Cyberthreats to Hospitals: Panacea, a Toolkit for People-Centric Cybersecurity

Sabina Magalini
Catholic University of the Sacred Heart

Daniele Gui
Fondazione Policlinico Gemelli

Pasquale Mari
Catholic University of the Sacred Heart

Matteo Merialdo
Rhea Group

Emanoulis Spanakis
Foundation For Research And Forth Technology Hellas

Vangelis Sakkalis
Foundation For Research And Forth Technology Hellas

Fabio Rizzoni
Fondazione Policlinico Gemelli

Alessandra Casaroli
Fondazione Policlinico Gemelli

Silvia Bonomi
Sapienza University of Rome

Healthcare organizations are an attractive target for cyber-attacks, because the digitization of health processes is emerging as a necessity. Healthcare is a rich source of valuable data and its defences are weak. The particular weakness of this domain is due to the high complexity and dynamism of the healthcare technological environment and to the fact that healthcare working environment has many characteristics that make human behaviour a cybersecurity hazard. Cyberattacks may have significant effects on the provision of health services. Concrete measures strengthening a healthcare setting must take into account number and diversity of hospital basic components and existing security policies. The purpose of this work is to present a cybersecurity toolkit for connected devices and people. Panacea toolkit supports hospitals performing preparedness activities for example: assessment of the nature and severity of a threat, identification of mitigation measures and adoption of mitigation strategies.

Keywords: hospital toolkit for cybersecurity, cybersecurity, hospitals, people-centric approach

INTRODUCTION

Healthcare is increasingly evolving towards digitalization: electronic health records have been developed (and widely adopted), teleconsultation and tele-expertise is thriving, *new technologies (Big data analytics, IoT, AI, High-Performance/Cloud/Mobile Computing, Block-chain)* and use of connected medical devices are on the rise. Nevertheless, many health organizations appear to lack information security measures and awareness, continue to use legacy information systems, or for reasons intrinsic to the application area, such as the large number of internal actors, processes, and interconnected systems, are incapable of reducing risks, vulnerabilities and attacks.

Healthcare organizations are an attractive target for cyber-attacks[1], because healthcare is a rich source of valuable data[2] and its defenses are weak. Key reasons of weakness include:

- *Complexity and dynamism*: 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 more supported legacy systems), digitalization of patient data. Complexity and dynamism are due to increase in the future. Data are going to be more and more exposed on more devices, in more places, to more people. Furthermore, many healthcare organizations are involved in digital transformation roadmaps and Covid-19 pandemic will probably accelerate this trend[3]
- *Human error*: (Branley-Bell, 2020) The healthcare working environment has many characteristics that make human behaviour a cybersecurity hazard and its change problematic. Work culture can lead to security being overlooked or perceived as a burden, particularly if it is perceived to detract from patient care. Working environment is also prone to regular changes to team structure through rotation of staff members and new intakes. Moreover, staff relationship with information systems and medical devices in many cases follows a many-to-one scheme: many staff member of clinical wards and laboratories access the same workstation (or interface), many times, during the day of work. This leads to high risk of poor attention to password management and of unlocked workstations. Other risky behaviours include use of USB devices and sharing of patient information (e.g., using instant messaging applications, like WhatsApp, rather than official systems to avoid having to leave the patient's bedside and emailing patients documents if they are unable to access them via official systems).

(ENISA, 2016) showed that threats based on human errors are perceived to have the highest likelihood of occurrence (4,21 in a scale from 1 to 5) and are rated as the second most "critical" threat in terms of impact on Hospital operations (70% of the respondents said that it is critical).

Poor cybersecurity in the healthcare industry has a high cost: according to a recent survey (Ponemon, 2019), the average cost of a successful cyberattack in the healthcare industry (hospital, clinics) is6.45 US $millions, including data breach detection and escalation, notification, lost business cost, post data breach response.

It is therefore evident that threats and potential damages to healthcare critical infrastructures due to cyberattacks require a fortification of the security features in the industry, for the benefit of the patients, as well as the health business entities and other stakeholders.

PANACEA Project (Protection and privacy of hospital and health infrastructures with smart Cyber security and cyber threat toolkit for data and people) is a three year Horizon 2020 funded research and innovation project, that started in January 2019[4]. It aims at delivering a complete cybersecurity toolkit providing a holistic approach for healthcare organizations, made up of a combination of technical and non-technical elements for a healthcare organization.

PANACEA will address all the aforementioned weaknesses contributing to a "people-centric" vision for cybersecurity in healthcare.

PANACEA Approach

PANACEA project's main objective is to improve the security posture of health care organizations by developing and validating the PANACEA toolkit, composed of nine tools, clustered in two sub-sets:

- *The Solution Toolkit,* used to provide cyber security assessment and preparedness of Healthcare ICT infrastructures and connected devices. It is made up of four technological tools (platforms for dynamic risk assessment and mitigation, secure information sharing, security-by-design and certification, identification and authentication) and of three organisational tools (models, guidelines, methodologies, best practices for training and education, resilience governance, secure behaviours nudging). An overview of the PANACEA Solution Toolkit is shown in Figure 1.

FIGURE 1
PANACEA SOLUTION TOOLKIT

- *The Delivery Toolkit,* used to support the adoption of the solution toolkit. It is made up of two support tools (a methodology to evaluate the ROI of cybersecurity interventions and implementation guidelines to assess the operational context and to customize and field the solution toolkit and other ex-ante mitigation actions).

The full set of PANACEA tools aims to support a healthcare organization in key preparedness activities: vulnerability assessment, identification and adoption of mitigation actions, mitigation through tools

embedding "beyond state-of-art" solutions, tailored on the healthcare specific context. Table 1 below shows which tools supports which activity.

TABLE 1
PANACEA TOOLS SUPPORTING CYBERSECURITY PREPAREDNESS ACTIVITIES

		Preparedness activities			
	Tools	Vulnerability assessment	Identification of mitigation measures	Adoption of mitigation measures	Mitigation
Solution toolkit	Dynamic risk assessment platform	x	x		
	Secure information sharing platform				x
	Security-by-design and certification platform	x	x		x
	Identification and authentication platform				x
	Training and education packages				x
	Resilience governance processes and organization	x	x	x	x
	Secure behaviors nudging initiatives	x	x		x
Delivery toolkit	Return on Investment evaluation method			x	
	Toolkit implementation guidelines			x	

In order to show how the people-centric paradigm is shaping the PANACEA toolkit, in the following section we will provide details about the underlying logic of one of the tools, the PANACEA Dynamic Risk Management Platform (DRMP), which will be a software tool implementing an integrated assessment of human and technical components (information systems, connected medical devices).

Dynamic Risk Management Platform

The PANACEA Dynamic Risk Management Platform (DRMP) constitutes one of the major components of the PANACEA toolkit. Its aim is to proactively protect a complex IT infrastructure (encompassing remote and IoT devices, remote networks, local networks) by analysing the current level of risk and suggesting mitigation actions to decrease the actual risk level with no (or minimum) impact on the healthcare organization business.

To this aim, the risk will be computed by taking inputs from results of a multi-dimensional threat analysis and those of the business impact analysis.

The computation of the risk will trigger the definition of mitigation actions (expressed in terms of a security measures) with the purpose of reducing the level of risk but containing the business impact that the actions themselves may cause.

One of the main innovative features of the DRMP is the ability to consider together both technical (i.e., ICT related) aspects and non-technical (i.e., human driven) aspects. This will enable the identification and proposal of both technical (i.e., precise actions on the IT infrastructure, from patching to architectural/configuration) and non-technical (organisational, procedural) security measures.

This will enable a more accurate security situation assessment by considering multiple dimensions of an attack instead of, for example, being limited to known vulnerabilities affecting the ICT part of the organization.

Once the multi-dimensional attack model is available, it is possible to use it in the monitoring process where new information can even be inferred by correlating multiple heterogeneous pieces of information.

FIGURE 2
PANACEA DRMP OVERVIEW

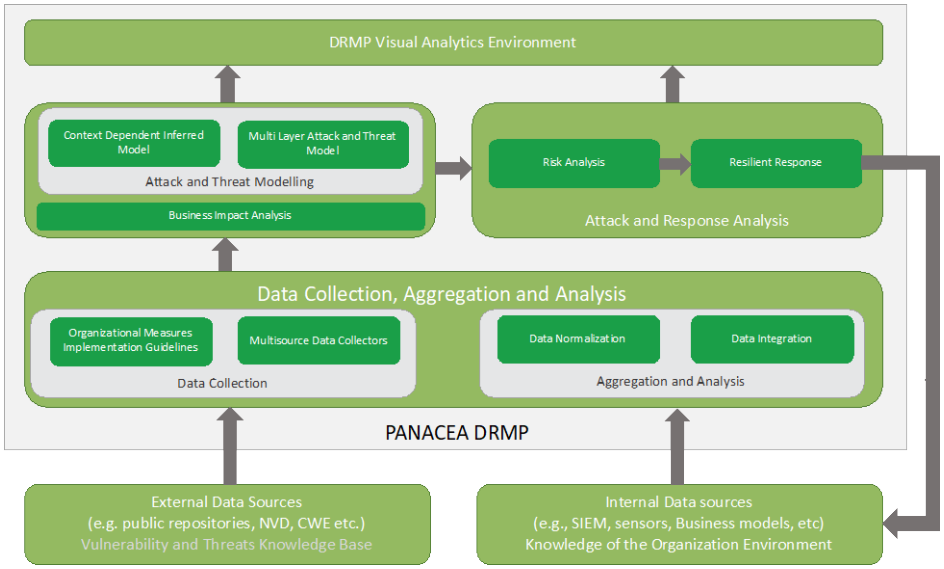

Figure 2 provides an overview over the PANACEA DRMP. The platform will be composed of 4 main functional components interacting with the monitored environment and gathering data from both internal and external data sources (including both its technical and non-technical part). Such macro-components are:

- Data Collection, Aggregation and Analysis,
- Business Impact Analysis,
- Attack and Threat Modeling,
- Attack and Response Analysis,
- Visual Analytics Environment.

The Data Collection, Aggregation and Analysis layer allows the collection, filtering, cleaning and aggregation of data. This is needed to cope with the huge amount of heterogeneous data extracted from internal data sources like network scanners, vulnerability scanners, business process management systems (BPMSs), access control policy list, organizational chart enriched with description of the professional roles and duties, and external data sources like vulnerability and threats repositories e.g., NVD (NIST, 2020), CVE(MITRE, 2020), CVSS (First.org, 2020), CWE(MITRE, 2020).

Once data have been collected, cleaned and normalized in the PANACEA data model, they are pushed up to the modules responsible for the Business Impact Analysis and the Attack and Threat modeling.

The aim of the Business Impact Analysis is to collect all the information related to business processes and to model their interdependencies. This task is fundamental as it is the base for both consequence estimation in the risk evaluation process and impact analysis in the selection of the best set of applicable countermeasures to contain the risk.

Conversely, the Attack and Threat modeling task is the base for the likelihood estimation of emerging risk. The threat model considered in PANACEA is based on the attack graph model(Kaynar, 2017) and

extends it in order to represent multiple layers that an attacker may traverse in order to reach its goal. In particular, our multi-layer attack graph will consider three main layers:

1. Device and Network layer where the ICT part of the organization will be modeled and analyzed.
2. Human layer representing relevant people involved in the organization, their roles and relationships inside the organization.
3. Access layer where we will represent the possible ways in which devices and services may be accessed and from who they can be accessed inside the organization.

This threat model will allow us to take a wider perspective and to consider additional factors that may affect the success likelihood of an attack.

Inside the Attack and Threat modeling there is also another important task to be performed: the *context inference*. The main objective of this task is to analyze business processes dependencies and the multi-layer attack graph structure to infer and rank most sensible targets (in relation to the business processes) and most probable entry points for an attacker. The output of this task will contribute to focus the analysis on critical scenarios first.

The Attack and Response Analysis has the aim to analyze the multi-layer attack graph and the business dependences in order to estimate the two main variables contributing to the risk quantification: (i) likelihood and (ii) consequences. Once the risk is estimated, the Resilient Response Analysis can evaluate the portion of the multi-layer attack graph contributing to the risk and based on that can plan the best set of mitigation actions to be performed to reduce the risk. This task can be performed by taking in to account multiple variables like the cost of the mitigation action (both direct in terms of resources needed to perform the mitigation and indirect in terms of impact on the business), the time needed to become effective and the gain in terms of risk reduction.

All the process described so far is supported by a Visual Analytics Environment having the aim to provide a centralized visual access to all the relevant DRMP pieces of information with the main goal of supporting the user situational awareness.

It will be connected to all the internal DRMP modules gathering data and synchronizing its behavior to relevant events (e.g., detection of a threat). It will be a compound of multiple coordinated views, presenting in an integrated way different facets of the underlying data and will rely on several analytical components that will be used for increasing the visual effectiveness of the different views and for dominating the inherent complexity of the managed data, explicitly supporting the situational awareness phases of perception and comprehension.

RELATED WORK

To the best of our knowledge, currently a comprehensive framework that is able to cover all the aspects addressed by the PANACEA Solution Toolkit does not exist. Existing solutions are just able to support, through independent tools, only a subset of services covered by the PANACEA Solution toolkit.

Focusing the attention on the DRMP, the main related work is represented by the PANOPTESEC proactive architecture presented in (Gustavo Gonzalez Granadillo, 2018). PANOPTESEC (PANOPTESEC Consortium, n.d.) is an FP7 project ended in 2016 whose aim was the design and development of a decision support system to facilitate security operators in protecting a critical infrastructure (specifically an energy and water provider). From the macro-component point of view, the PANACEA architecture looks very similar to the PANOPTESEC one, but its development is conversely very different and allows to model and analyse different aspects not covered in PANOPTESEC like human factors and IoT devices.

In addition, even if both the domain of application can be classified as critical infrastructures, the healthcare domain where PANACEA will be applied offers multiple challenges that requires specific solutions.

CONCLUDING REMARKS

This paper provides an overview of the PANACEA project main objectives: the PANACEA Solution Toolkit and the PANACEA Delivery Toolkit, with particular emphasis on the description of the PANACEA Dynamic Risk Management Platform (DRMP). The main innovation brought from DRMP is its ability to model, analyse and support decisions from a multi-layer perspective that allows to consider together both technical and non-technical factors contributing to risks identification. Particular attention is paid to humans and in particular to their interactions with the ICT component of the organization. This has been done primarily to address the main issues coming from recent surveys revealing that in the healthcare domain, humans represent themselves a vulnerability from the cyber security perspective and needs to be taken in to account in the risk management process not only as a potential vulnerability.

ENDNOTES

1. According to a recent survey (HIMSS, 2019) 82% of the respondent 71 US based hospitals had experienced significant security incidents in the Past 12 Months.
2. Healthcare is targeted due to the potential for financial (the value for a full set of medical credentials can be over $1000) or political gain, or to expose vulnerabilities by cybercriminals, hacktivists and political activists (Conventry, 2018).
3. Covid-19 in Europe has surfaced the weaknesses of the national health services and the need to invest in e-health and tele-health. ICT investments are expected to increase (IDC, 2020).
4. www.panacearesearch.eu

REFERENCES

Branley-Bell D., Coventry L., Sillence E., Magalini S., Mari P., Magkanaraki, A., & Anastasopoulou K. (2020). Your hospital needs you: Eliciting positive cybersecurity behaviours from healthcare staff. *Annals of Disaster Risk Sciences*, *3*(1).

Coventry. (2018). Lynne Coventry, Dawn Branley, (2018) Cybersecurity in healthcare: A narrative review of trends, threats and ways. *Maturitas*, *113*.

ENISA. (2016). *Smart Hospitals Security and Resilience for Smart Health Service and Infrastructure*.

First.org. (2020). *Common Vulnerability Scoring System v3.1.*

Gustavo Gonzalez Granadillo, S.D. (2018). *Dynamic risk management response system to handle cyber threats*. Future Generation Computer Systems.

Kaynar, K. (2017). A taxonomy for attack graph generation and usage in network security. *Journal of Information Security and Applications*, pp. 27–56.

MITRE. (2020). *CVE Home Page. Retrieved from Common Vulnerabilities and Exposure*. Retrieved from https://cve.mitre.org

MITRE. (2020). *CWE Home Page. Retrieved from Common Weakness Enumeration*. Retrieved from https://cwe.mitre.org

NIST. (2020). *National Institute of Standards and Technology - NVD*. Retrieved from https://nvd.nist.gov

PANOPTESEC Consortium. (n.d.). PANOPTESEC Home Page. Retrieved from http://www.panoptesec.eu

Thales. (2017). *Trends in Encryption and Data Security: Data Threat Report-Healthcare edition*.