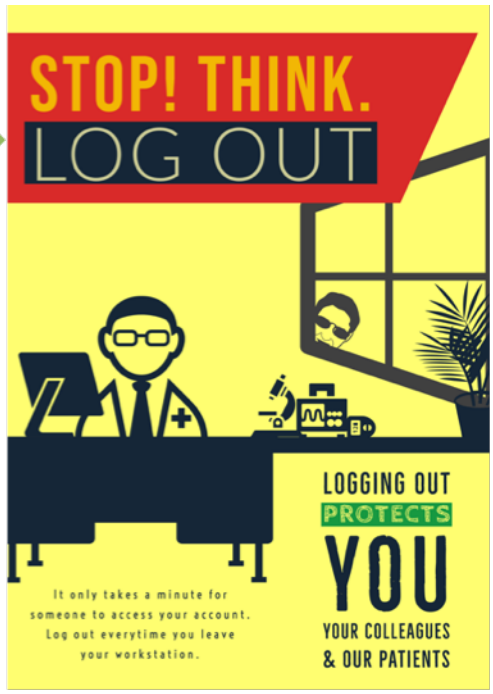
The **Secure Behaviour Nudging Toolkit (SBNT)** is a methodology designed to help staff responsible[18] for encouraging cybersecure behaviours within a healthcare organisation, built around proven psychological theories. The methodology goes through four steps: Assess, Identify, Develop and Evaluate (AIDE), as illustrated in the figure below[19]. These steps allow healthcare organisations to assess their current cybersecurity posture; identify behaviours to change, develop interventions and evaluate the outcomes. The figure below shows the AIDE approach to designing secure behaviour nudging.



The figure below lists the human vulnerabilities identified during the PANACEA project through focus groups involving staff (nurses, medical doctors, administrative and technical employees) from three healthcare organisations in Greece, Ireland and Italy[20] with an example of an informational nudge consisting of awareness raising displayed in lifts or canteens.

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



18 e.g. the Human Resources (HR) function, the managers, the Chief Information Security Officer (CISO).
19 For more details, see [24].
20 For more details see [25].

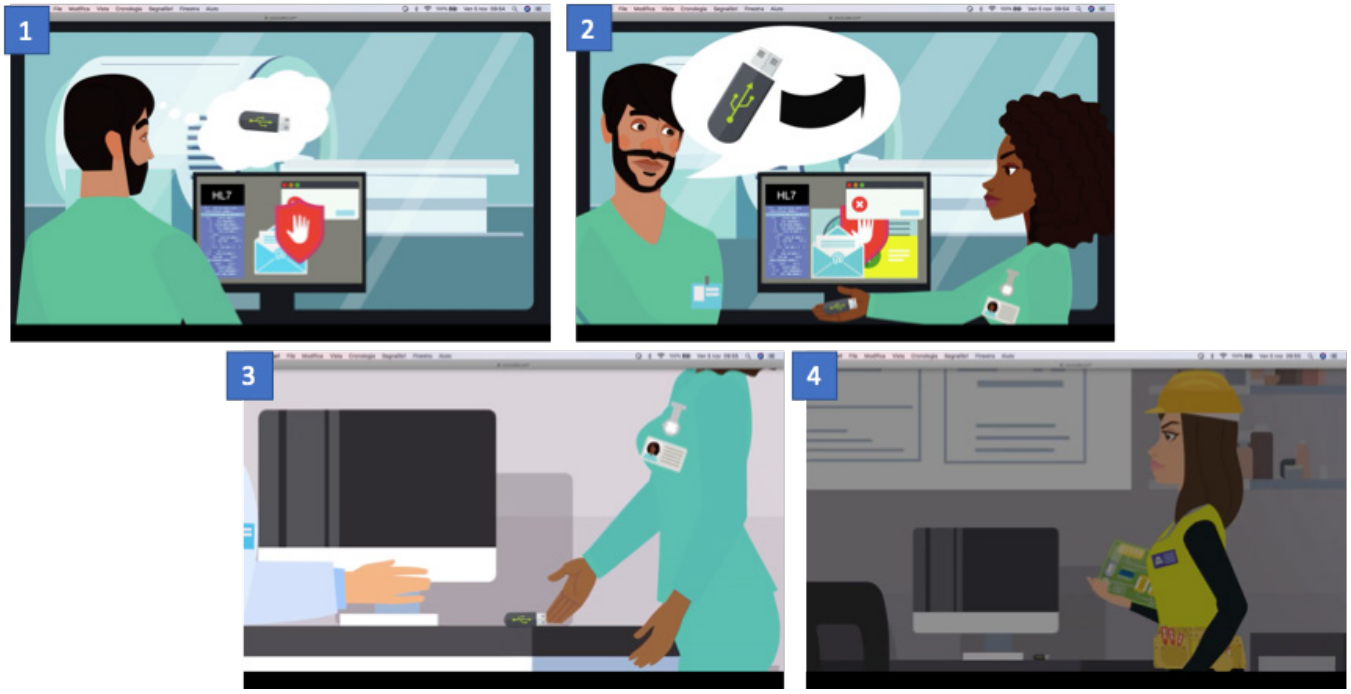
Training and Education for Cybersecurity Tool

The package for **Training and Education for Cybersecurity Tool** is designed to show, to anyone who works in a healthcare organisation, the close relationship between secure cyber-related behaviours, and the health and well-being of patients.

PANACEA workshops with healthcare organisation staff have shown time to be a key factor for cybersecurity. Many contributors have repeatedly stated that they could not afford the time to implement the IT and cybersecurity policies and processes. It is therefore highly unlikely that these same people would be willing to dedicate a substantial amount of time to cybersecurity training. Judicious media selection should make learning as striking and as impactful as possible in the shortest possible time span. E-learning is highly suited to HCOs. It can be: 1) rich in images, still or moving, 2) designed, developed and delivered in modules. 3) accessible at the learners' convenience, 4) available for multiple experiences, 5) layered and differentiated to appeal to a range of audiences, 6) largely independent of language, 7) realistic and graphic.

These concepts led to a decision that video-clips, lasting 1-2 minutes, can be an effective education solution in the HCO context. This has been achieved by implementing a set of eight videos[21], each dealing with specific risky situations, e.g. use of password, use of USB, phishing.

The figure below shows a sample of screenshots from a video-clip, to raise cybersecurity awareness of potential negative consequences of USB use.



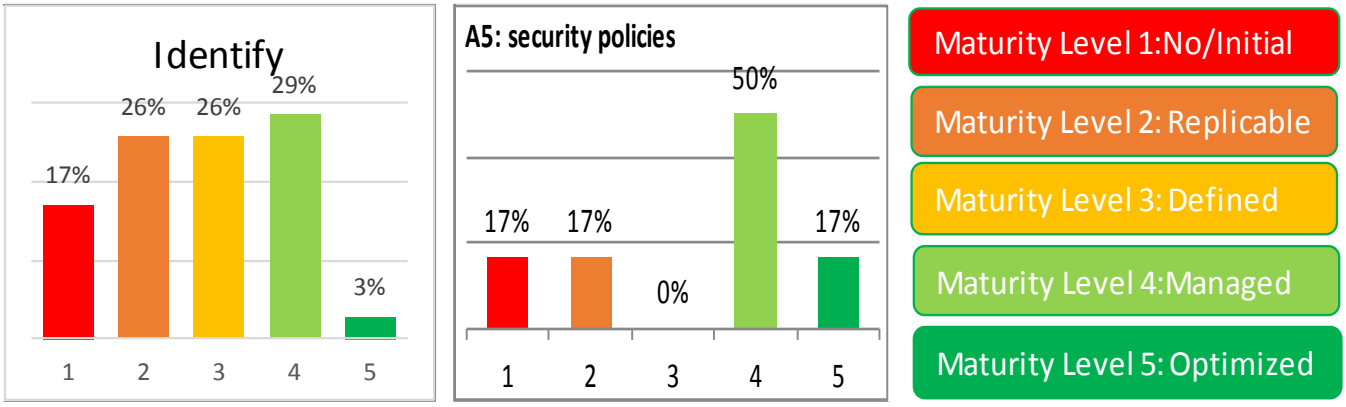
Resilience Governance Tool

The **Resilience Governance Tool** includes the **HealthCare Cybersecurity Governance Tool (HCGT)** and the **Healthcare Cybersecurity Organisation Model (HCOM)**.

The purpose of the HealthCare Cybersecurity Governance Tool is to evaluate the Information Security Management System (ISMS) of healthcare organisations as a standard entity for cybersecurity management. It enables the assessment of "Level of Gaps" in relation to diverse cybersecurity standards (ISO 27001, NIST SP800-53 and TOGAF-O-ISMS3), which are combined into a set of 133 "Security Controls" that also take into consideration specific security aspects of the healthcare domain. The tool supports the assessor in going through the "Security Controls"; the assessor inputs the maturity/implementation score for each control and has a dashboard to easily visualise the key areas of weakness

21 Video in short chapters are uploaded on an unlisted YouTube site, https://www.youtube.com/playlist?list=PLDfeq9anZOFFZXFTYr-H8h9c1XtaxLhZx; titles are in Italian, but the videos are language-independent because they are voiceless.

against the different standards, as depicted in the figure below, which shows the maturity of the healthcare organisation against one of the 5 NIST "functions"[22] Identify and one of the 14 ISO 27001 "control clauses"[23], A5: security policies[24].



The **HealthCare Cybersecurity Governance Tool is a set of guidelines** for organising the management of Cybersecurity in HCOs to assign responsibilities on all cybersecurity NIST functions. They apply three principles: 1) clearly distinguishing roles at strategic, tactical and operational level, 2) ensuring integration among risk management functions (Cybersecurity, Data Privacy, Physical security and clinical Risk Management), 3) ensuring that, in addition to Information Technology function, management and staff of all the hospital critical functions, such as, Clinical Engineering, Clinical Trials, Nurses and Medical Doctors management) are involved. It is recommended to 1) appoint a Chief Information Security Officer (CISO) 2) set-up a Risk Management Committee including CEO and all Heads of Department, 3) appoint in each Department through its director, an Information Security Reference Person (ISRP) acting as an interface between the Department and the Chief Information Security Officer (CISO).

Walkthrough of the Delivery Toolkit

Cyber Return-on-Investment

The **Cyber Return-on-Investment Tool** (C-ROI) supports management in prioritising cybersecurity investments through an extension of the functionality of the Resilience Governance Tool. It gives a structured method to:

- Pinpoint the weak points of the AS IS situation with respect to the outcomes provided by the RGT Tool, especially the HCG Tool.
- Estimate the cost of removing the weak points through investments.
- Prioritise the investments considering their impact on compliance and cost.

The Tool is independent in that it does not refer specifically to investments that can be covered with PANACEA Tools. However, it can be used to check the impact of a PANACEA Tool on the overall cybersecurity compliance and support decisions to adopt it.

Implementation Guidelines Tool

The **Implementation Guidelines Tool (IGT)** supports the management in deploying PANACEA Tools (both as individual Tools and integrated Toolkit, both technical and non-technical) in the specific context of the client (a healthcare organisation). It offers guidelines on:

- Assessing the operational context in terms of cybersecurity measures already in place and select the PANACEA Tools that can strengthen the HCO cybersecurity maturity level.

22 Identify, Protect, Detect, Respond, Recover, see [26].

23 https://multimatics.co.id/blog/jun/build-cyber-security-system-to-meet-global-standard-requirements.aspx; see also [27].

24 e.g., 3% of the controls assessing NIST I*dentify* "function" are at level 5; 50% of the controls assessing the ISO 27001 *A5: security policies* "control clause" are at level 4.

- Identifying roles and actors to be involved in the deployment and future use of the Tools (both technical and non-technical).
- Running the actual deployment, with recommendations for the diverse phases and actors involved in each phase.

How the PANACEA Toolkit can help Healthcare Organisations

The PANACEA Toolkit gives healthcare organisations a set of Tools that can help face all the challenges specific to the healthcare sector. The Toolkit enables the deployment of a holistic response to the challenge because it acts on three dimensions: **technology** (e.g., through the Dynamic Risk Management Platform), **organisation** (through Resilience Governance Tool), and **people** (e.g., through Secure Behaviour Nudging Tool).

This approach is expected to increase the probability of success of cyber-related interventions, vs mono-dimensional or bi-dimensional approaches. Examples are given for the procurement and deployment of new system or medical device, such as a new blood analyser deployed in 10 different clinical wards and networked with the Laboratory Information System, as reported in [28].

Table 3 below gives examples of use scenarios, illustrating which Tools can contribute to resolving specific challenges:

- The Security by Design Framework allows users to check the compliance of the item and of the provider with cybersecurity standards and best technical practices.
- The Dynamic Risk Management Platform allows users to simulate the impact on the security of the insertion of the new item into the existing network.
- The Identity Management Platform allows users to solve weaknesses in the access to the item.
- The Secure Behaviour Nudging Tool allows users to identify in advance any risk related to the human-machine interaction and to design appropriate nudges for staff (nurses, medical doctors) using the item.
- The Training and Education for Cybersecurity Tool allows users to rapidly implement a videoclip to build awareness on cybersecurity aspects for relevant staff contextually to the training on the use of the new item.
- The Resilience Governance Tool offers organisational guidelines outlining who should be involved in the procurement and deployment process.

Table 3: Tool Use Scenarios to improve Cybersecurity in Healthcare

Challenges and use cases (examples)	PANACEA Tools						
	DRMP	SbDF	SISP	IMP	SBNT	TECT	RGT
STRUCTURAL CHALLENGES (ROUTINE SITUATIONS)							
Human vulnerability Need to limit human errors due to multi-use and time pressure, e.g.: Intervention on the staff of a specific clinical department, where there is the feeling of diffused risky behaviours. The department's staff makes frequent shared use of workstations and networked medical devices. And needs to share clinical information with external actors (e.g., other hospitals, laboratories)	🔒		🔒	🔒	🔒	🔒	🔒
STRUCTURAL CHALLENGES (COVID-LIKE SITUATIONS)							
Telemedicine Need to ensure secure Telemedicine, e.g., Activation of a telemedicine service for non-severe COVID patients at home	🔒	🔒	🔒	🔒	🔒	🔒	🔒

Challenges and use cases (examples)	PANACEA Tools						
	DRMP	SbDF	SISP	IMP	SBNT	TECT	RGT
Smart working Need to ensure secure Smart-working, e.g.: sudden activation of smart-working for a high quantity of hospital staff in case of a pandemic	🔒		🔒		🔒	🔒	🔒
Quick onboarding of new staff Need to ensure secure rapid on-boarding of new staff in clinical activities, e.g., management, from a cybersecurity point of view, of the on-boarding of a batch of new staff to a new Intensive Care Unit (ICU) or clinical ward.				🔒	🔒	🔒	🔒
Non-healthcare sites used for healthcare operations Need to ensure secure adaptation to sanitary purposes of non-sanitary host structures, e.g.: management of an adaptation project aimed at ensuring the cybersecurity of a hotel, where healthcare staff from the Hospital are operating. The hotel is connected with the Hospital and clinical information is exchanged.	🔒	🔒	🔒	🔒	🔒	🔒	🔒
Specific types of cyber-threats Need to contrast stream of fake pandemic related messages, e.g., management of an awareness-raising campaign to avoid staff becoming victims of a pandemic-related cyberattack					🔒	🔒	🔒
REGULATORY CHALLENGES							
Directive (EU) 2016/1148 (NIS), GDPR (EU) 2016/679 Need to decide cybersecurity investments, e.g.: management of the investment portfolio decision under the constraint of budget limitation during the yearly budget definition process, to comply with indications from national authorities.	🔒				🔒		🔒
Procurement Guidelines (ENISA) 2020, Medical Device Regulation (EU) 2017/745 Need to cope with frequent procurement (selection, contracting) and deployment of new technology, e.g., management of a proposal for a new software (or a new networked medical device) from its evaluation to its deployment in the hospital.	🔒	🔒		🔒	🔒	🔒	🔒

Case Study: HSE Ransomware Attack

An example of what happens in the case of a successful cyber-attack is the **ransomware cyber-attack** that hit the **Health Service Executive (HSE) of Ireland**[25]. On 14 May 2021, the HSE suffered a major ransomware cyber-attack that resulted in the shutting down of all its ICT systems nationwide. It was the most significant cybercrime attack on an Irish state agency and the largest known attack against a computer system in a healthcare service. The attackers, a criminal gang known as Wizard Spider, used the Conti ransomware.

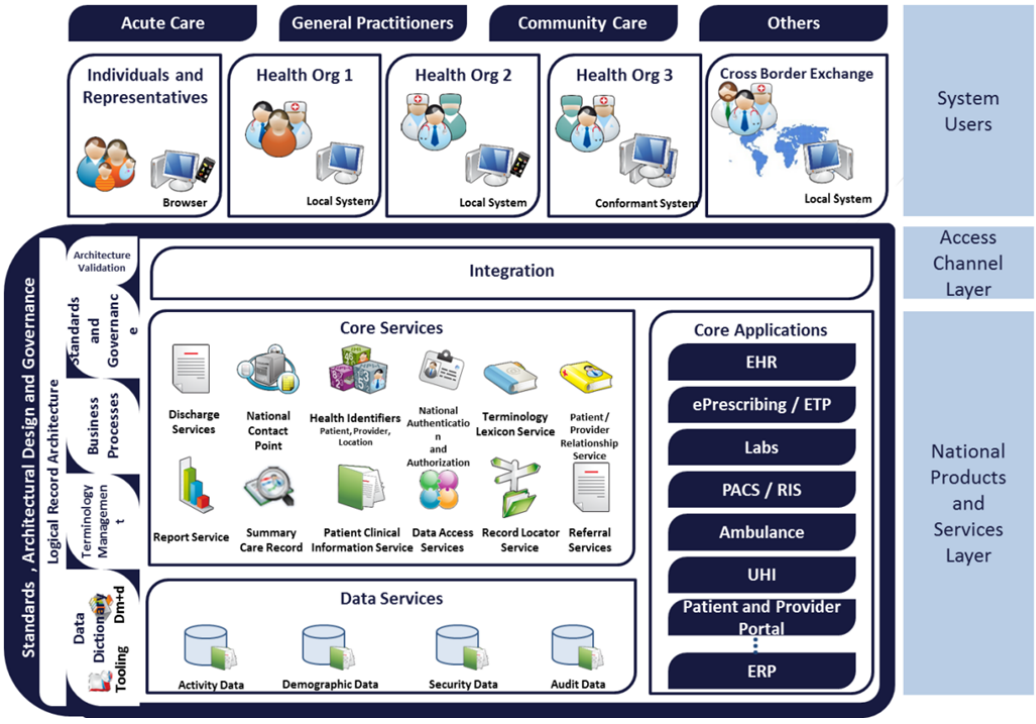
The incident gives a first-hand insight into what happened. It also offers an example of how the PANACEA Toolkit might have assisted in avoiding and recovering from the cyber-attack.

The Structure of the HSE and its ICT Network

The HSE is the publicly funded healthcare system in the Republic of Ireland, responsible for providing health and personal social services. The HSE is a large organisation bringing together over 100,000 people. The Executive was set up under the 2004 Health Act and came into official operation on 1 January 2005. It replaced the ten regional Health Boards, the Eastern Regional Health Authority and several other agencies and organisations. Bringing all these regional boards into one ICT Network was a significant challenge and even now some legacy issues are still used because of the amalgamation of so many different systems.

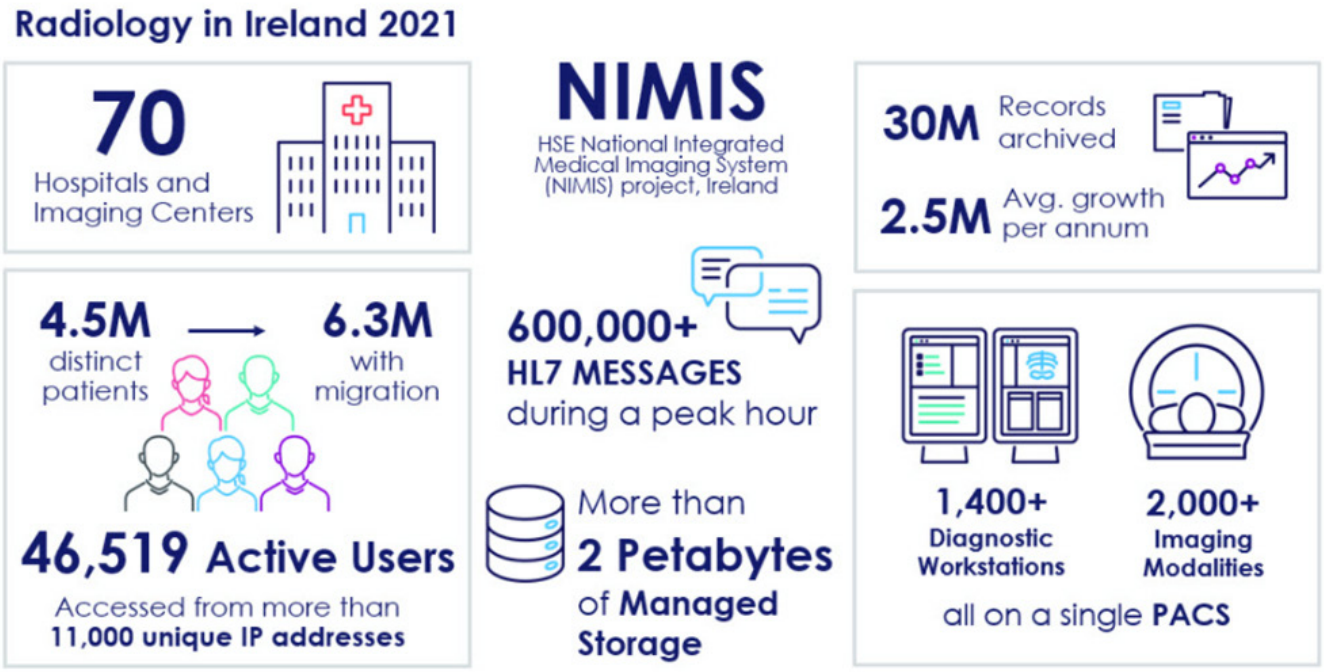
The ICT Directorate is responsible for the delivery of ICT services, projects and support across the HSE. The HSE Office of the Chief Information Officer (CIO) delivers ICT services and support across the HSE to a current user base of over 50,000 staff, using approximately 1,400 applications in 1,000 networked sites. The HSE provides a range of national applications to the acute voluntary sector. All contracted hospitals are connected through the National Health Network (NHN).

The figure below shows the ICT structure of the HSE and the interlinkages of the systems, such as the system users, the access channel layer, the National Products and services layer. The deployment includes medical device imaging workstations, Radiology Information System (RIS), Picture Archiving Communication System (PACS), Voice Recognition Systems, and other third-party systems.



25 Unless otherwise stated, the description of the attack and of its impact is based on the narration of the HSE Project Manager for COVID-19 Planning SSWHG and on the webinar "'Ransomware Attack on Irish Health Service" delivered by the H2020 No-Fear Project on 14 October 2021 (https://no-fearproject.eu/archives/1397) he coordinated.

To give a sense of size, the next figure shows the 2021 data for the HSE National Integrated Medical Imaging System (NIMIS).



NIMIS creates a framework for the delivery of radiology services across the country. A centralised database manages 3.5 million studies annually and supports the provision of radiology services to approximately 4.2 million patients across Ireland.

Typical hospital network features

A segmented network consisting of the following main *IP ranges*

- 10.40/10.240 – Core network subnets
- 10.241 / 10.242 vLAN for IP and VOIP traffic
- 10.84 local IP range for Radiology extended to 10.240.84 for NHN connectivity

All IP/VOIP traffic is managed via 10.241 10.242 VLAN across complete site with reserved ports on layer 3 switches allocated to telephony devices.

Typical Hardware HSE Hardware:

- Core Switches: Cisco 6500 or equivalent, Layer 3 switches equivalent to Cisco C3650
- Routing Protocol: OSPF (Open Shortest Path First)

Enterprise virus protection

- McAfee Agent -Version number: 5.5.1.342 Status: Managed Super-Agent: Peer to Peer
- McAfee Drive Encryption Agent Version number: 7.2.5.24 Language: Multiple
- McAfee Drive Encryption Version number: 7.2.5.24
- McAfee Endpoint Security Version number: 10.7
- Citrix Workspace-Store - Citrix Receiver Store Versions 21.2.0.0

The HSE, like other healthcare organisations, are innately vulnerable to attack as they are large organisations encompassing multiple bodies and groups, with people under life-and-death pressure whose attention is not always focused on cybersecure behaviours such as password strength.

Some of the outdated software packages on HSE computers, such as Windows 7, still in use in the health service at the time of the attack, was not the reason why the attack was successful. Efforts had been made prior to the hack to keep machines running that system off other parts of the network: they were not receiving security patches but they were sometimes needed to run older pieces of medical hardware that did not work with newer systems.

The Ransomware Attack

The attack affected almost every part of the healthcare system, which was already struggling to cope with the COVID-19 pandemic. The hackers are thought to have started several easily detectable cyber-attacks during the night of Thursday 13 May to conceal their earlier presence on the network, before triggering a full-scale ransomware attack at about 4am on Friday 14 May.

The attackers promised to unlock the encrypted data when the ransom was paid, while threatening to release the copied data if it was not paid. Hence it being referred to as a "double-extortion" as it not only threatened to cripple the system but also release the data.

On 7 May 2021, Colonial Pipeline, the company providing almost half of the fuel for the East Coast of the United States, was hacked by a criminal gang referred to as 'Darkside'. Six days later, officials at the Department of Health in Ireland noticed suspicious activity on their computer systems and contacted the National Cyber Security Agency. Based at the Department of the Environment in Adelaide Road in Dublin and with a staff of about 30 IT specialists, its job is to manage cybersecurity incidents across Government and provide guidance and advice to citizens and businesses on these incidents.

The Irish health service IT systems had avoided another ransomware attack four years ago when the WannaCry virus infected a quarter of a million machines in 150 countries including the UK's NHS. Yet, the 2021 cyber-attack, which first hit the Irish Department of Health and then the HSE, turned out to be the most serious ever attack on the State's critical infrastructure.

The National Cyber Security Team activated its crisis response procedures and called in FireEye, a commercial specialist IT incident response company. Investigators found a remote access Tool known as 'cobalt strike Beacon' on the system, which hackers used to move within computer networks before launching their virus and demanding a ransom, or as it is known in computer parlance, an "execution of a ransom payload". Unknown to anyone, the hackers had already been in the IT systems at least a week before.

The Department of Health acted quickly enough to prevent the cyber criminals from detonating their malware, known as Conti, on its systems. The IT specialists were able to detect, and stop an attempt to execute ransomware, through a combination of anti-virus software and the deployment of specific tools. The result is that the systems at the Department of Health were not badly damaged and were up and running again soon afterwards.

The HSE, however, was not so lucky. They first realised they were under attack in the early hours of Friday morning on 14 May. But by that time, it was too late. The criminals had executed their ransom payload and the HSE systems had been disabled.

The attack has badly damaged the HSE and its health services. It has had to shut down its systems and bring in specialists to carefully go through each part of its network, step by step, find the malware, block malicious IPs and domain names, protect privileged accounts, clean, rebuild and update all infected devices, ensure that the antivirus is up to date on all systems, make sure all devices are patched and ultimately restore the data.

Cobalt Strike

Cobalt Strike is a paid penetration testing product that allows an attacker to deploy an agent called *'Beacon'* on the victim machine. Beacon gives attackers a wealth of functionalities, including, but not limited to command execution, key logging, file transfer, SOCKS proxying, **privilege escalation**, Mimikatz, port scanning and lateral movement. Beacon is in-memory/file-less, in that it consists of stage less or multi-stage shellcode that once loaded by exploiting a vulnerability or executing a shellcode loader, will reflectively load itself into the memory of a process without touching the disk. It supports C2 and staging over HTTP, HTTPS, DNS, SMB named pipes as well as forward and reverse TCP; Beacons can be daisy-chained. Cobalt Strike comes with a Toolkit for developing shellcode loaders, called Artifact Kit. The Beacon implant has become popular amongst targeted attackers and criminal users as it is well written, stable, and highly customizable.

Conti ransomware

The attackers spreading Conti have switched gears to a completely fileless attack method. The ransomware, which calls itself Conti, is delivered at the end of a series of Cobalt Strike/meterpreter payloads that use reflective DLL injection techniques to push the malware directly into memory.

Because the reflective loaders deliver the ransomware payload into memory, never writing the ransomware binary to the infected computer's file system, the attackers eliminate a critical Achilles' heel that affects most other ransomware families: there is no artefact of the ransomware left behind for even a diligent malware analyst to discover and study.

Two-stage loading process

The first stage of the Conti ransomware process involves a Cobalt Strike DLL, roughly 200kb in size, that allocates the memory space needed to decrypt and load meterpreter shellcode into system memory. A portion of meterpreter shellcode, extracted from memory on an infected machine.

The shellcode, XORed in the DLL, unfurls itself into the reserved memory space, then contacts a command-and-control server to retrieve the next stage of the attack. This C2 communication is distinctive for several reasons. First, the malware appears to be using a sample Cobalt Strike configuration script called trevor.profile, published on a public Github archive.

Among the behaviours observed by responders, the ransomware immediately begins encrypting files while, at the same time, sequentially attempting to connect to other computers on the same network subnet, to spread to nearby machines, using the SMB port.

SMB scanning by Conti during the infection

Conti's developers have hardcoded the RSA public key the ransomware uses to perform its malicious encryption into the ransomware (files are encrypted using the AES-256 algorithm). This is not unusual; It means that it can begin encrypting files even if the malware is unable to contact its C2.

Unfortunately, that is not the only threat this ransomware poses to its targets: Conti ransomware has also adopted a "leaks" site like several other ransomware threat actor groups. The attackers spend some time on the target network and exfiltrate sensitive, proprietary information to the cloud (in recent attacks, the threat actors have used the cloud storage provider Mega).

The Response

The Government's position has been the same from the start: Ireland will not pay. No money changed hands and no agency, representative, or private individual, directly or by proxy, has or will pay any ransom and that none will be paid or disguised in any fees paid to a commercial company. The Government cannot be seen to capitulate to the demands or support the business model of organised crime.

The National Cyber Security Centre and the private IT specialist contractors also say they have not engaged at all with the criminal gang responsible. They are satisfied that this criminal gang knew that it had attacked a healthcare service and that its crime would impact on sick, elderly and vulnerable people including children.

Irish National Cyber Security Centre (NCSC)

The National Cyber Security Centre (NCSC) was founded in 2011 and is an operational arm of the Department of the Environment, Climate and Communications (DECC). The NCSC is responsible for advising and informing Government IT and Critical National Infrastructure providers of current threats and vulnerabilities associated with network information security.

The main roles of the NCSC are to lead in the management of major cyber security incidents across government, provide guidance and advice to citizens and businesses on major cyber security incidents, and develop strong international relationships in the global cybersecurity community for the purposes of information sharing. Since 2011, the unit has focused its efforts on building capacity and establishing a stable base for its operational work.

In the immediate aftermath of the cyber-attack, the NCSC activated its crisis response procedures and has provided support and assistance to the HSE and Dept. of Health in responding to and recovering from the incident. It has identified and listed the **Indicators of compromise**[26].

The following indicators of compromise have been seen in relation to this incident

- **Conti SHA256**: d21c71a090cd6759efc1f258b4d087e82c281ce65a9d76f20a24857901e694fc
- **Cobalt Strike SHA256:** 234e4df3d9304136224f2a6c37cb6b5f6d8336c4e105afce857832015e97f27a
- **Cobalt Strike SHA256:** 1429190cf3b36dae7e439b4314fe160e435ea42c0f3e6f45f8a0a33e1e12258f
- **Cobalt Strike SHA256:** 8837868b6279df6a700b3931c31e4542a47f7476f50484bdf907450a8d8e9408
- **Cobalt Strike SHA256:** a390038e21cbf92c36987041511dcd8dcfe836ebbabee733349e0b17af9ad4eb
- **Cobalt Strike SHA256:** d4a1cd9de04334e989418b75f64fb2cfbacaa5b650197432ca277132677308ce
- **Filename:** _EXE.bat
- **Filename:** _COPY.bat
- **Lazagne SHA256:** 5a2e947aace9e081ecd2cfa7bc2e485528238555c7eeb6bcca560576d4750a50

It has set up the monitoring of the network for further suspicious activity, paying particular attention to an activity related to pre-cursor malware that may have pre-empted the ransomware attack. (IcedID/BazarLoader/Trickbot etc.) and then go through the **remediation sequence**: Contain, Eradicate, Recover.

26 National Cybersecurity Center (NCSC), *Ransomware Attack on Health Sector – UPDATE*, 16 May 2021.

Remediation sequence

Contain

1. Isolate Domain Controllers
2. Block egress to the internet
3. Create clean VLANs for rebuild and recovery operations
4. Block malicious IPs and domain names
5. Protect Privileged accounts
6. Harden endpoints

Eradicate

1. Wipe, rebuild and update all infected devices.
2. Ensure antivirus is up to date on all systems.
3. Make sure all hardware devices are patched and up to date.
4. Use your offsite backups to restore systems - before restoration take steps to ensure your backups have not been exposed to malware.

Recover (The 5 Rs to Recovery)

1. Restore endpoints.
2. Re-image devices if required.
3. Re-set credentials.
4. Re-Integrate Quarantined systems.
5. Restore Services.

The Impact

The initial cost of the attack has been estimated at €100 million[27]. The final estimated cost could rise to half a billion euros[28]; this would include replacing outmoded technology that would normally be replaced over the next three years.

On 23 June, it was confirmed that at least three quarters of the HSE's IT servers had been decrypted and 70% of computer devices were back in use. By September 2021, over 95% of all servers and devices had been restored.

All elements of health services in Ireland have been affected

- Telecommunication
  - No permitted access to the web made many web-based systems unavailable.
  - No e-mail, so an alternative ad-hoc system was put in place. Use of 'Gmail' or alternative e-mail addresses was quickly set up for communications, but there were risks associated with this measure. It took three days to get access to 3/4G routers which were strategically placed to enable communication.
- Clinical operations
  - Generalised slowing of clinical processes, e.g., colonoscopies down by 70-80% and chemotherapy and daily elective procedures down by 50%[29], radiotherapy service was unavailable in the public hospital system for 30 days and critical treatment was contracted out to private facilities.
  - Unavailability of Laboratory System (APEX) led to restriction of investigations to "essential only", no service for General Practitioners, no Historical lookup - all results manually checked by staff, handwritten labels with associated risks such as poor handwriting.

27 27 May 2021, https://www.thejournal.ie/cost-of-cyber-attack-on-hse-5449643-May2021/.
28 23 June 2021, https://www.independent.ie/breaking-news/irish-news/cost-of-hse-cyber-attack-could-rise-to-half-a-billion-euro-40572038.html.
29 https://www.rte.ie/news/2021/0521/1222968-hse-cyber-attack-reid/.

- Even when some systems came back, they could not be used immediately. In particular, equipment needed to be recalibrated by the manufacturers and/or vendors before being cleared for use. This had to be done by a limited number of personnel and across all the hospitals for labs and medical devices.

- Administrative operations
  - Unavailability of Patient Administration System made it difficult to register patients.
  - Unavailability of payroll, ordering, etc. systems made it difficult to perform related process.

- Data
- 19 May 2021, the Financial Times reviewed private data for twelve individuals which had appeared online as a result of the breach.
- On 28 May, the HSE confirmed that confidential medical information of 520 patients, as well as corporate documents had been published online.
- It has been reported that the cybercriminals allegedly exfiltrated 700 gigabytes of the HSE's data[30].

30 https://www.eolasmagazine.ie/what-can-we-learn-from-the-hse-and-department-of-health-ransomware-attacks/.

How the PANACEA Toolkit could have helped avoid the cyber-attack and support Recovery

The PANACEA Toolkit has not been designed to detect attacks. However, concerning the HSE attack, it could have helped in the "Pre-Attack" phase, to minimise the probability of a successful attack, and the Recovery phase.

The analysis of the case shows that the Recovery phase has two streams of activities:

- Those regarding the information management in a situation where the systems are not fully available and data must be stored and exchanged with back-up systems; cyber-risk must be low, also in this operation mode.
- Those aimed at restoring the ICT capability and the related business processes; the recovery must be short in time, but should also be managed to eliminate some issues that made the pre-attack systems vulnerable.

Table 7: PANACEA Tools and their potential for coping with the attack on HSE

Phases ->	Pre-Attack	Recovery [Info/data management before restoring]	Recovery [activities to fully restore ICT capabilities]
Key question -> **Panacea Tools**	**Would PANACEA have helped to... Avoid the attack?**	**Would PANACEA have helped to.. Reduce cyber-risk?**	**Would PANACEA have helped to... Better manage the recovery?**
DRMP (Technical risk assessment)	🔒		🔒
SbDF (Security by Design)			🔒
SISP (Secure Information Sharing)		🔒	
IMP-H2M (Biometric identification)	🔒	🔒	🔒
SBNT (Nudges)	🔒	🔒	🔒
TECT (Video-clips)	🔒	🔒	🔒
RGT (Governance and maturity assessment)	🔒	🔒	🔒

The Tools that relate to **Behaviour (SBNT), Education (TECT) and Governance (RGT)** are considered to have the most significant impact. From the outset, these tools embed the concept that cybersecurity is the responsibility of all employees. The constant reminding and nudging as necessary will assist in creating a mind-set of cyber hygiene. Given the similarities between hand hygiene in the contest of healthcare awareness of infection control procedures, the education Tool building on and health hygiene and cyber hygiene would re-enforce each other.

One of the major outcomes of the analysis of the HSE Cyber-attack was the lack of emphasis that major stakeholders pose to ICT and cybersecurity. This was particularly true of senior clinical staff. Secure Behaviour Nudging, Education and Governance would go a long way in ensuring that ICT and cybersecurity are a key priority for management, because they raise the awareness that the human layer and the business layer are fundamental to the security of the ICT systems.

These Tools are useful in the **Pre-attack** phase. While they are not technical Tools and will not actually detect an attack, nevertheless they would have helped to anticipate detection, by raising awareness of unusual activity on the system and raising the level of suspicion.

These Tools would have helped reduce the cyber risk regarding **information exchange and data management**. They would re-enforce the behavioural traits that staff would have in data exchange and data management. It would raise

the risk appreciation for data back-ups from just a hardware risk to highlighting the need for segmented data storage for two location data back-ups.

In addition, the Tools for Education, Nudging and Cyber Security Governance have a clear application and advantage in the various stages of recovery. Having increased knowledge and awareness of the impact of a cyber-attack would also reduce recovery time and assist in prioritising recovery actions.

Even something as simple as knowing the terminology and having a very basic idea of how the ICT system operates is a major advantage in recovery stages.

Recovery after a serious cyber-attack is slow and protracted. It can take many weeks and, in that time, the real risk, i.e., the risk to patients increases with each day that passes.

While the system is recovering, there are many temporary workarounds put in place and ad-hoc solutions which are vulnerable in and of themselves. Knowing what is required to protect the temporary systems and ensuring that all the temporary data that is stored in a safe and retrievable manner is greatly assisted by good governance practices.

The **Dynamic Risk Management Platform (DRMP)** provides an overview of the state-of-the-art of cyber risk scenarios, current countermeasures, and vulnerability assessment methodologies with a particular emphasis on the healthcare domain. DRMP should deliver threat modelling, attack modelling, response management and it is very useful that the resultant data is presented as a visual analytics display. Such analysis is important in identifying key nodes on the network which have a higher vulnerability.

Being easy to use is a key factor in its implementation in hospital environments. It has a clear and obvious applications in preparing for and planning in the pre-attack phase. While it might not prevent the attack, it would have detected the vulnerabilities and shown which mitigation measures should have been implemented. With such mitigation measures in place, the DRMP can be used in iterative mode for continuous improvements.

Clearly, it cannot detect that an attack is in progress, but it was not designed for this purpose.

It would also reduce the length of the recovery phase and help prioritise recovery much as it does in the vulnerability analysis. As the system is being re-built, it can be used as an iterative process to check that the re-build has not introduced new vulnerabilities.

The Security by Design Framework (SbDF) focuses on preventing a cybersecurity breach rather than repairing the issue and restoring systems after cybersecurity breach has hit a healthcare organisation.

The HSE has many and varies devices: consideration of cybersecurity in the equipment procurement is key. Therefore, SbDF has a prominent role in recovery.

The **Secure Information Sharing (SISP)** supports the challenge of secure information sharing in healthcare in terms of interconnectivity, cloud computing, authentication, and interoperability.

Although it was designed for the high-level requirements for the transfer of data between healthcare organisations and cross-border scenarios, it can also be applied internally within a HCO to increase data security. This is particularly true of diagnostic data from CT and Radiography. From this point of view, it has a particular advantage in the recovery stage. One of the key priorities is to transfer the diagnostic imagery from the imaging site to the clinical team whose role is to interpret and make a diagnosis based on that imagery. SISP allows this to happen on normal commercial networks, which would have significantly reduced the impact of the cyber-attack on the HSE.

The Biometric identification (IMP H2M) via Smartphone could have aided to help avoid the attack.

In the HSE there are the same complications in using password and password protocols as in any healthcare organisation. Biometric identification via Smartphone or dedicated device could have been helpful in all phases of the cyber-attack. One of the key findings on the attack was that some of the compromised computers were in use by more than one user.

Iris scans, fingerprint readers can be challenging more than facial recognition. Not only will the IMP H2H overcome some of the reluctance to use more 'traditional' biometric identification but it will also be considerably user friendly. The HSE uses EHR systems extensively and this system should also improve the accuracy of recordkeeping, thus reducing errors. HSE staff would not be allowed to use their personal smartphones but have official phones.

In recovery, the entire issue of new and old passwords is eliminated, speeding up the response.

How to adopt the PANACEA Toolkit

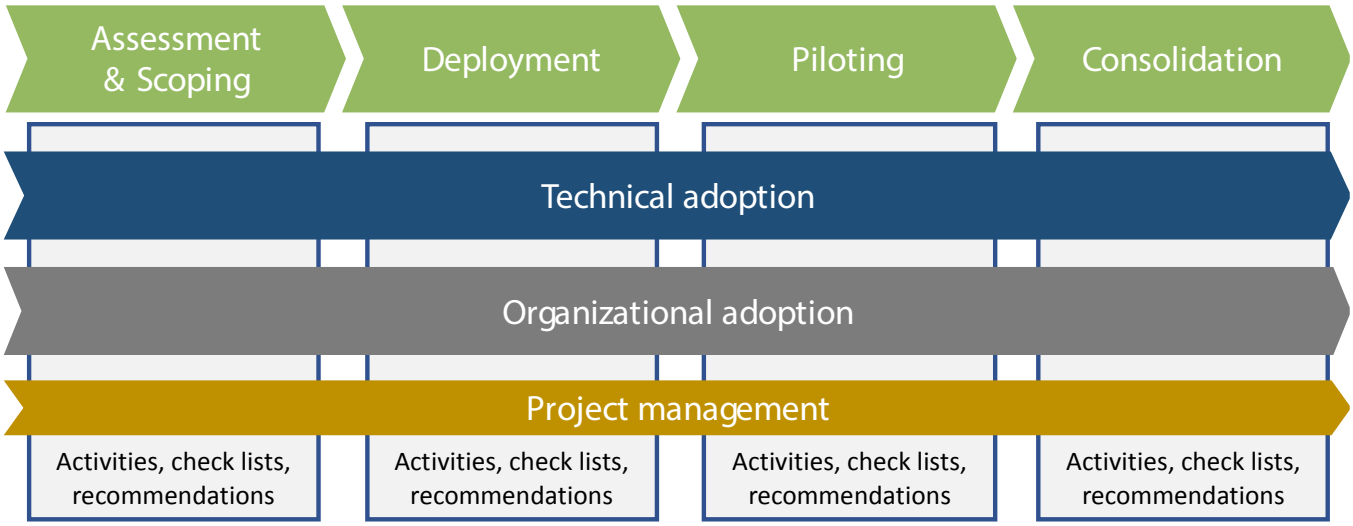
Adopting PANACEA as a Project

The adoption of the PANACEA Toolkit and its constituent part should be treated as a project with the purpose of selecting the Tools that fit the specific needs of an HCO, of running the actual deployment and first use piloting through use cases in limited contexts (e.g. a laboratory), identifying roles and actors to be involved in the deployment and future use of the Tools (both technical and non-technical).

The Implementation Guidelines have been drafted with the aim of supporting the management of an HCO in the initial adoption of PANACEA Tools (both as individual Tools and integrated Toolkit, both technical and non-technical) taking into account its specific technological and organisational context.

The implementation project is structured into four phases with three streams of activity (see Fig. 13). The guidelines cover all the phases and all the streams.

The figure below shows how the implementation project is structured.



The four phases include:

- **Assessment and Scoping**: consists of assessing the cybersecurity maturity level of the HCO and in defining the areas of intervention and the best modality of use, by the HCO, of the PANACEA Toolkit or any of its constituent parts.
- **Deployment**: consists of onboarding the Tools in the HCO and includes the installation of the technical Tools in the organisation's or consultant's premises.
- **Piloting**: consists of using the Tools in pilot use cases, both individually and as an integrated set.
- **Consolidation**: consists of extracting the lesson learned from the Piloting, in stabilising the organisational ownership of the Tools, in setting up the contractual framework regulating the relationship between the Tool providers and the HCO, and planning to extend adoption beyond the pilot use cases.

The three activity streams include:

- **Technical adoption**: includes the deployment and first use of the Tools into the existing HCO Cybersecurity measures to ensure contextualisation into the HCO technical and organisational environment.
- **Organisational adoption**: includes the activities such as the definition of roles, training, contracting with Tool providers to ensure that the right people in the HCO take ownership of the Tools and that the Tools are included in the HCO cybersecurity procedures.

Project management: includes the setting up of and monitoring the project, managing communication to ensure its execution in a reasonable time span, defining the roadmap to expand the use of the Tools beyond the pilot perimeter.

Ethical, Gender and Privacy Issues

Deployment and use of PANACEA Tools must consider that people and data related to them are involved. Table 8-1 shows the relevant ethical, gender and data privacy aspects for each Tool.

Table 8: PANACEA Tools and related ethical, gender and privacy issues

Tool	Ethical, gender and privacy issues
DRMP	The only issue regards the collection of the human data and credentials of healthcare staff that are part of the "human layer" modelled into the DRMP.
SbDF	No issue: no data regarding hospital staff or patients is used.
SISP	No issue: SISP is already designed to be GDPR compliant.
IMP	No issue: IMP-H2M is already designed to be GDPR compliant (e.g. it cannot capture the biometric data of people other than those intended and stores biometric elements on the individual user's device, not centrally.
RGT	No issue since no data regarding hospital staff or patients is used.
SBNT and TECT	SBNT and TECT already reflect the cosmopolitan nature of European Health Care Organisations in terms of Nudges and the Education videos. Questionnaires do not request information about facts such as age or gender to ensure there is no potential to establish the individual's identity. It is important to note that nudging is about encouragement, it is not about taking away freedom of choice. Individuals still have the option *not* to engage in the behaviour that they are being 'nudged' towards.

Conclusion

Many solutions for cybersecurity in healthcare exist in the marketplace. The PANACEA partnership sets itself apart as experts driving a holistic solution revolving around people, processes and technologies based on multi-disciplinary skills and know-how. As such, it offers healthcare organisations a strong and unique portfolio of solutions and expertise, tailored to cope with very specific challenges in healthcare, serving also an integrated solution covering classical technological and risk governance measures coupled with measures for human behaviours.

PANACEA Consortium

The PANACEA Toolkit has been developed by a Consortium of 15 Partners. They have agreed to jointly provide, after the end of the project, assessment, pre-certification and advisory services on cybersecurity to healthcare organisations, drawing on their multidisciplinary expertise and deep knowledge of the PANACEA Tools.

Table 8: PANACEA Consortium Partners and their Expertise for Healthcare Organisations

Partner		Country	Expertise
Aon Insurance & Reinsurance Brokers	AON	Italy	Risk governance
Foundation for Research and Technology Hellas	FORTH INSTITUTE OF COMPUTER SCIENCE	Greece	Clinical systems, information technology research
Foundation Policlinico Universitario Agostino Gemelli	Gemelli	Italy	HCO organisation, processes and technology
HSE-South South-West Hospital Group	Feidhmeannacht na Seirbhíse Sláinte Health Service Executive	Ireland	HCO organisation, processes and technology
IDEMIA Identity & Security France	IDEMIA	France	Biometric identification and authentication, Machine2Machine identification and authentication
Innovation Sprint	INNOVATION SPRINT	Belgium	Clinical Trial Systems, Machine2Machine identification and authentication
Irish Centre for Emergency Management	ICEM	Ireland	Emergency Management, Business Continuity
Rhea System	RHEA	Belgium	Cybersecurity software, Cyber range
Rina Consulting	RINA	Italy	Certification, security engineering and education
Sacred Heart Catholic University	UNIVERSITÀ CATTOLICA del Sacro Cuore	Italy	Healthcare management
7th Health Region of Crete		Greece	HCO organisation, processes and technology
Stelar Security Technology Law Research	Stelar	Germany	Regulatory and standardisation framework
Trust-It Services	Trust-IT Services communicating to markets	Italy	Technological communication and marketing
University of Northumbria at Newcastle	Northumbria University NEWCASTLE	UK	Psychology research
University of Rome La Sapienza	SAPIENZA UNIVERSITÀ DI ROMA	Italy	Cybersecurity research, visual analytics

Glossary of Terms

Acronym	Description
CISO	Chief Information Security Officer
C-ROI	Cyber-Return on Investment
CST	Compliance Support Tool
DRMP	Dynamic Risk Management Platform
EHR	Electronic Health Record
GDPR	General Data Protection Regulation
HCO	Healthcare Organisation
HCG-Tool	Healthcare Cybersecurity Governance Tool
HCOS-Model	Healthcare Cybersecurity Organisation Structure Model
ICT	Information and Communication Technologies
IGT	Implementation Guidelines Tool
IMP-H2M	Identity Management Platform – Human to Machine
ISO	International Organisation for Standardisation
ISRP	Information Security Reference Persons
KPI	Key Performance Indicator
LIS	Laboratory Information System
NIST	National Institute of Standards and Technology
OES	Operators of Essential Services
POCT	Point of Care Testing
RGT	Resilience Governance Tool
RGT HCG-Tool	Healthcare Cybersecurity Governance Tool
RGT HCOS-Model	Healthcare Cybersecurity Organisation Structure Model
SbDF	Security by Design Framework (including CST and SDSP)
SBNT	Secure Behaviour Nudging Tool
SDSP	Secure Design Support Platform
SISP	Secure Information Sharing Platform
TECT	Training & Education for Cybersecurity Tool

References

[1] Mohammad S Jalali, MSc, PhD; Jessica P Kaiser, MBA, *Cybersecurity in Hospitals: A Systematic, Organizational Perspective,* Journal of Medical Internet Research.

[2] *Life span of Biomedical Devices,* Biomedical Engineering Advisory Group SA.

[3] International Data Corporation (IDC), *How has COVID-19 Changed Industry ICT and Emerging Technology Investments in Europe?* https://interxion.azureedge.net/cdn/ff/VGlHOVLBzWxnmgxl4REDIx1oj30Ec0FBndmkaDhIpC8/1590664000/public/2020-05/IDC%20Study_3.pdf

[4] WHO, *Global patient safety action plan 2021–2030: towards eliminating avoidable harm in health care.*

[5] ENISA, *From January 2019 to April 2020, Main incidents in the EU and worldwide, ENISA Threat Landscape.*

[6] ENISA, *Smart Hospitals Security and Resilience for Smart Health Service and Infrastructures.*

[7] ENISA, *From January 2019 to April 2020, Sectoral/ thematic threat analysis, ENISA Threat Landscape.*

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[9] ENISA, *Procurement Guidelines for Cybersecurity in Hospitals.*

[10] Directive (EU) 2016/1148 of the European Parliament and of the Council concerning *measures for a high common level of security of network and information systems across the Union.*

[11] ENISA, *Mapping of OES Security Requirements to Specific Sectors.*

[12] *Regulation* (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 *on medical devices*, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC.

[13] *Regulation* (Eu) 2019/881 of the European Parliament and of the Council of *on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation* (EU) No 526/2013 (Cybersecurity Act).

[14] IBM Security and Ponemon Institute, *Cost of a Data Breach Report 2021.*

[15] The CyberPeace Institute, *Playing with Lives: Cyberattacks on Healthcare are Attacks on People.*
https://cyberpeaceinstitute.org/report/teaser/index.html
https://www.wired.co.uk/article/ransomware-hospital-death-germany

[16] German Hospital Hacked, Patient Taken to Another City Die, Associate Press, reported by SECURITYWEEK, https://www.securityweek.com/german-hospital-hacked-patient-taken-another-city-dies (accessed 23 November 2020).

[17] Sophos, *The State of Ransomware 2021.*

[18] Coveware Quarterly Ransomware Report, *Ransomware Demands continue to rise as Data Exfiltration becomes common, and Maze subdues,* https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report (Accessed 18 November 2021).

[19] K.Anastasopoulou et al., *Public and private healthcare organisations: a socio-technical model for identifying cybersecurity aspects.* In Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance (pp. 168-175).

[20] *PANACEA D1.1 Models of health services and of medical device lifecycle for cybersecurity,*
https://www.panacearesearch.eu/sites/default/files/PANACEA_D1.1_Models%20of%20health%20services%20and%20of%20medical%20device%20lifecycle%20for%20cybersecurity%20v1.0_0.pdf

[21] S. Bonomi, *Cyberthreats to Hospitals: Panacea, a Toolkit for People-Centric Cybersecurity*, Journal of Strategic Innovation and Sustainability.

[22] *PANACEA D2.2 Human Factors, Threat Models Analysis and Risk Quantification,* https://www.panacearesearch.eu/sites/default/files/D2.2_Final%20Deliverable_1.pdf

[23] E. G. Spanakis et al., *Emerging and Established Trends to Support Secure Health Information Exchange,* Frontiers in Digital Health.

[24] D. Branley-Bell et al., Your hospital needs you: *Eliciting positive cybersecurity behaviours from healthcare staff.* Annals of Disaster Risk Sciences: ADRS, 3(1), 0-0.

[25] L. Coventry et al. *Cyber-risk in healthcare: Exploring facilitators and barriers to secure behaviour.* In International Conference on Human-Computer Interaction (pp. 105-122). Springer, Cham.

[26] NIST-National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity.*

[27] ISO / IEC 27001 :2017 Information technology. Security techniques. Information security management systems. Requirements.

[28] S. Sfakianakis et al, *PANACEA resilient and secure Toolkit for healthcare infrastructures,* 43rd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC), Oct 31 - Nov 4, 2021. Virtual Conference.

To find out more about adopting the PANACEA tools as standalones or an integrated solution for cybersecurity in healthcare, contact us at:

panacearesearch.eu/contact-us

www.panacearesearch.eu

@H2020Panacea

/in/panacearesearch/

/channel/UC5k4hx6IQiRd0nXNtWK_jMQ

Panacea has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 826293