Panacea
People-centric cybersecurity in healthcare

Project Title	Protection and privAcy of hospital and health iNfrastructures with smArt Cyber sEcurity and cyber threat toolkit for dAta and people
Project Acronym	PANACEA
Project Number	826293
Type of instrument	Research and Innovation Action
Topic	SU-TDS-02-2018
Starting date of Project	01/01/2019
Duration of the project	36
Website	www.panacearesearch.eu

D2.1 ANALYSIS OF CYBER VULNERABILITIES AND SOA COUNTERMEASURES IN HCC

Work Package	WP2 RESEARCH ON ADVANCED THREAT MODELLING, HUMAN FACTORS, RESILIENT RESPONSE AND SECURE INTERCONNECTIVITY
Lead author	Emmanouil Spanakis (FORTH)
Contributors	S. Sfakianakis, V. Sakkalis (FORTH), S. Bonomi, S. Lenti, G. Santucci, M. Sorella, F. Tanasache (UROME), Lynne Coventry (UNAN), Dawn Branley-Bell (UNAN)
Peer reviewers	Matteo Merialdo (RHEA), Ivan Tesfai Ogbu (RINA)
Version	V01
Due Date	31/07/2019
Submission Date	31/07/2019

Dissemination Level: PU

	PU: Public
	CO: Confidential, only for members of the consortium (including the Commission)
	EU-RES. Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)
	EU-CON. Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC)
	EU-SEC. Classified Information: SECRET UE (Commission Decision 2005/444/EC)

The work described in this document has been conducted within the PANACEA project. This project has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement No. 826293.

Version History

Revision	Date	Editor	Comments
0.1	14/6/2019	E. G. Spanakis (FORTH)	Owner/Creator
0.2	16/6/2919	S. Sfakianakis (FORTH)	ToC definition
0.3	20/6/2019	Silvia Bonomi (UROME)	ToC review and finalization
0.41	25/6/2919	E.G. Spanakis, S. Sfakianakis (FORTH)	Update on the overall document
0.42	29/06/2019	S. Lenti, M. Sorella, F, Tanasache (UROME)	Initial contribution on sections 7, 10 and 11
0.51	9/7/2019	Silvia Garbin (AON)	Initial Contribution on section 9
0.52	10/7/2019	S. Bonomi, S. Lenti, G. Santucci, M. Sorella, F, Tanasache (UROME)	Second round of contribution to sections 7, 9, 10 and 11
0.53	25/7/2019	Dawn Branley-Bell (UNAN)	Update on various section and review of the document (sections 4 and 6)
0.6	25/7/2019	Mara Sorella, Silvia Bonomi (UROME)	Update, review and correction on several versions and ToC reformation
0.7	29/7/2019	Lynne Coventry (UNAN)	Update on Human behavioural Modeling
0.8	29/7/2019	Silvia Garbin (AON)	Update on section 9
0.9	30/7/2019	M. Matteo (RHEA), I.T. Ogbu (RINA)	Peer Review and Quality approval to release
1.0	31/7/2019	E.G.Spanakis, S. Sfakianakis, V. Sakkalis (FORTH)	Final Review and release

List of Contributors

The list of contributors to this deliverable are presented in the following table:

Section	Author(s)
Executive Summary	S. Sfakianakis, E.G.Spanakis, V. Sakkalis
Introduction	S. Sfakianakis, E.G.Spanakis, V. Sakkalis, Dawn Branley-Bell
Panacea Project Description	E. G. Spanakis, S. Sfakianakis, V. Sakkalis
Review Methodology	S. Sfakianakis, S. Bonomi, E.G.Spanakis
Cyber security in HealthCare	E. G. Spanakis, S. Sfakianakis, Mara Sorella, S. Bonomi
Vulnerability and threat modelling	E. G. Spanakis, S. Sfakianakis, V. Sakkalis, F. Tanasache
Human Behavioural Modeling	Lynne Coventry
Risk Quantification and Governance	Silvia Garbin, E.G.Spanakis, S. Bonomi
Attack response: Hardening approaches	M. Sorella
Visual Analytics for increasing situational awareness	S. Lenti, G. Santucci
Discussion and relation of finding to PANACEA research	S. Bonomi
Conclusion	S. Sfakianakis, E.G.Spanakis, V. Sakkalis

Keywords

HEALTH SERVICES VULNERABILITIES, CYBER-RISK SCENARIOS, CURRENT COUNTERMEASURES, CYBER ATTACKS, COUNTERMEASURES, HEALTH CARE DOMAIN, INTERNET OF THINGS, INTERNET MEDICAL THINGS

Disclaimer

Executive Summary

Healthcare is increasingly evolving towards digitalisation: electronic health records have been developed (and widely adopted), teleconsultation and tele-expertise is thriving, and use of connected HC devices is 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.

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. The Health IT domain has the amounts to the “lion’s share” in terms of the security related incidents and the impact caused, and therefore cybersecurity solutions need to be in place for the benefit of the patients, as well as the health business entities and other stakeholders.

PANACEA aims to demonstrate that security stems from awareness of cyber vulnerabilities - enabling healthcare facilities to assess the nature and severity of a threat, and sustainably decide to adopt strategies to strengthen preparedness and incident response. PANACEA aims to deliver a complete cybersecurity toolkit providing a holistic approach for Health Care Institutions made up of a combination of technical (SW platforms for dynamic risk assessment, dynamic risk management, secure information sharing & security-by-design) and non-technical (procedures, governance models, people behaviour tools) elements for a healthcare organization. The expertise is available in the consortium as a whole to deliver the tools, methodologies, workflows, and training to address the cybersecurity related challenges in the healthcare domain.

Consequently, this document aims to provide an overview of the state of the art in terms of cyber risk scenarios, current countermeasures and vulnerability assessment methodologies with a particular emphasis on the healthcare domain but also considering more general approaches that leave the floor open for their application in such challenging environment. The document contains a detailed overview of the actual situation, in terms of common vulnerabilities, possible relevant cyber-attack scenarios and related countermeasures, for the Health Care domain. Such analysis of the specific cyber risks in the context of the delivery of health and the identification of the domain-specific requirements are important for the adaptation and optimization of the PANACEA approach in healthcare. In addition, the current document includes a scientific and technological review of all the relevant aspects related to the design and implementation of a Dynamic Risk Management Platform (e.g., existing threat and attack models, risk identification and mitigation methodologies, etc.). Finally, the review presented in document tries to highlight the main challenges and research gaps currently existing in the healthcare domain but, for the sake of completeness, it also presents relevant results presented and discussed without specific reference to an application domain. This will help the PANACEA consortium to identify the most relevant state of the art approaches and to apply or extend them in the healthcare domain fighting challenges imposed by this extremely complex domain.

The structure of the main text of the document is as follows:

- Section 6 lays the ground presenting the specificities of the healthcare domain in terms of its demanding requirements for cybersecurity. Specificities of the domain are explained, alongside with statistical data and prior publications that reinforce the need for more cybersecurity awareness to be in place. We also present a number of risks, cyber threats, and scenarios and the current security approaches and countermeasures.

- In Section 7 we delve into the state of the art vulnerability and threat modelling approaches. Existing attack libraries, vulnerability assessment methodologies, and risk analysis methods are presented and we comment on their applicability in the healthcare domain.
- The Healthcare ecosystem consists of large cooperating organizations where people of different roles and responsibilities communicate and interact with each other. Therefore, in Section 8 the human component of the cyber security is studied and details of the human behavioural modelling and relevant theories and models of behaviour change are presented.
- In Section 9 business impact analysis, risk quantification and risk assessment concepts are introduced. Identification of the assets and their assessment, the potential threats, and their countermeasures are all tasks to be considered especially in the health domain where the patients’ safety could be at risk.
- The network hardening and other attack responses are the subject of Section 10, and the different, graph-based and optimization based methods are detailed.
- Visual analytics are demonstrated in Section 11 to easily identify network threats and gain important knowledge about their nature.
- Finally in Section 12 we provide a discussion and conclusions of the deliverable.

Table of Contents

List of figures

List of tables

1. Introduction

This deliverable reports the outcome of Task 2.1 - Health Services vulnerabilities, cyber-risk scenarios and current countermeasures included in Work Package 2 - Research on advanced threat modelling, human factors, resilient response and secure interconnectivity. This task performed a methodological review and analysis of the state of the art of cyber risk scenarios, current countermeasures and vulnerability assessment methodologies in the Healthcare (HC) domain. In addition, it provides a scientific and technological review of all aspects related to the design and implementation of a Dynamic Risk management platform (e.g., existing threat and attack models, risk identification and mitigation methodologies, etc.).

1.1 Purpose

This document provides a review and analysis of the state of the art in terms of cyber risk scenarios, current countermeasures and vulnerability assessment methodologies in the HC domain. In addition, it includes a scientific and technological review of all the relevant aspects related to the design and implementation of a Dynamic Risk management platform (e.g., existing threat and attack models, risk identification and mitigation methodologies, etc.). The document contains a detailed overview of the actual situation, in terms of common vulnerabilities, possible relevant cyber-attack scenarios and related countermeasures, for the HC domain.

1.2 Quality assurance

1.2.1 Quality criteria

The Quality Assurance (QA) in the PANACEA project relies on the assessment of a work product (i.e. deliverable) according to a lists of QA checks established with the Quality Assurance Manager (QAM) - RINA, validated at a project management level and centralized in the Project Management Plan (PMP).

For the purpose of the QA of this deliverable, it has been assessed according the following checklists:

- PEER REVIEW (PR) QA checklist: this deliverable is a report, it then requires a proper peer review according to the checks defined in this checklist. The reviewers have been identified by the QAM following the criteria of independence of evaluation (partners not contributing to the document and task) and robustness in terms of completeness of information, continuity and relevance of the current outcomes with the main related tasks. The peer reviewers identified are:
    - RHEA
    - RINA

1.2.2 Validation process

For the final validation of work products (i.e. deliverables) within the PANACEA project, a final QA review process MUST be applied before the final version is issued. This QA validation process follows the Quality Review Procedure established with the QAM and validated at project management level in order to guarantee the high quality level of work products and to validate its adequacy according to the defined quality criteria chosen and defined for each deliverable. The Quality Review Procedure itself and the selection of the QA Review Committee are described in the [PMP]. The QA validation process is scheduled in the QA Schedule [QASchedule] managed by the QAM.

1.3 Structure of the document

The structure of the document can be found below:

CHAPTER 1:	Introduction
CHAPTER 2:	Applicable and Reference Documents
CHAPTER 3:	Glossary of Acronyms
CHAPTER 4:	PANACEA project description
CHAPTER 5:	Review Methodology
CHAPTER 6:	Cyber security in HealthCare: scenarios and perspectives
CHAPTER 7:	Vulnerability and threat modelling
CHAPTER 8:	Human Behavioural modelling
CHAPTER 9:	Risk Quantification and Governance
CHAPTER 10:	Attack response: Hardening approaches
CHAPTER 11:	Visual Analytics for increasing situational awareness
CHAPTER 12:	Discussion and relation of finding to PANACEA research
CHAPTER 13:	Conclusion – deliverable concluding remarks

2. Applicable and Reference Documents

2.1 Applicable Documents (ADs)

The following documents contain requirements applicable to the generation of this document:

Reference	Document Title	Document Reference	Version	Date
[PMP]	PANACEA Project Manager Plan		0.5	01/01/2019
[QAPeer]	PANACEA Peer Review QA Checklist		0.5	01/01/2019
[QAReqs]	PANACEA Requirements Review QA Checklist		0.5	01/01/2019
[QASchedule]	PANACEA QA Schedule		0.5	01/01/2019

Table 1: Applicable Documents

2.2 Reference Documents (RDs)

The following documents have been consulted for the generation of this document:

Reference	Authors	Document Title	Document Reference	Version	Date
[Adebayo19]	Adebayo Omotosho, Benjamin Ayemlo Haruna & Olayemi Mikail Olaniyi	Threat Modeling of Internet of Things Health Devices, Journal of Applied Security Research	https://www.tandfonline.com/doi/abs/10.1080/19361610.2019.1545278?af=R&journalCode=wasr20		2019
[Ahmed18]	Ahmed, A., Latif, R., Latif, S	Malicious insiders attack in IoT based Multi-Cloud e-Healthcare environment:A Systematic Literature Review	https://link.springer.com/article/10.1007/s11042-017-5540-x		2018
[Ajzen91]	Ajzen, I	The theory of planned behavior. Organizational Behavior and Human Decision Processes	http://doi.org/10.1016/0749-5978(91)90020-T		1991
[Ajzen02]	Ajzen, I	Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior	http://doi.org/10.1111/j.1559-1816.2002.tb00236.x		2002
[Alberts03]	C. Alberts, A. Dorofee, J. Stevens and C. Woody	Introduction to the OCTAVE Approach	https://www.itgovernance.co.uk/files/Octave.pdf		2003

[Alberts99]	C. J. Alberts, S. G. Behrens, R. D. Pethia and W. R. Wilson	Operationally Critical Threat, Asset, and Vulnerability Evaluation SM (OCTAVESM) Framework, Version 1.0	https://resources.sei.cmu.edu/asset_files/TechnicalReport/1999_005_001_16769.pdf	1999
[Albrechtsen07]	Albrechtsen, E.	A qualitative study of users’ view on information security.	http://doi.org/10.1016/j.cose.2006.11.004	2007
[AlEroud17]	Ahmed AlEroud, George Karabatis	Using Contextual Information to Identify Cyber-Attacks	https://doi.org/10.1007/978-3-319-44257-0_1	2017
[Alhassan16]	J. K. Alhassan, E. Abba, O. M. Olaniyi and V. O. Waziri	Threat Modeling of Electronic Health Systems and Mitigating Countermeasures	http://ceur-ws.org/Vol-1830/Paper16.pdf	2016
[Almulhen11]	A. Almulhem	Threat Modeling for Electronic Health Record Systems	https://doi.org/10.1007/s10916-011-9770-6	2011
[Alsaleh13]	Mansour Alsaleh, Abdullah Alqahtani, Abdulrahman Alarifi, AbdulMalik Al-Salman	Visualizing PHPIDS Log Files for Better Understanding of Web Server Attacks	https://doi.org/10.1145/2517957.2517958	2013
[Ammann02]	P. Ammann, D. Wijesekara, S. Kaushik:	Scalable, graph-based network vulnerability analysis.	https://doi.org/10.1145/586110.586140	2002
[Ammann05]	P. Ammann, J. Pamula, J. A. Street, R. W. Ritchey	A host-based approach to network attack chaining analysis	https://doi.org/10.1109/CSAC.2005.6	2005
[Anderson10]	Anderson, C., & Agarwal, R.	Practicing safe computing: a multimethod empirical examination of home computer user security behavioural intentions.	https://dl.acm.org/citation.cfm?id=2017481	2010
[Angelini18]	Marco Angelini, Graziano Blasilli, Tiziana Catarci, Simone Lenti, Giuseppe Santucci	Vulnus: Visual Vulnerability Analysis for Network Security	https://doi.org/10.1109/TVCG.2018.2865028	2018
[Angelini19]	Marco Angelini, Silvia Bonomi, Simone Lenti, Giuseppe	MAD: A visual analytics solution for Multi-step cyber Attacks Detection	https://doi.org/10.1016/j.cola.2018.12.007	2019

	Santucci, Stefano Taggi			
[Arendt15]	Dustin Arendt, Russ Burtner, Daniel Best, Nathan Bos, John Gersh, Christine Piatko, Celeste Lyn Paul	Ocelot: user-centered design of a decision support visualization for network quarantine	https://doi.org/10.1109/VIZSEC.2015.7312763	2015
[Armitage01]	Armitage, C. J., & Conner, M.	Efficacy of the Theory of Planned Behaviour: A meta-analytic review.	http://doi.org/10.1348/014466601164939	2001
[Artz02]	Michael L. Artz	NetSPA : a Network Security Planning Architecture	http://hdl.handle.net/1721.1/29899	2002
[Argaw19]	Argaw, S. T., Bempong, N. E., Eshaya-Chauvin, B., & Flahault, A.	The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review.	https://bmcmedinformdecismak.biomedcentral.com/articles/10.1186/s12911-018-0724-5	2019
[Aurigemma14]	Aurigemma, S., & Mattson, T.	Do it OR ELSE! Exploring the Effectiveness of Deterrence on Employee Compliance with Information Security Policies.	https://pdfs.semanticscholar.org/4833/d4401020bab8ac2471c2209f656f3a664f31.pdf	2014
[Babiceanu16]	Radu F. Babiceanu, Remzi Seker	Big Data and virtualization for manufacturing cyber-physical systems: A survey of the current status and future outlook	https://doi.org/10.1016/j.compind.2016.02.004	2016
[Barnum14]	S. Barnum	Standardizing Cyber Threat Intelligence Information wit the Structured Threat Information eXpression (STIX)	https://stixproject.github.io/about/STIX_Whitepaper_v1.1.pdf	2014
[Bartsch12]	Bartsch, S., & Sasse, A. M.	How Users Bypass Access Control - And Why: The Impact Of Authorization Problems On Individuals And The Organization.	http://discovery.ucl.ac.uk/id/eprint/1389948	2012

[Beautement09]	Beautement, M., Sasse, A, & Wonham, M.	The compliance budget: Managing security behaviour in organisations.	10.1145/1595676.1595684	2009
[Beyst16]	B. Beyst	Which Threat Modeling Method	https://threatmodeler.com/2016/04/15/threat-modeling-methodology/	2016
[Biersack12]	Ernst Biersack; Quentin Jacquemart; Fabian Fischer; Johannes Fuchs; Olivier Thonnard; Georgios Theodoridis; Dimitrios Tzovaras; Pierre-Antoine Vervier	Visual analytics for BGP monitoring and prefix hijacking identification	https://doi.org/10.1109/MNET.2012.6375891	2012
[Boschetti11]	Alberto Boschetti, Luca Salgarelli, Chris Muelder, Kwan-Liu Ma	TVi: a visual querying system for network monitoring and anomaly detection	https://doi.org/10.1145/2016904.2016905	2011
[BouHarb13]	Elias Bou-Harb, Mourad Debbabi, Chadi Assi	Cyber scanning: A comprehensive survey	https://doi.org/10.1109/SURV.2013.102913.00020	2013
[Bui13]	Bui, L., Mullan, B., & McCaffery, K.	Protection motivation theory and physical activity in the general population: A systematic literature review.	http://doi.org/13548506.2012.749354	2013
[Bulgurcu10]	Bulgurcu, B., Cavusoglu, H., &Benbasat, I.	Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness.	https://misq.org/catalog/product/view/id/1393	2010
[Burns13]	Burns, S., & Roberts, L.	Applying the Theory of Planned Behaviour to predicting online safety behaviour.	http://doi.org/10.1057/cpcs.2012.13	2013
[Burns16]	A.J. Burns, M.E. Johnson, P. Honeyman	A brief chronology of medical device security	http://dx.doi.org/10.1145/2890488	2016
[Cagnazzo18]	M. Cagnazzo, M. Hertlein, T. Holz and N. Pohlmann	Threat modeling for mobile health systems	https://doi.org/10.1109/WCNCW.2018.8369033	2018

[Campbell]	Jamonn Campbell, Nathan Greenauer, Kristin Macaluso, Christian End,	Unrealistic optimism in internet events	https://doi.org/10.1016/j.chb.2004.12.005.	2007
[CAPEC]	CAPEC Community	CAPEC Website	https://capec.mitre.org/index.html	2019
[Cappers15]	Bram C.M. Cappers, Jarke J. van Wijk	SNAPS: Semantic network traffic analysis through projection and selection	https://doi.org/10.1109/VIZSEC.2015.7312768	2015
[Cappers18]	Bram Cappers, Paulus N. Meessen, Sandro Etalle, Jarke van Wijk	Eventpad: Rapid Malware Analysis and Reverse Engineering using Visual Analytics	https://doi.org/10.1109/VIZSEC.2018.8709230	2018
[Chen07]	Y. Chen, B. Boehm and L. Sheppard	Value Driven Security Threat Modeling Based on Attack Path Analysis	https://doi.org/10.1109/HICSS.2007.601	2007
[Chen08]	F. Chen, L. Wang, J. Su	A Heuristic Approach to Minimum-Cost Network Hardening Using Attack Graph	https://doi.org/10.1109/IAS.2008.38	2008
[Chen14]	Siming Chen, Cong Guo, Xiaoru Yuan, Fabian Merkle, Hanna Schaefer, Thomas Ertl	OCEANS: Online Collaborative Explorative Analysis on Network Security	https://doi.org/10.1145/2671491.2671493	2014
[Chen16]	I. Chen, J. Guo and F. Bao	Trust Management for SOA-Based IoT and Its Application to Service Composition	https://ieeexplore.ieee.org/document/6940301	2016
[Chen18]	Siming Chen, Shuai Chen, Natalia Andrienko, Gennady Andrienko, Phong H. Nguyen, Cagatay Turkay, Olivier Thonnard, Xiaoru Yuan	User Behavior Map: Visual Exploration for Cyber Security Session Data	https://doi.org/10.1109/VIZSEC.2018.8709223	2018
[Cheng13]	Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q.	Understanding the violation of IS security policy in organizations: An integrated model	http://doi.org/10.1016/j.cose.2013.09.009	2013

		based on social control and deterrence theory.		
[Cheng14]	Cheng, L., Li, W., Zhai, Q., & Smyth, R.	Understanding personal use of the Internet at work: An integrated model of neutralization techniques and general deterrence theory.	http://doi.org/10.1016/j.chb.2014.05.043	2014
[Cheng17]	P. Cheng, L. Wang, S. Jajodia, and A. Singhal	Refining CVSS-Based Network Security Metrics by Examining the Base Scores	https://link.springer.com/chapter/10.1007/978-3-319-66505-4_2	2017
[Chenoweth09]	Chenoweth, T., Minch, R., & Gattiker, T.	Application of protection motivation theory to adoption of protective technologies.	http://doi.org/10.1109/hicss.2009.74	2009
[Cherdantseva16]	Yulia Cherdantseva, Pete Burnap, Andrew Blyth, Peter Eden, Kevin Jones, Hugh Soulsby, Kristan Stoddart	A review of cyber security risk assessment methods for scada systems	https://www.sciencedirect.com/science/article/pii/S0167404815001388	2016
[Choi09]	Hyunsang Choi, Heejo Lee, Hyogon Kim	Fast detection and visualization of network attacks on parallel coordinates	https://doi.org/10.1016/j.cose.2008.12.003	2009
[Chu10]	Matthew Chu, Kyle Ingols, Richard Lippmann, Seth Webster, Stephen Boyer	Visualizing attack graphs, reachability, and trust relationships with NAVIGATOR	https://doi.org/10.1145/1850795.1850798	2010
[Claar10]	Claar, C., & Johnson, J.	Analysing the adoption of computer security utilizing the health belief model.	http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.473.5178&rep=rep1&type=pdf	2010
[Cleland-Huang14]	J. Cleland-Huang	How Well Do You Know Your Personae Non Gratae?	https://doi.org/10.1109/MS.2014.85	2014
[Cocioceanu18]	Cocioceanu, A. N., Raportaru, M.C., Spanakis, E.G., Markopoulos, Y., & Nicolin, A. I.	An Assessment Framework for Voice-Based Biometrics		2018

[Connolly12]	J. Connolly, M. Davidson, M. Richard and C. Skorupka	The Trusted Automated eXchange of Indicator Information (TAXII)	http://taxii.mitre.org/about/documents/Introduction_to_TAXII_White_Paper_November_2012.pdf	2012
[Corchado11]	Emilio Corchado, Alvaro Herrero	Neural visualization of network traffic data for intrusion detection	https://doi.org/10.1016/j.asoc.2010.07.002	2011
[Coventry14]	Coventry, L., Briggs, P., Blythe, J. M., & Tran, M.	Using behavioural insights to improve the public’ s use of cyber security best practices.	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/309652/14835-cyber-security-behavioural-insights.pdf	2014
[Coventry18]	L. Coventry and D. Branley	Cybersecurity in healthcare: A narrative review of trends, threats and ways forward	https://doi.org/10.1016/j.maturitas.2018.04.008	2018
[Crossler10]	Crossler, R. E.	Protection motivation theory: Understanding determinants to backing up personal data.	10.1109/HICSS.2010.311	2010
[Crossler14a]	Crossler, R. E., & Bélanger, F.	An Extended Perspective on Individual Security Behaviors: Protection Motivation Theory and a Unified Security Practices (USP) Instrument.	http://doi.org/10.1145/2691517.2691521	2014
[Crossler14b]	Crossler, R. E., Long, J. H., Loraas, T. M., & Trinkle, B. S.	Understanding Compliance with Bring Your Own Device Policies Utilizing Protection Motivation Theory Bridging the Intention-Behavior Gap.	http://doi.org/10.2308/isys-50704	2014
[CVE]	CVE Community	CVE Website	https://cve.mitre.org/	2019
[CWE]	CWE Community	CWE Website	https://cwe.mitre.org/	2019
[DAmico15]	Anita D'Amico, Michael Kocka	Information Assurance Visualizations for Specific Stages of Situational Awareness and Intended Uses: Lessons Learned	https://doi.org/10.1109/VIZSEC.2005.1532072	2005

[Darcy07]	D’Arcy, J., & Hovav, A.	Deterring internal information systems misuse	10.1145/1290958.1290971	2007
[Darcy09]	D'Arcy, J., Hovav, A., & Galletta, D.	User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach.	https://search.proquest.com/docview/208155167?accountid=12860	2009
[Darcy11]	D'arcy, J., & Herath, T.	A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings.	https://doi.org/10.1057/ejis.2011.23	2011
[Darcy12]	D'Arcy, J. & Devaraj, S.	Employee Misuse of Information Technology Resources: Testing a Contemporary Deterrence Model.	https://doi.org/10.1111/j.1540-5915.2012.00383.x	2012
[Davis89]	Davis, F. D., Bagozzi, R. P., & Warshaw, P. R.	User acceptance of computer technology: a comparison of two theoretical models.	https://www.jstor.org/stable/2632151	1989
[Davinson10]	Davinson, N., & Sillence, E.	It won’t happen to me: Promoting secure behaviour among internet users	https://doi.org/10.1016/j.chb.2010.06.023	2010
[Davinson14]	Davinson, N., & Sillence, E.	Using the health belief model to explore users’ perceptions of “being safe and secure” in the world of technology mediated financial transactions.	http://doi.org/10.1016/j.ijhcs.2013.10.003	2014
[Deng11]	M. Deng, K. Wuyts, R. Scandariato, B. Preneel and W. Joosen	A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements	https://doi.org/10.1007/s00766-010-0115-7	2011
[Denning13]	T. A. Denning, B. Friedman and T. H. Kohno	Security Cards: A security threat brainstorming toolkit	http://securitycards.cs.washington.edu/index.html	2013
[Deursen14]	N. van Deursen	HI-risk: a socio-technical method for the identification and monitoring of healthcare information security risks in the information society	https://www.napier.ac.uk/~/media/worktribe/output-181044/vandeursenpdf.pdf	2014

[Dewri07]	R. Dewri, N. Poolsappasit, I. Ray, and D. Whitley	Optimal security hardening using multi-objective optimization on attack tree models of networks	https://doi.org/10.1145/1315245.1315272	2007
[Dillon96].	Dillon, A., & Morris, M	User acceptance of information technology: Theories and models.		1996
[Dhillon01]	Dhillon, G., & Moores, S.	Computer crimes: theorizing about the enemy within.	http://doi.org/10.1016/S0167-4048(01)00813-6	2001
[Dhillon96]	Dillon, A., & Morris, M.	User acceptance of information technology: Theories and models.	http://hdl.handle.net/10150/105584	1996
[Dinev07]	Dinev, T., & Hu, Q.	The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies.	https://aisel.aisnet.org/jais/vol8/iss7/23	2007
[Doynikova17]	E. Doynikova, A. Chechulin and I. Kotenko	Analytical attack modeling and security assessment based on the common vulnerability scoring system	https://doi.org/10.23919/FRUCT.2017.8071292	2017
[Emirkanian16]	Mickael Emirkanian-Bouchard, Lingyu Wang	Towards Metric-Driven, Application-Specific Visualization of Attack Graphs	https://doi.org/10.1007/978-3-319-51966-1_8	2016
[Endlsey95]	Mica R. Endlsey	Toward a Theory of Situation Awareness in Dynamic Systems	https://doi.org/10.1518/001872095779049543	1995
[Etges18]	Etges, A.P.B. da S., Grenon, V., Lu, M., Cardoso, R.B., de Souza, J.S., Kliemann Neto, F.J., Felix, E.A.	Development of an enterprise risk inventory for healthcare	https://doi.org/10.1186/s12913-018-3400-7	2018
[Evesti17]	Antti Evesti, Teemu Kanstrén, Tapio Frantti	Cybersecurity Situational Awareness Taxonomy	https://doi.org/10.1109/CyberSA.2017.8073386	2017

[Filkins16]	Filkins, B. L., Kim, J. Y., Roberts, B., Armstrong, W., Miller, M. A., Hultner, M. L., … Steinhubl, S. R	Privacy and security in the era of digital health: what should translational researchers know and do about it?	https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4859641/	2016
[FIRST07]	Forum of Incident Response and Security Teams	A Complete Guide to the Common Vulnerability Scoring System Version 2.0	https://www.first.org/cvss/v2/cvss-v2-guide.pdf	2007
[FIRST18]	Forum of Incident Response and Security Teams	Common Vulnerability Scoring System v3.0: Specification Document	https://www.first.org/cvss/specification-document	2018
[Fishbein75]	Fishbein, M., & Ajzen, I. (1975).	Belief, attitude, intention, and behavior: An introduction to theory and research.	https://philarchive.org/archive/FISBAI	1975
[Fischer08]	Fabian Fischer, Florian Mansmann, Daniel A. Keim, Stephan Pietzko, Marcel Waldvogel	Large-Scale Network Monitoring for Visual Analysis of Attacks	https://doi.org/10.1007/978-3-540-85933-8_11	2008
[Fischer14]	Fabian Fischer, James Davey, Johannes Fuchs, Olivier Thonnard, Jörn Kohlhammer, Daniel A. Keim	A Visual Analytics Field Experiment to Evaluate Alternative Visualizations for Cyber Security Applications	http://dx.doi.org/10.2312/eurova.20141144	2014
[Fischer16]	Fabian Fischer	Visual Analytics for Situational Awareness in Cyber Security	https://kops.uni-konstanz.de/handle/123456789/36392	2016
[Floyd00]	Floyd, D., Prentice-Dunn, S., & Rogers, R.	A meta-analysis of research on protection motivation theory.	http://doi.org/10.1111/j.1559-1816.2000.tb02323.x	2000
[Forget08]	Forget, A.	Helping users create and remember more secure text passwords.	https://www.bcs.org/upload/pdf/ewic_hc08_v2_paper72.pdf	2008
[Fowler14]	J. Joseph Fowler, Thienne Johnson, Paolo Simonetto, Michael Schneider, Carlos	IMap: visualizing network activity over internet maps	https://doi.org/10.1145/2671491.2671501	2014

	Acedo, Stephen Kobourov, Loukas Lazos			
[Franke14]	Ulrik Franke, Joel Brynielsson	Cyber Situational Awareness – A Systematic Review of the Literature	https://doi.org/10.1016/J.COSE.2014.06.008	2014
[Frigault02]	M. Frigault, L. Wang, S. Jajodia, and A. Singhal	Measuring the Overall Network Security by Combining CVSS Scores Based on Attack Graphs and Bayesian Networks	https://link.springer.com/chapter/10.1007/978-3-319-66505-4_1	2002
[Furnell14]	Furnell, S., & Moore, L.	Security literacy: The missing link in today’s online society?	http://doi.org/10.1016/S13613723(14)70491-9	2014
[Gibbs75]	Gibbs, Jack P.	Crime, Punishment and Deterrence,	physical	1975
[Gove14]	Robert Gove, Joshua Saxe, Sigfried Gold, Alex Long, Giacomo Bergamo	SEEM: a scalable visualization for comparing multiple large sets of attributes for malware analysis	https://doi.org/10.1145/2671491.2671496	2014
[Grant09]	Grant, Maria J., and Andrew Booth.	A typology of reviews: an analysis of 14 review types and associated methodologies	http://dx.doi.org/10.1111/j.1471-1842.2009.00848.x	2009
[Greene10]	Greene, G., & D'Arcy, J.	Assessing the impact of security culture and the employee-organization relationship on IS security compliance.	https://pdfs.semanticscholar.org/b668/9ec392605cdafde46d304bdefbf0d92aa773.pdf	2010
[Gurung09]	Gurung, A., Luo, X., & Liao, Q.	Consumer motivations in taking action against spyware: an empirical investigation. Information	http://doi.org/10.1108/09685220910978112	2009
[Hagger02]	Hagger, M. S., Chatzisarantis, N. L. D., & Biddle, S. J.	A meta-analytic review of the theories of reasoned action and planned behavior in physical activity: Predictive validity and the contribution of additional variables	http://psycnet.apa.org/psycinfo/2002-12499-001	2002
[Han14]	KyoungSoo Han, BooJoong Kang, Eul G. Im	Malware Analysis Using Visualized Image Matrices	http://dx.doi.org/10.1155/2014/132713	2014

[Harrington06]	Harrington, S., Anderson, C., & Agarwal, R.	Practicing Safe Computing: Message Framing, Self-View, and Home Computer User Security Behavior Intentions.	https://aisel.aisnet.org/icis2006/93	2006
[Haselhorst17]	D. Haselhorst	HL7 Data Interfaces in Medical Environments: Understanding the Fundamental Flaw in Healthcare	https://www.sans.org/reading-room/whitepapers/vpns/hl7-data-interfaces-medical-environments-understanding-fundamental-flaw-healthcare-38005	2017
[Herath09a]	Herath, T., & Rao, H. R.	Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness.	http://doi.org/10.1016/j.dss.2009.02.005	2009
[Herath09b] (	Herath, T., & Rao, H. R.	Protection motivation and deterrence: a framework for security policy compliance in organisations.	http://doi.org/10.1057/ejis.2009.6	2009
[Herath14]	Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R.	Security services as coping mechanisms: An investigation into user intention to adopt an email authentication service.	http://doi.org/10.1111/j.1365-2575.2012.00420.x	2014
[Herrero09]	Alvaro Herrero, Emilio Corchado, María A. Pellicer, Ajith Abraham	MOVIH-IDS: A Mobile-visualization Hybrid Intrusion Detection System	https://doi.org/10.1016/j.neucom.2008.12.033	2009
[Homer08]	John Homer, Ashok Varikuti, Xinming Ou, Miles A. McQueen	Improving Attack Graph Visualization through Data Reduction and Attack Grouping	https://doi.org/10.1007/978-3-540-85933-8_7	2008
[Humaidi13]	Humaidi N, Balakrishnan V	Exploratory Factor Analysis of User’s Compliance Behaviour towards Health Information System’s Security.	https://doi.org/10.4172/2157-7420.1000123	2013

[Ifinedo12]	Ifinedo, P.	Understanding information systems security policy compliance: An integration of the theory of planned behaviour and the protection motivation theory.	https://doi.org/10.1016/j.cose.2011.10.007	2012
[Ifinedo14]	Ifinedo, P.	Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition.	http://doi.org/10.1016/j.im.2013.10.001	2014
[Ingols06]	K. Ingols, R. Lippmann and K. Piwowarski	Practical attack graph generation for network defense	https://doi.org/10.1109/ACSAC.2006.39	2006
[Inoue12]	Daisuke Inoue, Masashi Eto, Koei Suzuki, Mio Suzuki, Koji Nakao	DAEDALUS-VIZ: novel real-time 3D visualization for darknet monitoring-based alert system	https://doi.org/10.1145/2379690.2379700	2012
[Ion15]	Ion, I., Reeder, R., & Consolvo, S.	“... no one can hack my mind”: Comparing Expert and Non-Expert Security Practices.	https://dl.acm.org/citation.cfm?id=3235893	2015
[Jackle16]	Dominik Jäckle, Fabian Fischer, Tobias Schreck, Daniel A. Keim	Temporal MDS Plots for Analysis of Multivariate Data	https://doi.org/10.1109/TVCG.2015.2467553	2016
[Jajodia02]	S. Jajodia, S. Noel	Topological vulnerability analysis	https://doi.org/10.1007/978-1-4419-0140-8_7	2002
[Jajodia12]	Sushil Jajodia, Steven Noel, Pramod Kalapa, Massimiliano Albanese, John Williams	Cauldron mission-centric cyber situational awareness with defense in depth	https://doi.org/10.1109/MILCOM.2011.6127490	2011
[Jha02]	S. Jha, O. Sheyner, and J. Wing	Two formal analyses of attack graphs	https://dl.acm.org/citation.cfm?id=795177	2002
[Johnston10]	Johnston, B. A. C., &Warkentin, M.	Fear appeals and information security behaviors: An empirical study.	https://www.usenix.org/conference/soups2015/proceedings/presentation/ion	2010

[Jun-chun12]	Ma Jun-chun and Sun Ji-yin	Optimal network hardening model based on parallel genetic algorithm	https://ieeexplore.ieee.org/document/6322439	2012
[Jung01]	Jung, Bumsuk, Ingoo Han, and Sangjae Lee	Security threats to Internet: a Korean multi-industry investigation	https://www.sciencedirect.com/science/article/pii/S0378720601000714	2001
[Kumar08]	Kumar, N., Mohan, K., & Holowczak, R.	Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls.	http://doi.org/10.1016/j.dss.2008.06.010	2008
[ISE16]	Independent Security Evaluators	Securing Hospitals	https://www.securityevaluators.com/hospitalhack/	2016
[Kampanakis14]	P. Kampanakis	Security Automation and Threat Information-Sharing Options	https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6924671	2014
[Kaynar16]	K. Kaynar	A taxonomy for attack graph generation and usage in network security	https://doi.org/10.1016/j.jisa.2016.02.001	2016
[Khan17a]	R. Khan, K. McLaughlin, D. Laverty and S. Sezer	STRIDE-based Threat Modeling for Cyber-Physical Systems	https://doi.org/10.1109/ISGTEurope.2017.8260283	2017
[Khan17b]	S. A. Khan	A STRIDE Model based Threat Modelling using Unified and-Or Fuzzy Operator for Computer Network Security	http://dx.doi.org/10.12785/IJCNT/050103	2017
[Kokkonen16]	T. Kokkonen. J. Hautamäki, J. Siltanen and T. Hämäläinen	Model for sharing the information of cyber security situation awareness between organizations	https://doi.org/10.1109/ICT.2016.7500406	2016
[Komarkova18]	J. Komárková, L. Sadlek and M. Laštovička	Community based platform for vulnerability categorization	https://doi.org/10.1109/NOMS.2018.8406125	2018
[Kotonya98]	G. Kotonya and I. Sommerville	Requirements Engineering: Processes and Techniques	https://www.wiley.com/en-us/Requirements+Engineering%3A+Processes+and+Tec	1998

			hniques-p-9780471972082	
[Kott14]	Alexander Kott, Cliff Wang, Robert F. Erbacher	Cyber Defense and Situational Awareness: Foundations and Challenges	https://doi.org/10.1007/978-3-319-11391-3	2014
[Krishnan17]	S. Krishnan	A Hybrid Approach to Threat Modelling	https://pdfs.semanticscholar.org/550f/aeb15d64020c6a995c291b6b9f44f8be656d.pdf	2017
[Kruse17]	C. S. Kruse, B. Frederick, T. Jacobson and D. K. Monticone	Cybersecurity in healthcare: A systematic review of modern threats and trends	https://doi.org/10.3233/THC-161263	2017
[Lebek13]	Lebek, B., Uffen, J., Breitner, M., Neumann, M., & Hohler, B.	Employees’ Information Security Awareness and Behavior: A Literature Review.	http://doi.org/10.1109/HICSS.2013.192L	2013
[Lee08]	Lee, D., Larose, R., & Rifon, N.	Keeping our network safe: a model of online protection behaviour.	http://doi.org/10.1080/01449290600879344	2008
[Li10]	Li, H., Zhang, J., & Sarathy, R.	Understanding compliance with internet use policy from the perspective of rational choice theory.	http://doi.org/10.1016/j.dss.2009.12.005	2010
[Liang09]	Liang, H., & Xue, Y.	Avoidance of information technology threats: a theoretical perspective.	https://doi.org/10.2307/20650279	2009
[Liao10]	Qi Liao, Aaron Striegel, Nitesh Chawla	Visualizing Graph Dynamics and Similarity for Enterprise Network Security and Management	https://doi.org/10.1145/1850795.1850799	2010
[LOGRHYTHM]	LogRhythm	LogRhythm	https://logrhythm.com/	
[Ma16]	Z. Ma and C. Schmittner	Threat Modeling for Automotive Security Analysis	http://dx.doi.org/10.14257/astl.2016.139.68	2016
[Maglogiannis06]	Maglogiannis I, Zafiropoulos E	Modeling Risk in Distributed Healthcare Information Systems	https://ieeexplore.ieee.org/document/4463037	2006

[Mansmann09]	Florian Mansmann, Fabian Fischer, Daniel A. Keim, Stephen C. North	Visual support for analyzing network traffic and intrusion detection events using TreeMap and graph representations	https://doi.org/10.1145/1641587.1641590	2009
[Mansmann12]	Florian Mansmann, Timo Göbel, William Cheswick	Visual analysis of complex firewall configurations	https://doi.org/10.1145/2379690.2379691	2012
[Mathew06]	Sunu Mathew, Rich Giomundo, Shambhu J. Upadhyaya	Understanding multistage attacks by attack-track based visualization of heterogeneous event streams	https://doi.org/10.1145/1179576.1179578	2006
[McEachan11]	McEachan, R. R. C., Conner, M., Taylor, N. J., & Lawton, R. J.	Prospective prediction of health-related behaviours with the Theory of Planned Behaviour: a meta-analysis.	http://doi.org/10.1080/17437199.2010.521684	2011
[Mead17]	N. Mead, F. Shull, J. Spears, S. Heibl, S. Weber and J. Cleland-Huang	Crowd Sourcing the Creation of Personae Non Gratae for Requirements-Phase Threat Modeling	https://doi.org/10.1109/RE.2017.63	2017
[Mead18]	N. Mead, F. Shull, K. Vemuru and O. Villadsen	A Hybrid Threat Modeling Method	http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=516617	2018
[Microsoft]	Microsoft Corporation	SDL Threat Modeling Tool. Security Development Lifecycle	https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling	2018
[Millett19]	Millett, K., dos Santos, E., Millett, P.D.	Cyber-Biosecurity Risk Perceptions in the Biotech Sector	https://doi.org/10.3389/fbioe.2019.00136	2019
[Milne00]	Milne, S., Sheeran, P., & Orbell, S.	Prediction and Intervention in Health Related Behaviour: A meta-analytic review of Protection Motivation Theory.	http://doi.org/10.1111/j.1559-1816.2000.tb02308.x	2000
[Mitnick03]	Mitnick, K. D.	Are you the weak link?	https://elibrary.ru/item.asp?id=6433382	2003

[Murch18]	Murch, R.S., So, W.K., Buchholz, W.G., Raman, S., Peccoud, J.	Cyberbiosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy	https://doi.org/10.3389/fbioe.2018.00039	2018
[Myagmar05]	S. Myagmar, A. J. Lee and W. Yurcik	Threat Modeling as a Basis for Security Requirements	https://people.cs.pitt.edu/~adamlee/pubs/2005/sreis-05.pdf	2005
[Ney17]	P. Ney, K. Koscher, L. Organick, and L. Ceze and T. Kohno	Computer Security, Privacy, and DNA Sequencing: Compromising Computers with Synthesized DNA, Privacy Leaks, and More	https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-ney.pdf	2017
[Ng05]	Ng, B.-Y., & Rahim, M.	A socio-behavioral study of home computer users’ intention to practice security.	http://aisel.aisnet.org/pacis2005/20	2005
[Ng09]	Ng, B.-Y., Kankanhalli, A., & Xu, Y.	Studying users’ computer security behaviour: A health belief perspective.	https://doi.org/10.1016/j.dss.2008.11.010	2009
[Nobre19]	C. Nobre, M. Meyer, M. Streit, A. Lex	The State of the Art in Visualizing Multivariate Networks	http://dx.doi.org/10.31219/osf.io/upbm2	2019
[Noel03]	Steven Noel, Sushil Jajodia, Brian O'Berry, Michael Jacobs	Efficient minimum-cost network hardening via exploit dependency graphs	https://doi.org/10.1109/CSAC.2003.1254313	2003
[Noel03]	S. Noel, S. Jajodia, B. O’Berry, and M. Jacobs	Efficient minimum-cost network hardening via exploit dependency graphs	https://doi.org/10.1109/CSAC.2003.1254313	2003
[Noel04]	Steven Noel, Sushil Jajodia	Managing attack graph complexity through visual hierarchical aggregation	https://doi.org/10.1145/1029208.1029225	2004
[Noel05]	Steven Noel, Michael Jacobs, Pramod Kalapa, Sushil Jajodia	Multiple coordinated views for network attack graphs	https://doi.org/10.1109/VIZSEC.2005.1532071	2005
[Nunnally13]	Troy Nunnally, Penyen Chi, Kulsoom Abdullah, A. Selcuk Uluagac, John A.	P3D: A parallel 3D coordinate visualization for advanced network scans	https://doi.org/10.1109/ICC.2013.6654828	2013

	Copeland, Raheem Beyah			
[NVD]	National Institute of Standards and Technology	National Vulnerability Database	https://nvd.nist.gov/vuln-metrics/cvss	2018
[OHare08]	Scott O’Hare, Steven Noel, Kenneth Prole	A Graph-Theoretic Visualization Approach to Network Risk Analysis	https://doi.org/10.1007/978-3-540-85933-8_6	2008
[OLAYEMI16]	Olayemi Mikail, Olaniyi & Alhassan, John & Abba, Emmanuel & Waziri, Victor	Threat Modeling of Electronic Health Systems and Mitigating Countermeasures	http://ceur-ws.org/Vol-1830/Paper16.pdf	2016
[Ortiz15]	José Ortiz-Ubarri, Humberto Ortiz-Zuazaga, Albert Maldonado, Eric Santos, Jhensen Grullón	Toa: A Web Based Network Flow Data Monitoring System at Scale	https://doi.org/10.1109/BigDataCongress.2015.71	2015
[Ou03]	X. Ou, Wayne F. Boyer, M. A. McQueen	A scalable approach to attack graph generation	https://doi.org/10.1145/1180405.1180446	2003
[OWASP]	OWASP Project	OWASP Top 10 - 2017	https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf	2019
[Pahnila07]	Pahnila, S., Siponen, M., &Mahmood, A.	Employees’ Behaviour Towards IS Security Policy Compliance.	10.1109/HICSS.2007.206	2007
[Papadopoulos13]	Stavros Papadopoulos, Georgios Theodoridis, Dimitrios Tzovaras	BGPfuse: using visual feature fusion for the detection and attribution of BGP anomalies	https://doi.org/10.1145/2517957.2517965	2013
[Paxson99]	Vern Paxson	Bro: a system for detecting network intruders in real-time	https://doi.org/10.1016/S1389-1286(99)00112-7	1999
[Pecoud18]	Peccoud, J., Gallegos, J.E., Murch, R., Buchholz, W.G., Raman, S.	Cyberbiosecurity: From Naive Trust to Risk Awareness	https://doi.org/10.1016/j.tibtech.2017.10.012	2018
[Pernul95]	Pernul, Gunther	Information systems security: Scope, state-of-	https://www.sciencedirect.com/scienc	1995

		the-art, and evaluation of techniques	e/article/pii/026840 1295000105	
[Phillips98]	C. Phillips and L. Painton Swiler	A Graph-based System for Network-vulnerability Analysis	https://doi.org/10.1 145/310889.31091 9	1998
[Piquero96]	Piquero, A., & Tibbetts, S.	Specifying the direct and indirect effects of low self-control and situational factors in offenders’ decision making: Toward a more complete model of rational offending. Justice	http://doi.org/10.10 80/0741882960009 3061	1996
[Plotnikoff 10]	Plotnikoff, R. C., Lippke, S., Trinh, L., Courneya, K. S., Birkett, N., & Sigal, R. J.	Protection motivation theory and the prediction of physical activity among adults with type 1 or type 2 diabetes in a large population sample.	http://doi.org/10.13 48/135910709X478 826	2010
[Posey10] ().	Posey, C., Roberts, T., Lowry, P. B., Bennett, B., Courtney, J. F., & Behaviors, P.	Insiders’ Protection of Organizational Information Assets: A Multidimensional Scaling Study of Protection-Motivated Behaviors.	https://ssrn.com/ab stract=1668142	2010
[Potteiger16]	B. Potteiger, A. Kalaie and X. Koutsoukos	Software and attack centric integrated threat modeling for quantitative risk assessment	https://doi.org/10.1 145/2898375.2898 390	2016
[Puhakainen10]	Puhakainen, P., & Siponen, M.	Improving employees’ compliance through information systems security training: an action research study.	https://doi.org/10.2 307/25750704	2010
[QRADAR]	IBM	IBM QRadar	https://www.ibm.co m/security/security-intelligence/qradar	
[Rainer91]	Rex Kelly Rainer Jr., Charles A. Snyder & Houston H. Carr	Risk Analysis for Information Technology	https://doi.org/10.1 080/07421222.199 1.11517914	1991
[Ritchey00]	R. W. Ritchey and P. Ammann	Using model checking to analyze network vulnerabilities.	https://doi.org/10.1 109/SECPRI.2000. 848453	2000
[Rogers10]	Rogers, E	Diffusion of innovations.	ebook	2010

[Rogers75]	Rogers, R.	A protection motivation theory of fear appeals and attitude change.	http://doi.org/10.1080/00223980.1975.9915803	1975
[Rogers83]	Rogers, R.	Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation.	http://dx.doi.org/10.4236/jtr.2015.34023	1983
[Rogers84]	Rogers, R.	Changing health-related attitudes and behaviors: the role of preventative health psychology.	In Interfaces in Psychology.	1984
[Rosenstock88]	Rosenstock, I., Strecher, V., & Becker, M.	Social learning theory and the health belief model.	http://doi.org/http://dx.doi.org/10.1177/109019818801500203	1988
[Saini08]	V. Saini, Q. Duan and V. Paruchuri	Threat modeling using attack trees	https://dl.acm.org/ft_gateway.cfm?id=1352100&ftid=502241&dwn=1&CFID=55037246&CFTOKEN=fefff126f81b60a5-EFABE0EC-D5CE-CA63-6DC90997AD2DEC63	2008
[Saitta05]	P. Saitta, B. Larcom and M. Eddington	Trike v.1 Methodology Document	https://www.helpnetsecurity.com/dl/articles/Trike_v1_Methodology_Document-draft.pdf	2005
[Samy10]	Narayana Samy, G., Ahmad, R., Ismail, Z.	Security threats categories in healthcare information systems	https://www.ncbi.nlm.nih.gov/pubmed/20889850	2010
[Scandariato11]	R. Scandariato, K. Wuyts and J. Wouter	A privacy threat analysis framework: Supporting the elicitation and fulfillment of privacy requirements	https://doi.org/10.1007/s00766-010-0115-7	2014
[Scandariato15]	R. Scandariato, K. Wuyts and W. Joosen	A descriptive study of Microsoft's threat modeling technique	https://doi.org/10.1007/s00766-013-0195-2	2015
[Schneier00]	Schneier, B.	Secrets and Lies: Digital Security in a networked world.	https://www.amazon.co.uk/Secrets-Lies-Digital-Security-Networked/dp/0471	2000

			453803/ref=sr_1_1?keywords=secret+and+lies+digital+security&qid=1564587621&s=gateway&sr=8-1	
[Schneier01]	B. Schneier	Attack Trees	https://web.cs.du.edu/~ramki/papers/attackGraphs/SchneierAttackTrees.pdf	2001
[Shaid12]	Syed Z. M. Shaid, Mohd A. Maarof	Malware Behaviour Visualization	https://doi.org/10.11113/jt.v70.3512	2012
[Shan15]	L. Shan and M. M. Kokar	A Situation Assessment Framework for Cyber Security Information Relevance Reasoning	https://ieeexplore.ieee.org/document/7266729/metrics#metrics	2015
[Shevchenko18]	N. Shevchenko, T. A. Chick, P. O'Riordan, T. Scanlon and C. Woody	Threat Modeling: A Summary of Available Methods	https://resources.sei.cmu.edu/asset_files/WhitePaper/2018_019_001_524597.pdf	2018
[Sheyner02]	O. Sheyner, J. W. Haines, S. Jha, R. Lippmann, J. M. Wing	Automated Generation and Analysis of Attack Graphs	https://doi.org/10.1109/SECPRI.2002.1004377	2002
[Shiravi12]	Hadi Shiravi, Ali Shiravi, Ali A. Ghorbani	A Survey of Visualization Systems for Network Security	https://doi.org/10.1109/TVCG.2011.144	2012
[Shostack06]	A. Shostack, S. Lambert and S. Hernan	Uncover Security Design Flaws using STRIDE	https://adam.shostack.org/uncover.html	2006
[Shostack08]	A. Shostack	Experiences Threat Modeling at Microsoft	http://ftp.informatik.rwth-aachen.de/Publications/CEUR-WS/Vol-413/paper12.pdf	2008
[Shostack14]	A. Shostack	Threat Modeling: Designing for Security	https://www.wiley.com/en-us/Threat+Modeling%3A+Designing+for+Security-p-9781118809990	2014

[Sion18]	L. Sion, K. Yskout, D. V. Landuyt and W. Joosen	Solution-aware Data Flow Diagrams for Security Threat Modeling	https://doi.org/10.1145/3167132.3167285	2018
[Siponen06]	Siponen, M., Pahnila, S., &Mahmood, A.	A New Model for Understanding Users’ IS Security Compliance.	http://aisel.aisnet.org/pacis2006/48	2006
[Siponen07]	Siponen, M.T., Pahnila, S., &Mahmood, M.A.	Employees' Adherence to Information Security Policies: An Empirical Study.	https://doi.org/10.1007/978-0-387-72367-9_12	2007
[Siponen10A]	Siponen, M., Pahnila, S., & Mahmood, M. A.	Compliance with Information Security Policies: An Empirical Investigation.	http://doi.org/10.1109/MC.2010.35	2010
[Siponen10B]	Siponen, M., & Vance, A.	Neutralization: New insights into the problem of employee information systems security policy violations	https://doi.org/10.2307/25750688	2010
[Siponen14]	Siponen, M., Mahmood, M. A., & Pahnila, S.	Employees’ adherence to information security policies: An exploratory field study.	http://doi.org/10.1016/j.im.2013.08.006	2014
[Sommer10]	Robin Sommer, Vern Paxson	Outside the Closed World: On Using Machine Learning for Network Intrusion Detection	https://doi.org/10.1109/SP.2010.25	2010
[Spanakis17]	Spanakis, M., Manikis, G., Porwal, S., & Spanakis, E.G.	Developing a context-dependent tuning framework of multi-channel biometrics that combine audio-visual characteristics for secure access in eHealth platform for osteoarthritis management	https://www.semanticscholar.org/paper/Developing-a-Context-Dependent-Tuning-Framework-of-Spanakis-Manikis/e05e3ff87c865c6c8e4b36aa69c337f6959b1591	2017
[SPLUNK]	Splunk	Splunk	https://www.splunk.com/	
[Stanton05]	Stanton, J. M., Stam, K., Mastrangelo, P., & Jolton, J.	Analysis of end user security behaviors.	http://doi.org/10.1016/j.cose.2004.07.001	2005
[Strielkina18]	A. Strielkina, V. Kharchenko and D. Uzun	Availability models for healthcare IoT systems: Classification and	https://ieeexplore.ieee.org/document/8409099	2018

		research considering attacks on vulnerabilities		
[STIX]	OASIS Cyber Threat Intelligence (CTI)	Structured Threat Information Expression	https://oasis-open.github.io/cti-documentation/stix/intro	2018
[Stoffel13]	Florian Stoffel, Fabian Fischer, Daniel A. Keim	Finding anomalies in time-series using visual correlation for interactive root cause analysis	https://doi.org/10.1145/2517957.2517966	2013
[Sun17]	X. Sun, J. Dai, P. Liu, A. Singhal, and J. Yen	Using Bayesian Networks to Fuse Intrusion Evidences and Detect Zero-Day Attack Paths	https://link.springer.com/chapter/10.1007/978-3-319-66505-4_5	2017
[TAXII]	OASIS Cyber Threat Intelligence (CTI)	Trusted Automated Exchange of Intelligence Information	https://oasis-open.github.io/cti-documentation/taxii/intro.html	2018
[Taylor09]	Teryl Taylor, Diana Paterson, Joel Glanfield, Carrie Gates, Stephen Brooks, John McHugh	FloVis: Flow Visualization System	https://doi.org/10.1109/CATCH.2009.18	2009
[Theoharidou05]	Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E.	The insider threat to information systems and the effectiveness of ISO17799.	http://doi.org/10.1016/j.cose.2005.05.002	2005
[Theron17]	R. Theron, R. Magán-Carrión, J. Camacho, G. M. Fernndez	Network-wide intrusion detection supported by multivariate analysis and interactive visualization	http://dx.doi.org/10.1109/VIZSEC.2017.8062198	2017
[Tsigkas12]	Orestis Tsigkas, Olivier Thonnard, Dimitrios Tzovaras	Visual spam campaigns analysis using abstract graphs representation	https://doi.org/10.1145/2379690.2379699	2012
[UcedaVelez15]	T. UcedaVelez and M. M. Morana	Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis	https://www.wiley.com/en-us/Risk+Centric+Threat+Modeling%3A+Process+for+Attack+Simulation+and+Threat+Analysis-p-9780470500965	2015

[Ulicny]	B. Ulicny, J. Moskal, M. M. Kokar, K. Abe and J. K. Smith	Inference and Ontologies	https://doi.org/10.1007/978-3-319-11391-3_9	2014
[Vaar13]	Risto Vaar, Pawel N. Ski	Comparative Analysis of Open-Source Log Management Solutions for Security Monitoring and Network Forensics	http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.428.6404	2013
[Vance12]	Vance, A., Siponen, M., & Pahnila, S.	Motivating IS security compliance: Insights from Habit and Protection Motivation Theory.	http://doi.org/10.1016/j.im.2012.04.002	2012
[Vandenberghe08]	Grant Vandenberghe	Network Traffic Exploration Application: A Tool to Assess, Visualize, and Analyze Network Security Events	https://doi.org/10.1007/978-3-540-85933-8_18	2008
[Varga16]	Margaret Varga, Carsten Winkelholz, Susan Träber-Burdin	The Application of Visual Analytics to Cyber Security	https://pdfs.semanticscholar.org/6068/847497e9dc2dd17fa655c0e32d955c3279b5.pdf	2016
[Varga18]	Margaret Varga, Carsten Winkelholz, Susan Träber-Burdin	Cyber Situation Awareness	https://www.sto.nato.int/publications/STO%20Educational%20Notes/STO-EN-IST-143/EN-IST-143-02.pdf	2018
[Vroom04]	Vroom, C., & von Solms, R.	Towards information security behavioural compliance.	http://doi.org/10.1016/j.cose.2004.01.012	2004
[Wagner10]	Cynthia Wagner, Gérard Wagener, Radu State, Alexandre Dulaunoy, Thomas Engel	PeekKernelFlows: peeking into IP flows	https://doi.org/10.1145/1850795.1850801	2010
[Wagner15]	Markus Wagner, Fabian Fischer, Robert Luh, Andrea Haberson, Alexander Rind, Daniel A. Keim, Wolfgang Aigner	A Survey of Visualization Systems for Malware Analysis	http://dx.doi.org/10.2312/eurovisstar.20151114	2015

[Wang06]	L. Wang, S. Noel, and S. Jajodia	Minimum-cost network hardening using attack graphs	https://doi.org/10.1016/j.comcom.2006.06.018	2006
[Wang14]	L. Wang, M. Albanese, and S. Jajodia	Linear-Time Network Hardening	https://link.springer.com/chapter/10.1007/978-3-319-04612-9_5	2014
[Wang15]	Weijie Wang, Baijian Yang, Victor Yingjie Chen	A visual analytics approach to detecting server redirections and data exfiltration	https://doi.org/10.1109/ISI.2015.7165932	2015
[Wash2010]	Wash, R.	Folk models of home computer security.	10.1145/1837110.1837125	2010
[Williams07]	Leevar Williams, Richard Lippmann, Kyle Ingols	An Interactive Attack Graph Cascade and Reachability Display	https://doi.org/10.1007/978-3-540-78243-8_15	2007
[Williams08]	Leevar Williams, Richard Lippmann, Kyle Ingols	GARNET: A Graphical Attack Graph and Reachability Network Evaluation Tool	https://doi.org/10.1007/978-3-540-85933-8_5	2008
[Witte92]	Witte, K.	Putting the fear back into fear appeals: The extended parallel process model.	http://doi.org/10.1080/03637759209376276	1992
[Witte00]	Witte, K., & Allen, M.	A meta-analysis of fear appeals: Implications for effective public health campaigns.	http://doi.org/10.1177/109019810002700506	2000
[Woon05]	Woon, I. M. Y., Tan, G. W., & Low, R. T.	A protection motivation theory approach to home wireless security.	http://aisel.aisnet.org/icis2005/31	2005
[Workman08]	Workman, M., Bommer, W., & Straub, D.	Security lapses and the omission of information security measures: A threat control model and empirical test.	https://doi.org/10.1016/j.chb.2008.04.005	2008
[Wuyts15]	K. Wuyts and J. Wouter	LINDDUN privacy threat modeling: a tutorial	https://lirias.kuleuven.be/retrieve/331950	2015
[Wuyts18]	K. Wuyts, D. V. Landuyt, A.	Effective and efficient privacy threat modeling	https://doi.org/10.1145/3167132.3167414	2018

	Hovsepyan and W. Joosen	through domain refinements		
[Xie09]	A. Xie, G. Chen, Y. Wang, Z. Chen, J. Hu:	A new method to generate attack graphs	https://doi.org/10.1109/SSIRI.2009.32	2009
[Xiong19]	W. Xiong and R. Lagerstrom	Threat modeling - A systematic literature review	https://doi.org/10.1016/j.cose.2019.03.010	2019
[Yao08]	Yao, M. Z., & Linz, D. G.	Predicting self-protections of online privacy.	http://doi.org/10.1089/cpb.2007.0208	2008
[Yelizarov09]	Anatoly Yelizarov, Dennis Gamayunov	Visualization of complex attacks and state of attacked network	https://doi.org/10.1109/VIZSEC.2009.5375527	2009
[Yeo09]	Yeo, A.C., Rahim, M.M. &Ren, Y.y.	Use of Persuasive technology to change end-users IT security aware behaviour: A pilot study.	https://pdfs.semanticscholar.org/425c/cda9d2a26b235acf8b0b860a519e0272cf01.pdf	2009
[Yi13]	Shanzhen Yi, Yong Peng, Qi Xiong, Ting Wang, Zhonghua Dai, Haihui Gao, Junfeng Xu, Jiteng Wang, Lijuan Xu	Overview on attack graph generation and visualization technology	https://doi.org/10.1109/ICASID.2013.6825274	2013
[Yigit14]	B. Yigit, G. Gur, and F. Alagoz	Cost-Aware Network Hardening with Limited Budget Using Compact Attack Graphs	https://ieeexplore.ieee.org/document/6956752	2014
[Yu17]	Wei Yu, Fan Liang, Xiaofei He, William Grant Hatcher, Chao Lu, Jie Lin, Xinyu Yang	A survey on the edge computing for the internet of things	https://ieeexplore.ieee.org/document/8123913	2017
[Zhang09]	Zhang, L., & McDowell, W. C.	Am I Really at Risk? Determinants of Online Users’ Intentions to Use Strong Passwords.	http://doi.org/10.1080/15332860903467508	2009
[Zhang17]	Tianye Zhang, Xumeng Wang, Zongzhuang Li, Fangzhou Guo, Yuxin Ma, Wei Chen	A survey of network anomaly visualization	https://doi.org/10.1007/s11432-016-0428-2	2017

[Zhang18]	Y. Zhang, D. Zheng and R. H. Deng	Security and Privacy in Smart Health: Efficient Policy-Hiding Attribute-Based Access Control	https://ieeexplore.ieee.org/document/8334589	2018
[Zhao12]	Ying Zhao, Fangfang Zhou, Xiaoping Fan	A real-time visualization framework for IDS alerts	https://doi.org/10.1145/2397696.2397698	2012
[Zhao13]	Ying Zhao, FangFang Zhou, XiaoPing Fan, Xing Liang, YongGang Liu	IDSRadar: a real-time visualization framework for IDS alerts	https://doi.org/10.1007/s11432-013-4891-9	2013
[Zhao14]	Ying Zhao, Xing Liang, Xiaoping Fan, Yiwen Wang, Mengjie Yang, Fangfang Zhou	MVSec: multi-perspective and deductive visual analytics on heterogeneous network security data	https://doi.org/10.1007/s12650-014-0213-6	2014
[Zhou13]	Fangfang Zhou, Ronghua Shi, Ying Zhao, Yezi Huang, Xing Liang	NetSecRadar: A Visualization System for Network Security Situational Awareness	https://doi.org/10.1007/978-3-319-03584-0_30	2013
[Zhuo12]	Wei Zhuo, Yacin Nadjin	MalwareVis: entity-based visualization of malware network traces	https://doi.org/10.1145/2379690.2379696	2012

Table 2: Reference Documents

3. Glossary of Acronyms

Acronym	Description
AS	Autonomous System
BYOD	Bring Your Own Device
CCTA	Central Computer and Telecommunication Agency
CIS	Center for Internet Security
COBIT	Control Objectives for Information Technology
CRAMM	CCTA Risk Analysis and Management
CyPR	Cybersecurity Professional Register
DRMP	Dynamic Risk Management Platform
EHR	Electronic Health Record
EPPM	Extended Parallel Process Model
ERM	Enterprise Risk Management
FSP	Full-Scale Pilot
GA	Grant Agreement
GDPR	General Data Protection Regulation
HCO	Healthcare Organization
HC	Healthcare
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IoMT	Internet of Medical Things
IoT	Internet of Things
ISACA	Information Security and Control Association
ITIL	Information Technology Infrastructure Library
NIST	National Institute of Standards and Technology
OCR	Office for Civil Rights
PBC	Perceived Behavioural Control
PEU	Perceived Ease of Use
PHI	Protected Health Information (also Personal Health Information)
PII	Personally Identifiable Information
PMT	Protection Motivation Theory
PU	Perceived Usefulness
SA	Situational Awareness
SEB	Stakeholders Expert Board
SME	Small- and Medium-sized Enterprises
TAM	Technology Acceptance Model
TPB	Theory of Planned Behaviour
TRA	Theory of Reasoned Action
VA	Visual Analytics
WP	WorkPackage

Table 3: Table of acronyms

4. PANACEA project description

4.1 Overall concept

Healthcare is increasingly evolving towards digitalisation: electronic health records have been developed (and widely adopted), teleconsultation and tele-expertise is thriving, and use of connected HC devices is on the rise. It is evident that threats and potential damages to healthcare critical infrastructures due to cyberattacks require a fortification of the security features in the industry.

The PANACEA Research & Innovation Action, referred to as PANACEA, will demonstrate that security stems from awareness of cyber vulnerabilities - enabling healthcare facilities to assess the nature and severity of a threat, and sustainably decide to adopt strategies to strengthen preparedness and incident response.

PANACEA will deliver a Dynamic Risk Management Platform, analysing the risk of the IT infrastructure leveraging the healthcare processes. The Secure Information Sharing Platform will manage information sharing between healthcare organizations, multi-tenant and cross boundaries.

Since it is fundamental to consider cyber-security from the initial phases of development of a medical device or any IT-related system, PANACEA will develop a platform (Secure Design Support Platform) and related guidelines to help system architects on defining the security posture of a new system in development.

PANACEA will address the need to respond swiftly to a complex, multi-faceted cyber threat landscape, not only addressing technical aspect but also the need for highly-skilled cybersecurity professionals to help reduce cyber risks in healthcare and for a security culture where all staff are aware of the risks and the role their behaviour plays in reducing risk.

As general impacts, PANACEA looks to:

i. Reinforce Europe’s position as a key security provider for Healthcare IT systems;

ii. Allow for a continued development and improvement of fully tailored identity management and secure data management solutions for Healthcare;

iii. Proceed with the development of new prototypes to improve the security of IT infrastructures leveraging healthcare processes;

iv. Accelerate growth in the Healthcare ecosystem to attract more customers and to increase its market share with the target to reach $2bn revenues by 2020;

v. Extend and reinforce the European network of stakeholders and decision makers.

4.2 Project objectives

PANACEA will deliver two toolkits for **cybersecurity assessment and preparedness of Healthcare ICT infrastructures and connected devices**:

- The PANACEA **Solution Toolkit** (made up of 4 technological tools and 3 organizational tools) and
- The PANACEA **Delivery Toolkit** (made up of 2 support tools).

The technical tools of the toolkit will be demonstrated on relevant environments (the aim is to reach Technology Readiness Level[1] 6 for the four technological tools) and will benefit from ambitious research goals, achieved by moving beyond the current state of the art in strategic areas such as:

- **Dynamic risk assessment & mitigation** (threat modelling, attack modelling, response management through technical and non-technical security measures, visual analytics);
- Potential use of **Blockchain** for secure information sharing of healthcare data;
- **Identification & authentication** (cryptographic authentication protocols, biometric recognition/digital identity, IoMT identification);
- **Security-by-design** methods and tools for healthcare systems and software;
- **Secure behaviours decision models** and influencers.

Three end-use case scenarios, developed in Italy, Crete and Ireland, will provide a solid test-bed[2].

The PANACEA main objectives are listed below:

- Objective 1: Develop and validate tools for dynamic risk assessment and mitigation
- Objective 2: Develop and validate tools for Secure Information Sharing
- Objective 3: Develop and validate tools for System Security-by-design and certification
- Objective 4: Develop and validate tools for identification and authentication
- Objective 5: Develop and validate an educational package for cybersecurity in the health sector
- Objective 6: Develop and validate tools for resilience governance
- Objective 7: Develop tools for secure behaviours nudging
- Objective 8: Develop and validate Implementation Guidelines for cybersecurity solutions adoption
- Objective 9: Develop and validate a Security-ROI methodology
- Objective 10: Engage a representative community of stakeholders and identify a sustainability path for the PANACEA vision

4.3 Use Cases within PANACEA project

PANACEA offers a significant improvement in multiple areas (from threat awareness to security-by-design and secure information sharing).

However, results can only be measured in the context of realistic data, use cases and scenarios. At the same time, it is not possible to rely on the operational IT infrastructure of the hospitals for research, development and testing activities, due to their criticality. For this reason, the consortium will adopt the use of emulation environments based on a set of heterogeneous user scenarios developed by End Users and relevant for their businesses.

The User Scenarios will be co-designed with multiple end-user groups from Italy, Crete and Ireland. Aiming to provide a wide dataset representing different networks and organisations, heterogeneous threats and incidents situations.

[1] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/support/faq;keywords=/2890
[2] https://www.panacearesearch.eu/use-cases

User scenarios have a critical importance for the development, test and validation of the PANACEA toolkit: using virtualization techniques on private cloud environments, fractions of the end users’ IT infrastructures will be virtualized and emulated in order to create a safe virtual environment with affinity to the operational but fully available for testing and validation. User scenarios will be hence fundamental in order to understand how the emulation environments will need to be composed.

User Scenarios will be detailed in deliverable D1.4 (31 September 2019).

4.4 Innovations

PANACEA research will deliver two toolkits for cybersecurity assessment and preparedness of Healthcare IT infrastructures and connected devices: 1) The Solution Toolkit and 2) The Delivery Toolkit.

1- The Solution Toolkit will positively affect the cybersecurity of a Healthcare Centre (HCC) according to a holistic modality, assessing (and acting on) the physical, software and organizational/human components of the HCC, relevant for the cybersecurity.

It is composed of four technological tools:

- a dynamic risk assessment & mitigation tool (helping to perform risk assessment evaluation and mitigation measures)
- a secure information sharing tool for the protection of data
- a security-by-design & certification tool
- a tool for identification & authentication

Moreover, it comprises three organizational tools:

- a tool composed by models, guidelines and best practices for training & education
- a tool aimed at resilience governance
- a tool for secure behaviours nudging

Each component of the Solution Toolkit, can be implemented and used separately by the management and the security staff of the healthcare center. Once implemented, they operate by protecting an ecosystem made up of a variety of components, e.g.

- The Healthcare Center network composed of operators, patients, citizens, security staff, medical doctors, nurses, top management, employees and administrative staff.
- The clinical information systems and related processes (EHP, PHR)
- The administrative information systems
- The connected devices used in and outside of the hospital

The Solution Toolkit also manages the connections with other HCCs, even when this HCCs are not adopting PANACEA research's solutions (these are represented on the right).

2. The Delivery Toolkit is conceived as a support for the adoption of the Solution Toolkit. It involves two support tools:

- a methodology to evaluate the Return of Investment (ROI) of cybersecurity interventions, therefore the advantages of following a cybersecurity approach in a Healthcare Center
- a set of guidelines to be applied for the adoption of the Solution Toolkit

PANACEA research follows two Innovative approaches:

1) A holistic approach to cybersecurity: the underlying paradigm of PANACEA research is that real improvement in the domain of cybersecurity can only come from change in human behavior, technology and processes as part of a holistic solution. The Toolkit contains all of these ingredients; and the project is structured to facilitate co-design and close collaboration between end-users and researchers/developers

2) An impact-oriented approach: the Consortium has put itself in the shoes of the public health decision makers and of the HCC managers, as prospect users of PANACEA research, and has decided not only to design effective solutions, but also to make them easy to adopt.

The PANACEA research Toolkit is expected to be used for prevention purposes. The Toolkit helps the HCC to proactively protect the IT infrastructure. It does not include an incident management component.

The summary of the project mission has been consolidated to the following one:

PANACEA delivers people-centric cybersecurity solutions in healthcare. The Partners will execute on a 36-month, leanly-orchestrated research workplan, which envisages continuous involvement of end-users at 3 European healthcare centres, also comprising devices utilised for remote care & homecare settings. Ultimately, PANACEA delivers two toolkits for cyber security assessment and preparedness of Healthcare ICT infrastructures and connected devices: The PANACEA Solution Toolkit (made up of 4 technological tools and 3 organisational tools) and the PANACEA Adoption Toolkit (constituted of 2 support tools).

5. Review Methodology

The objective of this deliverable is to offer a review of the literature with respect to the cyber security risks and scenarios in the healthcare ecosystem. This document is a focused review aiming to demonstrate the extensively researched literature related to PANACEA seeking to identify significant state of the art works in the related research fields. This review is thus indented to analyze the huge amount of scientific and technical efforts spent around the three main topics examined in this document: threats, vulnerabilities and countermeasures for cyber risks. This document presents a scoping narrative review in order to identify the potential size and scope of the available research literature [Grant09]. Nevertheless, a comprehensive search process has been followed in order to aggregate and select the most relevant publications.

The following are the resources and resource-specific details that we have primarily used to conduct this review:

- Pubmed search using the query : "Cybersecurity" OR "Cyber Security" OR "Cyber Attack" OR "Cyber Risk" OR "Cyber Threat" OR "Data Breach" OR "Data Security" OR "Firewall" OR "Malware" OR "Phishing" OR "Ransomware" OR "Security Incident". This query located 979 results only in the last 5 years that were subject to subsequent screening and filtering.
- Clarivate Analytics Web of Science™, with the following as an advanced query on topics: TS= (("Health*" OR "Healthcare") AND ("Cybersecurity" OR "Cyber Security" OR "Cyber Attack" OR "Cyber Risk" OR "Cyber Threat" OR "Data Breach" OR "Data Security" OR "Firewall" OR "Malware" OR "Phishing" OR "Ransomware" OR "Security Incident")) and on English articles published in the last 5 years. This resulted in 445 papers that were manually filtered based on titles and abstracts. The following bar chart shows the top categories of the matched records:

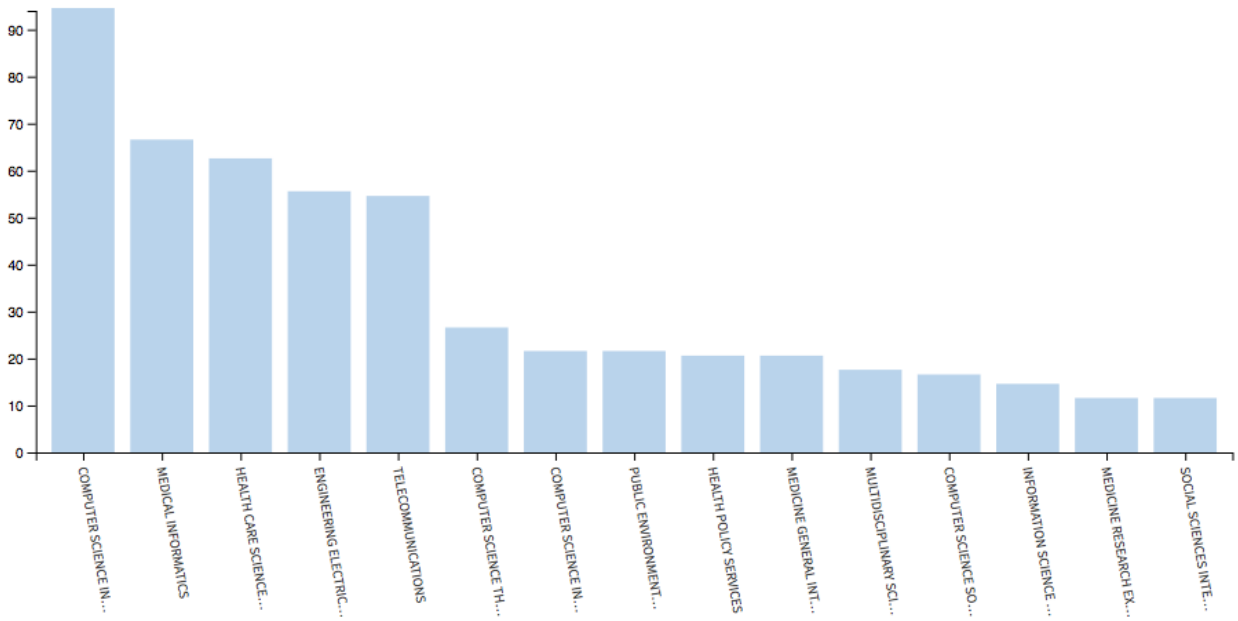

Figure 1: Top categories results by the Clarivate Analytics Web of Science

- Google scholar with more relaxed search terms, so that references to specific technologies and methodologies are found (e.g. for the STRIDE threat model)

Additionally, we have used web search to locate relevant news (e.g. for security incidents in healthcare organizations) as well as press releases and reports from major US and EU organizations and other stakeholders such as the US Department of Health and Human Services, and related rules and directives, e.g. the Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), etc.

The screening and selection of the papers to be included has been performed manually, as already mentioned, in most cases. Publications that, based on their abstracts, were considered to address issues and provide information and context outside of the objective of this review were excluded from further study. An extension to this manual curation process is the use of bibliometric tools that were used in specific, more focused, new, and hot domain areas, such as the Internet of Things (IoT) section.

Finally, considering the research approach that PANACEA is going to take, a review of the state of the art related to specific topics i.e., attack graph-based risk estimation and response, visual analytics supporting situational awareness, human behavioural modelling, has been carried out starting from the expertise of contributing partners that provided references to seminal works in this context.

The review presented in document tries to highlight the main challenges and research gaps currently existing in the healthcare domain but, for the sake of completeness, it also presents relevant results presented and discussed without specific reference to an application domain. This will help the PANACEA consortium to identify the most relevant state of the art approaches and to apply or extend them in the healthcare domain fighting challenges imposed by this extremely complex domain.

6. Cyber security in HealthCare: scenarios and perspectives

The healthcare sector has been capitalizing on digital advancements to improve overall patient experiences and outcomes - beginning with the adoption of electronic health records (EHRs) and continuing with the increased use of medical applications, online patient portals, connected medical devices, and wearables.

While Personal Identifiable Information (“PII”) generically refers to any data that could potentially identify a specific individual, and can be used for de-anonymizing data, in the specific context of HC, Protected Health Information (PHI) (also referred to as personal health information), generally refers to demographic information, medical histories, test and laboratory results, mental health conditions, insurance information, and other data that a healthcare professional collects to identify an individual and determine appropriate care.

In particular EHR refer to digital instances of PHI that HCO store in their electronic systems. EHRs allow doctors to access and keep track of PHI in or out of the office. It is also used to make it easier for providers to share information about patients. However, as technology use in healthcare grows, so does the risk of cyberattacks. As a matter of fact, PHI and EHRs are lucrative for cybercriminals since they contain highly valuable personal information, such as social security numbers and insurance information, which can be used for fraudulent purposes or sold for a profit. It can also be used to build exceptionally rich personal profiles, enabling identity theft, cyber espionage, and even extortion. On the black market, the going rate for a credit card number is 25 cents; however, an EHR can be worth hundreds or even thousands of dollars[3].

Nonetheless, SecurityScorecard’s most recent U.S. State and Federal Government Cybersecurity Report 2018[4], a ranking of the different industries according to “security performance”, found the healthcare industry ranking fourth.

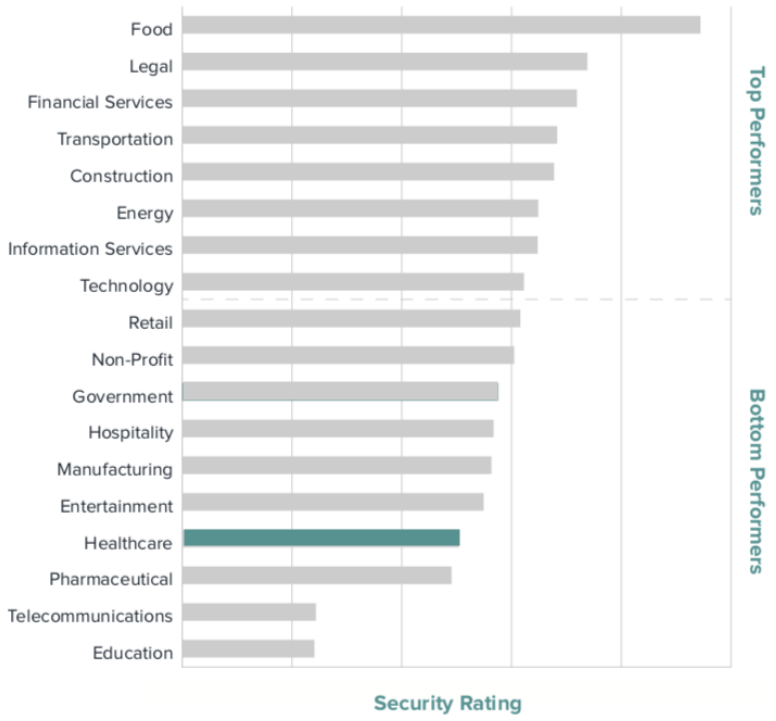

Figure 2: SecurityScorecard’s US sector ranking on security performance

[3] https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/
[4] https://securityscorecard.com/resources/2018-us-government-cybersecurity-research-report

Below we mention briefly the 10 top threats in healthcare as reported by Infosec in 2018[5].

Top Threat		Details
1	Ransomware and other malware	Healthcare operates in an intricate network of interconnected services, and devices. This interlocking network transfer information can be vulnerable to ransomware and other malware attacks. For example, in the UK National Health Service (NHS), theWannaCry ransomware attack, left hospitals forced to close, and the interruption of patients treatment because of an inability to access EHRs. *The HHS 'Wall of Shame', lists healthcare data breaches in the U.S., has a total of 288 data breaches affecting almost 4.7 million individuals from the beginning of the year to January 1, 2018. In the 1st quarter of 2017, there were four times as many ransomware variants detected than in the previous year*[6].
2	Phishing	A Verizon report dictates that about 66% of malware was initiated as an email attachment (or sms/text link) – this is known as phishing[7]. Phishing is a threat not only to personal and health data but also to authentication/login credentials. The National Health Information Sharing and Analysis Center have recently reported that the healthcare industry is at the most risk of fraudulent emails[8]. However, little is being done to combat this, with 98% of healthcare organizations not taking the first steps in helping to prevent phishing by setting in place Domain-based Message Authentication, Reporting & Conformance[9].
3	Insider threats	Insider threats to healthcare centers and hospital resources are a major concern and can be carried out by patients (freely entering such premises) as well as staff and can be both malicious and accidental. An HIMSS Cybersecurity Survey found that these threats were deemed to be worrying enough to set up specific programs of protection by 75% of respondents[10].
4	Insecure use of cloud services	Cloud computing is being taken up by healthcare as it offers many benefits not only in terms of access to healthcare services and data but also in cost efficiency and business development. In terms of security cloud computing also brings risks since data need to be protected within a cloud infrastructure (i.e. robust encryption, means of secure access, appropriate and effective authentication, etc.).
5	Healthcare data exposure risks	Healthcare has embraced Internet-connect devices in a bid to use health data to improve patient outcomes. Many Internet of Medical Things (IoMT) devices aggregate personal and health data stored in the cloud and used to analyze conditions, treatments, health status etc. In this case these devices may be affected by security issues like DDoS attacks (i.e. Mirai Bot of October 2016) making the protection of personal data in and around devices important in order to prevent exposure and redundancy issues.
6	The HC supply chain	The supply chain in HC has often been the weakest link in terms of cybersecurity. For example, the TRICARE breach, which resulted in 4.6 million military patient records being exposed was the result of a negligent supplier[11]. Ensuring that all suppliers within the HC service operate under the same security policies is challenging, but it is also a requirement of some regulatory frameworks such as the HIPAA Rules in the U.S., which extend the act's requirements to business associates.

[5] https://resources.infosecinstitute.com/top-10-threats-healthcare-security/#gref
[6] Proofpoint, Quarterly Threat Report Q1 2017: https://www.proofpoint.com/sites/default/files/pfpt-us-tr-q117-threat-report.pdf
[7] Verizon, Data Breach Investigations Report 2017: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
[8] Business Wire, Press Release: https://www.businesswire.com/news/home/20171128005546/en/Fifty-Seven-Percent-Email-%E2%80%9CFrom%E2%80%9D-Healthcare-Industry-Fraudulent
[9] https://www.researchgate.net/publication/324455350_2018_Verizon_Data_Breach_Investigations_Report
[10] HIMSS, 2017 HIMSS Cybersecurity Survey: http://www.himss.org/sites/himssorg/files/2017-HIMSS-Cybersecurity-Survey-Final-Report.pdf
[11] https://www.inforisktoday.com/tricare-breach-affects-49-million-a-4105

Top Threat		Details
7	Authentication issues	Authentication in healthcare is hard to balance in terms of security and usability. The reason is all the various cases that lead to the fact that both password and the way that they are used is dangerous. In HC, biometrics are being increasingly used for access control [Spanakis17], [Cocioceanu18]. However, as seen in the UK NHS WannaCry attack, some hospitals that used biometric drug access were unable to access the drugs, and override keys had to be used.
8	Use of legacy applications	Legacy applications and systems can leave considerable weaknesses for cybercriminal to exploit (i.e. WannaCry[12]). Regular penetration, patching and update testing is an important activity to do to find vulnerabilities in your infrastructure.
9	Lack of risk ownership	Security is a problem for everyone in an organization - behavioural factors around no-one taking ownership (e.g., bystander effect, "someone else will do it"). In healthcare, this extends across all disciplines, suppliers, and even patients. Building security awareness programs throughout the healthcare organization and beyond will create a foundation stone for a more 'healthy' system, especially in a time of technological changes. These must address behavioural issues and culture as well as awareness.
10	Poor healthcare funding	One thing that many healthcare services throughout the world are up against is poor funding and staffing issues. Programs of security awareness and improvements in technology all cost money for training and implementation. But healthcare should not be a luxury.

Table 4: Top ten threats in healthcare

The HIPAA Security Rule[13] defines a *security incident* as an *attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system*. Analogously, [14] defines a *breach* as, generally, an *impermissible acquisition, access, use, or disclosure* under the HIPAA Privacy Rule[15] *that compromises the security or privacy of the PHI*.

In this report we see that in 2017 in the UK, a catastrophic ransomware attack in the form of WannaCry caused havoc across at least 16 health trusts, with hospitals and doctor surgeries being affected, Accenture 2017[16]. Healthcare industry is today affected by cybercrime and study by Ponemon and IBM it was shown that the cost for healthcare breaches rises each year. In fact the cost per capita to healthcare for each breached record was, on average, $380[17].

Below we present examples of several other large-scale security breaches within HC[18].

- Anthem (**80M records compromised).** The largest HC breach to date affected Anthem, the second largest health insurer in the U.S. In late January 2015, the medical insurance provider began notifying 80 million individuals that their personal information was compromised in a December 2014 cyber-attack.
- Premera **(11M records compromised)** In March of 2015, Premera—a large medical insurance company—revealed that a hacker had accessed their network, compromising the data of 11 million individuals. The company didn't expound on how the hacker accessed the information, but it did disclose that they might have accessed "social security numbers, birthdays, emails, physical

[12] https://malware.wikia.org/wiki/WannaCry
[13] https://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html
[14] https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
[15] https://www.hhs.gov/hipaa/for-professionals/privacy/index.html
[16] Accenture, 2017 Cost of Cybercrime Study: https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf
[17] IBM, Ponemon 2017 Cost of Data Breach: https://www.ibm.com/security/data-breach
[18] https://www.bitsight.com/blog/security-breaches-healthcare

addresses, bank account information, clinical information and detailed insurance claims” to both past and present customers, dating back to 2002.\

- TRICARE (**4.9M records compromised).** This 2011 breach was unique for many reasons. According to Reuters, an employee for one of TRICARE’s vendors— Science Application International Corporation (now Leidos Holdings Inc.) — was transporting backup tapes that included electronic healthcare data for TRICARE’s patients when the employee’s vehicle was broken into and some of its contents stolen. Those tapes were among the items that the thief stole, but investigators didn’t believe the thief was after the tapes (or even knew what they were). In 2014, federal judges closed out all but two lawsuits that formed after the breach, citing that “the mere loss of data—without evidence that it has been either viewed or misused—does not constitute an injury sufficient to confer standing.”
- Community Health Systems (**4.5M records compromised)** In August 2014, Community Health Systems—which owns and operates over 200 hospitals across the U.S.—reported a massive cyberattack that compromised patient records. According to InformationWeek, the information, which included patient names, addresses, birthdates, telephone numbers, and social security numbers, was gathered as a result of an exploited SSL vulnerability, named Heartbleed. Interestingly, cybersecurity analysts have speculated that this breach and the Anthem breach were linked.
- Banner Health (**3.7M records compromised)** A data breach affecting up to 3.7 million individuals at Banner Health was disclosed in early August 2016. The data compromised included patient and physician names, addresses, social security numbers, clinical information, and health insurance information. It is believed that payment data used at vending machines and other food and beverage outlets was compromised as well. It is still unclear how attackers gained unauthorized access to Banner Health's servers and computer systems.
- Mass General Hospital (**4,300 Records Compromised).** In late May 2016, Mass General Hospital (MGH) announced that 4,300 dental patient records had been stolen. According to MGH, these records were not stored on their systems, but instead stolen from the network of a third-party vendor—Patterson Dental Supply Inc. (PDSI)—that assists the hospital in managing dental patients at several practices. The records stolen from PDSI included names, dates of birth, social security numbers, dental provider information, medical record numbers, and dental appointment information of MGH patients.
- Prosthetic & Orthotic Care Inc. (**number of compromised records unknown)** Prosthetic & Orthotic Care Inc. (P&O Care) recently announced a data breach that resulted in the exposure of critical patient information. The records exposed included PII and personal health information (PHI), such as names, contact information, patient identification numbers, diagnostic codes, appointment dates, billing amounts, social security numbers, birth dates, insurance providers, and photos of procedures. It has been reported that records were dumped in plain text on Pastebin. The P&O Care breach occurred after a hacker exploited a zero-day flaw—or an issue unknown to the vendor—within software the company had recently purchased.

In addition to data breaches, poor security can also impact upon patient care due to the potential compromise of health or eHealth equipment, including Io(M)T It is thus critical to develop a **strong security culture for citizens and the public and private healthcare sector**, by utilizing the relevant capabilities of the academic community and of other public and private sector stakeholders. As we present in Figure 3 the criticality of health-related infrastructures is enormous.

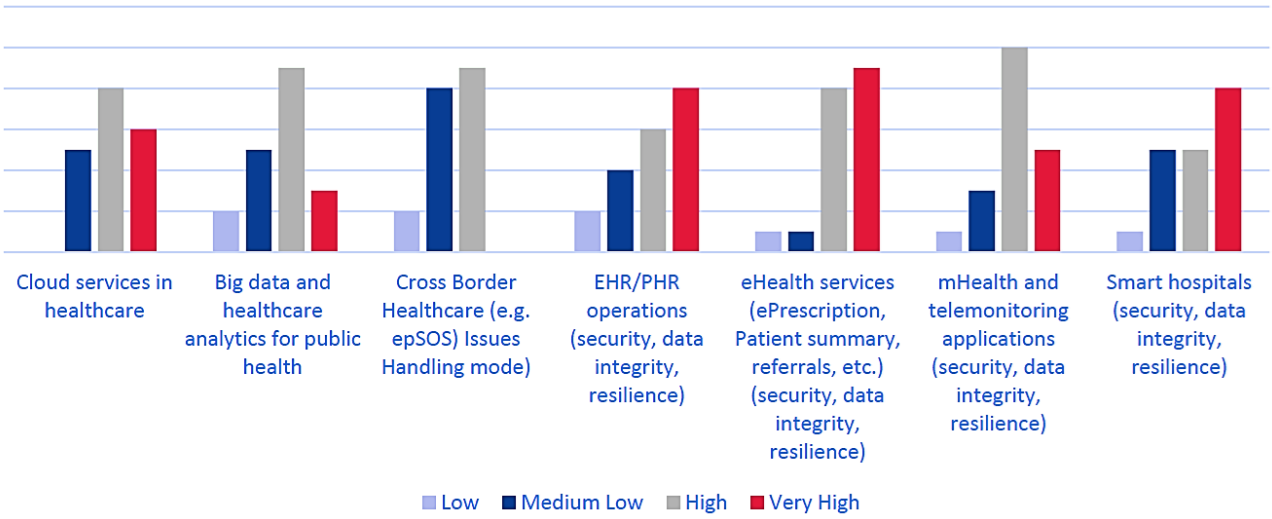

Figure 3: Cybersecurity in the healthcare sector[19]

Figure 4 and Figure 5 illustrate the *weakest spots,* respectively, *for attacks* and *areas of vulnerability* as reported by both HC personnel and non-HC personnel (visitors and patients).

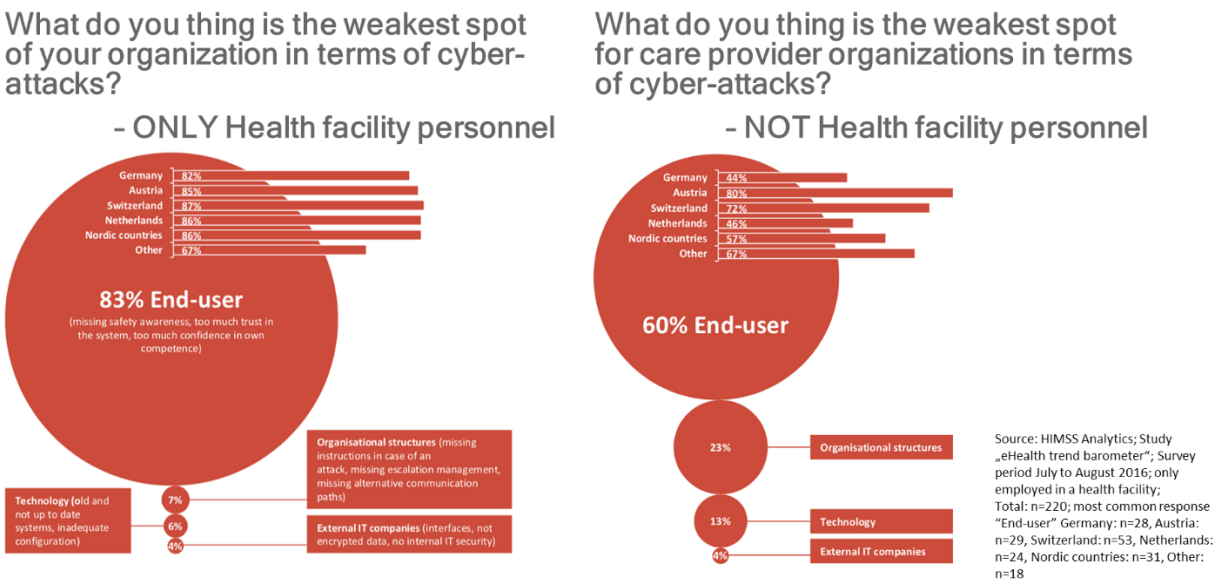

Figure 4: Weakest *spot by attacks*

[19] ENISA, Security and Resilience in eHealth Infrastructures and Services. https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services

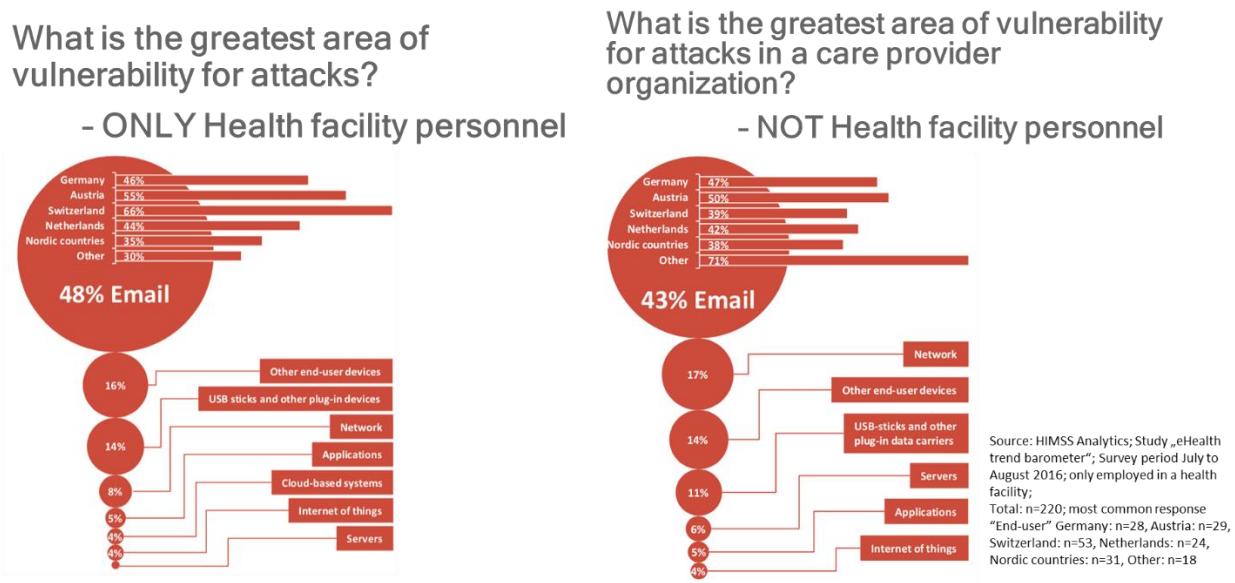

Figure 5: Weakness spot by area of vulnerability [20]

HC organizations face specific threats and security risks mainly due to the use of services and devices cloud services, unsecure networks, employee negligence, bring your own device (BYOD) policies, lack of internal identification and security systems, stolen devices with un-encrypted files and others.

Security can also impact upon patient care due to the potential compromise of health or eHealth equipment, also including Io(M)T security. In particular some facts:

- 58% of hospitals did not select their current security vendor in advance of a cybersecurity incident.
- 32% of healthcare organizations did not scan for vulnerabilities before an attack.
- 29% of respondents currently report they do not have an adequate solution to instantly detect and respond to an organizational attack.

The relatively bad security performance of the healthcare industry has given rise to a number of healthcare data breaches at an increasing rate the last couple of years. The US Department of Health and Human Services’ Office for Civil Rights (OCR) provides a “breach portal”[21] that we have used to retrieve the number and type of security incidents as well as the estimated number of individuals affected in the last three years. As shown in Figure 6, there has been a significant rise in the number of healthcare data breaches in 2018 and 2019, especially in the “Hacking/IT incident” category. In fact, as we are in the middle of the year at the time of writing, it is remarkable that year 2019 has outpaced the previous year by a large margin in this specific category.

[20] HIMSS Analytics; Study „eHealth trend barometer“; Survey period July to August 2016; only employed in a health facility;
[21] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

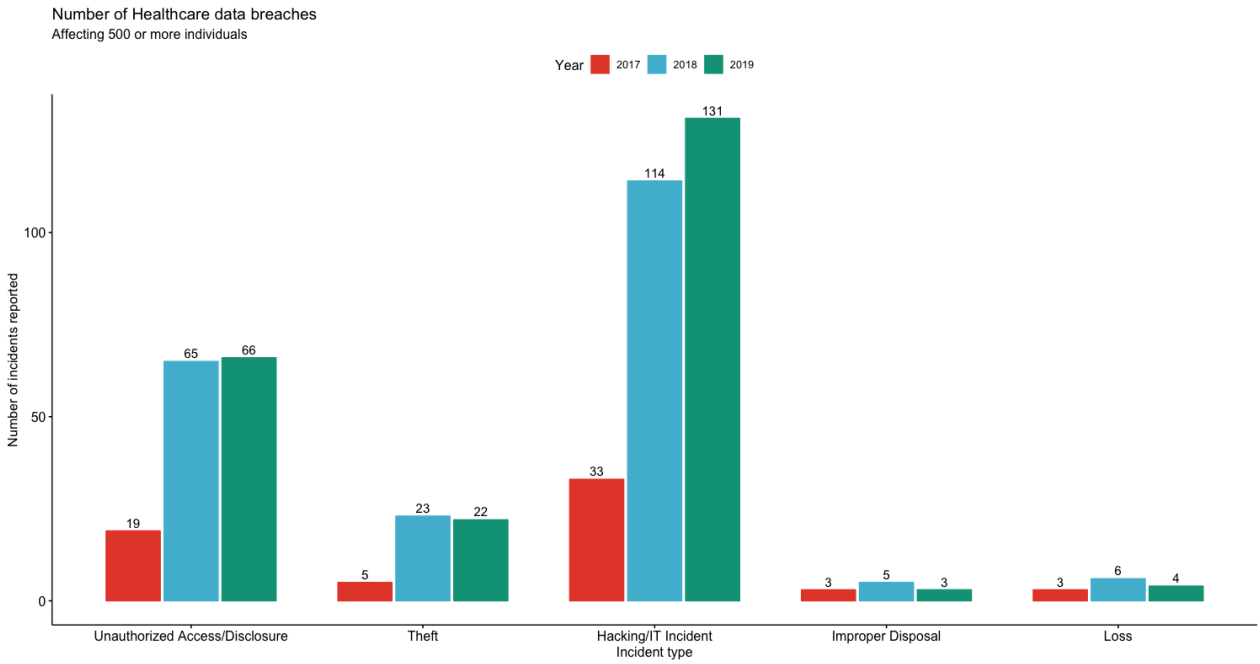

Figure 6: Number of security incidents in the US Health organizations per incident type and year. Data were downloaded in July 2019 from the Office of Civil Rights of the US Department of Health and Human Services and correspond to years 2017 to 2019 (https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf).

In addition to the number of data breaches, another important aspect is how many people are affected by these incidents. Figure 7 shows the total number of affected individuals per type of security incident and the year when it was reported.

Some relevant terminology:

- The HIPAA Security Rule defines a security incident as an attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. (45 CFR 164.304.)
- The HIPAA Breach Notification Rule defines a breach as, generally, an impermissible acquisition, access, use, or disclosure under the HIPAA Privacy Rule that compromises the security or privacy of the protected health information. (45 CFR 164.402).
- Health care provider means a provider of services, a provider of medical or health services, and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business. (45 CFR. § 160.103 (2012)).
- Health plan means an individual or group plan that provides, or pays the cost of, medical care (e.g. a health insurance issuer) (45 CFR. § 160.103)
- Personal identifiable information (“PII”) is any data that could potentially identify a specific individual, that is, any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII. Electronic Health Records is a real-time electronic system that stores patient’s health information. EHRs allow doctors to access and keep track of patient health information in or out of the office. It is also used to make it easier for providers to share information about patients. See “What is an electronic health record (EHR)?”, HEALTHIT.GOV https://www.healthit.gov/faq/what-electronic-health-record-ehr

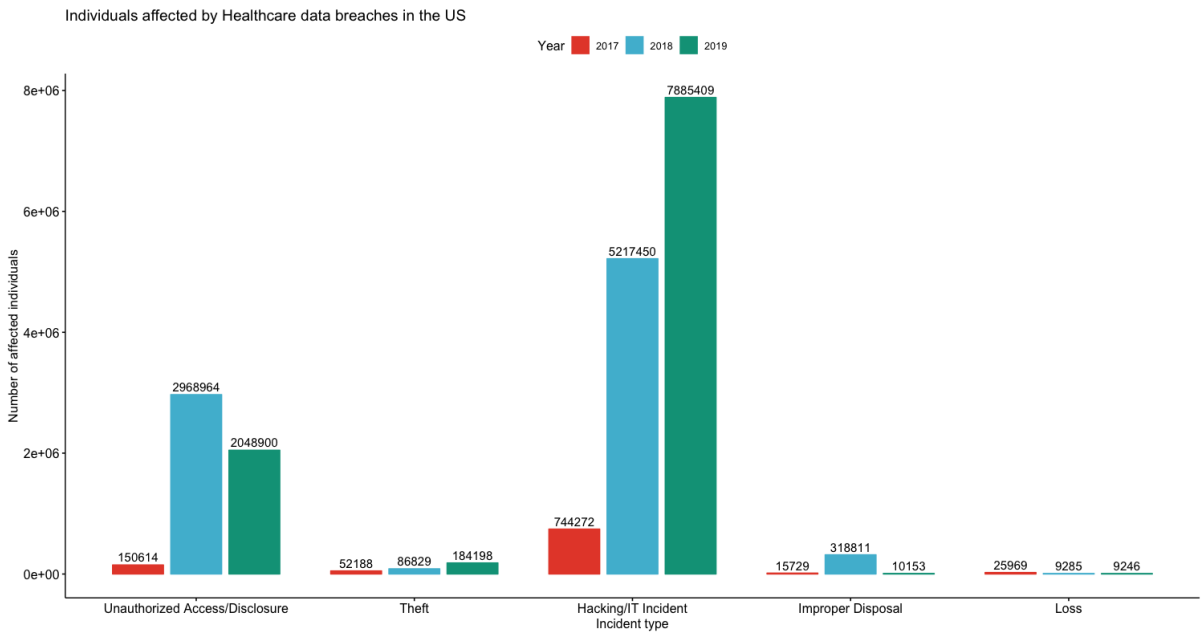

Figure 7: Total number of individuals affected by the security incidents in the US health sector in the last 3 years.

Again, the IT related security incidents have the most impact (i.e., greatest number of people affected). This type of incident also shows the most accelerated increase rate in 2018 and 2019. In Table 5 we present the top 15 breaches in the two last years, affecting the larger number of individuals.

Rank	Name of Covered Entity	Entity type	Individuals affected	Type of Breach	Year
1	Dominion Dental Services, Inc., Dominion National Insurance Company, and Dominion Dental Services USA, Inc.	Health Plan	2,964,778	Hacking/IT Incident	2019
2	Inmediata Health Group, Corp.	HC Clearing House	1,565,338	Unauthorized Access/Disclosure	2019
3	Iowa Health System d/b/a UnityPoint Health	Business Associate	1,421,107	Hacking/IT Incident	2018
4	Employees Retirement System of Texas	Health Plan	1,248,263	Unauthorized Access/Disclosure	2018
5	UW Medicine	HC Provider	973,024	Hacking/IT Incident	2019
6	CNO Financial Group, Inc.	Health Plan	566,217	Unauthorized Access/Disclosure	2018
7	Health Management Concepts, Inc.	Business Associate	502,416	Hacking/IT Incident	2018
8	Georgia Department of Human Services	Business Associate	435,339	Unauthorized Access/Disclosure	2018
9	AU Medical Center, INC	HC Provider	417,000	Hacking/IT Incident	2018
10	Columbia Surgical Specialist of Spokane	HC Provider	400,000	Hacking/IT Incident	2019
11	UConn Health	HC Provider	326,629	Hacking/IT Incident	2019

Rank	Name of Covered Entity	Entity type	Individuals affected	Type of Breach	Year
12	Metro Santurce, Inc. d/b/a Hospital Pavia Santurce and Metro Hato Rey, Inc. d/b/a Hospital Pavia Hato Rey	HC Provider	305,737	Hacking/IT Incident	2019
13	SSM Health St. Mary's Hospital - Jefferson City	HC Provider	301,000	Improper Disposal	2018
14	Women's Health Care Group of PA, LLC	HC Provider	300,000	Hacking/IT Incident	2017
15	Oklahoma State University Center for Health Sciences	HC Provider	279,865	Hacking/IT Incident	2018

Table 5: Top fifteen breaches in the two last years related to HCOs

In Table 5, HC provider refers to a provider of services, a provider of medical or health services, and any other person or organization who furnishes, bills, or is paid for HC in the normal course of business. Health plan means an individual or group plan that provides, or pays the cost of, medical care (e.g. a health insurance issuer).

6.1 Why healthcare is vulnerable to cyber attacks

It is evident from the previous analysis that there's an emergent need to secure healthcare organizations and their assets, and especially the most critical asset which is the patients' themselves and their health-related information. The data shown above underlines the fact that the Health IT has the largest impact and therefore cybersecurity solutions need to be in place for the benefit of the patients, as well as the health business entities and other stakeholders.

Nevertheless, many health organizations appear to lack information security measures and awareness, as the news and the statistics above confirm. The reasons for this can be traced to various factors[22,23]:

- The adoption of digital patient records, the automation of clinical systems, as well as the advent of modern implantable medical devices for the treatment and management of diseases [Burns16].
- The use of antiquated Electronic Medical Records (EMR), legacy operating systems and clinical applications that are not designed to securely operate in today's networked environment.
- The ease of distributing ePHI (electronic protected health information) both internally through mobile devices, USB drives, and laptops, and externally through third parties and Cloud services.
- Insufficient in-house expertise and security leadership makes it more difficult to reduce risks, vulnerabilities and attacks.

[22] KPMG Health Care and Cyber Security Report, (2015) https://assets.kpmg/content/dam/kpmg/pdf/2015/09/cyber-health-care-survey-kpmg-2015.pdf
[23] Ponemon Institute, The state of cybersecurity in healthcare organizations in 2018, https://ponemonsullivanreport.com/2018/03/the-state-of-cybersecurity-in-healthcare-organizations-in-2018/

- The heterogeneous nature of networked systems and applications (e.g. from Picture Archiving and Communication Systems (PACS) operating inside hospitals to connected personal health records accessible from patients' devices).

- The evolving threat landscape, where cyber-attacks today are more sophisticated (e.g. distributed denial-of-service, "ransomware", etc) and well-funded given the increased value of the compromised data on the black market: Healthcare organizations are targeted because of the value of patient medical and billing records.

6.2 Key assets in healthcare

The study report on securing hospitals published by the firm ISE (Independent Security Evaluators) [24] identifies the two primary assets found in the healthcare ecosystem: the patients' health, and the patients' health data. Patients' health is the most critical one, although it is in fact oftentimes neglected. Patients can be affected through direct or indirect, intentional or unintentional, acts of the medical staff or outside actors. Actually, any compromise and breach of patients' data can also affect the corresponding patients' health, as is the case of the modification of medical history for example. The second most important health-related asset is patients' health records, which contain valuable information including personally identifiable information (PII) such as social security number, health care provider information, credit card information, name, address, date of birth, etc. They also include protected health information (PHI) - like patient physical or mental health condition, diagnoses, treatments, details of patient visits, etc. Such information appears to have surpassed the value of more "traditional" data stolen, like for example credit cards numbers, in the deep web marketplaces, because it can be used for a variety of purposes[25]: from impersonating the victim[26] to open bank accounts, commit insurance fraud, etc., to harassment and blackmail.

The availability of healthcare services is also a major asset of medical facilities. They are divided into two distinct categories: critical services & administrative services. The first ones ensure continuity of care, including, among others, active/passive medical devices, medicine delivery systems and surgery equipment. The disruption of these services may have a devastating impact on patients' health. The administrative services are dedicated to the smooth hospital workflow. Systems handling work orders, medicine inventories, prescriptions, bills or appointments are part of these services. Their unavailability is however less critical as long as their downtime remains of short duration.

Secondary assets at risk relate to the operation of the hospitals and health organizations as business. Intellectual property assets, although less of concern for the patients, are of high value in healthcare facilities that host research labs. These assets can be drug formulas, experimental results, surveys, etc. and could represent years of work. Finally, the reputation of the organization and their physicians is also an important asset. A cyber-attack - regardless its nature - will harm the institution credibility if it is disclosed to the public. In addition, if the identity of specific medical staff is used to perform the attack (impersonation, credential theft, etc.), it may damage their reputation and career.

[24] https://www.securityevaluators.com/wp-content/uploads/2017/07/securing_hospitals.pdf
[25] E. Kangas, Why Are Hackers Targeting Your Medical Records? (2017) https://luxsci.com/blog/hackers-targeting-medical-records.html
[26] Ponemon Institute. Fifth annual study on medical identity theft. February 2015. http://medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf

6.3 Threats and cyber-attacks in healthcare

ISO/IEC 27000:2018[27] defines information security as the preservation of confidentiality, integrity and availability, but in a complex organization such as a hospital, or even the health ecosystem as a whole, more aspects of security need to be considered. Rainer et al [Rainer91] classified threats as physical, such as fire or power interruption, unauthorized physical or electronic access, and authorized physical or electronic access. In fact, the case study of [Samy10] reports that the most critical threat for a Hospital Information System is the power failure, followed by human error (e.g. erroneous deletion or modification of patient data by the stuff). The prominence of the power failure threat has been supported by other publications as well, e.g. [Maglogiannis06], and should surely be taken into account since it affects some key assets, such as the safety of the patients and medical stuff, the security of the software and critical clinical applications, and the operation of the organization in general.

Leaving behind physical security, [Pernul95] provided a classification of threats as follows: unauthorized disclosure, loss or destruction, and undesired use or modification. Specializing even further, [Jung01] categorized network security threats are as interruption, interception, modification, and fabrication, as follows:

1. Interruption: an asset of the system is destroyed or becomes unavailable. Examples include: destruction of a piece of hardware, the disabling of the file management system, erasure of a program or data file, and failure of an operating system manager.

2. Interception: an unauthorized party gains access to an asset. The party could be a person, a program, or a computer. Examples include: wiretapping, the illicit copying of files or programs, and traffic analysis.

3. Modification: the content of a data transmission is altered and results in an unauthorized action or result. Examples include: changing values of items, altering a program so that it performs incorrectly, and modifying the incoming messages.

4. Fabrication: an unauthorized party inserts counterfeit objects into the system. Examples include: insertion of spurious messages or the addition of records to a file.

Finally, van Deursen [Deurse14] argues that cyber-security is a multidisciplinary problem and many threats originate from social engineering, changes in society, or unexpected use of the technology, and proposes the sharing and analysis of non-technical security knowledge (i.e. from social subsystems and the environment) to complement technical risk intelligence tools.

The identification of risks is the first step in every successful risk management process. Focusing on the healthcare, da Silva [Edges18] have identified 28 risks and their scenarios that can potentially affect health care organizations from the point of view of the Enterprise Risk Management (ERM). These risks span the whole spectrum of the healthcare organization operation, relating to financial, operational, clinical, people relations and management, technology, and other aspects. The following table presents these risks, their classification, and the impact they may induce to potential targets.

[27] https://webstore.ansi.org/Standards/DS/DSISOIEC270002018

Risks	Risk Group	Short description	Risk Impact: Patient	Risk Impact: Financial	Risk Impact: Reputation	Risk Impact: Legal	Risk Impact: Social
Board governance – poor communication or lack of direction	Financial	Relationship with shareholders and the board of the organization; transparency in the information and results, capacity to prosecute governance. Mergers and Acquisitions. Conflict of Interest		x	x		
Business Interruption Due to Natural Catastrophe	Operational	Occurrence of internal or external events, which make it impossible for an organization to maintain its critical activities. Natural disasters must be allocated to this event. Earthquake or Hurricane.	x	x			x
Clinical batch claim	Clinical	With the increase of technologies and multiples techniques applied to patient to treat diseases, the batch claims have increased in size and frequency. Batch claims are frequently related to poor delivery of clinical service.	x	x	x		x
Conflicts due to organizational hierarchy	People	Responsibilities, leadership and respect among the employees and functions. The relationship between the decision-making process and hierarchy. The medical hierarchy needs to be balanced in favour of teaching, learning and patient safety rather than the exercise of power (WALTON, 2006).	x				
Cyber security	Information Technology	Invasion of an internal or external hacker that causes damage to the information security of the organization or its operational capacity. The use of	x	x	x	x	x

		ransomware is frequently present.					
Deficiency in development of technology and innovation	Clinical	Lack of technologic innovation or development of innovations that do not meet the organization’s needs. It is related organization’s ability to possess, dominate and use technological resources that have an effect on its operations. Effects on the quality of clinical procedures and patient experience, as well as valuation of the institution towards insurers can be perceived.	x	x	x		
Dependence on insurance companies	Financial	Negotiations with one health insurance company that accounts for 30% of the billing. The insurance company wants to reduce reimbursements for many medical tests and procedures.	x	x			
Dispute with insurance companies on reimbursements	Financial	An insurance company disputes the drugs, devices, or procedures used by the providers and hospital. The insurance company denies coverage.	x	x		x	
Electronic Health Record (EHR)	Information Technology	Difficulty in obtaining information due to error in communication, loss of processing power or difficulty in operating the Hospital’s system.	x			x	
Environment Protection Agency or similar	Compliance	Government agency comes to investigate and fines the hospital or a department of the hospital.	x	x	x	x	x
External media communication	Information Technology	Healthy external marketing and media communication about the hospital and close relations. Organizational information being shared before the formal process and department of the hospital. The	x		x	x	

		information timing can’t be the correct, or the information credibility can cause future problems.					
Financial batch claim emanating from reimbursement reform	Political	Financial risk for healthcare organizations associated with bundled services or healthcare outcomes.		x	x		x
Fraud committed by a provider	Financial	Insurance plan fraud committed by a doctor or a group of doctors through prescriptions. In addition, important medicines or equipment stolen from the hospital can also be considered like a fraud.	x	x	x	x	x
Government instability	Political	Reduction in the country’s healthcare budget	x	x			x
Loss of accreditation	Compliance	Loss of an important certification or accreditation.	x	x	x	x	
Non-compliance with laws and regulations	Compliance	A clinical trial is taking place without the proper Institutional Review Board (IRB) approval. Patients die while part of the research.	x	x	x	x	x
Loss of Occupational Safety and Healthcare Administration (OSHA in USA)	Compliance	The effect that working laws represent in how employees are being contracted. Any change in the formal orientations represent an effect for the hospital management.	x	x		x	
Organizational culture	People	The healthcare organization needs to be able to share and implement its culture among all the employees. New and old employees need to work conducted by the same values and principles independently of their own religion or origins.	x				
Physician wellness	People	50% rate of burnout amongst physicians discovered after taking a physician wellness survey that measures burnout and professional fulfilment.	x	x		x	

Relation between the School of Medicine or Residency program and hospital	Clinical	Interface between the SoM and the health service that may lead to interference of the university model to the business or, on the other hand, value the institution due to the teaching quality.	x		x		x
Active Shooter	Operational	Assault and active shooter threats to patients, families and hospital employees.	x		x	x	x
Sentinel events	Clinical	Sentinel events, near miss events, incidents or medical error that can cause lawsuit.	x	x	x	x	
Supply chain	Operational	Materials and equipment control and management. Political problems with countries that supply resources for hospitals.	x	x			x
Talent retention	People	Loss of a team of providers that are specialized in certain types of procedures. It can happen in function of bad recruitment processes, or bad human resources management.	x	x	x		x
Terrorism	Political	Terrorism attack close to the hospital.	x	x	x	x	x
Unethical conduct	Operational	Problems related with unethical employee conduct whether or not involving patients. Personal information, images or objects can be used without the approval of patient. Internal problems between employees can result in organization impact.	x	x	x	x	x
Union strike	Political	Union strikes among different classes of employees that can affect the hospital capacity to be operated.	x	x	x	x	
Use of social communication networks	Information Technology	Problems with confidential information being communicated through social media. A VIP: executive, actor, etc. Information is released on	x	x	x		x

		Facebook, what’s app or other.					

Table 6: Impact type for each risk

6.4 Risk scenarios

The identification of risks is the first step in every successful risk management process. Focusing on the healthcare, da Silva Etges et al [Etges18] have identified 28 risks and their scenarios that can potentially affect HCOs from the point of view of the Enterprise Risk Management (ERM). These risks span the whole spectrum of the healthcare organization operation, relating to financial, operational, clinical, people relations and management, technology, and other aspects. From the fifteen responders in the survey on the same publication, which were risk professionals in major hospitals in Brazil and the USE, we see that cyberattacks were ranked as the principal risk by the participants, followed by sentinel events and risks associated with human capital management (organizational culture, use of electronic medical records and physician wellness).

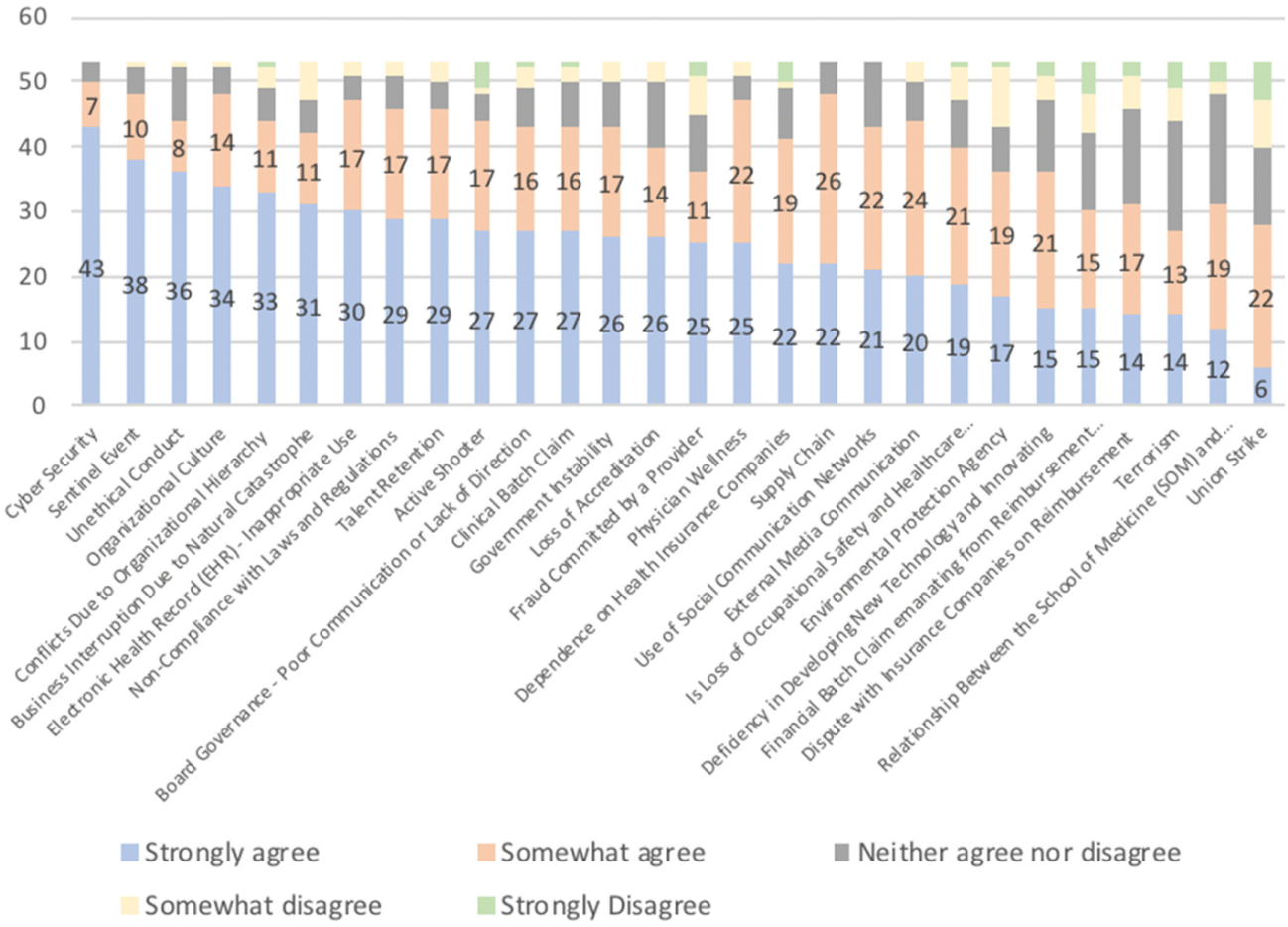

Figure 8: Highly ranked categories based on the perceived level of the risk importance

A comprehensive list of cyber-attacks and risk scenarios in the healthcare ecosystem is presented in [ISE2016] and shown graphically as Patient centered attack model in Figure 9. The authors define three attack surfaces that are shown in concentric circles around the patient.

Figure 9: A Patient Attack Model (**[ISE16]**)

The Primary attack surfaces are those vulnerabilities within a healthcare facility that, if exploited, could directly affect the patient, such as the active medical devices that directly interface with the patient (e.g. insulin pumps). If these are affected then they can deny or modify treatment, or even cause harm to the patient. The same holds true for other actors in the primary attack surface such as surgery equipment/systems and the physicians: any fault in this surface can severely hurt the patient, affect her treatment, or the medical history. The secondary attack surface does not harm directly the patient but can be (mis)used to support attacks against the primary attacks surface. Here we have passive medical devices, such as health monitors or sensors that inform or alert the clinical stuff about the patient’s status, the electronic health records, test results, etc. Compromising these interfaces can lead to incorrect treatment, corruption of the information stored, false medical events, etc. Finally, the tertiary attack surface includes financial and administration systems, inventory systems, power infrastructure, etc. that can have big impact to the hospital / organization as a whole, and of course indirectly to the patients.

As an example, for the secondary and tertiary attack, ransomware is quite probably the most popular cyber-attack hospitals face today. Usually the scenario is similar to the following:

- Attackers gain access to the hospital information systems using various methods, either through some physical means (e.g. a USB stick), exploitation of vulnerable and expired software, phishing or malicious emails.

- After gaining access (or subverting a user to their intended actions) they use a special virus that holds the system hostage by encrypting the data it contains. Therefore, it becomes completely inaccessible and unusable until hackers are paid a ransom.

- The successful attack on a hospital’s information systems and infrastructure through these means has a strong impact on the hospital’s operation. Indeed, if the data storage becomes inaccessible the availability of the systems is severely affected, and usually the hospitals do not have other choice than to pay the ransom.

This and other attacks, such as the “traditional” theft of information are frequent in the health domain but also elsewhere alike. Nevertheless, recent advances in biotechnology provide new attack surfaces. For example, authors in [Ney2017] were able to synthesize DNA strands that, after sequencing and post-processing, generated a file; when used as input into a vulnerable program, this file yielded an open socket for remote control. The term “cyberbiosecurity” is introduced by [Murch18] to cover a range of novel cyber-attack scenarios in life and medical sciences, at the interface of cybersecurity, cyber-physical security and biosecurity. In the overview found in [Peccoud18] a range of biosecurity risks are listed (see Figure 10):

- Bioinformatics databases could be corrupted by altering sequences or annotations. These changes could delay a research program or result in the uncontrolled production of toxic products or infectious agents.
- Tampering electronic orders or interception of shipments could result in the injection of nefarious products that compromise the operation of a facility.
- Computer-controlled processes are vulnerable to discrepancies between the physical parameters of the process and the data reported to the operator.
- Discrepancies between the physical characteristic of the product and test data could delay a research program or regulatory approval.

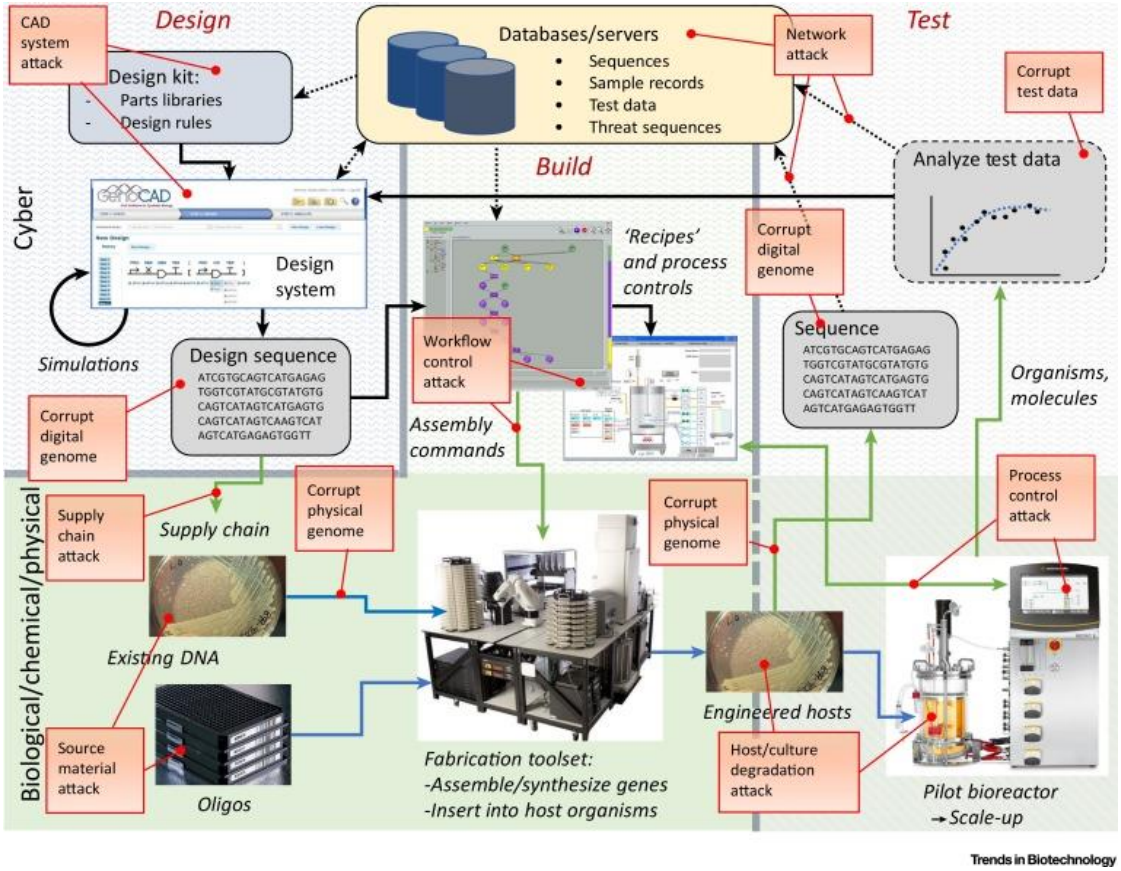

Figure 10: Potential attacks in biotechnology workflows (adapted from [Peccoud18])

The impact and the severity of these new (or re-targeted) attacks have been evaluated in a recent publication [Millett19], where thirteen individuals from the cybersecurity and biotech sector responded to a short questionnaire. The most notable cyber scenarios identified are:

- The theft, elimination or ransom of data, algorithms, or software with a direct or indirect impact on R&D or commercial operations;
- Modification of data, algorithms, or software with a direct or indirect impact on research and development or commercial operations;
- The loss of intellectual property or commercial advantage by data, algorithms, or software being available to competitors;
- Potential for the disabling or disruption of important systems or infrastructure leading to disruption of commercial operations or impeding good manufacturing practices;
- Manipulation of bio-manufacturing or automated systems to create risks.

All participants agreed that cyber-biosecurity risks are a real threat with no proper mitigation and management within the biotech sector.

6.5 Current cyber-security approaches

Today technical cybersecurity countermeasures are used to protect the confidentiality, integrity, and availability of data and information systems – especially in the healthcare domain. There is a wide array of such products available and it is important that all critical infrastructure organizational structures to add additional security measures, removing unneeded services, hardening systems, and limiting access (i.e. Virus Scanners, Antivirus components, privacy mechanisms, secure Multipurpose Internet Mail Extensions/Privacy Enhanced Mail, Secure Shell, Secure Electronic Transmission, Terminal Access Controller Access Control System, Kerberos, SSL, Transport Layer Security, Secure RPC (S/RPC), IPSec, Point-to-point Tunneling Protocol (PPTP), Challenge Handshake Authentication Protocol (CHAP), WAP/WEP and many more).

Today we can identify the following countermeasures types: Hi-Tech (electronic systems), Lo-Tech (physical security elements), and No-Tech (security elements that have no technology). These three must be used in combination to create a layered and effective security architecture.

Hi-Tech systems serve to automate repetitive monitor continuously without error, and report to and facilitate communication and coordinated response by security staff. They are used to handle vast amounts of information that could never be handled cost-effectively by humans.

Lo-Tech are usually among the most cost-effective security measures any organization can employ, including such things as Locks and Barriers, Lighting, Fencing, Signage and Other Physical Barriers (Territorial Reinforcement, Natural Surveillance, Natural Access Control). Lo-Tech elements are effective because in most cases they represent a single one-time investment that works daily without fail.

No-Tech elements can be described as:

- Comprehensive Risk Analysis and Assessment
- Policies and Procedures
- Cybersecurity Guard Programs
- Awareness and Training

No-Tech elements are the parts of security that users notice most.

Electronic healthcare information management systems are widely used today. The security of such systems, when used inside a healthcare infrastructure, is vital and has been studied extensively today. Today the innovation strives from mixing Hi-Tech, Lo-Tech, and No-Tech countermeasures to achieve an effective and cost-effective security framework using each element’s strengths and avoiding as much as possible its weaknesses. Below we try to provide some insight on how to model this situation.

In [OLAYEMI16], a threat security model is studied for identifying the threats and possible counter measures for authentication and authorization control. This threat model was the outcome of a procedure that guarantees the integrity, availability and confidentiality of health records. The procedure involves using STRIDE threat modelling tool to identify potential threats which were then ranked with respect to the amount of risk they pose to the system based on scores calculated using DREAD; a threat-risk rating model. The result is a collection of identified and rated threat in order of decreasing risk. The goal of this work is a threat rating model by information system security professional, leading to the development of secure systems and provide a guide to the order in which vulnerabilities should be patched in compromised existing systems.

The work of [Strielkina18] focused on certain risks for medical/health devices integrated within an infrastructure. This work presented a Markov model-set for a healthcare IoT infrastructure taking into account safety and security issues. A case study detailed attack on vulnerabilities of a healthcare IoT system.

The systematic literature review of [Ahmed18] identified top security threat and evaluated existing security techniques that may be used to combat this attack and specifically examined their applicability in IoT and Multi-Cloud based e-Healthcare environment. They observed that policy-based solutions for privacy concerns

actually exist but none of them specifically caters the Malicious Insiders threat in the integrated IoT and Multi-Cloud based e-Healthcare environment. Thus, this is a wide-open area for research. They found that it is necessary and critical to a Policy-based Framework in order to limit the malicious insiders’ threat particularly for IoT based Multi-Cloud e-Healthcare organizations as solutions based on policies are proved to be easily implemented and most effective in securing the important information.

Another interesting review from [Cherdantseva16] assesses the Supervisory Control and Data Acquisition (SCADA) systems. This work indicates that despite the large number of risk assessment methods for SCADA systems that exists there is still room for further research and improvements. In fact, it identifies that cybersecurity risk assessment methods for SCADA systems can be improved in terms of (1) addressing the context establishment stage of the risk management process, (2) overcoming attack- or failure orientation, (3) accounting for the human factor, (4) the capturing and formalisation of expert opinion, (5) the improvement of the reliability of probabilistic data; (6) evaluation and validation, and (7) tool support.

Finally, a lot of literature has been identified in terms of threat modelling of Electronic Health Systems and Mitigating Countermeasures. In [Alhassan16], a threat security model was proposed from identified threats and possible counter measures for authentication and authorization control. Their threat model was developed through a procedure that guarantees the integrity, availability and confidentiality of health records using STRIDE to identify potential threats which were then ranked with respect to the risk based on DREAD; a threat-risk rating model. The outcome is that the resulting threat rating model can be used as a guide to the order in which vulnerabilities should be patched in compromised existing systems. A similar approach to extract relative results was used for the case of IoT [Adebayo16].

6.6 Internet of Things: security aspects

Healthcare is a vast ecosystem, making applications for the Internet of Things in healthcare to be endless. Much like smart devices have infiltrated into spaces IoT has today taken hold of healthcare. The ambition is to create an Internet of Medical Things-IoMT ecosystem able to empower patient/citizens in their daily care activities and make them feel safer and be healthier, and also to improve how physicians deliver care as well. IoMT — networked medical devices and applications in healthcare IT — has the potential to change future strategies for healthcare organizations adding a new layer of possible benefits affecting diagnostics, treatments and in general patient health management in such a critical infrastructure area. The big caveat though in healthcare, is that like in any such environment, more connected devices means a larger attack surface, making security breaches to be a significant challenge for healthcare organizations – where security is not optional. This section is about the identification of IoT/ IoMT security methods for health care where conventional security mechanisms do not directly suit. We describe many of the constraints in terms of security for hardware (memory, computational and energy constraints, as well as tamper resistant packaging), software (embedded software constraint and dynamic security patch) and networking (mobility, scalability, multiplicity of devices, multiplicity of communication medium, multi-protocol networking, and dynamic network topology). We identify new constrains for future to come networking technologies (i.e. 5G) and will try to explain how resilient network services (i.e. DTN) for critical mHealth applications can ensure not only reliability of transmissions for smart things, but also security on different platforms and systems. The goal of this area of research is to establish a well-established security strategy to anticipate and prevent potential threats, and bridge any gaps across operations. At the core of this effort we must create a robust technology that can orchestrate electronic services and management of data ensuring security and privacy of all connected devices in a vast ecosystem. Finally, we will discuss the initiatives healthcare organizations need to take in order to manage and secure their environments.

The Internet of Things (IoT) is able to permeate our daily lives, providing important measurement and collection tools to inform our every decision. Millions of sensors and devices are continuously producing data and exchanging important messages via complex networks supporting machine-to-machine communications and monitoring and controlling critical smart-world infrastructures.

The Internet of Medical Things is a critical piece of the healthcare digital transformation that aims to act as building block in the development of cyber-physical smart pervasive frameworks able to support healthcare services. The goal is to use IoMT to better enable the management of a disease and the mindset and behavioural changes of the stakeholder for decreasing healthcare cost while increasing the health outcomes. At the same time, it defines new business models to enable changes in processes, productivity improvements, cost containment and enhanced user experiences.

The adoption of this technology into healthcare is arduous, and it requires planning and implementation. Healthcare organizations are vulnerable to modern trends and security threats. A system study on the issue of *Cybersecurity in healthcare* tried to identify cybersecurity trends, including ransomware, and identify possible solutions by querying academic literature[28]. The analysis, done in 2017, revealed that in fact healthcare industry lags behind in security. It need to clearly define cybersecurity duties, establish clear procedures for upgrading software and handling a data breach, use VLANs and deauthentication and cloud-based computing, and to train their users not to open suspicious code.

Another focused study in 2019, on the state of research concerning cyberattacks against hospitals and available best practice recommendations revealed that despite the growing interest in the research field, the available literature remains limited. There are important aspects of cybersecurity as well as specific medical fields - relying on various medical devices - neglected. This work identified six domains of research: context and trends in cybersecurity (27.8%), connected medical devices and equipment (29.9%), hospital information systems (14.4%), raising awareness and lessons learned (6.2%), information security methodology (15.4%), and specific types of attacks (6.2%) [Argaw18].

The rapid growth in the availability and incorporation of digital technologies and devices in healthcare creates extraordinary opportunities but brings with it unique challenges [Filkins16]. In healthcare connected devices are appealing targets for hackers for multiple reasons [Coventry18]:

- Healthcare organizations have many devices connected to their network and there can be gaps in their security
- Hospital security systems can overlook personal IoT devices brought in and out by patients, families and staff
- IoT devices for healthcare contain valuable Personally Identifiable Information (PII) and Personal Health Information (PHI), which can be exploited for profit

In a survey published by HIPAA Journal, 89% of healthcare executives said they have suffered a security breach resulting from adopting IoT, while 49% said malware is an issue.[14] One recent study sponsored by several major universities found poor information security practices among doctors, nurses and hospital IT staff, while another report published in Threat Post found many hospitals are failing to protect critical computer systems that can be manipulated by hackers. Healthcare organizations confront a unique challenge when it comes to information security. They are “systems of systems” with huge arrays of connected devices, including those that are sanctioned (purchased for patient care) and unsanctioned (personal devices with varying levels of security). This situation creates multiple entry points to the network, making central management difficult and creating a wide attack surface for cybercriminals.

Another survey notes that 90% of world's data generated over last two years making the requirement of robust security control for healthcare a necessity[29]. Cyber security flaws in medical devices could be detrimental for

[28] https://pdfs.semanticscholar.org/d937/adfdae8887a01541a662e1e6aa90086dcf6f.pdf
[29] https://www.medidata.com/en/blog/digital-health-in-remote-patient-monitoring/

the patients, creating problems such as instructing an infusion pump to overdose a patient with drugs or forcing a heart implant to deliver a deadly jolt of electricity/ PricewaterhouseCoopers study report $30billion annual cost hit to the U.S. healthcare system due to inadequate medical-device interoperability for data transfer[30]

The reasons to target IoMT devices could be summarized to the following facts:

- IoT devices can use only a limited versions of general purpose OS, embedded Linux and Android (short list…)
- Some devices – DO NOT SUPPORT a SECURITY client
- Manufacturers do not concern or include a security expert in the development process of the device
- IoT devices can be – on purpose BYOD – be transferred to a network that then can be infected and then the attacker can easily gain access to greater resources
- IoT devices are usually always on!
- An IoT device vulnerability most propably will propagated to all devices from a single manufacturer ("create once use many times strategy to meet market demands)

As an example, we need to mention *Mirai Botnet***.** A malware that exploits security holes in IoT devices, and has the potential to harness the collective power of millions of IoT devices into botnets, and launch attacks. In September 2016, the authors of the Mirai malware launched a DDoS attack on the website of a well-known security expert. A week later they released the source code into the world, possibly in an attempt to hide the origins of that attack. This code was quickly replicated by other cybercriminals, and is believed to be behind the massive attack that brought down the domain registration services provider, Dyn, in October 2016.[31]

Mirai was able to scan the Internet for IoT devices that run on the ARC processor. This processor runs a stripped-down version of the Linux operating system. If the default username-and-password combo is not changed, Mirai was then able to log into the device and infect it. It stills poses as one of the most dangerous thread since it is mutating and after its original creation the source code lives on. It has given birth to variants such as the Okiru, the Satori, the Masuta and the PureMasuta. The PureMasuta, for example, is able to weaponize the HNAP bug in D-Link devices. The OMG strain, on the other hand, transforms IoT devices into proxies that allow cybercriminals to remain anonymous. There is also the recently discovered - and powerful - botnet, variously nicknamed IoTrooper and Reaper, which is able to compromise IoT devices at a much faster rate than Mirai. The Reaper is able to target a larger number of device makers, and has far greater control over its bots.

As a recommendation IoMT devices should: Use best current software practices; Follow security & cryptography best practices; Be restrictive rather than permissive in communicating; Continue to function if Internet connectivity is disrupted or if cloud-backend fails; Support addressing and naming best practices; Ship with a privacy policy that is easy to find and understand; Disclose rights to remotely decrease IoT device functionality; IoT device industry should consider a cybersecurity program; IoT supply chain should play their part in addressing security & privacy issues.

In this section using the BIBLIOMETRIX tool (An R-tool for comprehensive science mapping analysis) [32] we were able to find and analyse most important papers as they were included in the webofscience directory. From these we selected the most cited ones and we briefly present them below.

[30] www.computing.co.uk/ctg/opinion/2390029/security-threats-of-connectedmedical-devices#
[31] https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/
[32] http://www.bibliometrix.org/

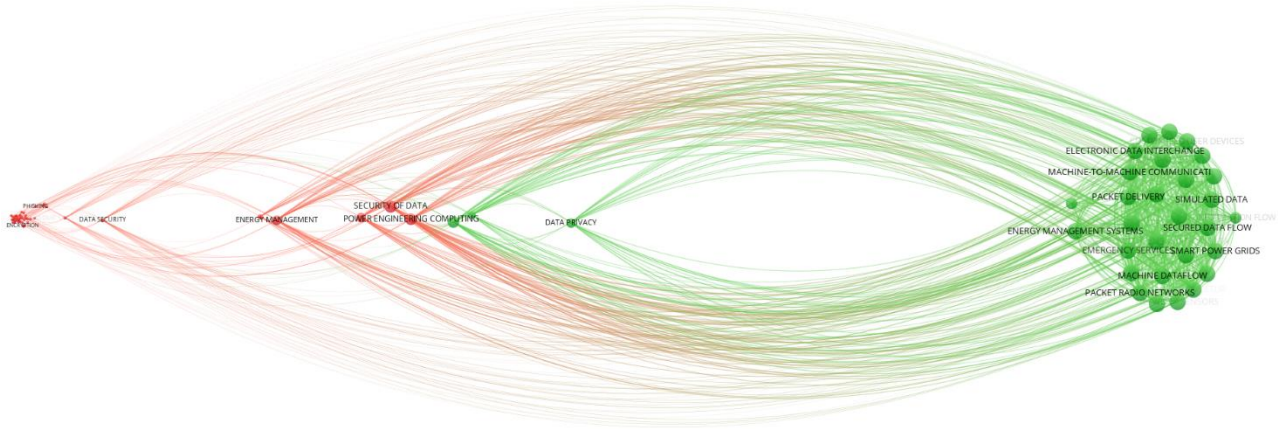

Figure 11: Cybersecurity & IoT & IoMT & healthcare as appears in the literature

The work of [Babiceanu16] provides a review of the current status of virtualization and cloud-based services for manufacturing systems and of the use of Big Data analytics for planning and control of manufacturing operations. Based on their findings they propose a framework for the development of predictive manufacturing cyber-physical systems that include capabilities for attaching to the Internet of Things, and capabilities for complex event processing and Big Data algorithmic analytics.

The paper of Chen 2016 introduces an adaptive and scalable trust management framework able to support service composition applications in SOA-based IoT systems. They explain the technical details for the development of a technique based on distributed collaborative filtering to select feedback using similarity rating of friendship, social contact, and community of interest relationships. This adaptive filtering technique is used to determine the best way to combine direct and indirect trust dynamically in order to minimize convergence time and trust estimation bias in the presence of malicious nodes performing opportunistic service and collusion attacks. This work clearly demonstrates the effectiveness of the proposed trust management through service composition application scenarios with a comparative performance analysis against EigenTrust and PeerTrust.

Today the IoT needs a strategy to mitigate the escalation of resource congestion, and edge computing is the emerging technology that is expected to solve any IoT localized computing needs that IoT faces. This is rather important in the healthcare domain where many efforts now exist in order to make all medical/healthcare devices transmission resilient to errors and network disconnection[33]. Edge computing essence is about migrating data computation or storage to the network ‘‘edge,’’ near the users forming a distributed structure of medical network that can balance traffic and avoid the peaks in IoMT networks, reducing the transmission latency between edge/cloudlet servers and end users, as well as reducing response times for real-time IoT applications in comparison with traditional cloud services.

In the paper of [Yu17], a comprehensive survey, analysing how edge computing improves the performance of IoT networks is presented. More than that many security issues that emerge are discussed trying to evaluate availability, integrity, and the confidentiality and propose a framework for security evaluation of IoT networks with edge computing.

[33] daphne.ics.forth.gr

Zhang in [Zhang18] is arguing on the fact that data security and user privacy concerns in eHealth have not been adequately addressed. It describes the flaws of ciphertext-policy attribute-based encryption not from a cybersecurity prism but also from a user acceptance and services limitation prism and proposes a privacy-aware s-health access control system, in which the key ingredient is a large universe CP-ABE with access policies partially hidden. In PASH, attribute values of access policies are hidden in encrypted SHRs and only attribute names are revealed.

From the above examples (mentioned) we can see that all the work that has been done so far is clustered. Below we see a conceptual map using the authors’ keywords and multiple correspondence analysis and Porter’s algorithm. PANACEA for healthcare is exactly focusing on how to bridge distributed research for healthcare.

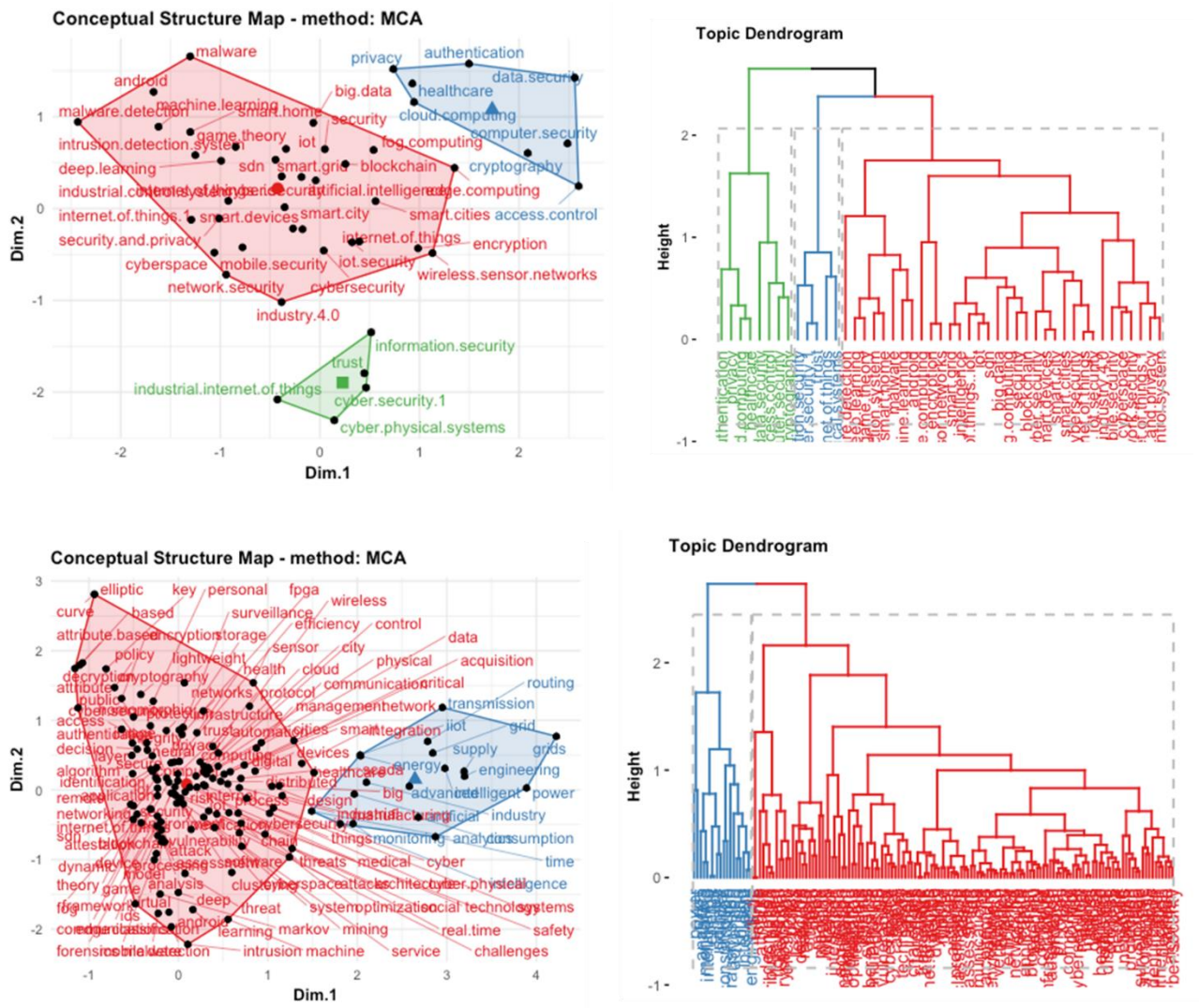

Figure 12: Conceptual map results when using keywords and multiple correspondence analysis and Porter’s algorithm

Apart from the literature on the various research outcomes and existing work we need also to mention other efforts from a policy makers and EU organization where the focus is on diagnosing cyber threats inside a hospital. In 2016 ENISA published a study that sets the scene on information security for the adoption of IoT

in Hospitals[34]. In this study through a risk-based approach a number of threats and vulnerabilities, analyses attack scenarios, as well as maps of common good practices were identified. The goal was to identify the risk and estimate the cost of a possible cyber security incidents in hospitals to show the necessity for assessment and protection in this critical infrastructure.

As a conclusion the report recommended the following that are highly accepted as the ground truth for healthcare organisations

- provide specific IT security requirements for IoT components and implement only state of the art security measures
- identify assets and how these will be interconnected
- Device manufacturers should incorporate security into existing quality assurance systems and involve healthcare organisation from the very beginning when designing systems and services.

ENISA through the EU Cybersecurity act will be the mediator and the EU Agency for Cybersecurity responsible to enforce a common cybersecurity framework to the companies’ products. This certification framework that will allow the emergence of tailored certification schemes for specific categories of ICT products, processes and services including the area of healthcare (see section 7.6.1).

[34] https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

7. Vulnerability and threat modelling

In the present era, security has become a fundamental issue in efficient and proper functioning of computer and network systems. Attackers routinely break into systems and in response, software vendors started providing security as a necessary feature for their products and network systems. As a result of years of research, many powerful techniques have been developed to solve a wide array of security problems. To prevent and mitigate a system, it is important to understand how different threats could damage a network system [Shostack14].

Systems security engineering is concerned with identifying security risks, requirements and recovery strategies. It involves well defined processes through which designers develop security mechanisms. Ideally, security engineering should be incorporated into the system design process as early as possible, preferably from the initial architecture specification, if possible. The earlier security concerns are addressed, the less time consuming and costly it is to fix future security problems [Shostack14].

Therefore, before developing a secure network, it is important to analyse the risk a network could be exposed to, including the level of damage an attack could cause to a system. The possible threats must be identified and be determined as which aspect of security would be violated by a certain attack, prior to establishing a network [Shevchenko]. Furthermore, it can’t be possible to use network layer protection (firewall, SSL, IDS, hardening) to stop or detect application layer attacks.

Most systems face a variety of threats, and more are being added constantly as technology changes. Threats can come from outside or within enterprises, and their impact, sometimes, has the potential to be devastating. The systems may not work properly, or sensitive information may be leaked, which would affect consumer confidence in the system provider. To prevent threats from taking advantage of system flaws, threat modelling methods can be used to adopt a defensive strategy [Shostack14].

There are various ways to identify and prioritize threats. A process of recognizing, measuring, and investigating potential threats of a system is called Threat Modelling.

Threat Modelling is considered the fundamental approach in identifying security weakness in software applications during the design phase in Software Development Lifecycle process. Various techniques have been published including STRIDE, Attack Tree, and Attack Library. Organizations tend to lean towards a single technique to perform their modelling exercise. Each of these techniques is weighed down by limitations, hence when implemented individually impacts the effectiveness and comprehensiveness of the exercise. However, in order to achieve meaningful output it is imperative to use each of these techniques appropriately to the corresponding activity in the threat modelling exercise.

In this section, we will provide a review of the most common approaches to threat modelling and vulnerability identification, classification, evaluation and assessment. These approaches are general enough to be adopted as basic building block in the healthcare domain (where some of them like STRIDE as already been applied – cfr. Section **Error! Reference source not found.**). In particular, Section **Error! Reference source not found.** will introduce what is an attack library by providing a list of them, while sections **Error! Reference source not found.** and **Error! Reference source not found.** will describe the most used vulnerability scoring and different types of threat modelling techniques, respectively. Section 7.4 focuses on specific threats in the healthcare domain while Section 7.5 details some formalism and frameworks that can be used to share and communicate threats.

7.1 Attack Libraries

An attack library is a useful tool for finding threats against a complex system – by constructing an indexing (library) service that may include many sets of attack tools (i.e. proof of concept, fully developed, theoretical). An attack library is thus a collection of attacks for finding threats against a specific application, organization or infrastructure. In other words, attack libraries are very useful tools to help you to defend your infrastructure. On the other hand, a threat library is an indexing (library) service that employees various threat modelling techniques to identify threats – that could be potentially used by an attacker.

In this case the idea is to provide as much details as possible for an attack type (for example code injection) to help threat modelers or the developer community to understand the landscape of threats. Any threat modelling technique adopting the attacker’s perspective is more of a checklist model, i.e., traverse the library of attacks applicable in the context of the application, analyse whether the threats are handled, and identify countermeasures.

There are many different ways to construct an attack library. You could collect sets of attack tools; either proof-of-concept code or fully developed (“weaponized”) exploit code can help you understand the attacks. Such a collection, where no modelling or abstraction has taken place, means that each time you pick up the library, each participant needs to spend time and energy creating a model from the attacks.

Today, such collections can be very useful for both attackers and security agents in order to guard a system against already collected knowledge (i.e. attack threat/attack checklists). When building an attack library, people have to make some trade-offs, so each library is designed to address a different scope. In the following we summarize the main three criteria that people take into account when building a new one:

- Audience: It refers to the people that are targeted by the library. In the following section we will see that high-level libraries like STRIDE (threat models) are not targeting the same audience that the Common Vulnerabilities and Exposure (CVE) which is specifically focused on vulnerabilities. Therefore, the library is depending from a strategic, tactical or operational level of a company it targets.
- Level of detail: It can go from very detailed to very abstracted. Both abstraction and a high level of details have advantages and drawbacks. A high level of abstraction makes easier to build a very structured library with clear categories, while a very detailed library makes it harder.
- Scope: It defines in which domain the library is useful. For instance, when considering Common Weakness Enumeration (CWE) it is only useful to gain knowledge over software weakness.

In the following, we will provide an overview of the main existing attack libraries, to better understand how they are structured and what they contain analysing them through the three criteria specified above.

7.1.1 OWASP Top Ten

Open Web Application Security Project (OWASP) is an online community working on Web application security. The philosophy behind it is to be both free and open to all. It has the purpose and scope to publish Web security recommendations and offer Internet users, administrators and companies’ reference methods and tools to control the level of security of its Web applications [Shostack14].

Periodically they release a list of the top ten web application vulnerabilities to educate developers and security professionals about the most important web application security weakness and its consequences [Krishnan17]. For each of these vulnerabilities, OWASP provides detailed threat agents, attack vectors, security

weaknesses, technical impact, business impact, countermeasures, and examples of attack scenarios. The last version of the top ten is the 2017 which is an update of the version 2013 (Figure 13).

OWASP Top 10 - 2013		OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Figure 13: The new 2017 classification and the old version of 2013

Lastly, we consider the three criteria for the OWASP Top Ten. The audience for this library is only IT persons. The library offers both a high level of detail and a way to go deeper for the developers. However, the scope is quite limited, since it only offers threats against web applications.

7.1.2 CAPEC

The Common Attack Pattern Enumeration and Classification (CAPEC) effort provides a publicly available catalogue of common attack patterns along with a comprehensive schema and classification taxonomy [Shostack14].

Attack patterns are descriptions of common methods for exploiting software systems. It describes how adversaries exploit weakness in applications and other cyber-enabled capabilities [CAPEC]. These patterns also help to categorize the attacks and teach the development community to better understand and effectively defend against the attacks. The CAPEC open database is maintained by the MITRE corporation, an American not-for-profit organization that supports some governmental agencies. MITRE also maintains other libraries, the Common Vulnerabilities and Exposures that we will discuss later [CAPEC].

CAPEC are well structured with a total of 519 attack patterns grouped into 9 (Figure 14) mechanism of attacks (version 3.1). CAPEC provides exhaustive details about the attacks : summary of attack, attack execution flow, attack prerequisites, typical severity, typical likelihood of exploit, methods of attack, examples - instances, attacker skills or knowledge required, resources required, probing technique, indicators - warnings of attack, solution and mitigation, attack motivation - consequences, injection vector, payload, activation zone, payload activation impact, security requirements, CIA impact, and technical context [Krishnan17].

Figure 14: Main attack categories of CAPEC taxonomy

Any organization or team new to threat modelling can be overwhelmed with information and miss out on important aspects to consider. Even experienced threat modelers may find this method more time consuming and thus adversely affecting productivity [Krishnan17].

Regarding the audience, CAPEC is designed for security experts and developers. Indeed, it has a high number of inputs (519 detailed attack patterns). When it comes to the level of details it is pretty high and in fact CAPEC provides a high quantity of knowledge over attack patterns. Finally, the scope of the CAPEC library is usually the application domain and more generally computer systems.

7.1.3 CWE

Common Weakness Enumeration (CWE) is a formal list of software weaknesses created by MITRE in order to [Krishnan17]:

- Serve as a common language for describing software security weakness in architecture, design, or code.
- Serve as a standard measuring stick for software security tools targeting these weaknesses.
- Provide a common baseline standard for weakness identification, mitigation, and prevention efforts.

As per version 3.3 there are in total 1140 CWEs which can be grouped based on various criteria (by research concepts, by development concepts, by architectural concepts). Each of the primary clusters have secondary clusters. Like CAPEC, the primary cluster is to categorize software weakness for better understanding. Details provided in each CWE include: description, applicable platform, common consequences, demonstrative example, observed examples, and related attack patterns [CWE].

The CWE provides the various weaknesses that may be exploited by malware and can be used to understand the attack and also determine the impact and malware behaviour. Figure 15 depicts a portion of the CWE structure; the red boxes represent the CWEs that are being used by the National Vulnerability Database (NVD) [Ulicny].

The CWE library is based on the same structure of the CAPEC library, meaning that there are three views which give people the different point of view to access the library. In addition, in the CWE library people can find many examples of code that would create a weakness in the software. The audience is clearly developers and security practitioners for the same reason than CAPEC. The level of details is really high with pieces of code, examples and advices. Finally, the scope of this library is software weaknesses, not covering any potential hardware weakness [CWE].

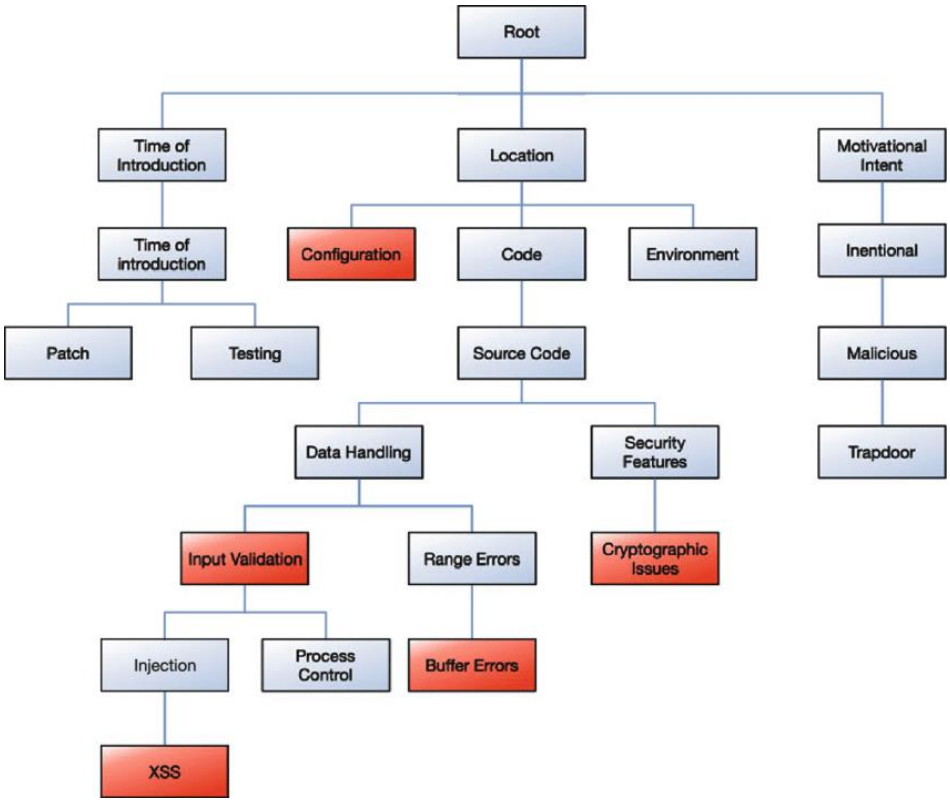

Figure 15: Portion of the structure of the common weakness enumeration

7.1.4 CVE and NVD

Common Vulnerabilities and Exposure is a dictionary of public information about security vulnerabilities (software and hardware). The purpose of this library is to list a maximum of the known vulnerabilities. This library has no specific structure except that each entry is identified by a CVE identifier. They are references of the form CVE-YYYY-NNNN where YYYY is the year of publication and NNNN is an identified number. Each reference is generated and attributed by MITRE.

CVE-ID	
CVE-2019-9969	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
XnView Classic 2.48 on Windows allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted file, related to xnview+0x385399.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• MISC:https://code610.blogspot.com/2019/03/crashing-xnview-248.html	
Assigning CNA	
MITRE Corporation	
Date Entry Created	
20190323	Disclaimer: The entry creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Figure 16: Example of a CVE entry

The contents of the CVE dictionary can be downloaded and at the time of writing it contains 119435 vulnerabilities. Each CVE is defined by a brief description of the vulnerability concerned, as well as a set of links that users can view for more information. The level of details concerning the vulnerability that can be

found in a CVE entry really depends on the links that are attached to this vulnerability [CVE]. We can see in the Figure 16 that for each entry there is a link to NVD database.

National Vulnerability Database is a U.S. Government vulnerability library product by the National Institute of Standards and Technology (NIST). NVD is based on the CVE dictionary. Each time a new CVE entry is published, the NIST analyses the CVE based on the description, references supplied and any supplemental data that can be found publicly at the time (version of the vulnerable software, status of the vulnerabilities, etc).

Each new entry in NVD has a score between 0 and 10. It is calculated based on the Common Vulnerability Scoring System (CVSS) that we will see later, considering both version 2 and version 3. It results in a more complete and more exploitable database than the basic CVE library.

Analysing CVE and NVD libraries through the three criteria, we can state that only experts can understand and used these libraries. Indeed, they are really specific to security vulnerabilities and contains many technical details. However, the level of details depends on the supplied references. Some of them are provided only by the brief description and other with all the complete CVSS score and other references to exploit it. Generally, the most important feature of these two libraries is that their scope is both software and hardware vulnerabilities [NVD].

7.2 Vulnerability scoring: CVSS

Nowadays, IT management must identify and assess vulnerabilities across many disparate hardware and software platforms. They need to prioritize these vulnerabilities and remediate those that pose the greatest risk. However, since there are so many to fix, and each being is scored using different scales, IT managers have to convert this amount of vulnerability data into actionable information.

In order to address this issue, the presence of a Common Vulnerability Scoring System is required. It offers the following benefits:

- Standardized Vulnerability Scores: In this way if an organization normalizes vulnerability scores across all of its software and hardware platforms, it can leverage a single vulnerability management policy.
- Open Framework: having a well-defined structured score, anyone can see the individual characteristics used to derive a score for a particular vulnerability, knowing exactly which properties gave it that score and having the possibility to compare with another one.
- Prioritized Risk: When an environmental score is computed, that is, capturing characteristics of a vulnerability that are associated with a IT environment, it represent the actual risk to an organization. Users know how important a given vulnerability is in relation to other vulnerabilities.

7.2.1 CVSS

The Common Vulnerability Scoring System (CVSS) is a method that “captures the principal characteristics of a vulnerability, and produces a numerical score reflecting its severity” [FIRST18, FIRST07, NVD].

Research by the National Infrastructure Advisory Council (NIAC) in 2003/2004 led to the launch of CVSS version 1 (CVSSv1) in February 2005, with the goal of being "designed to provide open and universally standard severity ratings of software vulnerabilities". This initial draft had not been subject to peer review or

review by other organizations. In April 2005, NIAC selected the FIRST to become the custodian of CVSS for future development.

CVSS offers the following benefits [FIRST18]:

- **Standardized Vulnerability Scores:** When an organization normalizes vulnerability scores across all of its software and hardware platforms, it can leverage a single vulnerability management policy.
- **Open Framework:** Users can be confused when a vulnerability is assigned an arbitrary score. “Which properties gave it that score? How does it differ from the one released yesterday?” With CVSS, anyone can see the individual characteristics used to derive a score.
- **Prioritized Risk:** When the environmental score is computed, the vulnerability now becomes contextual. That is, vulnerability scores are now representative of the actual risk to an organization. Users know how important a given vulnerability is in relation to other vulnerabilities.

The CVSS provides users of the method with a common and standardized scoring system within different cyber and cyber-physical platforms. A CVSS score can be computed by a calculator that is available online [FIRST07].

CVSS is composed of three metric groups: **Base**, **Temporal**, and **Environmental**, each consisting of a set of metrics [FIRST18]. These metric groups are described as follows:

- **Base**: represents the intrinsic characteristics of a vulnerability that are constant over time and across user environments. It is composed of two sets of metrics: Exploitability metrics and the Impact metrics. The Exploitability metrics reflect the ease and technical means by which the vulnerability can be exploited. That is, they represent the characteristics of the thing that is vulnerable, which we refer to formally as the vulnerable component. On the other hand, the Impact metrics reflect the direct consequence of a successful exploit and represent the consequence to the thing that suffers the impact, which we refer to formally as the impacted component.
- **Temporal**: reflects the characteristics of a vulnerability that may change over time but not across user environments. For example, the presence of a simple-to-use exploit kit would increase the CVSS score, while the creation of an official patch would decrease it.
- **Environmental**: represents the characteristics of a vulnerability that are relevant and unique to a particular user’s environment. These metrics allow the scoring analyst to incorporate security controls which may mitigate any consequences, as well as promote or demote the importance of a vulnerable system according to her business risk.

The purpose of the CVSS base group is to define and communicate the fundamental characteristics of the vulnerability. This objective approach to characterizing vulnerabilities provides users with a clear and intuitive representation of a vulnerability. Users can then invoke the temporal and environmental groups to provide contextual information that more accurately reflects the risk to their unique environment. This allows them to make more informed decisions when trying to mitigate risks posed by the vulnerabilities.

Figure 17: CVSS v2.0 Metric Groups

Feedback from vendors utilizing CVSSv1 in production suggested there were "significant issues with the initial draft of CVSS". Work on CVSS version 2 (CVSSv2) began in April 2005 with the final specification being launched in June 2007. Further feedback resulted in work beginning on CVSS version 3 in 2012, ending with CVSSv3.0 being released in June 2015. In the following, we will discuss the number of changes between CVSSv2.0 and CVSSv3.0.

Figure 17 and Figure 18 show the set of metrics for each metric group, considering respectively CVSS v2.0 and CVSS v3.0 [FIRST18, FIRST07].

When the Base metrics are assigned values by an analyst, the Base equation computes a score ranging from 0.0 to 10.0.

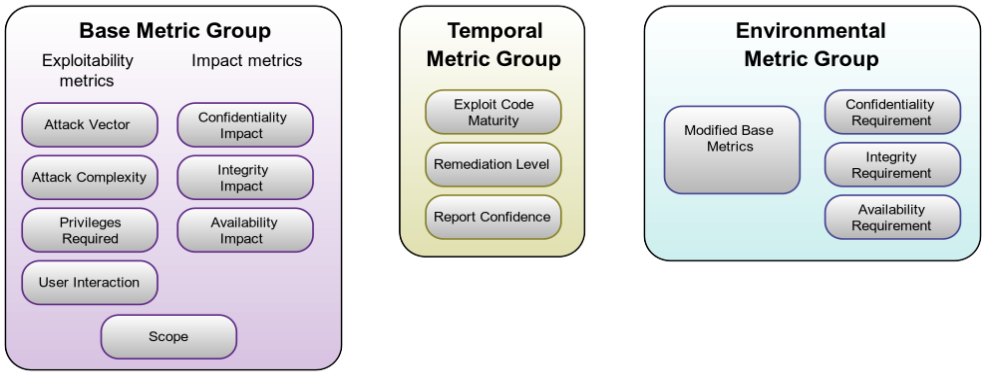

Figure 18: CVSS v3.0 Metric Groups

CVSS v3.0

The newer version of CVSS introduces a number of changes in the scoring system that reflect more accurately vulnerabilities that fall under the web application domain. The table below presents the main differences of the versions of CVSS with respect to the Base Metric Group [Doynikova17, Komarkova18].

	CVSS 2.0	CVSS 3.0	Comments
Exploitability Group	Access Vector	Attack Vector	Determines how the vulnerability is exploited. Besides the name, in version 3.0 the physical access is separated to specific value.
	Access Complexity	Attack Complexity	Describes the conditions beyond the attacker’s control that must exist in order to exploit the vulnerability. Besides the name, in version 3.0 it no longer takes into account interaction with the user (added separately).
	Authentication	Privileges Required	Describes the level of privileges an attacker must possess before successfully exploiting the vulnerability. In version 3, Authentication is substituted by Authentication, and the value of this index takes the minimum value if one does not need any privileges.
	N/A	User Interaction	Determines whether the vulnerability can be exploited solely at the will of the attacker, or whether a separate user (or user-initiated process) must participate in some manner.
Impact Group	Confidentiality	Confidentiality	Measures the impact to the confidentiality of the information resources managed by a software component due to a successfully exploited vulnerability. In version 3.0 Partial value is changed to Low and Complete to High.
	Integrity	Integrity	Measures the impact to integrity of a successfully exploited vulnerability. Integrity refers to the trustworthiness and veracity of information. In version 3.0 Partial value is changed to Low and Complete to High.
	Availability	Availability	Measures the impact to the availability of the impacted component resulting from a successfully exploited vulnerability. In version 3.0 Partial value is changed to Low and Complete to High.
	N/A	Scope	Is the ability for a vulnerability in one software component to impact resources beyond its means, or privileges. Formally, Scope allows to separate the affected component (the component that contains the vulnerability, for example, a software module, driver, etc.) from a component that is damaged (software, hardware, or network resource)

Table 7: Differences between CVSS v2.0 and CVSS v3.0

The important feature of CVSS is the fact that the characterization of vulnerabilities should be obvious to any expert and unambiguous. A number of uncertainties arising from the application of format version 2.0 has been fixed in the new version 3.0. The most important difference of the new format is that was additionally added

index Scope. The importance of it is due to the fact that in version 2.0 it was no clear to what the Impact caused by the vulnerability refers.

On the basis of performed analysis we concluded that the use of CVSS of version 3.0 will eliminate many of the ambiguities that existed previously, although not all of them. Furthermore, at the moment, primarily because of the lack of the description of the complete list of the vulnerabilities using the CVSS of version 3.0, it is impossible to consider this standard for an automatic application. In fact, the CVSS method is often used in combination with other threat modelling methods [Doynikova17].

7.3 Threat models

In the present era, security has become a fundamental issue in efficient and proper functioning of computer and network systems. Attackers routinely break into systems and in response, software vendors started providing security as a necessary feature for their products and network systems. As a result of years of research, many powerful techniques have been developed to solve a wide array of security problems. To prevent and mitigate a system, it is important to understand how different threats could damage a network system [Shostack14].

Systems security engineering is concerned with identifying security risks, requirements and recovery strategies. It involves well defined processes through which designers develop security mechanisms. Ideally, security engineering should be incorporated into the system design process as early as possible, preferably from the initial architecture specification, if possible. The earlier security concerns are addressed, the less time consuming and costly it is to fix future security problems [Shostack14].

Therefore, before developing a secure network, it is important to analyse the risk a network could be exposed to, including the level of damage an attack could cause to a system. The possible threats must be identified and be determined as which aspect of security would be violated by a certain attack, prior to establishing a network [Shevchenko]. Furthermore, it can’t be possible to use network layer protection (firewall, SSL, IDS, hardening) to stop or detect application layer attacks.

Most systems face a variety of threats, and more are being added constantly as technology changes. Threats can come from outside or within enterprises, and their impact, sometimes, has the potential to be devastating. The systems may not work properly, or sensitive information may be leaked, which would affect consumer confidence in the system provider. To prevent threats from taking advantage of system flaws, threat modelling methods can be used to adopt a defensive strategy [Shostack14].

There are various ways to identify and prioritize threats. A process of recognizing, measuring, and investigating potential threats of a system is called Threat Modelling.

Threat modelling is also known as Architectural Risk Analysis. Threat modelling involves identifying the possible threats and rating them based on their risk factors. Modelling methods are used to create an abstraction of the system. Such abstraction contains profiles of potential attackers, including their goals (in terms of assets) and methods, and a catalogue of potential threats that may result [UcedaVelez15]. Proper identification of threats and appropriate selection of countermeasures reduces the ability of attackers to misuse the system. In that respect, threat modelling looks at the system from an adversary’s perspective to help designers anticipate attack goals and determine answers to questions about what the system is designed to protect, and from whom. Any type of system can benefit from threat modelling.

There many threat modelling methods that have been developed. However, not all of them are comprehensive. Some of them focus on the abstraction and encourage granularity while others are more people-centric. Other methods focus specifically on risk or privacy concerns. Methods can be combined to create a more robust and well-rounded view of potential threats.

In conclusion, to best use threat modelling, it should be performed early in the development cycle. This means that potential issues can be caught early and remedied, preventing a much costlier fix down the line. Thinking about security requirements with threat modelling can lead to proactive architectural decisions that allow for threats to be reduced from the start [Myagmar05].

Xiong et al [Xiong19] presents the first systematic literature review on threat modelling. They collected 176 articles without overlap from the four leading databases (IEEE Xplore, Scopus, Springer and Web of Science). Articles were classified into three clusters and 122 of them were removed from further consideration when manually screened. The final 54 articles were classified three clusters to better categorize them.

The main findings of this work are that, threat modelling is a diverse field lacking common ground, and the definitions are numerous and used in many different ways. Also, the threat modelling work remains to be done manually, which can be time-consuming and error-prone. Moreover, the form of threat modelling is flexible (graphical, formal, qualitative, quantitative), sometimes with a focus on being general and other times more specific, and validation methods are of varied types.

Occasionally, some systematic reviews that focus upon “threat modelling” as a keyword, may miss articles that are using the same technique but refer to it by a different name, e.g., attack/defence trees, attack graphs, and graphical modelling for security.

Within PANACEA, we will accurately analyse the existing models to inherit relevant concepts while designing an innovative set of system, threat and attack reference models. In particular, we will focus the analysis on existing tools for threat modelling that model threats by relying on the knowledge and expertise of security operators. As an example, the self-direction principle of OCTAVE (see 7.3.10) means that people inside the organisation are in the best position to lead the evaluation and make decisions. Moreover, for PANACEA project we will focus on attack graphs as threat modelling, considering it as an input for one of the technical tools, DRMP (Dynamic Risk Management Platform).

In the following we will present the most used threat modelling methods. They come from a variety of sources and target different parts of the process. We can state that no one threat modelling method is recommended over another; the decision of which method(s) to use should be based on the needs of the project and its specific concerns.

7.3.1 STRIDE and its Derivations

STRIDE is currently the most mature threat modelling method. Invented by Loren Kohnfelder and Praerit Garg in 1999 and adopted by Microsoft in 2002, STRIDE represents a mnemonic for six different types of security threats [Shostack06]. STRIDE analyses vulnerabilities against each system component which could be exploited by an attacker to compromise the whole system (see Figure 19).

STRIDE uses a general set of known threats based on its name, STRIDE, which stands for Spoofing identity, Tampering with data, Repudiation, Information disclosure, Denial of service, and Elevation of privilege (see Table 8 for threat type definitions.). This acronym can be used as a mnemonic for discovering threats while navigating the system’s model created in phase one.

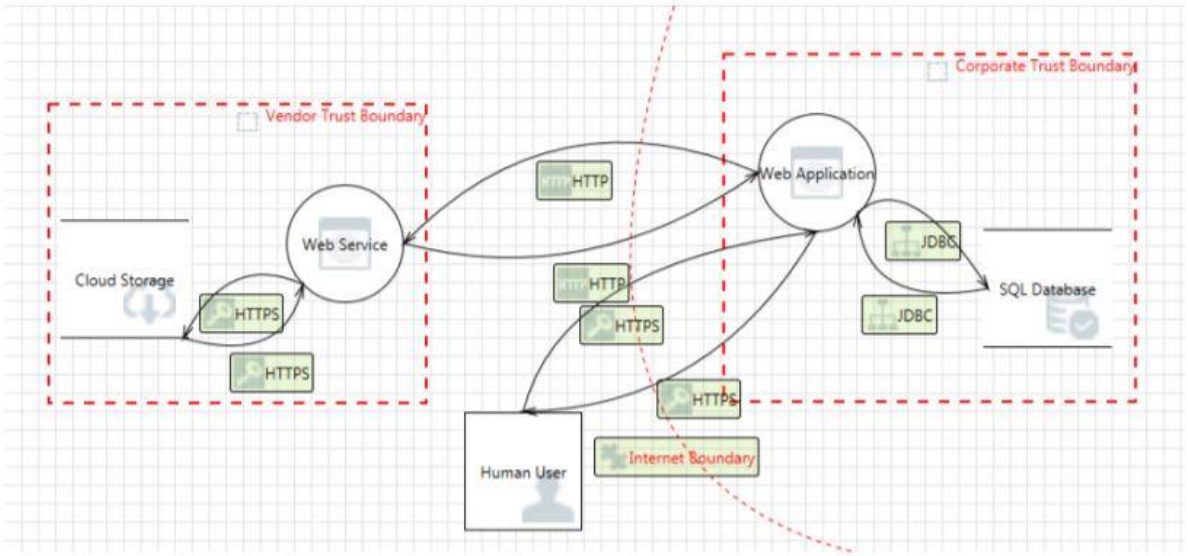

Figure 19: Example of a Data Flow Diagram with System Boundaries

Using STRIDE, the classification of threats is done by categorizing the kind of exploit by attacker or intruder. Furthermore, because it covers numerous attacks and is a simpler yet comprehensive approach for threat identification, STRIDE is considered the most widely used method for analysing the threat level. [Khan17b].

Following the STRIDE model, starting from S and ending at E gives a dense sense of direction as well as a definitive pattern to form a model which covers almost all the possible threats which may occur to a network or computer. STRIDE has evolved over time to include new threat-specific tables and the variants STRIDE-per-Element and STRIDE-per-Interaction [Shostack14, Ma16, Khan17a].

STRIDE-based threat modelling can be performed in two possible ways [Shostack14]:

i. STRIDE-per-element: STRIDE-per-element is more complex as it analyses behaviour and operations of each system component. However, it may not be sufficient to identify certain threats that are not evident from the data flow diagram (DFD). In certain scenarios, threats show up in the interactions between system components.
ii. STRIDE-per-interaction: STRIDE-per-interaction therefore enumerates threats against system interactions by considering tuples (origin, destination, interaction). Comparatively, STRIDE-per-interaction is easier to perform, and its protection strategies are normally enough to protect system (as cyber-attacks normally involve malicious interactions between system components).

STRIDE evaluates the system detail design in different steps. The goal of step one is to model the in-place system. By building data flow diagrams (DFDs), you identify system entities, events, and boundaries of the system [Shostack06]. Accurate DFDs dictate how successful your STRIDE will be. However, using DFDs as the only input to threat modelling is limiting because it does not provide a means for representing security-related architectural decisions [Sion18].

	Threat	Property Violated	Threat Definition	Example
S	Spoofing Identity	Authentication	Pretending to be something or someone other than yourself	Ahmed pretending to be Khalid.
T	Tampering with data	Integrity	Modifying something on disk, network, memory, or elsewhere	Modifying a packet as it goes over the network.
R	Repudiation	Non-repudiation	Claiming that you didn’t do something or were not responsible; can be honest or false	“I didn’t login to your email account"
I	Information disclosure	Confidentiality	Providing information to someone not authorized to access it	Allowing a student to read other students grades and GPA etc.
D	Denial of service	Availability	Exhausting resources needed to provide service	Blocking the internet access to legitimate user by sending numerous packets at once over the network
E	Elevation of privilege	Authorization	Allowing someone to do something they are not authorized to do	Allowing a distant internet user to run commands, but going from a limited user to admin is also EoP

Table 8: STRIDE Threat Categories

The goal of step two is to find threats. To help in this step, some sources offer checklists and tables that assist in describing threats, property violations, typical victims, and what an attacker does. After gathering discovered threats and mitigation strategies, this information should be documented and prioritized [Shostack08].

Despite this method is easy to adopt, it can be time consuming [Shostack14]. STRIDE’s main issue is that the number of threats can grow rapidly as a system increases in complexity. In fact, STRIDE method has a moderately low rate of false positives and a moderately high rate of false negatives [Scandariato15]. STRIDE has been successfully applied to cyber-only and cyber-physical systems.

Even though Microsoft no longer maintains STRIDE, it is implemented as part of the Microsoft Secure Development Lifecycle (SDL) with the Threat Modelling Tool, which is still available [Microsoft]

Several authors represent modified STRIDE methods. Martins et al., in their presentation *Towards a Systematic Threat Modelling Approach for Cyber-Physical Systems*, use the STRIDE method with NIST guidelines instead of Microsoft security mediation strategies [Scandariato15].

7.3.2 DREAD

Microsoft developed another similar method called DREAD, which is also a mnemonic with a different approach for asset:

- Damage potential (How much are the assets affected?)
- Reproducibility (How easily the attack can be reproduced?)
- Exploitability (How easily the attack can be launched?)

- Affected users (What’s the number of affected users?)
- Discoverability (How easily the vulnerability can be found?)

It assigns one of three values (0, 5, 10) to the first four categories and one of four values (0, 5, 9, 10) to the last category, which “allows for an average value to be calculated to represent the risk of the entire system” [Potteiger16, Kotonya98].

7.3.3 PASTA

The Process for Attack Simulation and Threat Analysis (PASTA) is a risk-centric threat framework developed in 2012 by Tony UcedaVélez [UcedaVelez15]. Risk centric has the objective of mitigating what matters. Essentially, it covers the answer to the question “If there is little to no impact, why spend time/ money on security?”.

The PASTA process is designed to integrate with security engineering and risk management process including security incident response and vulnerability management process that are used by most business today. The main objective of PASTA is to help organizations to engineer applications and systems that are resilient to targeted cyber attacks such as Distributed Denial of Service (DDoS) and malware automated/botnet based attacks.

At high level the PASTA process consists of several activities performed at each of the seven stages of the process that are outlined in Figure 20.

Figure 20: PASTA Stages

The main goals of PASTA process are:

- Improving visibility of cyber-threat risks: by providing risk management and information security with a holistic view of the company assets and the risk exposure from the perspective of the attackers/threat actors.
- Extending the organization protection domains: the compliance domain is considered as a factor in documenting security requirements, but PASTA focuses beyond the traditional compliance driven security domains by focusing on cyber threats as today compliance driven security controls can be bypassed by advanced and emerging threats.
- Leveraging existing application security processes: PASTA stages and activities leverage data and processes used today for traditional security compliance assessments such as vulnerability assessment, security tests/ pen testing and secure code analysis but widen the focus to threats and attacks.
- Integrating with the SDLC by providing an application threat modelling process that organizations can follow to address security issues from the inception of the software development lifecycle to the production delivery.
- Increasing the maturity of the organization in software security by evolving from vulnerability assessments to threats and attack analysis as the drivers for determining the risk mitigation strategy.

PASTA aims to unify business objectives and technical requirements. In each stage it uses a variety of design and elicitation tools. For example, high-level architectural diagrams are used during stage two for identifying the technical scope. DFDs are used in stage three. During stage six, attack trees and use and abuse cases are built for analysis and attack modelling.

This method elevates the threat modelling process to a strategic level by involving key decision makers and requiring security input from operations, governance, architecture, and development].

Despite being widely regarded as a risk-focused framework, PASTA has a hacker-focused perspective. In fact, the process produces an asset-centric output in the form of an enumeration of threats and scores [Shostack14].

7.3.4 LINDDUN

LINDDUN is a privacy threat modelling methodology that aids the analyst in the elicitation of privacy threats. It is a model-based approach, as the methodology requires a data flow diagram (DFD) as representational model of the system to analyse. This DFD will serve as basis for the analysis, as each of its elements will be examined thoroughly for privacy threats. The methodology is also knowledge-based as it provides an overview of the most common attack paths associated with a set of privacy threat categories [Wuyts15].

Similar to STRIDE, this method is a mnemonic, meaning the threat categories in question are coded in the method name: Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, Non-compliance [Shevchenko].

The attack paths are represented as threat trees that detail possible causes of threats that are related to the main threat categories and are specific to a particular DFD element type (entity, data flow, data store, or process).

LINDDUN provides systematic support to elicit and mitigate privacy threats. It starts with a DFD of the system that defines the system’s data flows, data stores, processes, and external entities. Systematically iterating over all model elements and analysing them from the threat categories point of view, LINDDUN users identify a threat’s applicability to the system and build threat trees [Deng11].

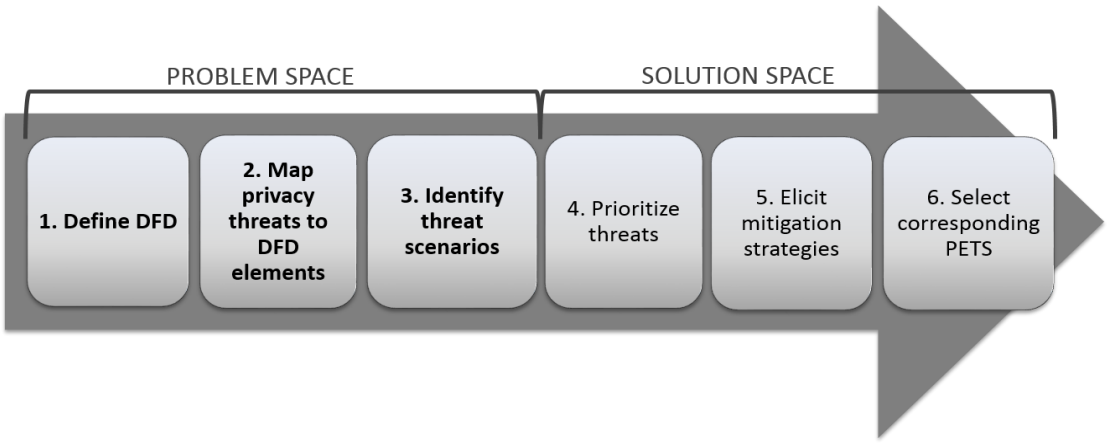

Figure 21: LINDDUN Methodology Steps

Figure 21 summarizes the six main steps of the LINDDUN methodology. The first three steps are situated in the problem space, as they focus on identifying the threats in the system [Scandariato14]. In particular, Steps 2 and 3 are essentially questionnaires that guide the user through the initial analysis process of identifying the threats in the system. Step 2 involves mapping threat categories to the parts of the system where they may appear. Step 3 involves identifying scenarios in which these threats could occur. The remaining three steps are solution-oriented, as they aim at resolving the threats that were identified [Shevchenko, Wuyts18].

The strength of LINDDUN is its systematic approach in guiding the analyst through the privacy assessment exercise effort, combined with its extensive privacy knowledge base. However, the LINDDUN method is labour intensive and time consuming. It suffers from the same issues as STRIDE: the number of threats can grow rapidly as a system increases in complexity. In the presentation Effective and Efficient Privacy Threat Modelling Through Domain Refinements, Wuyts et al., noticed that efficiency and effectiveness of the method is negatively impacted by generically applicable threats [Wuyts18].Persona non Grata

Persona non Grata (PnG) is a threat modelling method that focuses on the motivations and skills of human attackers. It represents archetypal users who behave in unwanted, possibly nefarious ways [Shevchenko].

Modelling PnGs can help us to think about the ways in which a system might be vulnerable to abuse and use this information to specify appropriate mitigating requirements. The PnG approach makes threat modelling more tractable by asking users to focus on attackers, their motivations, and abilities. Once this step is completed, users are asked to brainstorm ideas about targets and likely attack mechanisms that the attackers would deploy [Cleland-Huang14].

The theory behind this approach is that if engineers can understand what capabilities an attacker may have, and what types of mechanisms they may use to compromise a system, the engineers will gain a better understanding of targets or weaknesses within their own systems and the degree to which they can be compromised. Some critics of this approach argue that a PnG can often take users down the wrong path. For example, for a system related to national security, users might reason that the system may be the target of a sophisticated attack from another nation state [Mead17].

PnG is easy to adopt but is rarely used or researched. It produces fewer false positives and has high consistency but tends to detect only a certain subset of threat types. This technique fits well into the agile approach, which incorporates personas [Schevchenko18].

7.3.5 Security Cards

Security Cards is a technique that has the goal to identify unusual and complex attacks. It is not a formal method but more of a brainstorming technique. This technique makes use of a deck of cards (see Figure 22), with which the analysts can answer questions about an attack, such as “by whom?” “why might the system be attacked?” “what assets are of interest?” and “how can these attacks be implemented?” [Denning13].

Human Impact	Adversary’s Motivations	Adversary’s Resources	Adversary’s Methods
• the biosphere • emotional well-being • financial well-being • personal data • physical well-being • relationships • societal well-being • unusual impacts	• access or convenience • curiosity or boredom • desire or obsession • diplomacy or warfare • malice or revenge • money • politics • protection • religion • self-promotion • world view • unusual motivations	• expertise • a future world • impunity • inside capabilities • inside knowledge • money • power and influence • time • tools • unusual resources	• attack cover-up • indirect attack • manipulation or coercion • multi-phase attack • physical attack • processes • technological attack • unusual methods

Figure 22: Security Cards Dimensions

The deck contains 42 cards to facilitate threat discovery activities categorized as follows: Human Impact (9 cards), Adversary’s Motivations (13 cards), Adversary Resources (11 cards), and Adversary’s Methods (9 cards) [Denning13, Mead17].

Security Cards activities help identify almost all of the threat types but produce a high number of false positives and are better used to address non-standard situations. Also, this method is rarely used in industry [Schevchenko18].

7.3.6 hTMM

The Hybrid Threat Modelling Method (hTMM) was developed by the Software Engineering Institute in 2018. Unlike what we have seen so far, it consists of a combination of SQUARE (Security Quality Requirements Engineering Method), Security Cards, and PnG activities [Mead].

The targeted characteristics of the method include no false positives, no overlooked threats, a consistent result regardless of who is doing the threat modelling, and cost-effectiveness. The following are the main steps of the method [Mead, Mead18]:

- Identify the system you will be threat modelling.
- Apply Security Cards based on developer suggestions.
- Once this data has been collected, you will have enough information to prune those PnGs that are unlikely or for which no realistic attack vectors could be identified.

- Summarize the results using tool support.
- Once this is done, you can continue with a formal risk assessment method, using these results, and the additional steps of a security requirements method such as SQUARE, perhaps tailoring the method to eliminate steps you have already accounted for in the threat modelling exercise.

7.3.7 Quantitative Threat Modelling Method

Like hTMM, also this hybrid method is given by the union of other threat modelling methods. In fact, it consists of Attack Trees, STRIDE, and CVSS methods applied in synergy. It was introduced during the HotSoS2 conference in Pittsburgh, PA in April 2016 by Bradley Potteiger, Goncalo Martins, and Xenofon Koutsoukos. The authors aimed to address a few pressing issues with threat modelling for cyber-physical systems that had complex interdependencies among their components [Schevchenko18].

The first step of the Quantitative Threat Modelling Method (Quantitative TMM) is to build component attack trees for the five threat categories of STRIDE. This activity shows the dependencies among attack categories and low-level component attributes. After that, the CVSS method is applied and scores are calculated for the components in the tree.

An additional goal for the method is to generate attack ports for individual components. These attack ports (effectively root nodes for the component attack trees) illustrate activities that can pass risk to the connected components. The scoring assists with the process of performing a system risk assessment. If an attack port is dependent on a component root node with a high-risk score, that attack port also has a high-risk score and has a high probability of being executed. The opposite is also true [Potteiger16].

7.3.8 Trike

Trike is a unified conceptual framework for security auditing from a risk management perspective through the generation of threat models in a reliable, repeatable manner. Trike was created in 2005and as other methods, starts with defining a system. This method can be used by a security auditing team to completely and accurately describe the security characteristics of a system from its high-level architecture to its low-level implementation details. Trike also enables communication among security team members and between security teams and other stakeholders by providing a consistent conceptual framework [Saitta05].

As a result of the previous step, an actor-asset-action matrix can be created, where the columns represent assets, and the rows represent actors. Each cell of the matrix should be divided into four parts, one for each action of CRUD (creating, reading, updating, and deleting). In these cells, the analyst should assign one of three values: allowed action, disallowed action, or action with rules.

One benefit of this tool is the ability to integrate both software centric and attack centric approaches by autonomously generating attack graphs based off of the requirements model and implementation model input [Potteiger].

However, the Trike scale system seems too vague to represent a formal method. Unfortunately, Trike version 2.0 is not well maintained, and there is no documentation, even though its site is up and running [Schevchenko18].

7.3.9 VAST

VAST (Visual, Agile and Simple Threat modelling) method was created by Anurag Agarwal and is based on ThreatModeler, an automated threat modelling platform. The fundamental value of this method is the scalability and usability that allow it to be adopted in large organizations throughout the entire infrastructure to produce actionable and reliable results for different stakeholders [Beyst16].

In fact, among all threat modelling methodologies, the only one that supports enterprise-wide scalability is VAST. It is unique considering a specific point of view, because it is founded on the idea that threat modelling is only useful if it encircles the entire software development life cycle (SDLC), throughout the whole enterprise.

Recognizing differences in operations and concerns among development and infrastructure teams, VAST requires creating two types of models: application threat models and operational threat models. Application threat models use process flow diagrams, representing the architectural point of view. Operational threat models are created with an attacker point of view in mind based on DFDs [Shevchenko].

In general, there is no silver bullet for security operations planning, and different modelling methods may suit some businesses better than others. It’s important to understand the specific existing development, IT management and security operations processes before settling on a modelling format.

7.3.10 OCTAVE

OCTAVE, standing for *Operationally Critical Threat, Asset and Vulnerability Evaluation***,** was created in 2001 at Carnegie Mellon University for use by the U.S. Department of Defence. It is a comprehensive, risk-based assessment and planning tool for organizations looking for a framework to identify and manage risks in their information security departments [Alberts03].

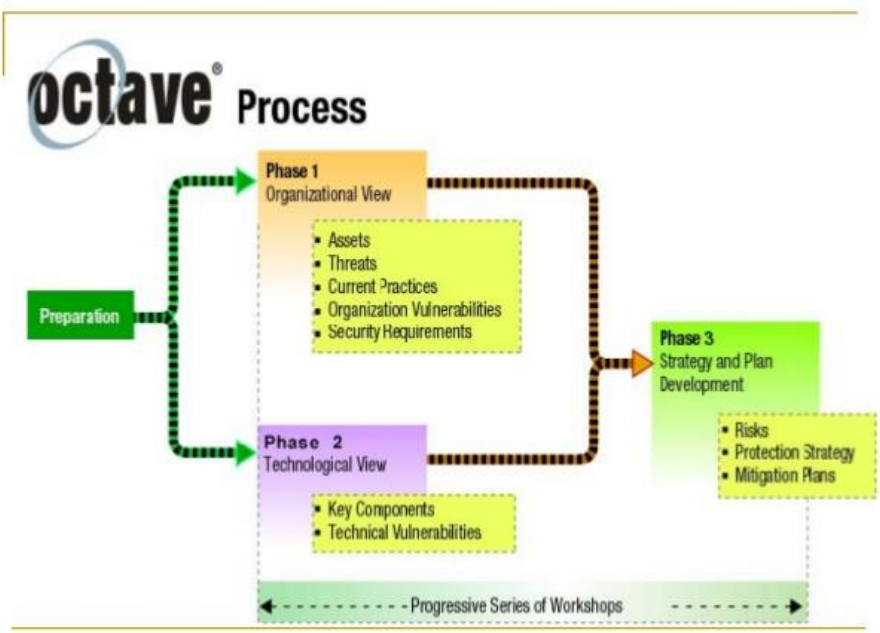

Figure 23: OCTAVE Phases

The use of OCTAVE is self-guided, that is, an organization can implement and manage the framework internally, utilizing its employees with technical expertise who have security responsibilities. Unlike the typical technology-focused assessment, which is targeted at technological risk and focused on tactical issues, OCTAVE is targeted at organizational risk and focused on strategic, practice-related issues [Alberts03].

OCTAVE method is based on eight processes that are broken into three phases (see Figure 23) [Alberts03, Alberts99, Shevchenko]:

- **Phase 1: Build Asset-Based Threat Profiles.** The two major functions of this phase are gathering information from across the organization and defining threat profiles for critical assets. This is an organizational evaluation.
- **Phase 2: Identify Infrastructure Vulnerabilities.** During this phase, the analysis team evaluates key components of systems supporting the critical assets for technological vulnerabilities. This is an evaluation of the information infrastructure.
- **Phase 3: Develop Security Strategy and Plans.** The primary purpose of this phase is to evaluate risks to critical assets and develop an organizational protection strategy and risk mitigation plans. This is an identification of risks to the organization’s critical assets and decision making.

The OCTAVE Method was primary developed for the large organizations (e.g., 300 employees or more). Large organizations generally have a multi-layered hierarchy and are often divided or geographically distributed.

As a consequence, to the addressed targets (large organizations), it was developed OCTAVE-S that is a new version tested for small organizations, ranging from 20 to 80 people. It is designed for organizations that can empower a team of three to five people to conduct all evaluation activities, without the need for formal data-gathering activities [Alberts].

The negative aspects of OCTAVE are that the process requires a significant time commitment, and the documentation is not so simple, being very large and vague. About that, there are planned updates to OCTAVE that may impact these negatives parts, but the exact effects are currently unknown [Shevchenko].

7.3.11 Attack Graphs

Attack graphs are graph-based threat models used to capture the inter-dependencies between vulnerabilities and security conditions that have been identified in a target network. Such security conditions can be, among others, the network policies instrumented on the network, such as routing tables or firewall rules.

The attack graph generation process is usually driven by a set of initial privileges that the attacker is assumed to possess at the beginning. An attack graph correlates the vulnerability exploits that can be employed by a potential attacker on the network hosts and shows the potential evolution of multi-step attacks. In particular, the eventual target/leaf nodes of a possible attack graph identify the goal privileges that the attacker aims to gain at the end.

A *full* attack graph tries to identify all possible attack paths from the initial privileges to the goal privileges, while a *partial* attack graph shows a portion of these possible attack paths (not necessarily all).

Models of attack graphs

Following a taxonomy by [Kaynar] we classify attack graph models in terms of the content of their nodes (note that there can be overlaps between the classes):

State-based Attack Graphs contain network state nodes indicating a snapshot of the target network features at a specific point on the attack graph. A state represents the presence of a specific vulnerability or product on a network host, an attacker privilege obtained on a network host, the existence of a reachability condition between any two network hosts or even the effects of the attacks on the network performance.

Vulnerability-based Attack Graphs contain vulnerability nodes which can indicate vulnerability identifiers (e.g., CVE [CVE]) or exploit descriptions/names.

Host-based Attack Graphs contain nodes representing the target network hosts. This kind of attack graphs is also commonly referred as *topological attack graphs* [Jajodia, Ingols].

Attack Scenario-based Attack Graphs contain attack scenario nodes representing coordinated attacker actions or attacker plans. They can be formed by summarizing vulnerability-based attack graphs.

Most of the past works related to attack graph generation utilize state and vulnerability nodes.

In the model introduced in [Phillips], the inputs of an attack graph include configuration files, attacker profiles, and a database of attack templates. The nodes of the attack graph correspond to nodes of attack templates instantiated with particular users and machines, whereas edges are labelled with probabilities of success or cost of attacks. Such nodes correspond to actual machine configurations on specific network nodes. \

In [Ou], a single level attack graph model is used, where each node of the attack graph represents a logical statement and the edges define the relationship between network configuration and what privileges the attacker potentially could gain. In [Ingols] the authors introduce the *multiple-prerequisite* attack graph structure. This structure models attacker privileges and reachability conditions as state nodes in the attack graph.

Graph core building method	**Attack graph model**			
	State based	Vulnerability based	Host based	Attack scenario based
Logic based	[Ou],[Ritchey], [Sheyner], [Jha]	[Ritchey], [Jha]		
Graph based	[Phillips], [Ammann02], [Ammann05], [Jajodia],[Ingols], [Wang14], [Chen], [Yigit]	[Ammann02], [Jajodia], [Wang14]	[Xie], [Amman05]	[Phillips], [Kotenko]
Other	[Sun], [Frigault], [Jun-chun]			

Table 9: Classification of related works according to the attack graph modelling choices and core building method

In [Ammann02], the attack model defines the vulnerabilities, exploits and privileges of the attacker on a host computer as its main elements, and their relations. All these definitions are encapsulated in manually-defined attack templates. The vulnerabilities and privileges serve as pre- and post-conditions for the exploits.

As an example of host-based attack graph formation, in [Ammann05] a single level attack graph model is introduced, where the nodes represent the hosts on the target network and the edges represent the highest access level that can be obtained by an attacker reaching the target hosts starting from the source hosts. Later, in [Xie], the authors propose a novel two-tiered attack graph model where the higher level is formed by host access graphs that are built using sub-attack graphs at the lower level. In [Kotenko], an attack graph model that contains a 3-tiered layered hierarchical structure is presented, composed of atomic attack instances (low level), attack purposes and stages constituting attack scenarios (mid-level), and combination of attack scenarios (high level).

Core-building phase

Depending on the specific model considered (and on the granularity of information), nodes and edges in such graphs might refer to different information, and this directly affects the complexity of the attack graph core building process, i.e., the core algorithm used to construct the attack graphs. In this phase, some of the possible paths may also be pruned when forming the resulting attack graph. In this section, we compare the various techniques based on the main algorithmic approach used, dividing them in Logic-based and Graph-based methods.

- **Logic-based methods** form Attack paths using logic deduction methods (resolution, model checking, etc.). Network states are represented by facts and vulnerability exploits are represented by relational predicates over these facts.
- **Graph-based methods** tackle the attack graph building problem as a graph traversal problem and attack paths are created during backward, forward or bidirectional graph searches. This searching process may sometimes approach to the logic-based deduction methods, especially when attack templates containing variables indicating network security states and predicates are used, and instantiated during the search.

In Table 9 we classify all works mentioned in this section, with respect to the attack graph models described in the previous paragraph and the core building algorithm. We also consider other algorithms that do not fall into this scheme in the “Other” category.

For the Logic-based core building methods, in [Ritchey], model checking is applied to the analysis of multi-step network attacks. Known vulnerabilities on network hosts, connectivity between hosts, initial capabilities of the attacker are described as states and exploits as transitions between states. The user specifies the security conditions that are not to be reached by an attacker as a model composed of temporal logic formulas. This is given to a model checker as its input and the reachability in terms of given goal states is given as a query. The model checker then produces a counterexample if a sequence of exploits can lead to any of the goal states. The model tool is improved later in [Sheyner] to find all the counter examples to a given security condition.

In [Ou] the authors propose MulVAL (Multihost, multistage, Vulnerability Analysis), whose main focus is on the root causes of the attack. MulVAL applies logic deduction rules to get from the initial facts (initial attacker privileges on starting machines) to the goal facts representing target attacker privileges. A reasoning engine, XSB, allowing tabled execution is used for this purpose. Tabled execution aids in preventing duplicate

computation of the facts and resolving the loops in the resulting graph. Both time and space complexity are on the order of the square of the number of hosts in the network for which the attack graph is to be computed.

In [Jha], model checking is used instead to enumerate all attack paths. A modified model checker is used to take as input the finite-state machine created from network information. The model checker provides all counterexamples to a query about the safety of the goal states (i.e., all possible attack paths). The problem of finding the minimum possible attack that leads to the given goal conditions is shown to be intractable. One apparent limitation of this approach is that all attack paths are explicitly enumerated in its result, which leads to a combinatorial explosion.

For graph-based methods, [Phillips] is the first attempt proposing the concept of attack graphs, presenting a graph-based approach for generating them.

[Amman02] introduces a two-pass breadth-first search algorithm with a specific attribute marking procedure to generate the nodes of a multi-layer graph. The first step uses a node-marking technique that first links exploits by starting from the attacker’s initial state, and marks nodes to determine the termination condition of the attack. Then prunes irrelevant states by searching backwards from the goal state. A *monotonicity assumption* is introduced, to address the scalability of model checking-based approaches. It states that exploits will never cause the attacker to relinquish any previously obtained privileges. Attack paths can then be implicitly modeled as paths in a directed graph including exactly one copy of each exploit and its pre- and post-conditions; edges interconnect exploits to their pre- and post-conditions. The assumption thus reduces the complexity of attack graph from exponential to polynomial in the number of hosts. However, it also makes some attacks impossible if they disable services or invalidate vulnerabilities.

Additionally in [Amman05], a graph-based method is used to generate an attack graph which shows only the worst-case attack paths to all compromisable hosts, i.e. those leading to the highest access levels that can be obtained, when attacking from a host to other hosts with a direct exploit. After that, a transitive closure on this graph is computed to reflect the effects of indirect application of the exploits. Their algorithm has a $O(n^3)$ time complexity.

In [Jajodia], the authors describe the attack-graph generation tool TVA (Topological Analysis of Network Attack Vulnerability), which assumes the monotonicity property of attacks of [Amman02], and thus has polynomial time complexity in the number of hosts. The central idea is to use an exploit dependency graph to represent the pre- and post-conditions for an exploit. Then a graph search algorithm is used to chain the individual vulnerabilities and find attack paths that involve multiple vulnerabilities.

In [Ingols] the authors introduce NETSPA (Network Security Planning Architecture), which creates a network model using firewall rules and network vulnerability scans. It then uses the model to compute network reachability and attack graphs representing potential attack paths for adversaries exploiting known vulnerabilities. This discovers all hosts that can be compromised by an attacker starting from one or more locations. For a network with n hosts, NETSPA core graph building phase has a cost of $O(n \cdot \log n)$.

Attack Trees

Attack trees provide a formal, methodical way of describing the security of systems, based on varying attacks. Using attack trees to model threats is one of the oldest and most widely applied techniques on cyber only systems as well as cyber-physical and physical systems [Shevchenko].

Attacks trees were defined by Bruce Schneier to model threats against computer systems. By understanding all the different ways in which a system can be attacked, we can likely design countermeasures to thwart those attacks. Further, by understanding who the attackers are, not to mention their abilities, motivations, and goals, maybe we can install the proper countermeasures to deal with the real threats. Attack Trees provide a formal, methodical way of describing the security of systems, based on varying attacks. A tree structure is used represent attacks against a system, where the tree root is the goal for the attack, and the leaves are ways to achieve that goal. Each goal is represented as a separate tree. Thus, the system threat analysis produces a set of attack trees. Usually it takes a few iterations of decomposing the goal to build the tree (see Figure 24) [Saini08].

While examining different methods to achieve the goal, it may become obvious that this can be accomplished in multiple ways. To incorporate these different options into the tree, AND and OR nodes should be used. **OR** nodes are used to represent alternatives and **AND** nodes are used to represent different steps toward achieving the same goal. Once the tree is built, one can assign values to the various leaf nodes, then make calculations about the nodes. Once the values are assigned, one can calculate the security of the goal [Schneier01].

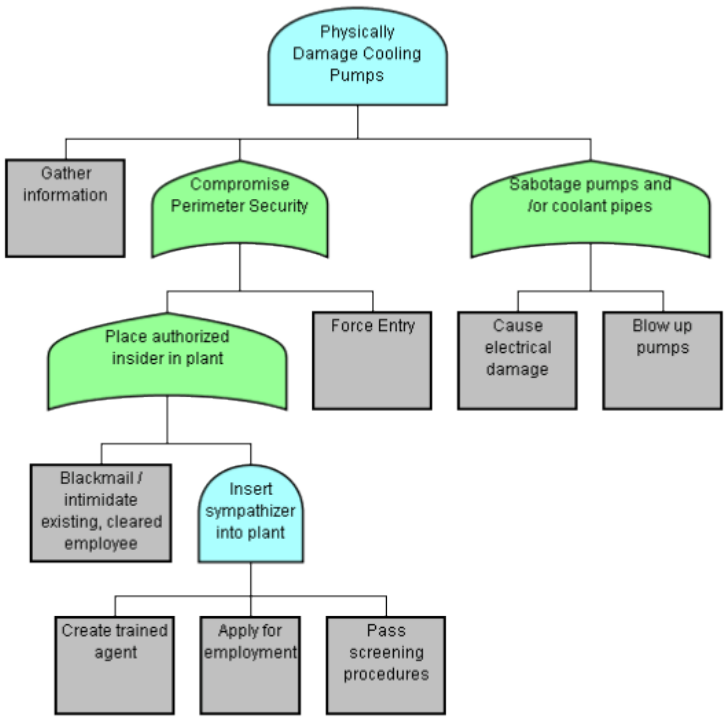

Figure 24: Attack Tree Example

Attack trees are easy to understand and adopt but are only useful when the system and security concerns are well understood. This method assumes that analysts have high experience of cybersecurity. In recent years, this method has often been used in combination with other techniques and within frameworks like STRIDE, CVSS, and PASTA [Shevchenko].

7.4 Threat modelling in healthcare

Nowadays, more healthcare providers are migrating from traditional paper-based medical record systems to EHR systems. Thus, electronic healthcare technology is prevalent around the world and creates huge potential to improve clinical outcomes and transform care delivery. However, the adoption of healthcare technology is arduous, and it requires planning and implementation time.

In the last years there are increasing concerns relating to the security of healthcare data and devices. Increased connectivity to existing computer networks has exposed medical devices to new cyber security vulnerabilities. Healthcare is an attractive target for cybercrime for two fundamental reasons: it is a rich source of valuable data and its defences is weak [Coventry18].

As already specified, EHR systems serve as information management systems for health records of patients which are various data generated from interactions between patients and medical personnel. There is a need for assurance that these records are securely protected from attacks. For a system as complex as an EHR system, the number of possible attacks is potentially very large.

Cybersecurity breaches include stealing health information and ransomware attacks on hospitals and could include attacks on implanted medical devices. In this sense, advances in mobile health (mHealth), respectively IoT-Health, are likely to reduce costs and improve the quality of healthcare.

In the case of an e-health system, a threat is any action or event that may lead to malfunction of the system and services it provides or to patient health record data disclosure or incidental such as the failure of a patient’s medical device, and that can compromise the confidentiality, integrity and availability of the system. The threats faced by EHS may lead also to the violation of privacy laws. These threats may be classified as authentication, accounting and authorization threats as generally known to other management systems such as banking and manufacturing. Securing this area of e-health involves information security and privacy as well as physical safety.

Furthermore, common legacy protocols used in medical environments often lack security and privacy aspects. [Haselhorst17] showed that the often *“HL7”* protocol has no security or privacy mechanisms specified especially in version two, which is the most deployed solution in production systems.

Given the increasing importance of cybersecurity for safe, effective, and reliable health care delivery, there is a need to provide an overview of the literature at the intersection of cybersecurity and health care. Works like [Coventry18] has defined a narrative review to explore the most interesting question from deep research about cybersecurity and healthcare. They used the PubMed database as data source to collect 1249 articles to have the right information relating to the following research questions: *Why is healthcare vulnerable? Why is healthcare targeted? What threats and consequences are healthcare currently experiencing? What is the role of legislation and standards? How can the healthcare sector move forward?*

In [Kruse17] the reviewers conducted three separated searches through CINAHL and PubMed (MEDLINE) and the Nursing and Allied Health Source via ProQuest databases. Using keywords with Boolean operators, database filters, and hand screening, they identified 32 articles that met the objective of the review. As a result, the analysis of the 31 articles showed the healthcare industry lags behind in security.

In their study [Alhassan16] proposed a threat model for Electronic health systems that captures the possible attacks that may be carried out against an EHS. They used STRIDE threat model to identify potential threats which were then ranked based on the security risk posed using a DREAD threat-risk ranking model.

Furthermore, possible countermeasures to authentication and authorization control threats on the system were discussed.

Considering different threat modelling methodology, [Almulhen11] used the attack tree as threat model to analyse attacks affecting HER systems. The analysis is based on a proposed generic client-server model of HER system. Then, the developed attack tree is discussed with some system properties that enable quantitative and qualitative analysis, also considering a list of suggested countermeasures.

The majority of works on threat modelling in healthcare is focusing on telehealth and is not paying attention to mobile health specific threats, especially if the data is stored in a cloud environment. In [Cagnazzo18] the researchers focus their activity on security challenges offering a mitigation solution especially with a focus on authentication and encryption for resource constrained devices. In particular, they identified assets in a prototyped mobile health ecosystem and classified threats with the STRIDE methodology. Furthermore, they identified associated risk levels using DREAD and there were highlighted some possible mitigation strategies in order to provide a reasonable trustworthy environment.

Future research has to focus on the exploration, exploitation and mitigation of the vulnerabilities and the correlation between security threats and patient safety. Furthermore, also the legacy protocols and standards like “*DICOM*” or “*HL7*” has to be evaluated from a security perspective. This could be done if the Common Vulnerability Scoring System is expanded by possible patient harms. Another important aspect is defining a well-defined strategy in order to perform software and firmware updates on past, current and future devices and architectures allowing them to be resilient to modern and future threats.

7.5 Cyber threats information sharing

Nowadays, cybersecurity is a complex and multifaceted problem domain and continues to become more so. Almost all systems and data are digitalized and connected using data networks forming a cyber-domain. Furthermore, the dependence on complex technology continues to grow and, at the same time, the threat environment continues to grow and evolve in dynamic and daunting ways [Kokkonen16].

Today's evolving threat environment also brings with it far more complex attack scenarios. Alongside commoditized threats, more advanced capabilities that were rare in the past are now commonplace. Adversary behaviour is not solely focused on widespread, disruptive activity, but rather it often involves more targeted, lower profile multi-stage attacks that aim to achieve specific tactical objectives and establish a persistent foothold into the enterprises [Barnum14].

Thus, it is very important to know the situation and risk level of your own assets both in civilian and military domains ad also both in public and independent organizations or individuals. Since information becomes available daily, there is a need to share some information like new product vulnerabilities with all the entities. In few words, if the awareness of threats is shared between enterprises is could be used as an early warning and preparation for new threats [Kampanakis14].

The security community has been thinking about information sharing for a long time. Multiple efforts have been made by different entities, including governments and CSIRTs over the world. In many white papers, it is stated that “information sharing is one of the most heard suggested solutions for increasing cyber resilience”. In many cases there was different collaborations among organizations for achieving better cyber resiliency, maintaining business continuity or cyber-incident response capability [Kampanakis14, Barnum14].

The information exchange should be done between devices in a machine-to-machine (M2M) level according to four phases: information collection, transmission of filtered information, analysis of information and operations executed based on the analysis [Kokkonen, Shan15].

There are numerous security data-sharing options. Even though there is considerable overlap among them, not all address the same needs. In the previous sections, we already introduced and summarized one of them. In fact, in 6.2.4 we saw CVSS, which is widely used by vendors to assess the impacts and prioritize their vulnerabilities. Another example is the Common Vulnerabilities and Exposures (CVE) that is a dictionary of public, known information security vulnerabilities used by many IT vendors to evaluate their flaws in the systems.

Mitre Corporation has developed standards called Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII) for describing and collaborating cyber threat information in a standardized and structured manner. STIX ontology-based situation assessment framework is presented in [Shan] and as a result it has been mentioned that the mechanism performed well. Both STIX and TAXII have been transitioned to OASIS Advanced open standards for the information society.

7.5.1 STIX

Structured Threat Information Expression (STIX) is a language developed in an open, collaborative forum allowing the specification, capture, characterization and communication of standardized cyber threat information. Using a structured fashion, it supports more effective cyber threat management processes and application of information.

A variety of high-level cyber security use cases rely on such information including [Barnum14]:

- Analysing cyber threats
- Specifying indicator patterns for cyber threat
- Managing cyber threat response activities
- Sharing cyber threat information

STIX provides a common mechanism for addressing structured cyber threat information across and among this full range of use case improving consistency, efficiency, interoperability, and overall situational awareness.

As specified before, STIX supports a range of core use cases involved in cyber threat management. In Figure 25 are provided some simple overviews of these use cases.

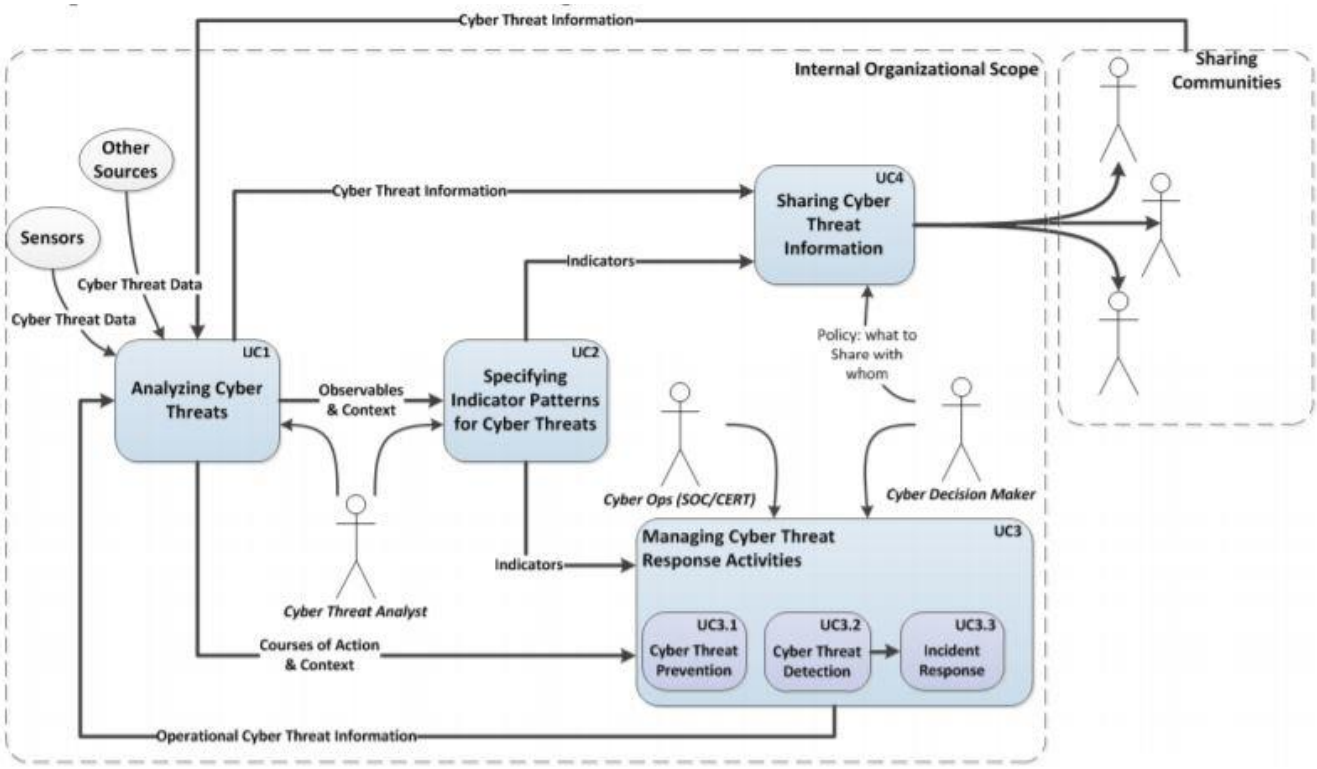

Figure 25: Core Use Cases Targeted by STIX

In this sense, STIX allows to a cyber-threat analyst to identify its use case starting from reviewing structured and unstructured information regarding cyber threat activity from a variety of manual or automated input sources. Then, the analyst seeks to understand the nature of relevant threats, identify them, and fully characterize them such that all of the relevant knowledge of the threat can be fully expressed and evolved over time. From this understanding and characterization, the analyst may then specify relevant threat indicator patterns, suggest courses of action for threat response activities, and/or share the information with other trusted parties. For example, in the case of a potential phishing attack, a cyber-threat analyst may analyse and evaluate a suspected phishing email, analyse any email attachments and links to determine if they are malicious, determine if the email was sent to others, assess commonality of who/what is being targeted in the phishing attack, determine whether malicious attachments were opened or links followed, and keep a record of all analysis performed [Barnum14].

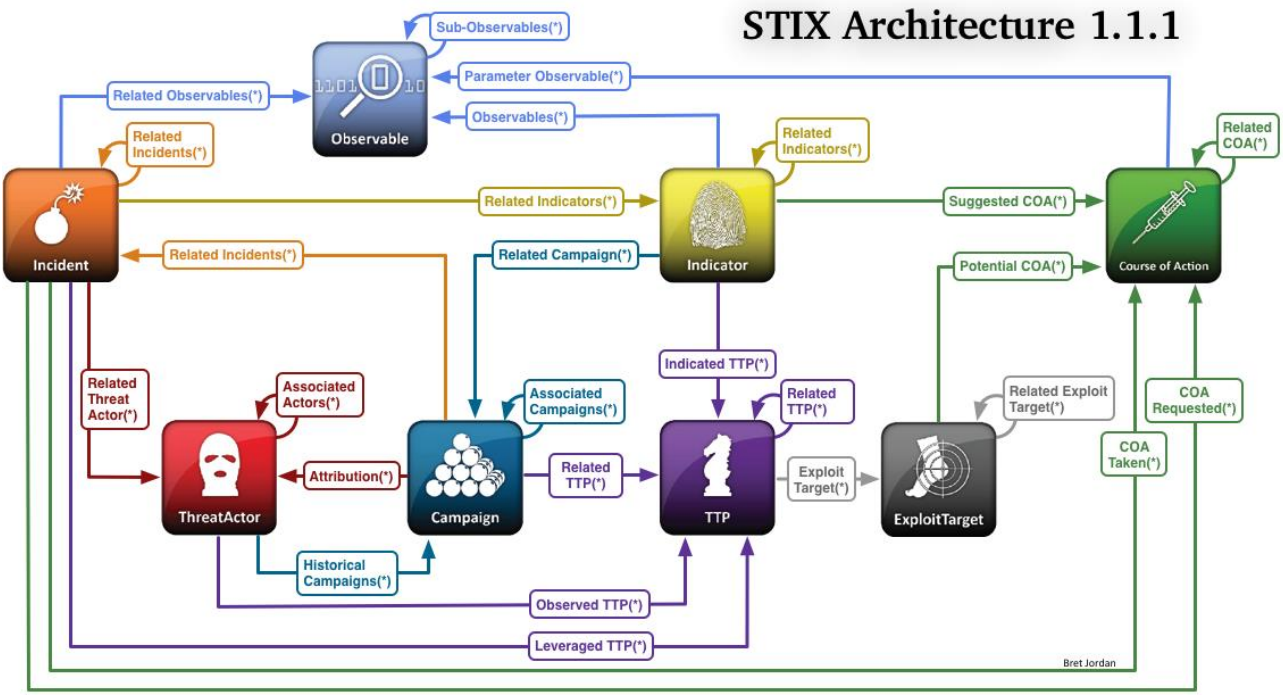

Figure 26: STIX Architecture

The STIX architecture 1.1.1 consists of eight constructs: Observable, Indicator, Incident, TTP, ExploitTarget, CourseOf Action, Campaign and ThreatActor. Table 8 will briefly characterize all of them. Figure 26 illustrates the construct interrelationships based on the inherent meaning and content of each. Connecting arrows between construct icons indicate relationships in the form of content elements within the construct at the root of the connecting arrow, that is of the conceptual type of the construct at the head of the connecting arrow and is suggested but not required to utilize the specific STIX implementation of that construct. The bracketed asterisk on each of the arrow labels represent the cardinality, that is, it implies that each relationship may exist zero to many times.

The structured content of each construct is fleshed out in detail within the language implementation. In the present STIX is at its version 2.0. The OASIS Cyber Threat Intelligence (CTI) Technical Committee (TC) decided to merge the two specifications (STIX 1.0 and STIX 2.0) into one. STIX 2.0 requires implementations to support JSON serialization, while STIX 1.x was defined using XML. Though both XML and JSON have benefits, the CTI TC determined that JSON was more lightweight, and sufficient to express the semantics of cyber threat intelligence information. It is simpler to use and increasingly preferred by developers [STIX].

The eight core constructs are: Observable, Indicator, Incident, TTP, ExploitTarget, CourseOf Action, Campaign and ThreatActor. Table 10 will briefly characterize all of them.

Construct Name	Description
Campaign	A grouping of adversarial behaviours that describes a set of malicious activities or attacks that occur over a period of time against a specific set of targets.
Observable	Stateful properties or measurable events pertinent to the operation of

	computers and networks. Information about a file (name, hash, size, etc), a registry key value, a service being started, or an HTTP request being sent are all simple examples of observables.
Indicator	Contains a pattern that can be used to detect suspicious or malicious cyber activity. Indicators convey specific Observable patterns combined with contextual information intended to represent artefacts and/or behaviours of interest within a cyber-security context.
Incident	Discrete instances of Indicators affecting an organization along with information discovered or decided during an incident response investigation.
TTP	Tactics, Techniques and Procedure (TTP) are representations of the behaviour or modus operandi of cyber adversaries. It is a term taken from the traditional military sphere and is used to characterize what an adversary does and how they do it in increasing levels of details.
ThreatActor	Individuals, groups, or organizations believed to be operating with malicious intent.
ExploitTarget	Vulnerabilities or weaknesses in software, systems, networks or configurations that are targeted for exploitation by the TTP of a ThreatActor.
CourseOfAction	An action taken to either prevent an attack or respond to an attack.

Table 10: STIX Structure

7.5.2 TAXII

The community-driven Trusted Automated eXchange of Indicator Information (TAXII), provides technical mechanisms for cyber threat information sharing that are applicable to a wide range of sharing needs yet flexible enough to accommodate existing cyber threat information sharing implementations [Connolly12, Kampanakis14].

TAXII is a set of technical specifications and supporting documentation for the secure, platform-independent exchange of high-fidelity cyber threat information. TAXII specifications are designed to enhance interoperability of different cyber security solutions rather than espouse a specific technology or product. Developed through community consensus and participation, TAXII will enable more efficient and comprehensive threat exchange through automation and the articulation of a detailed, cyber threat information model. To achieve this, TAXII utilizes a standardized cyber threat information representation and defines a supporting exchange framework [Connolly12].

TAXII supports three different threat information sharing architecture [TAXII]:

1. **Hub and Spoke** is a sharing model where one organization functions as the central clearinghouse for information, or hub, coordinating information exchange between partner organizations, or spokes. Spokes can produce and/or consume information from the Hub.

2. **Source/Subscriber** is a sharing model where one organization functions as the single source of information and sends that information to subscribers.

3. **Peer to Peer** is a sharing model where two or more organizations share information directly with one another. A Peer to Peer sharing model may be ad-hoc, where information exchange is not coordinated ahead of time and is done on an as-needed basis, may be well defined with legal agreements and established procedures, or somewhere in the middle.

TAXII offers an agreed-upon way of describing and exchanging machine-consumable cyber threat indicators, leaving vendors free to determine how their products produce, consume, or otherwise take advantage of TAXII specified data flows.

The goals of TAXII are to [Connolly12]:

- Enable timely and secure sharing of threat information both within and between cyber defender communities
- Leverage consensus standards to enable the sharing of actionable indicators and more across organization and product/service boundaries
- Extend indicator sharing to enable robust, secure, high-volume exchanges of significantly more expressive sets of cyber threat information
- Support a broad range of use cases and practices common to cyber threat information sharing communities
- Leverage existing mature standards, where appropriate
- Eventual adoption by one or more international standards organizations

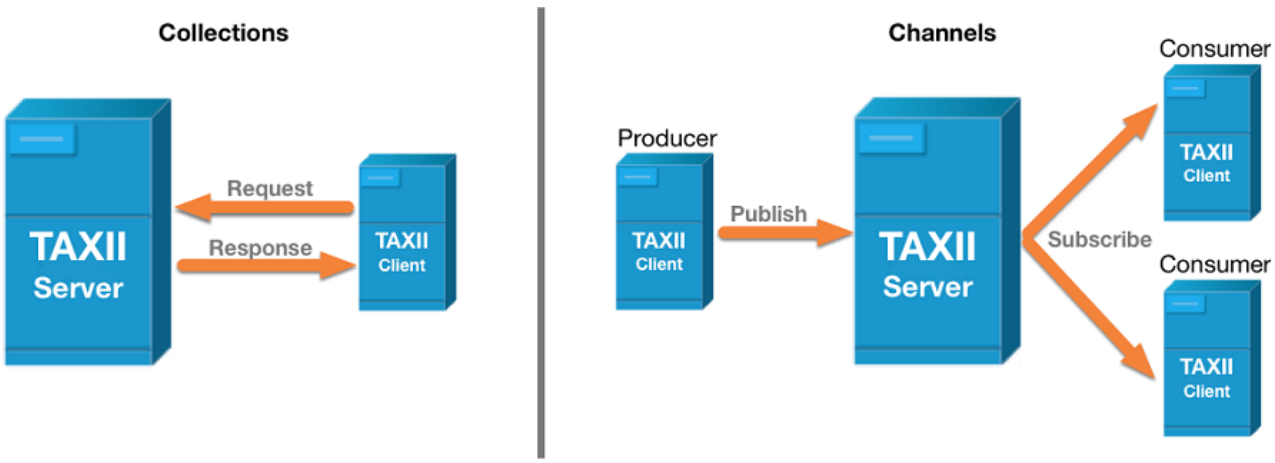

Figure 27: Two TAXII primary services

TAXII is not creating a sharing community. Rather, it enables communities to share. Today, TAXII is at its version 2.0. In particular, TAXII 2.0 defines a RESTful API (a set of services and message exchanges) and a set of requirements for TAXII Clients and Servers. As depicted in Figure 27, TAXII defines two primary services to support a variety of common sharing models [TAXII]:

- **Collection** - A Collection is an interface to a logical repository of CTI objects provided by a TAXII Server that allows a producer to host a set of CTI data that can be requested by consumers: TAXII Clients and Servers exchange information in a request-response model.
- **Channel** - Maintained by a TAXII Server. A Channel allows producers to push data to many consumers and consumers to receive data from many producers: TAXII Clients exchange information with other TAXII Clients in a publish-subscribe model.

TAXII relies on existing protocols when possible. In addition, TAXII uses HTTPS as the transport for all communications, and it uses HTTP for content negotiation and authentication.

TAXII was specifically designed to support the exchange of cyber threat data represented in STIX, and support for exchanging STIX 2.0 content is mandatory to implement. However, TAXII can also be used to share data in other formats. It is important to know that STIX and TAXII are independent standards: the structures and serializations of STIX do not rely on any specific transport mechanism, and TAXII can be used to transport non-STIX data [TAXII].

Security information sharing is one of the most critical issues for organizations to increase the defence capability against security threats. Furthermore, as we have seen before, TAXII allows construction of complex information sharing topologies between different actors.

Several proposals have focused on developing theoretical foundations for information sharing. A model to share classified security information between organizations with the lowest possible risks is proposed in Kokkonen et al. This is a theoretical model that relies on the use of STIX and TAXII [Kokkonen16].

8. Human Behavioural Modelling

So far in this document, the focus has been on the technical aspects of cybersecurity. However, organisations need to adopt technical, procedural and human defences to protect against security threats. Medical information and device security cannot be achieved solely through technological solutions [Herath09b; Schneier00; Vance12]. Organisations adopting this combination of technology, process and human behaviour to protect their information systems assets and resources are considered to be more effective [Darcy07; Li10; Schneier00; Stanton05; Vance12]. However there is still much to understand about the human component and how to optimise employees’ digital (and physical) security behaviours. Traditionally, employees have been considered to be a weak link in the security chain as their behaviour is estimated to account for a large portion of security breaches [Dhillon01; Mitnick03; Theoharidou05; Vroom04]. Yet there is little understanding about how to improve this situation.

To address the human component of cyber security we need to understand the factors which affect human behaviour in general and cyber security behaviours in particular. The literature on behaviour change in different domains is immense and difficult to manage. The research specific to cyber security is sparse and fragmented. There is a considerable gap between what is currently known and what needs to be understood in order to holistically protect an organisation against security threats in different domains particularly healthcare. In particular, the following points are missing:

- Reliable behavioural data on individual employees (in different roles) digital and physical security behaviours.
- Research on the factors influencing employees’ security practices or lack thereof.
- A universal theory of human behaviour or how to change human behaviour, and specifically security behaviours.
- Agreement between stakeholders on the necessary behaviours required.

8.1 What are security behaviours?

There are two types of security behaviours to consider firstly those protective behaviours as outlined in a company’s security policy or expected by its culture and secondly the adoption and effective use of specific security technology. There is a lack of consensus on recommended security behaviours in the workplace. [Posey10] identified 67 protection-motivated behaviours, clustered into 14 categories. They argue that these are volitional behaviours that seek to protect the information security of the employee’s organisation. These behaviours include co-worker reliance (e.g., reminding his/her co-workers of information security guidelines and protocols adopted by their organisation), immediate reporting of suspicious behaviour (e.g., immediately reporting a co-worker’s negligent information-security behaviour to the proper organisational authorities), and equipment location and storage (e.g., staff keeping laptops or other electronic devices issued to them by their organisation with them at all times). A lack of engagement in these behaviours may contribute to a successful security breach. Research, therefore, needs to address individual security behaviours in the workplace and how such behaviours are influenced. Advice on appropriate behaviours is constantly changing, as threats change and people realise that some advice has been unactionable, for example looking for a https web address with a green padlock is no longer seen as sufficient advice and the definition of strong passwords has now changed from a meaningless combination of letters, numbers and special characters to three random words[35].

[35] https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0

Some of the more consistently recommended actions within government reports, research studies and survey instruments are listed below:

Account security/authentication, including use of strong passwords, password management, password change frequency; *Running the latest version of software/operating systems*; *Anti-phishing/Scam prevention*, including staying informed about risks, identifying phishing emails; *Privacy protection*, including cookies, control of personal information; *Browser protection*, including checking use of HTTPS protocol, secure websites, logging out of websites [Coventry14; Crossler14a; Furnell14; Ion15].

Security behaviour in the workplace is largely conceptualised as a single Information Security (IS) policy compliance behaviour, with less known about the context that promotes compliance. Within such a policy, many different behaviours may be outlined, each of which may be influenced by different factors. IS policies differ depending on the organisation’s security maturity and their protection needs. These differences create problems when trying to compare organisations and behaviours.

8.2 Categories of employee security behaviour

Security behaviours can fall into one of six categories, [Stanton05] based on two dimensions: Intentionality (attack or defend) and technical expertise as highlighted in Figure 28.

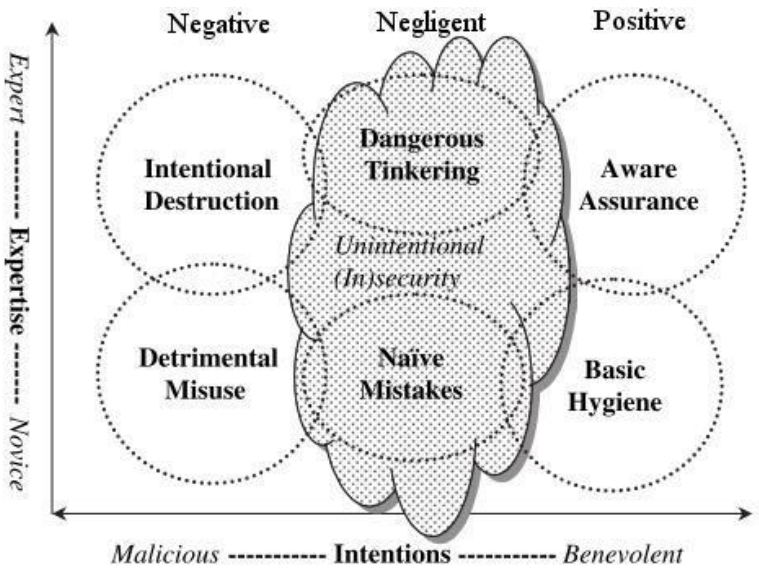

Figure 28: Two-factor taxonomy from Stanton et al. [Stanton05]

These categories are briefly described below:

- **Basic Hygiene**: simple behaviours that have a clear role in protecting information and devices (e.g. locking work computer when leaving station)
- **Aware Assurance**: behaviours that require more technical expertise (e.g. recognising a backdoor program on a work PC)
- **Naïve mistakes**: when there is no clear intention to do harm and the behaviours require minimal expertise (e.g. using a weak password)
- **Dangerous tinkering**: when there is no clear intention to do harm and the behaviours require expertise (e.g. setting up a gateway that inadvertently allows outsider access)

- **Detrimental misuse**: clear intention to do harm and behaviours only require minimal expertise (e.g. using the work email to distribute spam)
- **Intentional destruction:** clear intention to do harm and behaviours require technical expertise.

8.3 What influences security behaviour?

Alongside understanding what behaviours are expected from employees, it is also important to understand what factors influence whether or not they will display that behaviour. A growing body of literature is examining what influences employees to display protective security behaviours [Herath09a; Ifinedo11; Ifinedo14; Vance12] and the role that unusable systems, policies and procedures play in insecure practice [Albrechtsen07; Bartsch12; Beautement09; Inglesant10].

All behaviours are embedded in a particular context and are therefore subject to the influence of that context. Thus, digital and physical security behaviours in the healthcare context are influenced by *inter alia* the commitment to the organisation, the commitment to patient safety, the desire to do the right thing, the behaviours of peers, the time available to do the task, the awareness of security risks and the degree of technical competence, to name but a few possible influencers. There is an increasing body of research which examines such influences on peoples’ behaviour and we have distilled this rich literature into a set of *influencers* which can help us to understand and hopefully change behaviour. The aim here is to present an overview of those known influencers, showing the relevance to cyber security where possible. We will then report models of behaviour which focus on different subsets of those influencers and that have subsequently given rise to theories of behaviour. Note that these influencers may arise from the following factors:

Design: For example, a system that builds in usable security from the start will generate fewer problematic user behaviours as a result. A poorly designed system coupled with an onerous and unusable bolt-on security policy may generate insecure behaviours as people ‘workaround’ their security guidelines simply in order to get their main job done.

Social context: People do not operate in a vacuum and are highly influenced by the activities and attitudes of their superiors and peers.

Personal attributes: Reflecting the knowledge and skills, beliefs, attitudes, emotional state and personality of that individual. All of these can influence security behaviours in complex, interdependent ways.

Existing research investigating what influences individuals’ engagement in security behaviours has used theories from psychology and other disciplines to identify drivers of security. Studies may utilise some constructs from different behavioural theories or may study a single theory in isolation in an attempt to explain as much variance as possible in the outcome variable. Using models from behaviour literature is useful to understand the processes that underpin security behaviours. By identifying the influencers of secure and insecure behaviour, interventions can be designed to promote secure behaviour based on the strength of the relationships between the theoretical constructs and the security behaviour of interest.

Many models within psychology aim to understand the causes of individuals’ behaviours and ultimately find ways to stimulate positive behaviour change. The following section discusses those which have previously received the most attention within the information security domain. These theories will be discussed along with research that has demonstrated their efficacy.

8.4 Models of behaviour change used in security research

This section outlines theoretical models that are consistently used within behavioural IS research. [Lebek13] conducted a literature review on employees’ information security behaviour across 113 publications and found that four commonly used theories were the Theory of Planned Behaviour/Theory of Reasoned Action, General Deterrence Theory, Protection Motivation Theory and the Technology Acceptance Model.

8.4.1 The Theory of Reasoned Action and Theory of Planned Behaviour

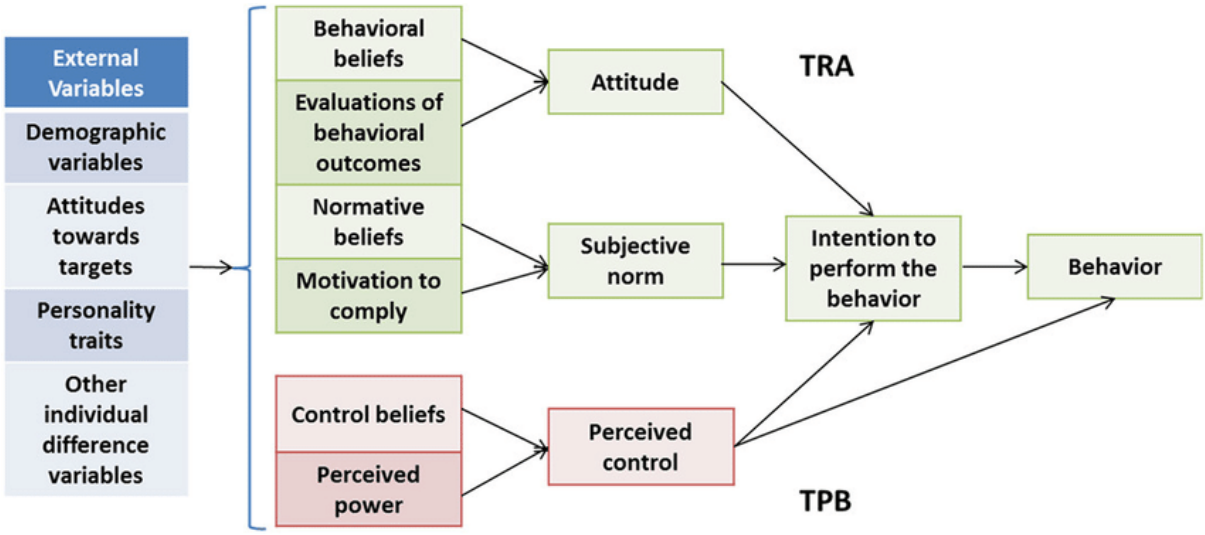

Figure 29: Theory of Reasoned Action and Theory of Planned Behaviour

The Theory of Reasoned Action (TRA; Fishbein75) and the Theory of Planned Behaviour (TPB; Ajzen91) are examples of continuum theories and are widely used to explain the relationship between attitudes and behaviour (see Figure 29). These models aim to explain and predict attitudes towards behaviours, and in this case security behaviours, and posit that attitudes are a function of beliefs and values [Fishbein75]. An individual’s attitude towards behaviour is the result of the perceived likelihood of outcomes associated with the behaviour and the expected value or evaluation of those outcomes. The overall desirability of the behaviour is based on the sum of the expectancy and value of outcomes. The TPB [Ajzen91] suggests that intention drives behaviour and that intention is in turn driven by attitude, subjective norms and an individual’s belief in their competence to perform that behaviour (Perceived Behavioural Control; PBC).

The TRA and TPB have identical attitudinal and social norm-related components and posit behavioural intention as preceding behaviour. The TPB [Ajzen91] extends the TRA by adding PBC as a variable that affects intention towards behaviour and is the individual’s perception of how easy it is to perform the behaviour, PBC can also act as a predictor of actual behaviour. Ajzen added PBC as the TRA did not account for behaviours that were not under volitional control. The addition of PBC allows an understanding of how people deal with situations where they may lack conscious control over behaviour by accommodating unconscious elements in behaviours [Ajzen02].

The TPB further distinguishes between three types of salient beliefs: behavioural (expected consequences of behaviour), normative (expectations about how significant others behave), and control (ability to perform the behaviour). These beliefs play a significant role in determining the three influencers of intention; attitude, subjective norms and PBC respectively.

Research has shown the predictive power of TPB constructs on intention and behaviour with ranges from 39% for intention and 27% for behaviour [Armitage01] and 50% for intention and 29% for behaviour [Hagger02] The addition of PBC has been found to add 6% to the prediction of intention independently of variables shared with TRA in a meta-analysis by [Armitage01].

8.5 Protection Motivation Theory

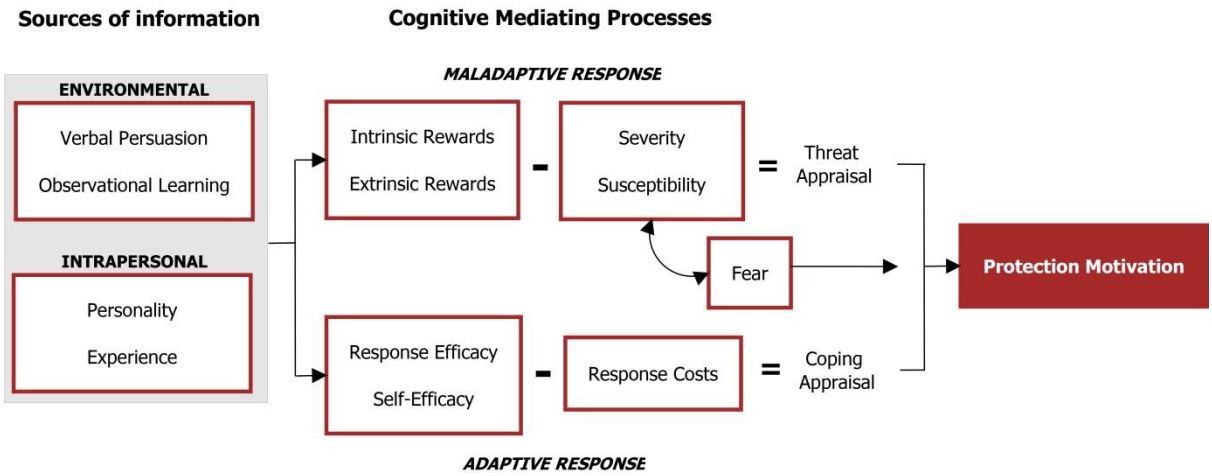

Figure 30: Protection Motivation Theory

Protection Motivation Theory (PMT) was developed by [Rogers75] to explore the effects of persuasive messages and risk perceptions (see Figure 30). The model was initially developed to explain fear appeals but has been further revised by [Rogers83; Rogers84] to propose that humans protect themselves using threat and coping appraisals.

The Extended Parallel Process Model (EPPM) is a fundamental development of PMT that explains how people appraise and respond to threats [Witte92]. People typically exhibit two types of response to a threat – either controlling/responding to the threat (adaptive: danger control response) or controlling the fear (maladaptive: fear control response) they feel from the threat. The second response does not address the threat, therefore the risk remains. However, this second response occurs when they feel they cannot cope with the threat. It is important to balance a user’s perception of their ability to cope with a threat with their perception of the severity and likelihood of the threat to ensure that they deal with the threat appropriately. Increasing threat appraisal (for example through the use of scare appeals) can be counterproductive if it results in the individual perceiving the threat as outside of their control. Therefore, behaviour change interventions can be more effective if they focus upon increasing the individuals coping appraisal (for example through providing them with the knowledge and/or tools required to feel more confident in their ability to address the threat).

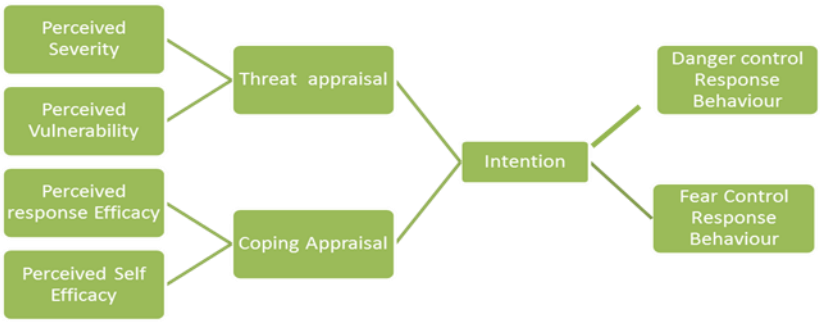

Figure 31: EPPM Model

Maladaptive actions (such as those arising from the maladaptive fear control response, i.e. denying a risk exists) are those that place an individual at risk; this includes the absence of security behaviours that may lead to negative consequences (such as not encrypting a USB stick). High intrinsic or extrinsic rewards, such as getting the job done faster heighten the likelihood of undertaking maladaptive coping (controlling the fear). In contrast, adaptive actions (i.e., threat control response) are the protective security behaviours that mitigate the threat. The sources of threat and coping information are either environmental (e.g. observational learning, verbal persuasion) or intrapersonal (e.g. prior experience).

Milne, Sheeran, and Orbell [Milne00] in a meta-analysis of PMT found a moderately strong average correlation (0.40) between protection motivation (intention) and future behaviour. Floyd, Prentice-Dunn, and Rogers [Floyd00] in a meta-analysis of 65 studies using PMT found that the overall effect size was moderate (d=.52) for the prediction of over 20 health behaviours. Coping appraisal has been found to have the strongest associations with protection motivation [Bui13; Floyd00; Milne00; Plotnikoff10].

8.5.1 Deterrence Theory

In the context of security, theoretical considerations of deterrence are important for understanding the misuse of technology at work. Unlike erroneous or accidental behaviours that can lead to a security breach, misuses of information systems are knowingly performed and violate the organisational IS policy. These can be malicious (e.g. stealing confidential information) and non-malicious (e.g. circumventing a security process to save time and effort for productivity).

Deterrence theory (see Figure 32) is a prominent theory from criminology which posits that people make decisions about committing a crime (or breaking organisational rules and procedures) based on the benefits and costs. It focuses on formal sanctions such as the legality of acts and argues that the higher an individual’s perceived certainty, severity and swiftness of the sanctions following the act, the more they are deterred from it [Gibbs75].

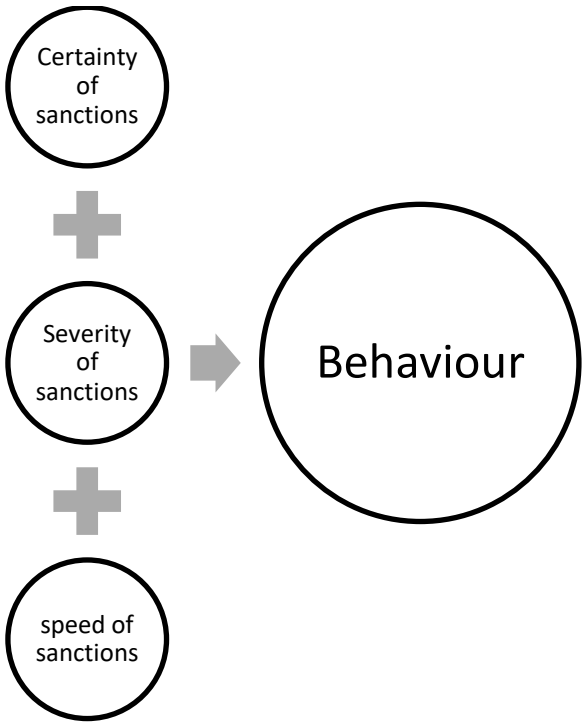

Figure 32: Deterrence Theory

Formal sanctions in the workplace will be described in the IS policy of the organisation which may include disciplinary action. Sanctions can also be informal and include shame and social disapproval [Piquero96]. When sanctions are less certain and severe, employees may not fully comply with the IS policies because they do not expect to be punished by their organisation.

8.5.2 Technology Acceptance Model

An important consideration when disseminating a piece of security software across an organisation is the extent to which it will be accepted and used by employees. There has been a wealth of research and support of the Technology Acceptance Model (TAM) developed by Davis (1989). Based on the TRA, the model attempts to explain why a user will accept or reject technology. Initially developed to explain organisational users’ behaviour, the model has been adopted to explain regular users’ adoption intentions and behaviour. The model posits that the perceived usefulness of the system and perceived ease of use are two important beliefs that influence an individual’s attitude towards the system (see Figure 33). Perceived usefulness (PU) is defined as “subjective probability that using a specific application system will increase his or her job performance within an organisational context” [Davis89] (p.985). Perceived ease of use (PEU) is defined as “the degree to which a person believes that using a particular system would be free from effort” [Davis89] (p.985). Like TRA, TAM argues that usage is determined by intention which is in turn influenced by attitude and perceived usefulness. Studies adopting TAM either explore the effect of perceived usefulness and perceived ease of use directly on intention or look at the mediating role of attitude on intention with little variation in explanatory power between the two approaches [Dillon96].

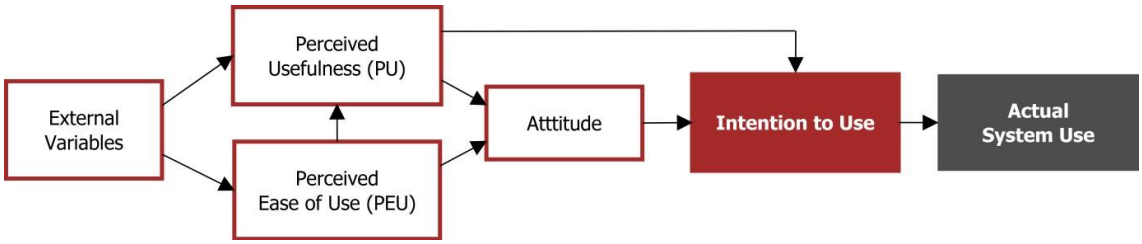

Figure 33: Technology Acceptance Model

Table below shows the use of these theories in organisational security research.

Theory utilized in IS compliance literature	References
The Theory of Planned Behavior (TPB)	• [Ifininedo11; Ifinedo14] • [Herath09b] • [Humaidi13] • [Bulgurcu10] • [Yeo09] • [Pahnila07] • [Siponen14]
The Theory of Reasoned Action (TRA)	• [Pahnila07] • [Siponen07]
Protection Motivation Theory (PMT)	• [Ifininedo11] • [Workman08] • [Herath09b] • [Pahnila07] • [Siponen06] • [Siponen07] • [Siponen14] • [Johnston10] • [Crossler14b] • [Vance12]
Health Belief Model	• [Ng09] • [Davison14]
Deterrence Theory	• [Herath09b] • [Pahnila07] • [Siponen10A] • [Siponen07] • [Siponen10B] • [Aurigemma14] • [Cheng14] • [Cheng13] • [Darcy12] • [Darcy09]

Table 11: Psychological theories in organisational security research

These psychological theories share overlapping constructs. So, whilst studies may adopt different theories, the underlying constructs under investigation may be the same or similar. In reality, many cybersecurity

studies use a mix of constructs from different theories. Additional constructs not covered in the behavioural models are also used. The following table presents a summary of some of the research investigating the role of different constructs in influencing security behaviours.

Influencer	Security behaviour	Supported studies	Unsupported studies
Norms (Social)			
Social pressures/ Subjective norms	ISP compliance	[Bulgurcu10] [Herath09a] [Herath09ab] [Ifinedo12]	
	Password creation		[Forget08]
	Anti-spyware adoption		[Dinev07]
	Anti-virus	[Ng05]	
	backing up	[Ng05]	
	Online privacy protection/ Protective online behaviour	[Yao08] [Burns13]	
Security Culture	ISP compliance	[Greene10]	
monitoring	Deter information systems abuse	[Darcy09]	
	Password creation		[Forget08]
Incentives – rewards and punishment/ cost benefits			
Sanctions/penalties	ISP compliance	[Herath09a]	[Pahnila07] [Siponen10B]
	Deter information systems abuse	[Darcy09]	
	Password creation		[Forget08]
Response cost	ISP compliance	[Herath09b], [Beautement09]	[Ifinedo11]
	Adopting anti-spyware software	[Chenoweth09] [Gurung09]	
Incentives – Coping appraisal			
Self Efficacy/ Perceived behavioural control	Anti-spyware adoption	[Dinev07]	
	Anti-virus	[Ng05]	
	backing up	[Ng05]	
	Online privacy protection Protective online behaviour	[Yao08] [Burns13]	
Self-efficacy	ISP compliance	[Herath09a][Bulgurcu 10] [Ifinedo12][Siponen0 7] [Herath09b]	
	Email security behaviour	[Ng09]	
	Security software use	[Gurung09] [Stafford10] [Claar10]	[Dinev07] [Chenoweth09]
	Adopting anti-spyware software	[Claar10]	
	firewall	[Lee08] [Claar10]	
	Anti-virus behaviour	[Ng05]	
	Anti-virus	[Ng05]	

Influencer	Security behaviour	Supported studies	Unsupported studies
	backing up	[Yao08]	
	Online privacy protection	[Dinev07]	
Perceived ease of use	Anti-spyware adoption	[Kumar08]	
	Firewall adoption	[Ng05]	
	Anti-virus and backing up	[CAMPBELL07]	
Optimism Bias	Internet events	[CAMPBELL07]	
Incentives – Threat appraisal			
Perceived Severity	IS compliance	[Herath09b] Siponen14] [Vance12] [Pahnila07] [Siponen06] [Siponen07]	[Ifinedo11]
	Email security behaviour	[Ng09]	
	Adopting anti-spyware software	[Chenoweth09] [Liang09]	
	Usage of anti-spyware	[Gurung09]	
	Spyware, firewall & anti-virus		[Claar10]
	Anti-virus behaviour		[Lee08]
	Wifi security	[Woon05]	
	Password behaviours		[Zhang09]
	Back ups		[Crossler10]
Perceived Vulnerability	ISP compliance	[Ifinedo11] [Pahnila07] [Siponen06] [Siponen07]	
	Adopting anti-spyware software	[Chenoweth09] [Claar10]	[Gurung09]
	firewall	[Claar10]	
	Anti-virus behaviour	[Claar10] [Lee08]	
Perceived Threat	Adopt anti-spyware	[Stafford10]	
Response efficacy	ISP compliance	[Ifinedo12] [Herath09b] [Johnston10]	
	Adopting anti-spyware software	[Chenoweth09] [Gurung09]	
Commitment			
Organizational commitment	ISP compliance	[Herath09b]	
Citizenship	Likelihood to adopt security measures to protect computer and protect the internet	[Anderson10]	
Capability			
Knowledge & experience	Anti-spyware behaviour and software use	[ACKERMAN09] [Dinev07]	
	Anti-virus behaviour	[Lee08]	

Influencer	Security behaviour	Supported studies	Unsupported studies
	Online privacy protection	[Yao08]	
Training & Education	Deter information systems abuse	[Harrington06]	
	virus protection	[Yeo09]	
	Password management, email management	[Puhakainen10]	
Attitude and motivation			
Attitude - general	ISP compliance	[Bulgurcu10] [Pahnila07] [Herath09a]	
	Firewall		[Kumar08]
	Adopting anti-spyware	[Dinev07]	
	Anti-virus	[Ng05]	
	backing up	[Ng05]	
	Protective online behaviour	[Yao08] [Burns13]	
Psychological Ownership	Likelihood to adopt security measures to protect computer and protect the internet	[Anderson10]	
	Firewall adoption	[Kumar08]	
Mental Models	Risks – viruses and hackers	[Wash10]	

Table 12 summary of some of the research investigating the role of different constructs in influencing security behaviours.

9. Risk Quantification and Governance

To date, many efforts have been made to classify information security threats, especially in the healthcare sector. However, there are still many unknown risks which may threaten the security of health information and their resources, especially within hospital environments. Healthcare organizations usually manage and process inherently sensitive data which require special protection, especially in view of the implementation of the new European legislation on data protection (GDPR, European Regulation 2016/679).

During a cyber-risk assessment there are three core concepts that must be properly defined:

- *Assets*: Any valuable items belonging to an organization that can be exploited by threats. Assets can be both tangible (e.g., technical infrastructures, systems components, overall systems) and intangible (e.g., organization’s reputation, business processes, etc.).
- *Vulnerabilities*: Weaknesses which can be exploited by attackers to compromise assets. Such weaknesses could be essential parts of the asset, but they also could be related to control procedures that are in place to protect assets.
- *Threats*: Actions that could adversely impact an asset. Typically involves exploiting a vulnerability. Such actions may be deliberate (e.g., stealing corporate data) or accidental (e.g., being the victim of a social engineering attack).

The cyber risk is the combination of these three concepts, in addition to the likelihood of a successful threat or attack occurring, and the damage that may cause to assets[36].

The cyber risk is usually expressed as a numerical value (i.e., monetary value) which identifies the loss resulting from the occurrence of a damaging event. There are several quantitative methods used for cyber risk calculation. They differ depending on whether the loss refers only to value of the asset involved, or to the impact on the business activities.

The cyber risk is calculated as,

$$R = P \times W \times V$$

where

- R is the risk value;
- P is the occurrence probability of an accident causing losses over a defined period;
- W is the loss value following a single accident;
- V is the vulnerability of a system information to a given threat.

One of the most used approach for risk quantification is the Mehari method. The main objective of Mehari is to provide a methodology for risk analysis and risk management that complies with ISO/IEC 27005:2008. This quantitative risk model is intended for providing a qualitative and quantitative assessment of the effectiveness of the security services that are in place within organizations. According to the author, each risk scenario is function of two important parameters: the occurrence probability of cyber incidents and the impact they can

[36] Nurse et al. 2017. “Security risk assessment in Internet of Things systems”. Special Issue on “Establishing Trust in the Internet of Things” https://www.computer.org/it-professional/

cause on organizations. The seriousness level of risk scenarios is given based on initial (intrinsic) impact and likelihood of multiple scenarios. However, the method suggests evaluating the implementation of proper security actions (countermeasures) to assess the residual risk remaining from transferring part of the risk to third parties.

An additional valuable risk assessment is represented by the CRAMM[37] Method. The CRAMM methodology is developed according to three main phases:

- Identification and assessment of assets;
- Identification of vulnerabilities and potential threats;
- Identification and selection of countermeasure.

The approach divides assets into groups (e.g. physical, logical, and virtual) and associates threats and vulnerabilities to each group, also considering cross-dependences between assets. Effective countermeasures are identified based on the vulnerabilities threatening each asset group. The method is equipped with a software tool for the management of the various activities and the production of the final reports with suggestions on the countermeasures to be taken.

The technological explosion nowadays forces organizations to change their functioning and structures. Organizations are depending more on their information system then they did in the past. A dysfunction of such centre can paralyze all the system and could have disastrous consequences for the company at many levels (e.g., financial, reputation). The use of security metrics could bring a great number of organizational and financial advantages for the organization as they are able to locate the problems and arise opportunities to solve them. In addition, the use of security metrics makes it possible to check and attest that the activities of the organization are in agreement with the applicable laws (compliance concept).

Metrics is the term used to define a measure based on a reference. Security is the protection from or the absence of danger. A security metrics define the state or degree of safety relative to a reference point in order to avoid danger.

A standardized set of security metrics would have a set of required attributes, such as:

- Being quantitative;
- Being objective;
- Being based on a formal model;
- Being repeatable;
- Having a time dimension.

In recent times, there are numerous approaches to monitoring and measuring information security. Most of them are generally applied to technical IT security systems, saying little about the overall security of the organization and providing little guidance for effective management of security[38].

[37] CRAMM: Central Computer and Telecommunication Agency (CCTA) Risk Analysis and Management
[38] Information Security Management Metrics by W. Krag Brotby, CISM. New York: Auerbach Publications,

High-level guidance for information security governance has been developed by the information Security and Control Association (ISACA), which proposes 5 outcomes of information security governance and management:

1. Strategic alignment of information security with business strategy to support organizational objectives;
2. Risk management by executing appropriate measures to manage and mitigate risks and reduce potential impacts on information resources to an acceptable level;
3. Resource management by utilizing information security knowledge and infrastructure efficiently and effectively;
4. Performance measurement by measuring, monitoring and reporting information security governance metrics to ensure that organizational objectives are achieved;
5. Value delivery by optimizing information security investments in support of organizational objectives.

The Center for Internet Security (CIS)[39] has defined a set of security metrics that can be grouped in management metrics, operational metrics or technical metrics based on their purpose and audience. Management metrics provide information on the performance of business functions, and the impact on the organization strategies. Operational metrics are used to understand and optimize the activities of business functions. Technical metrics provide technical details.

The information security business has designed many security frameworks that are internationally used. Among the most popular are the Control Objectives for Information Technology (COBIT), the ISO 27000 series of standards, specifically designed for information security matters and the Information Technology Infrastructure Library (ITIL). Professionals also often refer to the set of documents about information security that the United States National Institute of Standards and Technology (US NIST) publish under the Special Publication 800 Series. Those frameworks enumerate some metrics that are tightly connected to the control objectives of the frameworks. The control objectives covered are:

- information security policy document
- review of the information security policy
- inventory of assets
- ownership of assets
- Acceptable use of assets.

The following table describes most popular security metrics standards.

Security Metrics Standards	Definition
ISO/IEC 27000 series	Provides guidance on how an organization, through the use of metrics, identifies the adequacy of in-place security controls, policies, and procedures.
USA NIST (National Institute of Standards and Technology)	In 2003, the NIST came up with a Guide for Information Security Metrics. The NIST metrics is designed for US federal government use but its standards can be applied to other organizations with differing environments.

2009.

[39] Perpétus Houngbo, Joël Hounsou, "Measuring Information Security: Understanding And Selecting Appropriate Metrics", International Journal of Computer Science and Security (IJCSS), Volume (9) : Issue (2) : 2015

Security Metrics Standards	Definition
COBIT (Control Objectives for Information and related Technology)	Good-practice framework created by international professional association ISACA for information technology management and IT governance

Table 13: Security metrics standards

The purpose of performing a risk assessment is to ensure that the security controls (when implemented) fully commensurate with the risks. The process helps to prioritize which controls require to be implemented as security metrics share a notable relationship with risk management. It can be said that many of the decisions that the security metrics support are in essence risk management decisions, since the ultimate purpose of all security activities is management of security risks. Therefore, metrics can supplement specific risk management activities by directly contributing input for analysis as well as an organization's overall capability to deal with the risks it faces by facilitating continual improvements to security.

9.1 Business Modelling

Business impact analysis and risk assessment concepts enable adequate business continuity planning as they deliver essential information about the impact of resources’ disruption on business.

Several studies exist trying to relate the ICT layer with the business layer. Bahşi et al. [Bahşi] provide a systematic literature review of the studies which propose a framework for the impact assessment of cyber actions on missions or business processes up to 2018. In this study, they deeply evaluated 22 papers that are those closer to the focus of this section. In the following, we will highlight the main findings of [Bahşi] and we will provide some additional and novel references to enrich this analysis.

Concerning horizontal modelling, i.e., modelling the business process itself, we can summarize the main representation and formalism as reported in the following Table:

Representation	References	Discussion
Business Process Modeling Notation (BPM)	[Choobineh], [Creese], [Musman], [Angelini]	Exploits specific construct to represent the control flow of horizontal tasks.
Probabilistic Graphical Models	[Granadillo]	Defines business function nodes and maps them to the business process nodes
Others	[Shaw]	Discrete Time Events, Reliability Models mainly applied to cyber-physical systems

Table 14: Summary of Business Process Representations and Formalisms

Concerning the modelling of vertical dependencies between organization assets and business processes, the following approaches are the main used:

Representation	References	Discussion
Dependency Graph and Probabilistic Graphs	[Jakobson], [Granadillo]	Edges between different layers represent vertical dependencies, i.e.,

Representation	References	Discussion
		interactions between technology and business processes.
Matix	[Choobineh]	It maps assets to mission tasks

Table 15: Summary of Business Process – Asset Dependencies Approaches.

Among the research challenges listed by [Bahşi], it is possible to consider that the analysed papers do not consider the cross-organizational nature of most enterprise and military operations. This also applies to the HC domain where there exists several business functions that may span over different asset networks and this is still an open problem. In addition, the development of automatic- or semi-automatic methods for the identification of dependencies is a significant issue that requires more interest from the research community. Concerning this point, a recent result is represented by [Kott] where dependencies are directly inferred by analysing network traffic generated by business processes. To this aim, some heuristics have been defined based on the notion of similarity between patterns.

Economic impact has been considered in few works while almost all of them consider the impact of the mission capabilities with a strong focus on the service/mission continuity.

Given all the studies analysed in [Bahşi], many of them try to calculate the economic impact based on the cost of loss of production and quality. Some works mention loss of reputation and liability costs but not propose a method for their calculation.

Thus, among all the research challenges listed in [Bahşi], the following still remain:

1. Requirement for new models that are able to consider money losses (also indirectly due to loss of reputation).
2. Requirement for automatic and/or semi-automatic techniques that allows the mission impact model to evolve dynamically according to the evolving nature of an organization, and that are able to consider the temporal dimension.

It is noteworthy, that none of the identified studies, currently, have been applied in the HC domain but they consider the military contexts, cyber-physical systems and enterprise. However, we believe that they could represent a good starting point for the PANACEA context.

9.2 Policies, Legal and Regulatory considerations for countermeasures

In this historical period of technological progress, security is becoming fundamental for healthcare facilities. There are several actions that healthcare organizations should implement to protect themselves from both internal and external threats, including the development of policies and procedures relating to information security. Given the proliferation of products, applications and services that collect personal and health-related information, some general concepts[40] related to patient data privacy and cybersecurity are reported in the following:

i. Notice: Notify the user about the fact and purpose of data collection, as well as any subsequent deviations from the originally stated conditions of data use;

[40] Lyapustina S. et Armostrong K., 2018. Regulatory Considerations for Cybersecurity and Data Privacy in Digital Health and Medical Applications and Products. Inhalation Magazine.

ii. Choice: Give users a choice to opt-in or opt-out of participating in the data collection process;
iii. Access: Provide users with a method access data about themselves and to content data’s accuracy;
iv. Security: Implement security measures to prevent unauthorized or inappropriate use of data or disclosure of personal information.

Legal and regulatory developments related to cybersecurity are increasing in the last decades. At European level, GDPR (General Data Protection Regulation) and ISO 27001 are two important compliance standards that aim to strengthen data security and reduce the risk of data breaches. GDPR is a regulation in EU law that regulates how companies process and protect personal data relating to individual citizens in the EU. ISO 27001 is an international management standard that provides a proven framework for managing information security. It uses an integrated set of recommended policies, procedures, documents and technologies in the form of an Information Security Management System[41].

GDPR and ISO 27001 have lots in common and we report a comparison between these two standards, their commonalities are provided below:

- *Availability, confidentiality and data integrity*:
  GDPR Art.5 specifies general principles for data processing, such as protection against unauthorized processing, loss, destruction or accidental damage. In Article 32 more detailed guidelines are given, specifying that organizations are required to implement, operate and maintain technical and organizational measures to ensure data security, such as encryption, resilience of processing systems and services and the ability to restore the availability of personal data.
  On the other hand, ISO 27001 controls aim to help organizations ensure data confidentiality, availability and integrity. Based on clause 4, ISO 27001 requires organizations to identify internal and external issues that could impact security programs. Clause 6 requires them to determine their own IT security objectives and create a security program to help organization to achieve these objectives. Clause 8 sets standards for the ongoing maintenance of the security program and requires organizations to document the same program to demonstrate regulatory compliance.
- *Risk assessment*:
  Both standards require a risk-based approach to data security.
  GDPR Art.35 requires companies to perform data protection impact assessments to assess and identify risks to personal data.
  ISO 27001 advises organizations to conduct accurate risk assessments to identify threats and vulnerabilities that could affect activities and to select appropriate information security measures based on the results of the risk assessment.
- *Processors management*:
  GDPR Art. 28 requires creating a *'data processing agreement'* when data processing is carried out on behalf of a controller.
  ISO 27001 clause 8 obliges organizations to identify which actions are outsourced and to ensure that they can be monitored. Clause A.15 provides specific guidance on relations with suppliers and requires organizations to monitor and review the delivery of services by suppliers.
- *Breach notification*:
  According to GDPR Art. 33-34, organizations must notify the authorities within 72 hours of discovery of a personal data breach. Data owners must also be informed without delay in case of *"high risk to the rights and freedoms of data subjects".*

[41] https://www.itgovernance.co.uk/iso27001

ISO 27001 section A.16 *"Management of information security incidents"* does not specify an exact time frame for data breach notification, but states that organizations should report security incidents in a timely manner to allow 'timely corrective action' to be taken.

- *Data protection by design and by default*:
  GDPR Art. 25 states that companies must implement technical and organizational measures during the design phase of all projects so that they can ensure data privacy from the outset, *"privacy by design".* In addition, organizations should protect data privacy by default and ensure that only the information necessary for each specific purpose of processing is used, *"privacy by default".*
  Similar requirements are highlighted in ISO 27001. Clause 4 requires organizations to understand the scope and context of the data collected and processed, while clause 6 recommends performing periodic risk assessments to ensure the effectiveness of their program security management.
- *Retention of records*:
  GDPR Art. 30 requires organizations to keep records of their processing activities, including data categorization, processing purposes and a general description of technical and organizational measures relevant for security aims.
  ISO 27001 states that organizations shall document their security processes as well as the results of their security risk assessments and risk processing (clause 8). In accordance with section A.8, information activities shall be inventoried and classified, business owners shall be assigned and procedures for the use of acceptable data shall be defined.

By implementing GDPR requirements and by following best practices provided by ISO 27001 standard, it is possible to build an integrated system to guarantee the security management of data.

Lastly since 27th of June 2019 the EU Cybersecurity Act[42] came into force. In a shift towards a role that adds more value to the European Union, ENISA, which will henceforth be known as the EU Agency for Cybersecurity and will receive a permanent mandate. In order to scale up the EU’s response to cyber-attacks, improve cyber resilience and increase trust in the Digital Single Market, the EU Cybersecurity Act aims to:

1. Strengthen ENISA, the European Union Agency for Cybersecurity to improve the coordination and cooperation in cybersecurity across EU Member States and EU institutions, agencies and bodies;
2. Establish an EU cybersecurity certification framework that will allow the emergence of tailored certification schemes for specific categories of ICT products, processes and services. Companies will be able to certify their products, processes and services only once and obtain certificates that are valid across the EU.

This framework for cybersecurity certification will play a critical role in increasing trust and security in products and services that are crucial for the Market. It will be a homogeneous act that will act a a common framework for EU-wide valid cybersecurity certificate schemes, there is an increasing risk of fragmentation and barriers in the single market.

The EU Agency for Cybersecurity, ENISA, with the help of national experts will prepare the technical ground for the certification schemes that will then be adopted by the European Commission through implementing acts. The EU-wide certification framework creates a comprehensive set of rules, technical requirements, standards and procedures to agree each scheme. Each scheme will be based on agreement for the evaluation of the security properties of a specific ICT-based product or service e.g. smart cards. *This certificate will attest that ICT products and services that have been certified in accordance with such a scheme comply with specified cybersecurity requirements.* The resulting certificate will be *recognized in all EU Member States*, making it easier for businesses to trade across borders and for purchasers to understand the security features

[42] https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework

of the product or service. In fact, the use of certification schemes will be voluntary unless future EU legislation prescribes an EU certificate as a mandatory requirement to satisfy a specific cybersecurity need but EU will assess the possible need for mandatory certification for certain categories of products and services.

10. Attack response: Hardening approaches

In this section we will provide an overview on current approaches that can be adopted in order to implement an attack response trough the definition of the proper countermeasures. More in details, we will focus our attentions on approaches based on the attack graph model as this seems to be a valid tool to both model threats and vulnerabilities, it enables and support a risk evaluation and quantification process and it supports also the definition of response plans to mitigate risks.

10.1 Attack graph-based response

A very important application of attack graph is clearly devoted to attack response, and this branch of research is commonly referred as *network hardening*, i.e., recommending security defence measures and mitigation actions against possible cyber threats. These can be in the form of vulnerability patches, modifications for filtering rules on firewalls and routers, optimal IDS/IPS and firewall locations, user rights on host applications or topological changes.

Similar to attack graph generation, near-optimal defence measure recommendation suffers from the scalability problem caused by the growing size of target networks and their corresponding attack graphs, as well as due to the increased number of defence measures available to the network administrator [Kaynar]. Network hardening approaches generally use the attack graphs generated by accounting for the goal privileges pointing to the critical network assets, and further take into account a cost model for the hardening decisions.

The algorithms utilized in attack graph-based defense measure recommendation can broadly be divided in two categories: graph-based and optimization-based methods.

10.1.1 Graph based approaches

This type of approaches is based on graph traversal methods. Assuming that a number of attack paths exists that involve a goal target service resident on some host, the aim is to find a minimum-cost combination of the initially satisfied privileges that can be negated (eliminated) by the network. This area of research follows into the category of *minimum cost network hardening* [Kaynar], based on the notion of finding *critical sets*, i.e., a set of exploits (and corresponding conditions) whose removal from the attack graph will invalidate all attack paths. At its core, a critical set essentially corresponds to the concept of a cut set in graph theory.

It has been shown that finding critical sets with the minimum cardinality is NP-hard [Sheyner] by reduction from the minimum cover problem, whereas finding a minimal critical set (i.e., a critical set with no proper subset being a critical set) is polynomial [Jha]. However, this solution ignores the critical fact that not all vulnerabilities (with associated exploits) are under the direct control of administrators, the solution is thus not always directly enforceable. [Noel,Wang06] introduce the concept of network hardening with respect to initially satisfied conditions, aiming at identifying the set of conditions which can disable the attack goals. This approach has an unavoidable exponential worst-case complexity, because the result itself may be exponential in size in the number of initial conditions (and the attack graph). In [Wang14] the authors devise a heuristic solution to address the scalability issue and to handle dependent hardening options via a new model based on the concept of defense measure actions which are formally defined and entailed by a composite defense plan. They also propose a near-optimal approximation algorithm for the network hardening problem scaling almost linearly – for certain values of the parameters – with the size of the attack graph.

10.1.2 Optimization based approaches

The second type of network hardening algorithms is based on combinatorial optimization methods. Examples of optimization criteria that can be specified are: minimizing the total cost of the applied defense measures, maximizing the number of eliminated attack paths reaching the goal conditions, minimizing the total residual damage on the target network hosts after applying the near-optimal set of defense measures, etc.

Casting near-optimal defense measure recommendation problem into a multi-objective optimization problem is the approach taken in [Dewri]; starting from an attack graph, the authors compute a potential *damage value* for each node, minimizing the total hardening cost and residual damage, and solve it using a genetic algorithm. In [Chen07], a solution to the minimum cost network hardening problem based on Reduced Ordered Binary Decision Diagrams (ROBDDs) is presented. In [Jun-chun] the authors formalize a mathematical model employing attack graphs to represent the network hardening problem as a non-restraint optimization problem with penalty. A parallel, genetic algorithm is used to solve the resulting optimization problem. In [Yigit], a heuristic method to find a cost-effective network hardening solution with a limited budget is proposed. The method uses as input an attack graph that contains only the possible attack paths which can reach pre-specified critical resources in the target network. The exploit or initial security condition contributing most to the elimination of these attack paths with least cost is greedily selected at each step of the attack graph traversal until the total cost exceeds the allocated budget.

10.1.3 Limitations

The main drawbacks behind tools from early works is that they cannot suggest actionable remediation actions at the vulnerability patching level, driven by non-accurate information about the relationship between vulnerabilities and their exploitability. This is linked to the unavailability at the time of metrics that evaluate factors such as exploitability and remediation level (CVSS v2, 2007 [CVSS1] and, in particular CVSS v3 2012 [CVSS2; CVSS3]).

More recently, a few efforts have been made to integrate such metrics to compute assessments of networks security at various granularities. In [Frigault], later refined in [Cheng] the authors aim at combining vulnerabilities’ CVSS scores mapping them to probabilities and using a Bayesian inference approach to propagate them along attack paths (seen thus as a Bayesian Network). Furthermore, recent works also incorporate zero-day (i.e., unknown) vulnerabilities, developing a novel security metric that attempts to estimate how many such vulnerabilities would be required for compromising network assets, while in [Sun] they are introduced in the bayesian network of [Cheng].

While these recent approaches go in the direction of assessing the risks related to cyber-attacks in computer networks, they do not directly translate to actual hardening directions or recommendations. In this light, it is of particular interest addressing the following open points left by previous work.

Most works assume that network conditions are to be hardened independently. This assumption does not hold true in real network environments. Realistically, network administrators can take actions that affect vulnerabilities across the network, such as pushing patches out to many systems at once. Further, the same hardening result may be obtained through more than one action. Another related question is coping with hardening solutions with conflicting or overlapping actions that cannot be independently implemented. Overall, to provide realistic recommendations, the hardening strategy must take such factors into account.

10.2 Design and implementation of a Dynamic Risk management platform

A Dynamic Risk Management Platform (DRMP) should assist and support cyber security operators in taking informed decision to increase the overall security level of a given organization.

Driven by common information security governance best practices like the NIST CSF[43] or the ISO/IEC 27002[44,45], a DRMP should be able to monitor the environment, analyse the actual situation, plan corrective actions and execute them. This pattern is continuously repeated in an infinite loop that has the aim of a continuous improvement of the security level.

Supported by the ISO/IEC 31000[46], security is evaluated by estimating and assessing risks and by planning corrective actions that tries to optimize the risk reduction.

As far as we know, many independent efforts have been devoted to study innovative solutions for each individual phase of the control loop but still few complete results covering the end-to-end process exists.

To the best of our knowledge, the main results in this field is represented by the outcome of the PANOPTESEC project[47] where a DRMP has been designed, implemented and tested in the context of a critical infrastructure provider.

The PANOPESEC system is composed by two main control loops: (i) the proactive chain planning for risk reduction in good periods i.e., when no attack is in place and (ii) the reactive chain planning for attack containment and deployment of mitigation action that reduces the risk in the short term.

In [Gonzalez-Granadillo], the authors describe the proactive side of the dynamic risk management response system (DRMRS). Their DRMRS adopts a quantitative risk-aware approach that provides a comprehensive view of the threats, by considering their likelihood of success, the induced impact, the cost of the possible responses, and the negative side-effects of a response. Responses are selected and proposed to operators based on financial, operational and threat assessments.

[43] https://www.nist.gov/cyberframework
[44] https://www.iso27001security.com/html/27002.html
[45] https://www.iso.org/standard/54533.html
[46] https://www.iso.org/iso-31000-risk-management.html
[47] http://www.panoptesec.eu/

11. Visual Analytics for increasing situational awareness

Massive amounts of network data are generated, collected, stored and available to security analysts; standard approaches, however, are inadequate to make sense of these ever increasing volumes of complex data. This complexity makes very challenging to have the right information at the right moment and, more in general, to enhance Situation Awareness (SA) for informed decision making in the cyber security domain [Kott14] [BouHarb13; Paxson99; Sommer10; Vaar13]. Endlsey presented a model of SA in dynamic environments in [Endlsey95] (see Figure 34). The first step in achieving SA is to perceive the status, attributes, and dynamics of relevant elements in the environment. The second step concerns the comprehension of the situation, based on a synthesis of disjointed elements. These elements, put together to form patterns, take on meaning in light of pertinent operator goals. In the last step, the knowledge of the status and dynamics of the elements and the comprehension of the situation drive the ability to project the future actions of the elements in the environment. Evest et al. [Evesti17] build a taxonomy of SA in cybersecurity. The taxonomy categorises terminology, makes it possible to recognise missing areas, and to understand the area in a uniform way. Moreover, the taxonomy helps to select the most effective techniques to be used in a specific SA implementation.

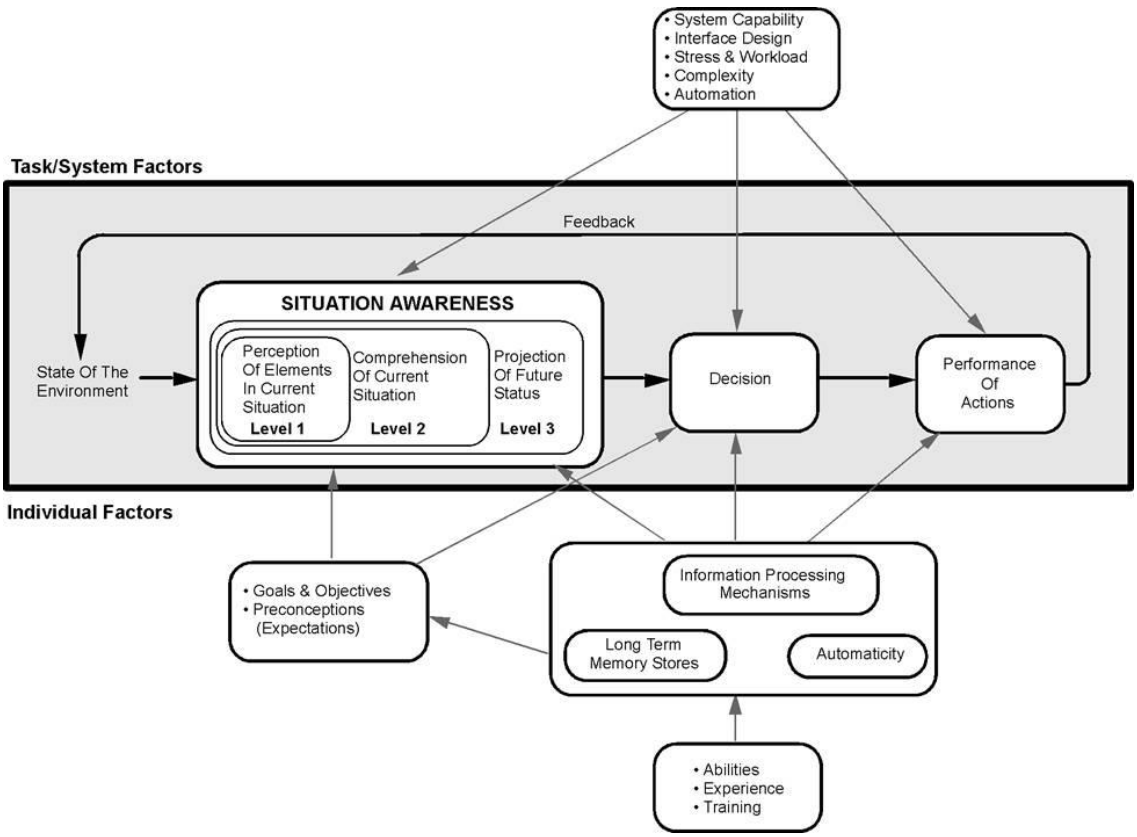

Figure 34: Situational Awareness model [Endlsey95]

Situational awareness and cyber security have a strong need for visualization support to involve the analysts in complex data analysis tasks [Varga16; Varga18]. Very often, it is not sufficient to identify specific attacks and current alerts but it is required to be aware of the current operational situation. Furthermore, a comprehensive analysis of the menaces require that the context is preserved; fully automated techniques might not be appropriate in these situations and Visual Analytics (VA) techniques can be a support to gain SA to eventually enhance cyber security. An advantage provided by VA is that decision makers may focus their full cognitive and perceptual capabilities on the analytical process, while allowing them to apply advanced

computational capabilities to enlarge the discovery process. The final goal is to gain knowledge from heterogeneous data sources combining automatic analysis that uses methods from Knowledge Discovery in Databases (KDD), statistics, mathematics and human capabilities to perceive, relate and conclude. Visual Analytics tools use different visualization techniques that can be divided into five categories:

1. Standard 2d/3d displays: in this category can be found bar charts, x-y/x-y-z plots and line graphs;
2. Geometrically transformed displays: landscapes, parallel coordinates and scatter plot matrices are examples of this category;
3. Iconic Displays: these are compact representations of attributes of multi-dimensional data items which were previously mapped onto icons (e.g., needle and star icons) or glyphs;
4. Dense Pixel Display: such as matrix visualizations, in which each data point is mapped to a pixel and then everything is grouped into adjacent areas representing individual data dimensions;
5. Stacked Display: the category is almost entirely made by hierarchical data, such as treemaps, and hierarchical layout for multi-dimensional data, such as dimensional stacking.

In the cybersecurity domain, data are very often arranged in networks, multivariate both on nodes and edges. Due to this reason, it is particularly interesting to examine the taxonomy of the layout of multivariate networks as the one presented by Nobre et al. in [Nobre19]. The layouts are basically three and they are orthogonal to the five categories of visualization types; the first layout family is the Node-Link, then there are the Tabular Layouts, and finally the Implicit Tree Layouts, in which edges are not containing any information or they are completely omitted. The first layout type, the Node-Link, is the most common graphical representation of a network and therefore it has also many different models which can be divided into three subgroups:

1. On-Node/On-Edge Encoding: marking and/or changing size of node/edge;
2. Attribute-Driven Positioning: assigning nodes and edges according to one or more attributes, usually in fixed layouts like a geographic map;
3. Attribute-Driven Faceting: grouping nodes according to attributes, having regions of similar elements.

The Tabular Layouts can be found in three different forms:

1. Adjacency Matrix: nodes represented by rows and columns, and edges by the cells of the matrix;
2. Quilts: same as adjacency matrix but nodes are assumed to be partitioned into layers and no links exist within a given layer;
3. Biofabric: each node is in a row of the table and edges are drawn between nodes in columns.

The Implicit Tree Layouts can be divided into:

1. Inner Nodes and Leaves: layouts in which the hierarchy is encoded by adjacency and so a child node is adjacent to its root, just like Sunburst;
2. Leaf-Centric: the screen space is allocated for the leaves of a multivariate tree and the hierarchy is encoded by inclusion and nesting.

In the cyber security scenario, there exist a lot of systems to visually analyze, explore and monitor the current situation aiming at identifying patterns and insights. Franke and Brynielsson presented a systematic review of literature about cyber situational awareness in [Franke14] not limited to publications related to visualization. They concluded that some areas such as the cyber situational awareness in industrial control systems are more mature than, for examples, risk of deception or cyber battle damage awareness in military operations. Shiravi et al. presented a comprehensive survey of visualization systems for network security in [Shiravi12] classifying them with respect to their use cases. The authors stressed the fact that most of these systems are suitable for offline forensics analysis, while the *“process of achieving situational awareness is closely related*

to the capability of a system in conducting real time analysis”. D’Amico and Kocka in [DAmico05] proposed guidelines to approach designing visualization techniques for maintaining SA in complex domains. More in detail, they highlighted how visualization techniques should be carefully selected or designed to support one of the three phases of SA (perception, comprehension or projection) through one of the five standards uses of visualization: monitoring, inspecting, exploring, forecasting and communicating (see Figure 35).

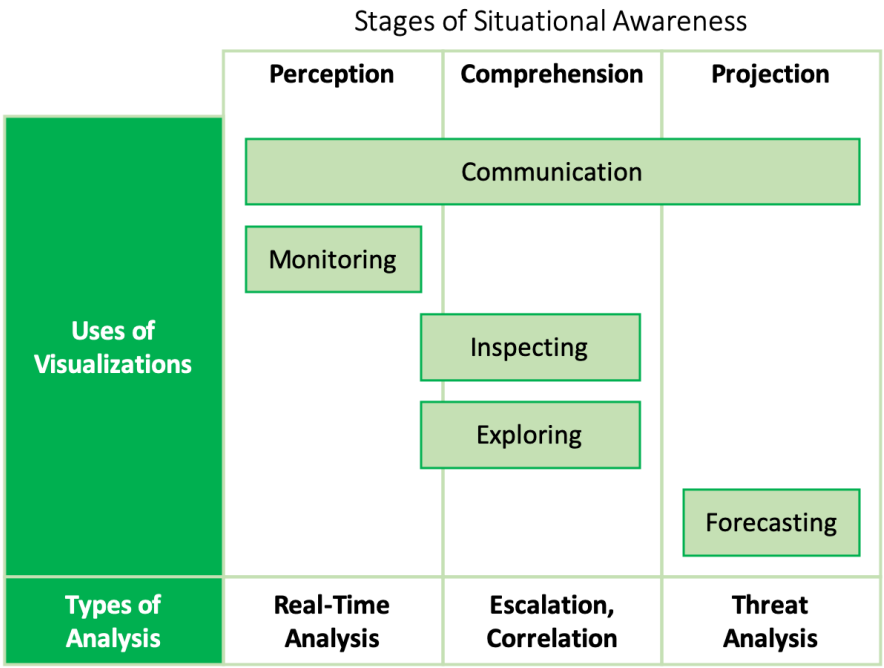

Figure 35: Relation between stages of situational awareness, visualization usage and anylsis type; modified from [DAmico05]

Fischer proposed in his PhD dissertation [Fischer16] a taxonomy that includes previous categorizations and provides a homogeneous view. In the following, we use the classifications presented in these works, adapting and updating them to our needs. More in detail, we will present the different categories providing a systematic review of the ones strictly related to the project and few examples of the others.

11.1 Use Cases

An important element to categorize existing works is the intended use case. Inspired by previous works, we identify two macro categories: Network Activity and Network Threats. The first category is related to the analysis of network activity, which includes traffic, log events and alerts. Works in the second category focuses on network threats, supporting the forensic analysis of specific attacks and resulting anomalies.

11.1.1 Network Activity

Systems in the Network Activity category focus not only on threats but also on the overview and management of network utilization.

Some works focus upon the communication among internal hosts and servers but in relation to communicating external IPs. Boschetti et al. [Boschetti11] present a tool that combines multiple visual representations of network traces designed and tightly coupled to support different levels of visual-based querying and reasoning

required for making sense of complex traffic data. Taylor et al. [Taylor09] present a suite of visualization tools that are intended to complement command line tools that are used by analysts to perform forensic analysis of Network Flows data. The tool is based on three visual paradigms: 1). Activity diagrams that display various aspects of multiple individual host behaviours as color coded time series, 2). Connection bundles that show the interactions among hosts and groups of hosts, and 3). The NetBytes viewer that allows detailed examination of the port and volume behaviours of an individual host over a period of time.

Increasing the level of detail, the analysis of activity on particular ports provides a different perspective which supports the detection of malicious programs that manifest themselves through unusual and irregular port activity. Stoffel et al. [Stoffel13] developed a visual analytics application to find correlations and similar behaviours between different devices by integrating similarity models and analytics combined with well-known, but task-adapted, time-series visualizations. Mansmann et al. [Mansmann12] present a visualization tool to support the network administrator in the complex task of understanding firewall rule sets and object group definitions. The tool consists of a hierarchical sunburst visualization, which logically groups rules or object groups according to their common characteristics, a color-linked configuration editor and classical tree view components for rules and object groups.

In other works, the main display is devoted to the representation of hosts and servers. The intent is to display the current state of a network by visualizing the number of users, system load, status, and unusual or unexpected host or server activities [Shiravi12]. The work of Arendt et al. [Arendt15] describes the user-centered design and development of a decision support visualization for active network defense. It helps the cyber analyst assess threats to a network and quarantine affected computers from the healthy parts of a network. The described web-based, visualization prototype integrates and visualizes multiple data sources through the use of a hybrid space partitioning tree and node link diagram. Wang et al. [Wang15] designed a visual analytics system to allow analysts to overview network traffic and identify such suspicious such activities as server redirection attack and data exfiltration. Through aggregating traffic data along the two dimensions of duration and payload, the system reveals key network traffic characteristics for the analyst to identify security events.

11.1.2 Network Threats

Works in the Network Threats category aim at supporting the inspection of current anomalies, threats and attacks. Shiravi et al. [Shiravi12] propose a classification of this category, further refined by Fischer [Fischer16] in four different use cases.

The main goal of some works is to support the understanding of the evolution of routing patterns over time. Biersack et al. [Biersack12] give a survey of visualization methods that have been developed for BGP monitoring, in particular for the identification of prefix hijacks. They illustrate how network visualizations have the potential to assist an analyst in detecting abnormal routing patterns in massive amounts of BGP data. Papadopoulos et al. [Papadopoulos13] present a scheme for visualizing and exploring BGP path change anomalies. It uses a set of BGP features that are capable of quantifying the degree of anomaly of each path change event. Moreover, visual methods are introduced for performing the efficient fusion of these multiple features.

Other works provide visualizations to explore and understand inter-related datasets and clusters describing large-scale attack campaigns with the goal of determining their root causes and deriving their modus operandi. Fischer et al. [Fischer14] combine a multi-criteria clustering algorithm, tailor-made for the identification of attack campaigns with three interactive visualizations, namely treemap representations, interactive node-link diagrams, and chord diagrams, to allow the analysts to visually explore and make sense of the resulting multi-dimensional clusters. Tsigkas et al. [Tsigkas12] present a visual analytics tool introducing a new kind of graph

visualization that exploits the nodes degree to provide a simplified and more abstract, yet accurate, representation of the most important elements of a security data set and their inter-relationships. The main goal of the visual analytics tool is to provide security analysts with an effective way to reason interactively about various attack phenomena orchestrated by cyber criminals.

Visualizations more related to the scope of project aid an administrator in not only the detection of attacks but also the display of multistep attacks. Different types of attacks show different behaviours and accordingly different visual patterns appear [Shiravi12]. These visualizations use different types of data sources; the most frequently used data sources are Network Traces, both Packet Traces (i.e., full IP packets transferred over the network) and Network Flows (i.e., aggregation of packets on a flow-based level enriched with metadata).

Starting from Packet Traces data, Cappers and van Wijk [Cappers15] propose a bottom-up pixel-oriented approach for network traffic analysis where the expert starts with low-level anomalies and iteratively gains insight into higher level events through the creation of multiple selections of interest in parallel. The tight integration between visualization and machine learning enables the expert to iteratively refine anomaly scores, making the approach suitable for both post-traffic analysis and online monitoring tasks. Nunnally et al. [Nunnally13] propose a novel 3D Parallel coordinate visualization tool for advanced network scans and attacks that uses flow data, filtering techniques, and state-of-the art 3D technologies to help network administrators detect distributed and coordinated network scans. Corchado et al. [Corchado11; Herrero09] introduce an IDS that applies neural projection architectures to detect anomalous situations taking place in a computer network. By its visualization facilities, the proposed IDS allows providing an overview of the network traffic as well as identifying anomalous situations tackled by computer networks, responding to the challenges presented by volume, dynamics and diversity of the traffic, including novel (0-day) attacks. Theron et al. introduce a new visualization tool for network-wide intrusion detection in [Theron17]. Combining Principal Component Analysis (PCA) and a new variant called Group-wise PCA (GPCA) with the capabilities of interactive visualization, the resulting tool allows the user to navigate through the enormous amount of data collected in the network, in order to find anomalous or unexpected behaviours.

Using Network Flows, Ortiz-Ubarri et al. [Ortiz15] present TOA, a web-based data monitoring system (NMS) that consists of a collection of scripts that automatically parse network flow data, store this information in a database system, and generate interactive timeline charts for network visualization analytics. Choi et al. [Choi09] presents a tool for detecting unknown large-scale Internet attacks including Internet worms, DDoS attacks and network scanning activities. It displays network traffic on the plane of parallel coordinates using the flow information such as the source IP address, destination IP address, destination port and the average packet length in a flow. Fowler et al. [Fowler14] propose a novel visualization, IMap, which enables the detection of security threats by visualizing a large volume of dynamic network data. In IMap, the Internet topology at the Autonomous System (AS) level is represented by a canonical map (which resembles a geographic map of the world), and aggregated IP traffic activity is superimposed in the form of heat maps (intensity overlays). Wagner et al. [Wagner10] introduce a method for getting insights into IP related data flows validating it by inspecting traffic of high-interaction honeypots. Cappers et al. [Cappers18] present a case study of the visual analytics tool EventPad and illustrate how it is used to gain quick insights in the analysis of PCAP traffic using rules, aggregations, and selections.

Considering also IDS/IPS alerts, Inoue et al. [Inoue12] present an alert system called DAEDALUS which is based on large-scale darknet monitoring. The paper presents a novel real-time 3D visualization engine that enables operators to grasp visually and in real time a complete overview of alert circumstances and provides highly flexible and tangible interactivity. Yelizarov et al. [Yelizarov09] present a technique whereby the operator, using visualization alone, is able to display the full picture of events occurring in the network. The main feature of this method is the high recognition ratio of complex attacks as the sequence of constituent common events. Mansmann et al. [Mansmann09; Fischer08] propose a system to support analysis of IDS logs

that visually pivots large sets of Net-Flows. In particular, two visual representations of the flow data are compared: a treemap visualization of local network hosts, which are linked through hierarchical edge bundles with the external hosts, and a graph representation using a force-directed layout to visualize the structure of the host communication patterns. Zhao et al. [Zhao12; Zhao13] present a novel visualization framework for IDS alerts that can monitor the network and perceive the overall view of the security situation using radial graph in real-time. The framework utilizes five categories of entropy functions to quantitatively analyze the irregular behavioural patterns, and synthesizes interactions, filtering and drill-down to detect the potential intrusions.

Other systems consider other data sources and target specific issues of the network security domain. Zhao et al. [Zhao14] propose a visual analytics system composed of multiple coordinated views to support the analysis of multiple heterogeneous network security datasets. Alsaleh et al. in [Alsaleh13] correlate IDS logs with the corresponding web server logs and plot the security-related events. Liao et al. [Liao10] highlight how very often visualizations are more focused on point-to-point communications that involve hosts IP addresses and port numbers that on users and applications and propose a tool to overcome this issue. Chen et al. [Chen18] propose a map-based visual metaphor and create an interactive map for encoding user behaviours. It enables analysts to explore and identify user behaviour patterns and helps them to understand why some behaviours are regarded as anomalous. Furthermore, some works face general issues and the cybersecurity domain are used as usage scenario. For example, Jäckle et al. [Jackle16] propose Temporal Multidimensional Scaling (TMDS), a novel visualization technique that computes temporal one-dimensional MDS plots for multivariate data which evolve over time and demonstate its usefulness in two case studies in the network security field. Using a sliding window approach, MDS is computed for each data window separately, and the results are plotted sequentially along the time axis, taking care of plot alignment. TMDS plots enable visual identification of patterns based on multidimensional similarity of the data evolving over time.

Orthogonal to the others, the last use case is the support in the analysis of malware samples both statically (i.e., the malware is processed and disassembled to reveal interesting patterns) and dynamically (i.e., the malware is executed within a sandbox environment to reveal its behaviour). Wagner et al. [Wagner15] provide a systematic overview and categorization of malware visualization systems from the perspective of visual analytics (see Figure 36). Additionally, they identify and evaluate data providers and commercial tools that produce meaningful input data for the reviewed malware visualization systems.

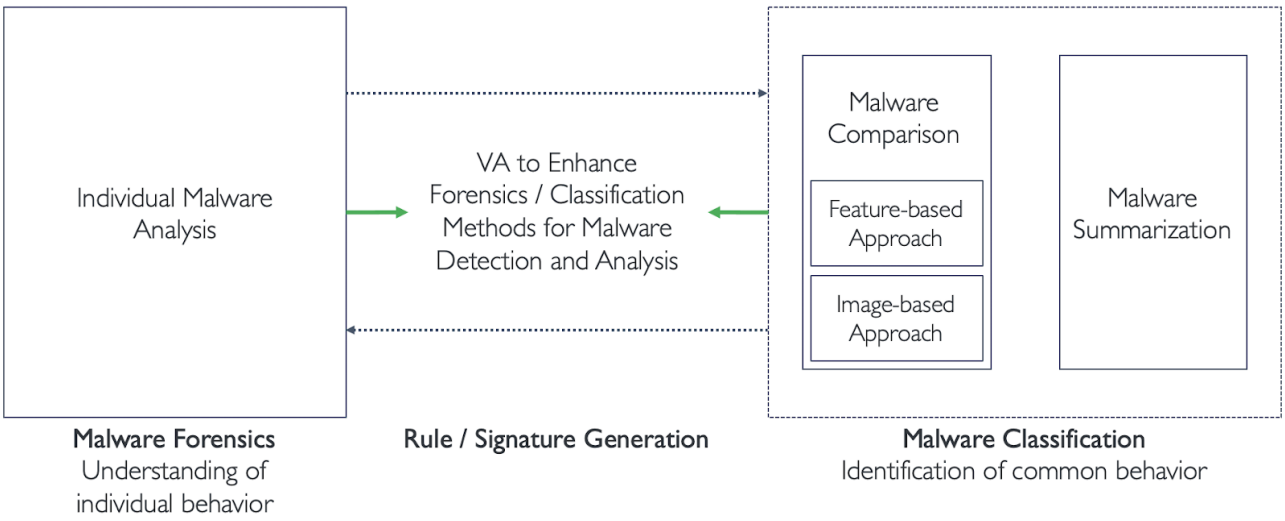

Figure 36: Malware visualization taxonomy, modified from [Wagner15]

The systems for Individual Malware Analysis support the individual analysis of primarily single malware samples to gain new insights of its individual behaviour related to malware forensics. Zhuo and Nadjin [Zhuo12] present a utility that provides security researchers a method to browse, filter, view and compare malware network traces as entities. They propose a cell-view to represent a set of streams generated by a malware instance consisting of a circular timeline, a disk panel to display details-on-demand, and a set of cilia oriented clockwise along the timeline to represents the set of streams. Visualization tools for Malware Comparison are primarily used for the comparison of n to m malware samples for the identification of common behaviours (e.g., the malware family) to support malware classification. A first approach is to explore and compare different malware samples based on extracted features. In [Gove14] of Gove et al., malware attributes are assigned to meaningful categories to compare multiple malware samples through set comparison overviews and dynamic filtering. Similarity histograms and Venn diagrams are used to compare samples with respect to categories. A second approach is to generate visual images based on binary data or the behaviour logs of the malicious software. Shaid and Maarof [Shaid12] visualize malware through images representing their behaviour (i.e., what malware does, exhibits, or causes to its environment during live execution) defined through their API calls, previously sorted and grouped based on the level of maliciousness. Systems for Malware Summarization summarize the behaviours of n different malware samples to identify similarities and to gain new insights of their common behaviour. Han et al. [Han14] generate RGB-colored pixels on image matrices using the opcode sequences extracted from malware samples using dynamic analysis and calculate the similarities for the image matrices.

Commercial tools that very often use VA techniques to enhance SA are Security Information and Event Management (SIEM) systems that provide real-time analysis of security alerts generated by network hardware and applications. They combine the characteristics of Security Information Management (SIM) systems that supply reporting and analysis on long-term, with the characteristics of Security Event Management (SEM) systems that deal with real-time monitoring. Their main capabilities are: data aggregation, correlation, alerting, compliance, retention, forensic analysis. They take advantage of VA tools especially to support patterns visualization and the identification of activities that don’t fall in standard patterns. Their structure is often a dashboard which includes a series of visualizations integrated together. Splunk [SPLUNK] products are used for IT operations, application performance management, business intelligence and, increasingly, for security event monitoring and analysis. They provide predefined dashboards, correlation rules, searches, visualizations and reports to support real-time security monitoring and alerting, incident response, and compliance reporting use cases. LogRhythm [LOGRHYTHM] combines event, endpoint and network monitoring capabilities, an integrated incident response workflow and automated response capabilities using a risk-based prioritization scoring algorithm. The QRadar platform [QRADAR] enables collection and processing of security event and log data, NetFlow, network traffic monitoring using deep-packet inspection and full-packet capture, and behaviour analysis for all supported data sources.

Attack graph visualization

In this section we will focus our attention on attack graph visualization as this model is able to enable and support: a) threat and vulnerabilities analysis, b) risk evaluation and quantification process and c) identification of response plans to mitigate risks. The NetSPA tool [Artz02; Ingols06] of Artz computes attack graphs and comprises a component that generates a visual representation of the computed attack graph. NetSPA graphing subsystem makes the attack graph simpler by pruning it: when a node is identified as a target, every node that is reachable from that node is deleted; similarly, paths that do not lead to a target node are deleted. While this approach efficiently simplifies the attack tree, it is based on the hypothesis that all of the attacker’s goals have been properly identified and that a node can be either a target node or an intermediate node but not both of them, which might be a strong assumption in some cases. Williams et al. [Williams07; Williams08] extended NetSPA by proposing GARNET, a treemap based visualization that reflects physical or logical topology and allows for displaying node reachability and evaluating the actual situation by interacting with the

system. Chu et al. [Chu10] presents a tool named NAVIGATOR (Network Asset VIsualization: Graphs, ATtacks, Operational Recommendations) as an improvement to GARNET. Using NAVIGATOR, users can visualize the effect of server-side, client-side, credential-based, and trust-based attacks. By varying the attacker model, NAVIGATOR can show the current state of the network as well as hypothetical future situations, allowing for advance planning.

Noel and Jajodia [Noel04] addressed attack graph usability through aggregation and interaction. Aggregation is performed following various rules such as “multiple exploits deal with the same attacker/victim couple”, “machines belong to the same subnetwork”, “a given deviceexhibits various vulnerabilities”, etc. Users can also perform un-aggregation to obtain details on parts of the attack graph. Noel et al. [Noel05] extended this work with supplementary representations, i.e., adjacency matrices that offer other opportunities to drill-down into attack graphs and to evaluate the impact of changes in the network configuration. O’Hare et al. [OHare08] presented another extension of this work that allows to evaluate the consequences of hardening on the attack graph, the evaluation method being presented in [Noel03]. Homer et al. [Homer08] proposed another simplification of attack graphs based on trimming “useless”, i.e., redundant attack paths.

Jajodia et al. [Jajodia12] describe advanced capabilities for mission-centric cyber situational awareness, based on defense in depth, provided by the Cauldron tool. Cauldron automatically maps all paths of vulnerability through networks, by correlating, aggregating, normalizing, and fusing data from a variety of sources. It provides sophisticated visualization of attack paths, with automatically generated mitigation recommendations. Flexible modeling supports multi-step analysis of firewall rules as well as host-to-host vulnerability, with attack vectors inside the network as well as from the outside.

Different works explored the degree of integration and maturity between the visualization and the underlying attack graph models; particularly for the reactive phase, the focus is in discovering anomalies in the network and correlating them with the attack graph for early attack detection; Emirkanian-Bouchard et Wang [Emirkanian16] explored metric driven techniques for visualizing attack graphs, based on presenting the most critical parts, with context specific visualizations. Yi et al. [Yi13] proposed a comparative overview on several open source and commercial solutions for attack graphs generation and visualization. Zhang et al. [Zhang17] proposed a survey on network anomaly visualizations, and AlEroud et Karabatis [AlEroud17] provided a comprehensive survey on existing prediction models for intrusion detection. Mathew et al. [Mathew06] proposed a visualization tool that displays attack tracks based on security events detected by IDSs or collected in log files. As such, this tool helps security operators in understanding ongoing attacks and evaluating the dynamic risk level. Regarding the response to ongoing attacks, Vandenberghe [Vandenberghe08] introduced NTE (Network Traffic Exploration), a system to explore network traffic to identify attacks. Among other representations, NTE proposes a visualization that maps network events to networks diagrams. This mapping therefore displays the attack sequences. Users can obtain more information about proposed responses to attacks, secondary effects as well as operational and IT impacts.

Chen et al. propose OCEANS [Chen14] that has the aim to create deeper insights in detecting network events by allowing close collaboration among security analysts. It allows to share information between users through a multi-level visualization that shows temporal overview, IP connections and detailed connections. Angelini et al. [Angelini19] present a Multi-step cyber Attack Detection (MAD) Visual Analytics solution aiming at assisting security operators in improving their network security by analyzing the possible attacks and identifying suitable mitigations. Moreover, during an attack, the system visually presents the security operator with the relevant pieces of information allowing a better comprehension of the attack status and its probable evolution, in order to make decisions on the possible countermeasures. Complementary to the aforementioned work, Angelini et al. [Angelini18] present VULNUS (VULNerabilities visUal aSsessment), a visual analytics solution for dynamically inspecting the vulnerabilities spread on networks, allowing for a quick understanding of the network status and visually classifying nodes according to their vulnerabilities. Moreover, VULNUS computes

the approximated optimal sequence of patches able to eliminate all the attack paths and allows for exploring sub-optimal patching strategies, simulating the effect of removing one or more vulnerabilities.

12. Discussion and relation of finding to PANACEA research

In Chapters 5-11 we discussed the current state of the art approaches to identifies threats, vulnerabilities, risks and identify the corresponding countermeasure with particular emphasis on the results obtained in the Health care domain.

From the literature review carried out it is possible to summarize the following existing limitations:

- ***Immaturity of the Heath care domain with respect to cyber security***. In Chapter 6, we provided an overview of current top10 risks and incidents in the healthcare domain. It is clear that the healthcare domain is particularly appealing to cyber attackers and at the same time it is not yet ready to fight them properly. As we discussed in Chapter 7, there exists a plethora of threat models and repositories that may help, at different level of granularity and details, to characterize cyber security issues and possible attacks. However, all of them are not domain specific and thus they require a certain effort to be applied and instantiated in a specific domain. All the existing results specifically related to the healthcare domain (cfr. Chapter 6.2 and 6.3) are looking just to a specific confined problem and they do not provide a general framework to globally increase the security level of healthcare organization. Existing approaches to threat modelling and vulnerability identification are valid guidelines but they require a certain degree of adaptation to be tailored to the healthcare domain in order to capture all the possible peculiarities of this specific environment.
- ***Lack of a global view in the threat and vulnerability identification***. From the detailed review reported in Chapters 7-11, it is clear that many models and tools have been designed to represent and analyse a specific view of a complex organization i.e., the ITC view or the business view or the human view. However, at the best of our knowledge, no effort has been done so far to consider together all these dimensions characterizing a complex ecosystem. Few efforts try to combine the ICT layer with the business layer but so far, no effort tried to relate those layers with the interacting humans. To the best of our knowledge, there not exists a model that is able to represent interactions between humans (e.g., medical personnel, non-medical personnel, patients, cyber security operators, ICT operators etc…), ICT infrastructure and business services and that is able to support a larger risk identification process.
- ***Lack of a global view in the risk identification and mitigation process***. Current Risk evaluation and quantification techniques do not take explicitly in to account consequences for the ICT infrastructure following by the lack of awareness of human being. This is partially due to the considerations done in the previous point about the lack of a model that is able to characterize the environment both from the ICT point of view and from the human point of view.
  Additionally, when considering cyber risks, the risk treatment and the definition of mitigations and countermeasures usually is done at purely at the technical level i.e., by identifying actions that will act directly on the ICT infrastructure by modifying its configuration and set up (e.g., modifying firewall rules, installing patches, performing software and firmware updates, switching off services/machines/devices) or a non-technical level i.e., by identify missing policies and/or identify when and where a training program should be performed.

The PANACEA research goes in the direction of reducing such limitations by:

- Define new models that are able to capture the multi-dimensional relationships that exist between the ICT layer, the business layer and the human layer in order to provide a larger picture of possible threats and vulnerabilities that may lead to an attack.
- Define new methods that will enable to analyse and evaluate risks by leveraging on the multi-dimensional view provided by our models.
- Define new methods to mitigate risks that consider together both technical and non-technical aspects in order to propose the best response.

13. Conclusion

PANACEA project aims to deliver a people-centric cybersecurity solution in healthcare. PANACEA will design and implement two toolkits for cyber security assessment and preparedness of Healthcare ICT infrastructures and connected devices: the PANACEA Solution Toolkit (made up of 4 technological tools and 3 organisational tools) and the PANACEA Delivery Toolkit (made up of 2 support tools)[48]. To achieve this goal we identified a number of measurable objectives to allow PANACEA research to reach beyond the current state-of-the-art in a number of relevant areas: Dynamic risk assessment and mitigation; Secure information sharing; System Security-by-design and certification; Identification and Authentication; Educational packages for cybersecurity in the health sector; Resilience governance; Secure behaviours nudging; Guidelines for cybersecurity; Security-ROI methodology and finally on the Engagement of community Stakeholders.

WP2 – "Research on advanced threat modelling, human factors, resilient response and secure Interconnectivity" aims in providing a deep insight of both scientific and technological state of the art on cybersecurity in healthcare, relevant risk scenarios, current countermeasures technologies and vulnerability methodologies, current approaches on human behavior and nudging. Task *T2.1: "Health Services vulnerabilities, cyber-risk scenarios and current countermeasures*" goal was to perform a focused literature review and an analysis for existing cyber risk scenarios, current countermeasures and vulnerability assessment methodologies in the HC domain. This document reports our findings with a particular emphasis on the healthcare domain but also considering more general approaches that leave the floor open for their application in such critical environment. We provide a detailed overview of the current situation, in terms of common vulnerabilities, possible relevant cyber-attack scenarios and related countermeasures. In addition, we provide a scientific and technological review of all the relevant aspects related to the design and implementation of a Dynamic Risk Management Platform (e.g., existing threat and attack models, risk identification and mitigation methodologies, etc.). Finally, we highlighted a number of important challenges and research gaps currently existing in the healthcare domain. The goal of this report is to assist PANACEA efforts in identifying most relevant state of the art approaches and to apply or extend them in the healthcare domain fighting challenges imposed by this extremely complex ecosystem. The importance of the work performed, not existing in such a form in the literature, is thus related to the adaptation and optimization of the PANACEA approach.

For our detailed literature review we used 380 related sources from which 330 were refereeing to existing papers, published in journals and periodicals, as well as presented in distinguished conferences and focused workshops, and around 50 public knowledge sources available online. Our effort was to identify and narrow existing work within the areas of interest of the PANACEA project for: Cyber security in HealthCare: scenarios and perspectives; Vulnerability and threat modelling; Human Behavioral modelling; Risk Quantification and Governance; Attack response: Hardening approaches; Visual Analytics for increasing situational awareness and to project our finding for PANACEA research.

More specifically:

- Section 6 presented the specificities of requirements for cybersecurity in HC. Specificities of the domain are explained, alongside with statistical data and prior publications that reinforce the need for more cybersecurity awareness to be in place. We presented a number of risks, cyber threats, known breaches and scenarios and the current security approaches and countermeasures. Our analysis showed that HC organizations face a number of threats and security risks mainly due to the use of

[48] https://www.panacearesearch.eu/innovations

services and devices, unsecure networks, employee negligence, bring your own device (BYOD) policies, misuses of common services (i.e. email), user privileges for access on sensitive systems, lack of internal identification and security systems, etc..

- In Section 7 we delved into the state of the art vulnerability and threat modelling approaches. Our analysis provided a detailed review of the most common approaches to threat modelling and vulnerability identification, classification, evaluation and assessment. These approaches are general enough to be adopted as basic building block in the healthcare domain. We described existing attack libraries, vulnerability assessment methodologies and risk analysis methods. We presented specific threats in the healthcare domain and included formalisms and frameworks that can be used to share and communicate threats.
- Section 8 provided insights about the human component and how to optimise employees’ digital (and physical) security behaviours. We showed that even though traditionally, employees have been considered to be a weak link in the security chain as their behaviour is estimated to account for a large portion of security breaches, there is little understanding about how to improve this. We emphasized on how to understand the factors which affect human behaviour for cyber security and showed evidence on the fact that the related research is sparse and fragmented. We identified thus a considerable gap between what is currently known and what needs to be studied in order to holistically protect an organisation against security threats in different domains particularly healthcare (i.e. to address the human component of cyber security we need to: provide reliable behavioural data on individual employees, research on the factors influencing employees’ security practices or lack thereof, provide a universal theory of human behaviour towards security and an agreement between stakeholders on the necessary behaviours required).
- Section 9 presented the governance, business impact analysis, risk quantification and risk assessment concepts for cyber security in healthcare. Identification of the assets and their assessment, the potential threats, and their countermeasures are all tasks to be considered especially in the health domain where the patients’ safety could be at risk. Our literature findings showed that business analysis and risk assessment are required in order to enable adequate planning for delivering essential information about the impact of resources’ and the unwanted disruption on business for a cyber-security inside net. Most of the existing studies try to calculate the economic impact based on the cost of loss of production and quality. We found that currently none of the existing studies and related results have actually been applied in the HC. On the other hand, our finding show the apparent progress in terms of policies, legal and regulatory considerations (i.e. GDPR, EU Cybersecurity Act).
- Section 10 provided an overview on current approaches that can be adopted in order to implement an attack response trough the definition of the proper countermeasures. We focused our attention on approaches based on the attack graph model as this seems to be a valid tool to both model threats and vulnerabilities. This model is able to enable and support both the risk evaluation and quantification process and the definition of response plans to mitigate risks. We also described the need of a Dynamic Risk Management Platform (DRMP) for supporting cyber security operators in taking informed decision to increase the overall security level of a given healthcare organization
- Finally, section 11 provided our findings on Visual analytics for increasing situational to easily identify network threats and gain important knowledge about their nature. Our findings showed that most of the visual analytics techniques for cyber security do not explicitly focus on dynamic real-time characteristics. However, concerning situational awareness, such capabilities are crucial and thus important for PANACEA. An important element to categorize existing works is the intended use case. Inspired by previous works, we identify two macro categories: Network Activity and Network Threats.

In conclusion, this document provided our findings and an overview of the state of the art in terms of cyber risk scenarios, current countermeasures and vulnerability assessment methodologies in the healthcare domain. This detailed review, as described in section 12, and all our findings will be used and exploited, throughout PANACEA project, to support the research, modeling, design and implementation for the:

- *Dynamic risk assessment and mitigation tools for threat modelling, attack modelling, response management and visual analytics*
- *Secure information sharing tools, to measure data integrity and consistency performance tradeoffs for Identification/Authentication tools and Internet of Things (IoT)/Internet of Medical Things (IoMT)*
- *Secure behaviors nudging tools for the analysis and promotion of cyber secure behaviors within a healthcare organization*.