ΟΙΚΟΝΟΜΙΚΟ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΑΘΗΝΩΝ

ATHENS UNIVERSITY
OF ECONOMICS
AND BUSINESS

ΣΧΟΛΗ ΕΠΙΣΤΗΜΩΝ &
ΤΕΧΝΟΛΟΓΙΑΣ ΤΗΣ
ΠΛΗΡΟΦΟΡΙΑΣ
SCHOOL OF INFORMATION
SCIENCES & TECHNOLOGY

ΜΕΤΑΠΤΥΧΙΑΚΟ ΣΤΑ
ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ
MSc IN **INFORMATION SYSTEMS**

Master's dissertation:

Health data security and privacy

Professor and Programme Director in Department of Informatics: Dr. Dimitris Gritzalis

Graduate student: **Michael Stefanoudakis**	Graduate student number: p314815

ATHENS

SEPTEMBER 2020

Thesis Acknowledgements

First and foremost, I would like to express my sincere gratitude to the Programme Director of MSc in Information Systems and supervisor, Professor Dr. Dimitris Gritzalis for the continuous support of my study. His guidance helped me in all the time of preparation and writing of this thesis.

Besides my supervisor, I would like to thank my thesis advisor PhD candidate George Iakovakis for his motivation, enthusiasm, and encouragement and of course for the continuous advising for the writing of this thesis.

Last but not least, I would like to thank my family: my wife Alexandra Koronia for her patience, my daughter Maria Stefanoudakis and also my parents Manolis Stefanoudakis and Agapi Stefanoudakis for supporting me spiritually throughout my life.

Abstract

Through this senior thesis we try to expand the issue of eHealth Data Security and Privacy. The purpose of this study is to present the current situation in Europe, and in particular in Greece regarding the implementation of security legislation and policies. Nowadays especially, the COVID-19 crisis has made the prevention an urgent need and the lessons that humanity has learned lessons that hopefully are enough to highlight the role of security and privacy in the whole eHealth ecosystem.

In this thesis we will analyze aspects of eHealth like cyber threats, eHealth specific issues on security and privacy, state-of-the-art cybersecurity measures and solutions, and eHealth cybersecurity and privacy issues associated with the COVID-19. To have a better understanding of all these mentioned above, firstly we define eHealth according to International Organizations like WHO and European Union, and we present a National eHealth component map that provides the useful information in order to understand what is included in eHealth governance, eHealth solutions, eHealth infrastructure and eHealth enablers. Another significant point of this thesis is the eHealth subsectors, like mHealth, Telehealth, Electronic Health Records systems, Social media in Health Care and Legal frameworks for eHealth. Furthermore we show through figures the ICTs pillars and ICTs supporting the eHealth, such as Cloud Computing, Fog and Multi-Access Edge Computing (FMEC), Internet of (Medical) Things, Artificial Intelligence, Blockchain Technology, 5G, and Big Data.

In addition, an extended reference not only of terms and concepts in cybersecurity is necessary to be presented, but also the relationship between cybersecurity and other security domains. Also the Security Services and Mechanisms like Authentication Service, Access Control, Data Confidentiality, Data Integrity, Non Repudiation, and Availability Service are analyzed.

At this point it is worth mentioning the taxonomy of Security Threats and attacks in general. More specifically are presented Threat Actors, Threat Sources, Methods and Tools that can affect IT systems. We take into account not only adversarial attacks but non-adversarial threats as well. Studying the past few years, we can summarize the

cyberthreat landscape through the timeline of security attacks on health care data from 1989 to 2019, and specifically for the year 2019 the data breach statistics related to healthcare. As far as it concerns special issues of eHealth sector, it could be summarized in a list which includes: a) the concurrent use of many emerging ICTs which have in fact developed in the last decade and each of them presents its own security issues, b) the billions of people who benefit from the eHealth services, c) the multidimensional information contained in medical records, d) the proliferation of mobile devices, especially smartphones, which mainly results in the heavy use of wireless networks for myriads of mobile applications and, in many circumstances functioned as fog nodes, e) the extended use of web services such as email and, also, of web applications and finally f) the plethora of medical things. Through this thesis we came to the conclusion that is necessary to follow and use guidelines for edifying the eHealth ecosystem security like the foremost used guideline of *NIST: Framework for improving critical infrastructure cybersecurity*. Regarding with eHealth assets and relevant threats, we must emphasize that if we map them, then we can assess possible attacks and identify security measures and use potential good practices to protect systems. We depict horizontal models and vertical as well, to identify assets for FMEC – Fog and Multi-Access Edge Computing, and for IoMT – Internet of Medical Things. If we want to categorize the eHealth Ecosystem assets in high level, we can do it, as follows: a) Medical things, b) FMEC devices, c) Communications, d) Infrastructure, e) Platform and Backend, f) Decision Making g) Application and services and finally h) Data. Moreover, with mapping critical assets and relevant threats, we can assess possible attacks and identify security measures and use potential good practices to protect systems. In this study, we tried to cover a wide range of security tools as solutions, for the confrontation of the main threats such as:

protection

- Endpoint protection

- Network Management

The dramatic experience of COVID-19 especially in countries such as Italy and USA obviously has highlighted the importance of effective eHealth cybersecurity due to successful attacks in eHealth security. Also we present primary cases of COVID-19 digital public health technologies, in Taiwan, Singapore, and Spain.

Nevertheless, we must take into consideration how ethical principles, raise ethical and legal issues in relation to digital public health technologies against COVID-19. There is no surprise that during the COVID-19 pandemic, more sophisticated intrusion methods, were detected and reported. In conclusion, we must say that despite the progress of cybersecurity in eHealth sector, there are still many significant factors that have as a result failures to effective cybersecurity implementation of security measures in healthcare organizations. Certainly, future surveys on cybersecurity measures would be useful to cover the implementation of all emerging technologies in the sector of eHealth ecosystem.

Key - Words: **Attack, Cyber Attack, Threat, Vulnerability, Adversarial threat sources, Non-adversarial threat sources, Security service, Security mechanism, Countermeasures, security measures, Attack Vector.**

Table of contents

Table of figures

Table of tables

Acronyms and abbreviations

AA	Authentication and Authorization
AI	Artificial Intelligence
AIOTI	The Alliance for the Internet of Things Innovation
BAN	Body Area Network
BD	Big Data
CASB	Cloud Access Security Brokers
CC	Cloud Computing
CII	Critical Information Infrastructure
CoAP	Constrained Application Protocol
COVID-19	Corona Virus Disease 2019
CPS	Cyber Physical System
CSIRT	Cyber Security Incident Response Team
DoS	Denial of Service
DDoS	Distributed Denial of Service
EC	European Commission
EHR	Electronic Health Records
EMR	Electronic Medical Record
ENISA	European Union Agency for Network and Information Security
ETSI	European Telecommunications Standards Institute
EU	European Union
FMEC	Fog and Multi-Access Edge Computing
GDPR	General Data Protection Regulation
HIT	Health Information Technology
H2M	Human-to-Machine
IAM	Identify and Access Management
ICT	Information and Communications Technology

IDS	Intrusion Detective Systems
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IoT	Internet of Things
IPS	Intrusion Preventive Systems
ISO	International Organization for Standardisation
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardisation Sector
LAN	Local Area Network
LoRaWAN	Long Range Wide Area Network (Low Power)
M2M	Machine-to-Machine
MEC	Multi-Access Edge Computing
MIMT	Man In The Middle
ML	Machine Learning
MQTT	Message Queuing Telemetry Transport
NCCoE	National Cybersecurity Center of Excellence
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
OS	Operating System
OSI	Open Systems Interconnection
PAN	Personal Area Network
PET	Privacy Enhancing Technologies
PHR	Personal Health Record
TTP	Tactics Techniques and Procedures
WAF	Web Application Firewalls
WAN	Wide Area Network
WHO	World Health Organization

1 Introduction

eHealth is the use of Information and Communication Technologies (ICTs) for health and integrates a bunch of ICTs. Also, security and privacy presenting the greatest challenges for all ICTs. eHealth is prevalent around the world and transforms the care delivery, but there is also increasing concerns relating to the security of healthcare data and devices. Nowadays, the amount of data handled by information systems grows exponentially, which implies higher exposure of patients' sensitive data. The security and privacy of the data collected from devices, either during their transmission through communication networks or while stored, are major unresolved concerns. ICTs integration challenges, including different medical technologies, combined with the requirement to share information between newly merged organizations creating new vulnerabilities. This tendency does is growing up and these new vulnerabilities have not gone unnoticed by cybercriminals seeking to access and exploit the data being shared. Cyber threats are increasing in scale and severity and organizations recognize that Cybersecurity is more than ever a priority for eHealth.

The scope of this work is to expand on security and privacy issues in the eHealth sector. In particular, we will explore the current situation in Europe and Greece regarding the implementation of security legislation and policies.

Chapter 2 and 3 introduces the main concepts and terms used throughout this thesis.

In **Chapter 2** the eHealth-related terms and concepts are provided. More specifically we have extracted useful information provided by the World Health Organization related to eHealth. Next, eHealth subsectors and Information and Communications Technologies related to eHealth are presented.

In **Chapter 3**, we introduce the security and privacy-related concepts and the foremost important of Standards Developing Organizations (SDOs) that are involved within the development or promotion of standards that are being developed for various aspects of cybersecurity in standardization related to cybersecurity. The field security in generally consists of measures to deter, prevent, detect, and correct security violations that involve the transmission of information. That is a broad statement that covers a host of possibilities.

In **Chapter 4**, a comprehensive taxonomy of the most common cyber threats is provided. Also attack methodology and a brief timeline of security incidents, threats landscape and trends are presented in this chapter.

Proceeding in the **Chapter 5**, readers of the thesis can receive information about the differences between security and privacy. The need for security guidelines is emphasized at this point and a presentation of the NIST Core Framework is made.

In **Chapter 6** we focus on cybersecurity measures and solutions in the eHealth sector and more specifically we try to analyze technical measures, eHealth security measures and solutions to defend against threats. An important issue that arose recently is the coronavirus pandemic.

In **Chapter 7** we present the COVID-19 related information for the security of systems and people’s privacy.

Last but not least in **Chapter 8** and **Chapter 9** not only useful conclusions of our thesis are presented, but also directions for a future work.

Important notice: the terms Cybersecurity and information security are related to security and safekeeping ICT systems against data threats and information breaches. Nevertheless, there are quite a few differences between them. In this thesis, these two terms used interchangeably and we clarify the differences whenever necessary.

2 eHealth

The role of eHealth is vital in promoting universal health coverage in a variety of ways. eHealth helps provide services to people and communities through telehealth or mHealth, simplifies the training of the health workforce through the use of eLearning, and makes education more widely accessible especially for those who are isolated and enhances diagnosis and treatment by providing accurate and timely patient information through health records. eHealth through the use of ICT, improves the operations and financial efficiency of health care systems [1].

The most important and specialized organization in the world in the field of healthcare is the World Health Organization (WHO)[1], an agency of the United Nations. The WHO is responsible for international public health and plays a central role shaping and monitoring eHealth's future. Greece is member state of the European Union (EU) - therefore implements its policies and actions. So, our intention is to draw all the relevant information about the work primary from their sources.

WHO defines health positively as "*a state of complete physical, mental, and social well-being and not merely the absence of disease or infirmity*" and eHealth as " *the use of Information and Communication Technologies (ICTs) for health*."[2].

EU defines eHealth as digital health and care: "*digital health and care refers to tools and services that use information and communication technologies (ICTs) to improve prevention, diagnosis, treatment, monitoring and management of health and lifestyle. Digital health and care has the potential to innovate and improve access to care, quality of care, and to increase the overall efficiency of the health sector*"[3].

We must disambiguate the terms eHealth and "Smart health care". Smart health care it is also an integration of a bunch ICTs, but "*refers to solutions that can operate completely autonomously*" [2], so it is a subsector of eHealth sector.

2.1 WHO and eHealth

WHO is playing a central role in shaping and monitoring eHealth future as acknowledges that the field is quickly transforming the delivery of health services and systems around the world. WHO special eHealth unit, cooperates with agencies at the global, regional and country level "*to promote and strengthen the use of ICT in health development, from applications in the field to global governance*".

---

[1] https://www.who.int/
[2] https://www.who.int/ehealth/en/
[3] https://ec.europa.eu/health/ehealth/overview_en

World Health Organization (WHO) and the International Telecommunication Union (ITU) are the major United Nations agencies for health and telecommunications respectively, and in 2012 collaborated in order to publish the National eHealth Strategy Toolkit [3]. This is a guide that could be used to provide the basis and the methods to achieve a national eHealth vision, and, also frameworks for development and monitoring. From this guide we have extracted interesting information, which we present as follows:

a. Useful Definitions for eHealth Records

In [3] a terminology related to digital health records is provided as follows:

Electronic Medical Record (EMR) is "*a computerized medical record used to capture, store and share information between health-care providers in an organization, supporting the delivery of health services to patients. EMR systems may stand alone or may be integrated with other information systems in a health services organization. They function as the legal record created during the provision of care to the patient*."

Electronic Health Record (EHR) is "*a computerized health record used to capture, store, access and share summary information for a patient between health-care organizations and providers. Examples of information include demographics, medical history, medication and allergies, immunizations, discharge summaries and other summary information. Typically, EHRs are developed to support the provision of care across health-sector or geographical boundaries. They may also be used by individuals and their caregivers to take a more active role in the management of their own health*."

Personal Health Record (PHR) is "*a computerized health record created and maintained by an individual who is proactive in the management of her or his own health. The record can be private, or made available to health-care providers. PHRs can store a diverse range of information such as an individual's allergies, adverse drug reactions, chronic diseases, family history, illnesses and hospitalizations, medications, diet and exercise plans, and test results.*"

b. A National eHealth Component Map

In [3] the aforementioned agencies present a sample national eHealth component map, as shown in Figure 1. This map provides the whole picture for eHealth and provides useful information in order to understand what is included in eHealth governance, eHealth solutions, eHealth infrastructure and eHealth enablers.

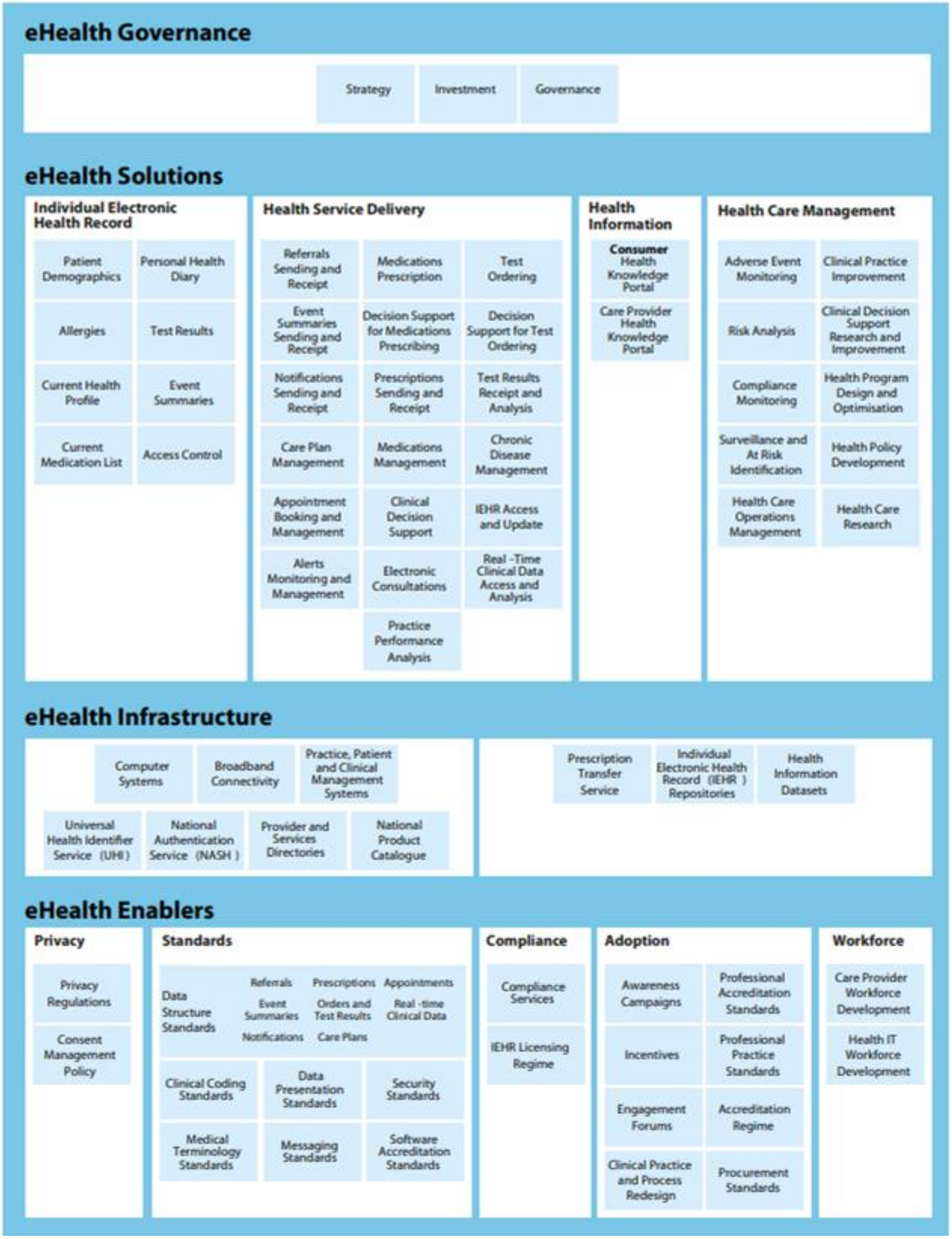
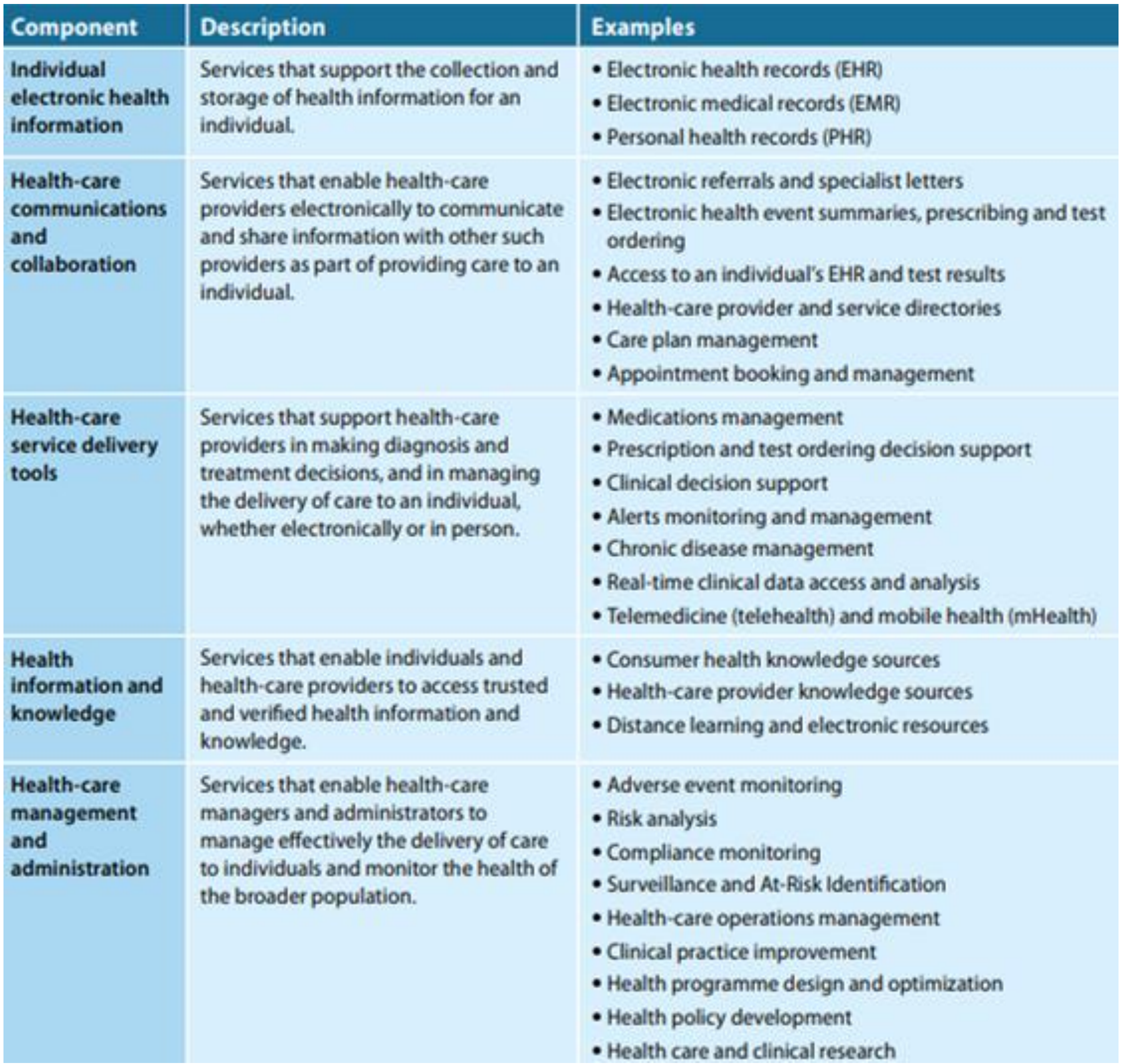

eHealth Governance
Strategy
Investment
Governance
eHealth Solutions
Individual Electronic Health Record
Patient Demographics
Personal Health Diary
Allergies
Test Results
Current Health Profile
Event Summaries
Current Medication List
Access Control
Health Service Delivery
Referrals Sending and Receipt
Medications Prescription
Test Ordering
Event Summaries Sending and Receipt
Decision Support for Medications Prescribing
Decision Support for Test Ordering
Notifications Sending and Receipt
Prescriptions Sending and Receipt
Test Results Receipt and Analysis
Care Plan Management
Medications Management
Chronic Disease Management
Appointment Booking and Management
Clinical Decision Support
IEHR Access and Update
Alerts Monitoring and Management
Electronic Consultations
Real -Time Clinical Data Access and Analysis
Practice Performance Analysis
Health Information
Consumer Health Knowledge Portal
Care Provider Health Knowledge Portal
Health Care Management
Adverse Event Monitoring
Clinical Practice Improvement
Risk Analysis
Clinical Decision Support Research and Improvement
Compliance Monitoring
Health Program Design and Optimisation
Surveillance and At Risk Identification
Health Policy Development
Health Care Operations Management
Health Care Research
eHealth Infrastructure
Computer Systems
Broadband Connectivity
Practice, Patient and Clinical Management Systems
Universal Health Identifier Service (UHI)
National Authentication Service (NASH)
Provider and Services Directories
National Product Catalogue
Prescription Transfer Service
Individual Electronic Health Record (IEHR) Repositories
Health Information Datasets
eHealth Enablers
Privacy
Privacy Regulations
Consent Management Policy
Standards
Data Structure Standards
Referrals
Prescriptions
Appointments
Event Summaries
Orders and Test Results
Real -time Clinical Data
Notifications
Care Plans
Clinical Coding Standards
Data Presentation Standards
Security Standards
Medical Terminology Standards
Messaging Standards
Software Accreditation Standards
Compliance
Compliance Services
IEHR Licensing Regime
Adoption
Awareness Campaigns
Professional Accreditation Standards
Incentives
Professional Practice Standards
Engagement Forums
Accreditation Regime
Clinical Practice and Process Redesign
Procurement Standards
Workforce
Care Provider Workforce Development
Health IT Workforce Development

Figure 1. National eHealth component map. [3]

c. Common eHealth Services and Application Components

eHealth improving the flow of information, through electronic means, to support the delivery of health services and the management of health systems. Figure 2 depicts common eHealth service and application components.

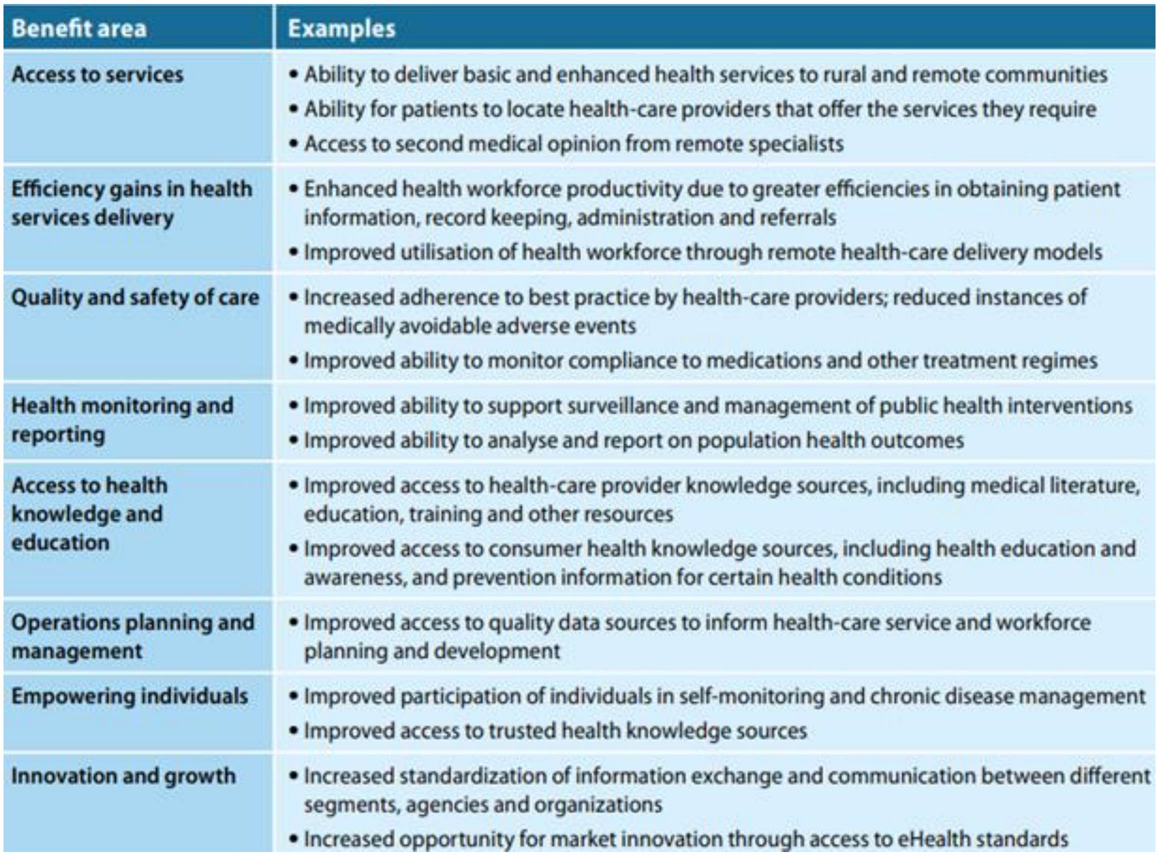


Component	Description	Examples
Individual electronic health information	Services that support the collection and storage of health information for an individual.	• Electronic health records (EHR) • Electronic medical records (EMR) • Personal health records (PHR)
Health-care communications and collaboration	Services that enable health-care providers electronically to communicate and share information with other such providers as part of providing care to an individual.	• Electronic referrals and specialist letters • Electronic health event summaries, prescribing and test ordering • Access to an individual's EHR and test results • Health-care provider and service directories • Care plan management • Appointment booking and management
Health-care service delivery tools	Services that support health-care providers in making diagnosis and treatment decisions, and in managing the delivery of care to an individual, whether electronically or in person.	• Medications management • Prescription and test ordering decision support • Clinical decision support • Alerts monitoring and management • Chronic disease management • Real-time clinical data access and analysis • Telemedicine (telehealth) and mobile health (mHealth)
Health information and knowledge	Services that enable individuals and health-care providers to access trusted and verified health information and knowledge.	• Consumer health knowledge sources • Health-care provider knowledge sources • Distance learning and electronic resources
Health-care management and administration	Services that enable health-care managers and administrators to manage effectively the delivery of care to individuals and monitor the health of the broader population.	• Adverse event monitoring • Risk analysis • Compliance monitoring • Surveillance and At-Risk Identification • Health-care operations management • Clinical practice improvement • Health programme design and optimization • Health policy development • Health care and clinical research

Figure 2. Common eHealth services and application components. [3]

d. eHealth Benefits

Generally speaking, the use of ICTs in every public or private sector offers a viable, easy to use, cost-effective and efficient methodology for providing services, monitoring, information, knowledge, and research. ICT provides noteworthy benefits not only in realizing health goals, but also in representing what has been accomplished and at what cost. There are certainly disadvantages and challenges, but we will not go into them at this point. Figure 3 depicts eHealth benefits.



Benefit area	Examples
Access to services	• Ability to deliver basic and enhanced health services to rural and remote communities • Ability for patients to locate health-care providers that offer the services they require • Access to second medical opinion from remote specialists
Efficiency gains in health services delivery	• Enhanced health workforce productivity due to greater efficiencies in obtaining patient information, record keeping, administration and referrals • Improved utilisation of health workforce through remote health-care delivery models
Quality and safety of care	• Increased adherence to best practice by health-care providers; reduced instances of medically avoidable adverse events • Improved ability to monitor compliance to medications and other treatment regimes
Health monitoring and reporting	• Improved ability to support surveillance and management of public health interventions • Improved ability to analyse and report on population health outcomes
Access to health knowledge and education	• Improved access to health-care provider knowledge sources, including medical literature, education, training and other resources • Improved access to consumer health knowledge sources, including health education and awareness, and prevention information for certain health conditions
Operations planning and management	• Improved access to quality data sources to inform health-care service and workforce planning and development
Empowering individuals	• Improved participation of individuals in self-monitoring and chronic disease management • Improved access to trusted health knowledge sources
Innovation and growth	• Increased standardization of information exchange and communication between different segments, agencies and organizations • Increased opportunity for market innovation through access to eHealth standards

Figure 3. eHealth benefits. [3]

In May 2005 WHO established an eHealth strategy and advised its member states to plan for appropriate eHealth services in their countries. In the same year, WHO launched the Global Observatory for eHealth (GOe), an initiative dedicated to the study and promotion of eHealth. From the day of its establishment, GOe provides WHO member states with information and guidance on effective policies and standards related to eHealth.

2.2 eHealth subsectors

The WHO Global Observatory defines eight thematic subjects, each offering its perspective on the contribution of eHealth to universal health coverage. This thematic separation defines eHealth subsectors related to work and provides us useful concepts and terms in work. These subsectors are described in detail as follows.

2.2.1 mHealth

WHO defines in [1] mHealth[4] (also known as mobile health) as "*the use of mobile devices – such as mobile phones, patient monitoring devices, personal digital assistants (PDAs) and wireless devices – for medical and public health practice*". mHealth is an important subsector of eHealth and includes a broad spectrum of services and applications. For example, we could mention telephone helplines and text message appointment reminders, mobile telehealth and, mobile access to digital health records. mHealth has a major contribution to realizing the goal of provision healthcare globally through making services available to remote individuals and communities. mHealth is the solution to increase access to and provision of health services in areas wherever mobile communications technology infrastructure has been prioritized concerning Internet infrastructure. The penetration of mobile computing technology globally brings with it the chance for mHealth to possess a different impact than traditional health services. mHealth applications[5] categorized in Table 1 according to [1] (see also Figure 4).

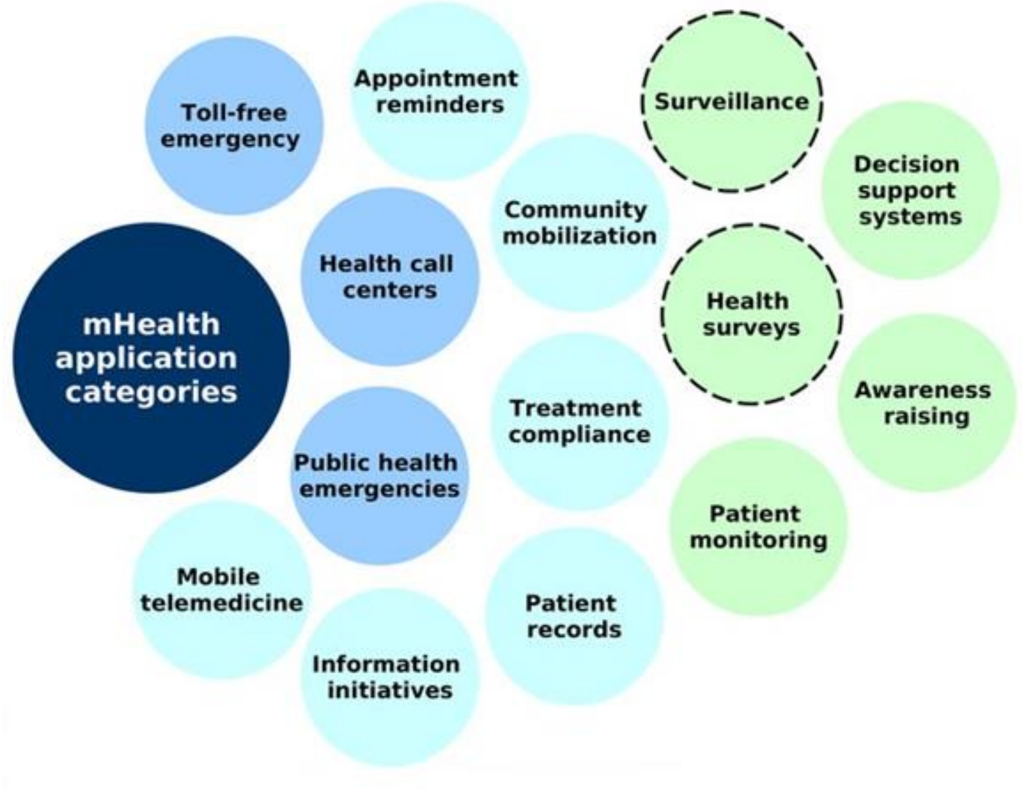


Figure 4. mHealth application categories. [4]

Table 1. Categorization of mHealth application categories. [1]

---

[4] "m" is a shortcut for mobile and used as a prefix to denote the use of mobile and multimedia telecommunication technologies, integrated into administration systems and depending on wireless technologies in various domains (i.e. mLearning, mCommerce etc.)

[5] a common shortcut for application that used in literature is app

Accessing/providing health services
• Toll-free emergency: Free telephone hotlines for health emergencies provided by trained personnel and pre-recorded messages and linked to response systems
• Health call centers/health care telephone helplines: Health care advice and triage provided by trained personnel and pre-recorded messages
• Reminder to attend appointments: Reminder messages provided by health services to patients to make or attend an appointment using mobile ICT[6]; message can be text, voice or multimedia.
• Mobile telehealth: Consultation between health care practitioners or between practitioners and patients using mobile ICT.
• Management of disasters and emergencies
• Treatment adherence: Reminder messages (text, voice or multimedia) provided by health services to patients aimed at achieving medication adherence using mobile ICT; messages can be.
Accessing/providing health information
• Community mobilization/health promotion campaigns : Health promotion campaigns conducted using mobile ICT to raise the awareness of target groups. Messages conveying information can be text, voice or multimedia.
• Access to information, databases and tools: Access to health sciences literature, resources and databases using mobile ICT.
• Patient records: Access to electronic patient information (such as EHR/EMR, laboratory results, X-rays, etc.) using mobile ICT
• mLearning: Access to online educational resources using mobile ICT
• Clinical decision support systems: Access to decision support systems using mobile ICT
Collecting health information Health system
• Patient monitoring: Data capture and transmission for monitoring a variety of conditions in a range of settings using mobile ICT.
• Health surveys: Data collection, management and reporting of health surveys using mobile ICT. May involve any combination of networked mobile devices.
• Disease surveillance: Routine, emergency and targeted data collection, management, and reporting for public health surveillance using mobile ICT. May involve any combination of networked mobile devices.

2.2.2 Telehealth

According to [1] telehealth is the "*delivery of health care services, where patients and providers are separated by distance. Telehealth uses ICTs for the exchange of information for the diagnosis and treatment of diseases and injuries, research and evaluation, and for the continuing education of health professionals.*" Telehealth contributes to achieving universal health coverage by improving access for people in remote areas, elderly and vulnerable to quality, cost-effective, valuable health services

---

[6] Mobile ICT refers to mobile devices or hand-held computers such as mobile phones, laptops, tablets or PDAs, which can be used for text, voice or image communication, and can collect, process and report data.

wherever they may be. Telehealth (also referred in the literature as Telemedicine) is probably one of the most well-known and best established of all eHealth services. The most common telehealth sectors according to [1] are:

- Teleradiology
- Teledermatology
- Telepathology
- Telepsychiatry
- Remote patient monitoring

The term "connected health" also used in literature. According to [2], "*connected health, in general, refers to any digital health- care solution that can operate remotely, with additional components of continuous health monitoring, emergency detection and can alarm capabilities." Connected health mainly focuses on the mission to improve the quality and efficiency of health care by enabling self-care and complementing it with remote care.*"

2.2.3 Electronic Health Records systems

As mentioned *EHRs support the provision of healthcare and used by individuals and their caregivers to the management of their own health*. Therefore, EHR systems are an important component of eHealth, where all people have access to all health services they need, of sufficient quality to be effective. A well-functioning EHR system, according [1] "*improves the quality, accuracy and timeliness of patient information at point of care and play a pivotal role in eHealth by providing insight into health care costs, utilization and outcomes, promoting quality of care, reducing costs, supporting patient mobility, increasing reliability of information and providing access to patient information to multiple health care providers*." Data from other health information system data in combination with EHR systems will highlight elements of concern and health services delivery, public health and, social factors. Therefore it's crucial whether a country has introduced a national EHR system and if there is legislation governing its use. EHR applications include [1]:

- Primary care facilities such as clinics, secondary care facilities such as hospitals and tertiary care facilities referral from primary/secondary care.
- Information systems such laboratory, pathology and pharmacy, Picture Archiving and Communication System (PACS) and, automatic vaccination alerting systems.
- Electronic medical billing systems and supply chain management information systems.

2.2.4 Social media in Health Care

The world's communications have changed drastically due the invention of Internet. With this change came the inevitable rise of social media for both personal and business purposes. The term social media defined in [5] as “*Internet-based tools that allow individuals and communities to gather and communicate; to share information, ideas, personal messages, images, and other content; and, in some cases, to collaborate with other users in real time*”. Social media can be grouped by purpose, serving functions such as:

- Social networking (e.g. Facebook, Twitter, Instagram)
- Professional networking (e.g. LinkedIn)
- Media sharing (e.g. YouTube)
- Knowledge and information aggregation (e.g. Wikipedia)

Billions of users daily and billions of devices have access to the internet and it has opened up a global marketplace to business and individuals across the world. As associate degree extension of this, social media penetrated in each sector and health isn't any exception. Social media impacts on eHealth, as it increases the involvement of health care consumers in their own health and might promote health care in general and it can even be accustomed improve dissemination of knowledge to and from the health workforce. There is no doubt that social media has revolutionized eHealth across the world.

Use of social media in health care organizations aim to [1]:

- Promote health messages as a part of health promotion campaigns. An example is the campaign that took place recently from all the countries worldwide, during the pandemic of COVID-19.
- Managing patient appointments
- Seek feedback on services
- Make general health and emergency announcements

Use of social media from individuals and communities aim to [1]:

- Learn about health issues and help decide which health services to use
- Provide feedback to health facilities or health professionals
- Run community-based health campaigns and participate in community-based health forums

2.2.5 Legal frameworks for eHealth

This subsector identifies the policy and legislative environment of eHealth in a country and is strong connected with privacy. It is aim to show the degree of protection and control that individuals have of their health-related data in a digital environment. Therefore, according to [1], it is crucial if a country:

- Defines medical jurisdiction and, liability of eHealth services such as telehealth
- Addresses patient safety and quality of care based on data quality, data transmission standards or clinical competency criteria
- Protects the privacy of personally identifiable data of individuals irrespective of whether it is in paper or digital format and, the privacy of individuals' health-related data held in electronic format.
- Governs the sharing of digital data between health professionals in other health services in the same country through the use of an EHR and, the sharing of personal and health data between research entities.
- Allows individuals electronic access to their own health-related data when held in an HER, to demand their own health-related data be corrected when held in an EHR if it is known to be inaccurate, to demand the deletion of health-related data from their HER, to specify which health-related data from their EHR can be shared with health professionals of their choice
- Governs civil registration and vital statistics and national identification management systems

2.3 Information and Communications Technologies related to eHealth

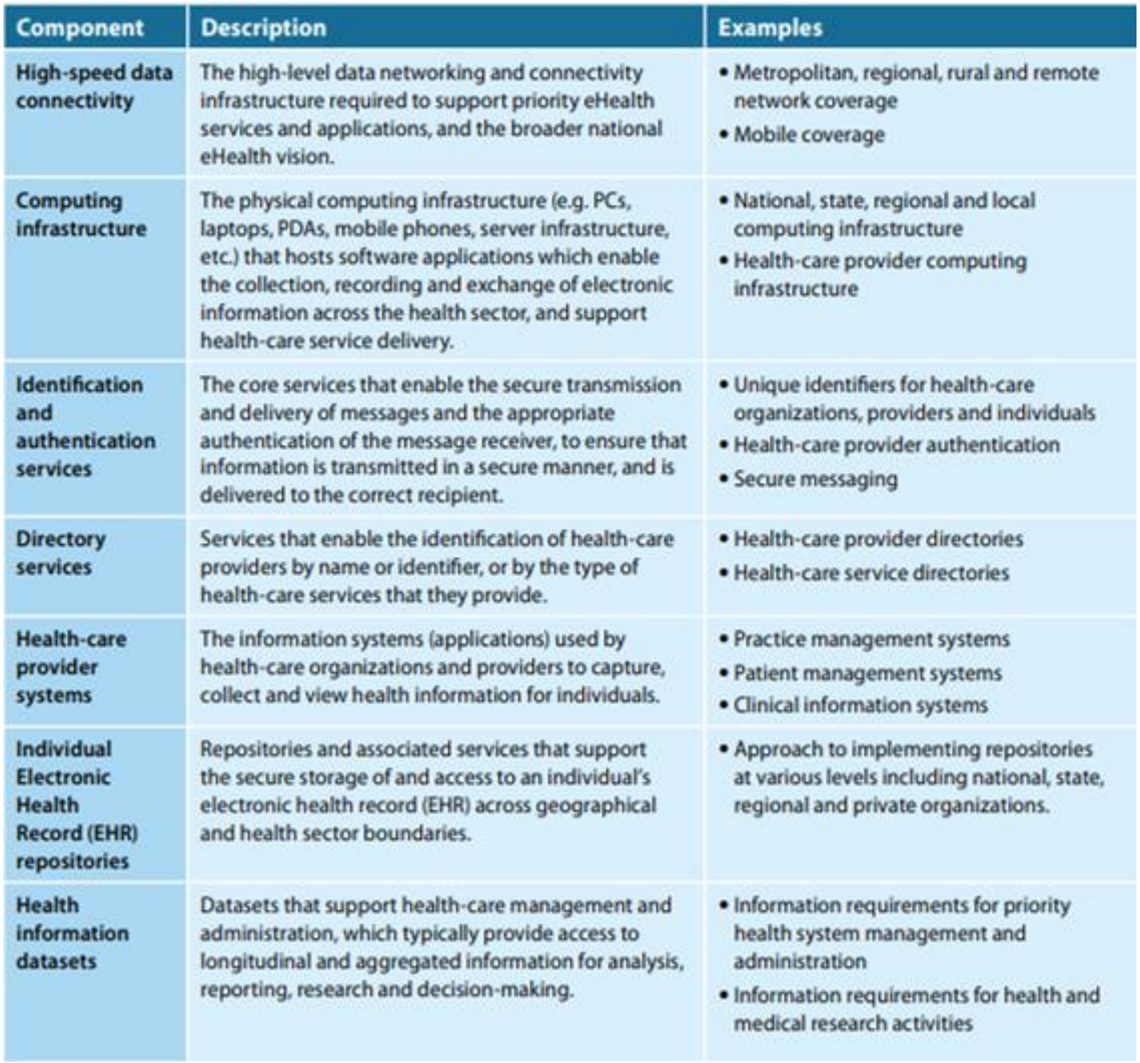
The purpose of this thesis is to investigate security and privacy issues in eHealth sector and eHealth is based on a number of ICTs. Therefore, in order to investigate these issues, we must explore the main characteristics of these ICTs in relation to eHealth and its interdependencies with other enablers. In other words, we must identify the essential technology building blocks concerning the eHealth. Technologies and applications is a significant step in assessing security requirements.

In order to identify the ICTs related to eHealth, first of all it is important to have the knowledge of eHealth infrastructure components. According to [3], components include:

- High speed data connectivity
- Computing infrastructure
- Identification and authentication services
- Directory services
- Individual EHR repositories

- Health-care provider systems
- Health information datasets

Description and examples of these components depicted in Figure 5.



Component	Description	Examples
High-speed data connectivity	The high-level data networking and connectivity infrastructure required to support priority eHealth services and applications, and the broader national eHealth vision.	• Metropolitan, regional, rural and remote network coverage • Mobile coverage
Computing infrastructure	The physical computing infrastructure (e.g. PCs, laptops, PDAs, mobile phones, server infrastructure, etc.) that hosts software applications which enable the collection, recording and exchange of electronic information across the health sector, and support health-care service delivery.	• National, state, regional and local computing infrastructure • Health-care provider computing infrastructure
Identification and authentication services	The core services that enable the secure transmission and delivery of messages and the appropriate authentication of the message receiver, to ensure that information is transmitted in a secure manner, and is delivered to the correct recipient.	• Unique identifiers for health-care organizations, providers and individuals • Health-care provider authentication • Secure messaging
Directory services	Services that enable the identification of health-care providers by name or identifier, or by the type of health-care services that they provide.	• Health-care provider directories • Health-care service directories
Health-care provider systems	The information systems (applications) used by health-care organizations and providers to capture, collect and view health information for individuals.	• Practice management systems • Patient management systems • Clinical information systems
Individual Electronic Health Record (EHR) repositories	Repositories and associated services that support the secure storage of and access to an individual's electronic health record (EHR) across geographical and health sector boundaries.	• Approach to implementing repositories at various levels including national, state, regional and private organizations.
Health information datasets	Datasets that support health-care management and administration, which typically provide access to longitudinal and aggregated information for analysis, reporting, research and decision-making.	• Information requirements for priority health system management and administration • Information requirements for health and medical research activities

Figure 5. eHealth infrastructure components. [3]

The European Commission communication on ICT standards [6], launched in 2016, has identified the following priority areas as the essential technology building blocks concerning the eHealth: 5G communications [7]**,** Cloud Computing (CC) [8], The Internet of things (IoT) [9], Big Data [10] and Cybersecurity. However, it has already been four years since this communication launched and during these years, these technologies developed significantly – for example Cloud Computing [11]-[12]. Also, many technologies and state-of-the-art research has been proposed as Artificial

Intelligence (AI) and Blockchain technology [13]. So, investments are needed to enable their use for better health and care outcomes.

ICTs pillars and ICTs supporting the eHealth are depicted in Figure 6.

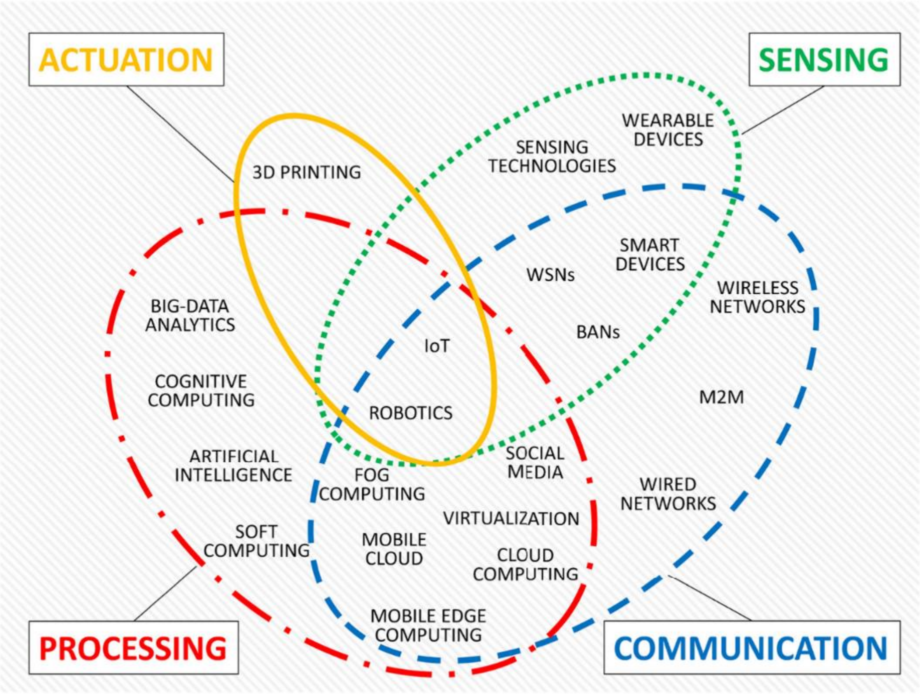


Figure 6. ICTs pillars and ICTs supporting the eHealth. [14]

The Internet, as the infrastructure allowing global addressing and communication, is essential to eHealth in all aspects and facilitates communication between many limited devices and humans. IoT connects “things” (as shown in Figure 7) into a network of computing intelligence without the involvement of a human. IoT is one of the dominant fields in academic research and applications in the public or private sector and industrial applications.

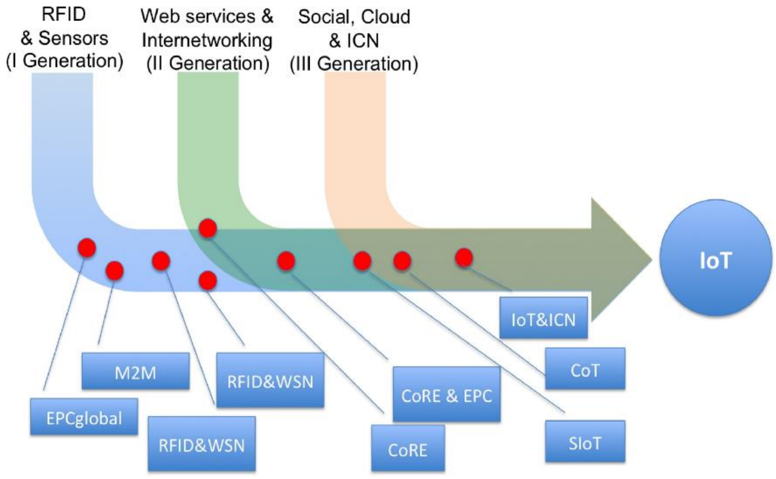

RFID & Sensors (I Generation)
Web services & Internetworking (II Generation)
Social, Cloud & ICN (III Generation)
IoT
IoT&ICN
CoT
M2M
RFID&WSN
CoRE & EPC
EPCglobal
RFID&WSN
CoRE
SIoT

Figure 7. Evolution of the IoT. [15]

The IoT transforms healthcare, as shown in Figure 8, and, plays an important role in real-time monitoring, better emergency response, easy access to patients’ data, remote access to healthcare, and connectivity among stakeholders in the smart healthcare ecosystem [16], [17].

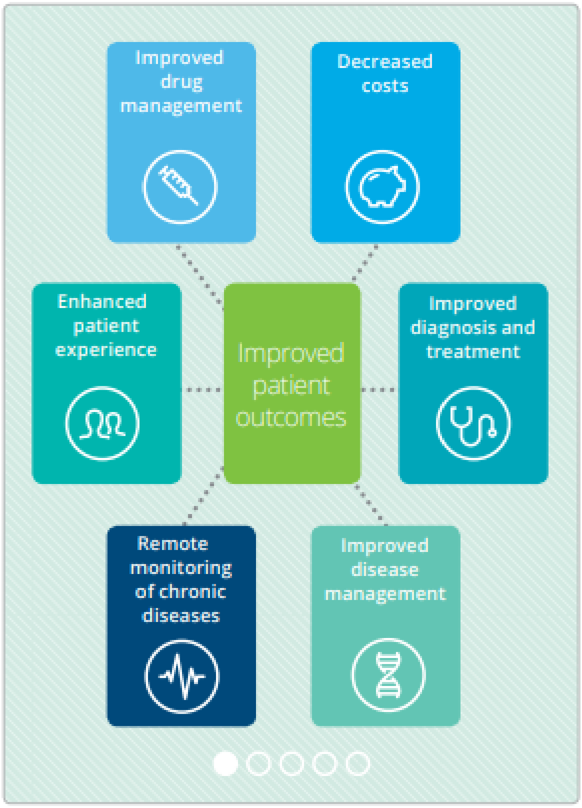

Improved drug management
Decreased costs
Enhanced patient experience
Improved patient outcomes
Improved diagnosis and treatment
Remote monitoring of chronic diseases
Improved disease management

Figure 8. The impacts of IoT in healthcare. [17]

However, the integration of IoT technology in every sector (consequently in the eHealth sector) brings several challenges, including data storage, data management, exchange of data between devices, security and privacy, and unified and ubiquitous access. The ICT that can address these challenges is Cloud Computing (CC) technology. Nowadays CC is a computing utility more than technology [11]. Computing services and the hole infrastructure (servers, databases, networking), software, and Big Data analytics over the internet provide faster deployment, flexible resources, and economies of scale. Furthermore, the current shift from the centralized scenario of CC to decentralized CC technologies [11] such as Fog Computing [18] and Multi-Access Edge Computing (MEC) - formerly Mobile Edge Computing [19] (recently in the all-encompassing expression FMEC, i.e. Fog and Multi-Access Edge Computing) is taking the headline. FMEC technology performs data analytics on edge devices, so it enables real-time processing and reduces costs. The proliferation of mobile devices and FMEC technologies ensures a foundation for the evolution of IoT in the eHealth sector to revolutionize every aspect of human lives. One of the best definitions that exist, for the IoT in today’s landscape is given by [15]: “*a conceptual framework that leverages on the availability of heterogeneous devices and interconnection solutions, as well as augmented physical objects providing a shared information base on global scale, to support the design of applications involving at the same virtual level both people and representations of objects.*” A high-level representation of the IoT conceptual framework is sketched in Figure 9.

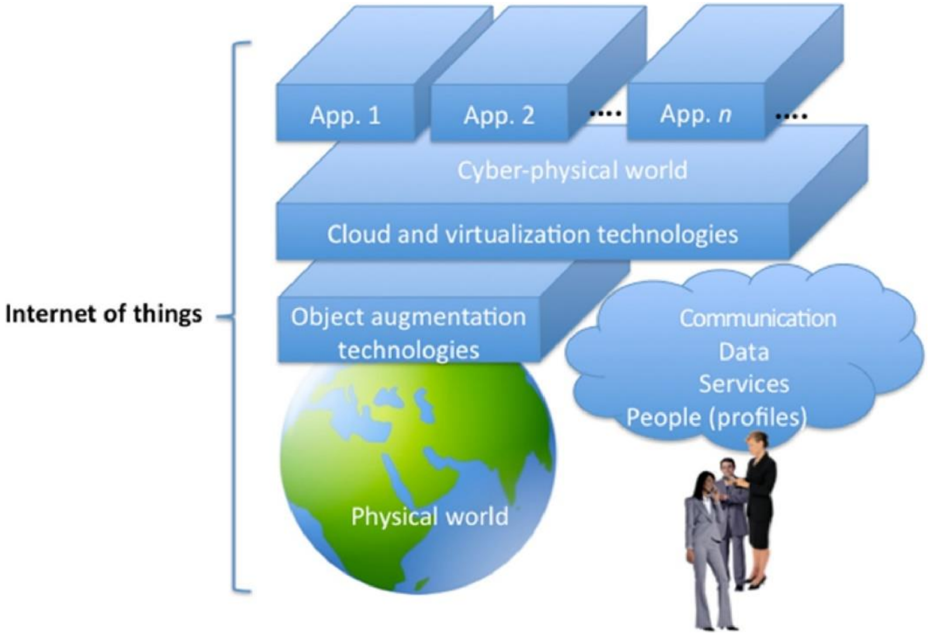


Figure 9. A high-level representation of the IoT conceptual framework. [15]

The IoT, CC and, FMEC, Big Data and, AI are revolutionizing eHealth and its whole ecosystem like Industry 4.0 is doing for the manufacturing sector, moving it towards Healthcare 4.0 [20]-[21]. The basic architecture of Healthcare 4.0, shown in Figure 10. Interested readers are referred to IoT reviews carried out by [15] - [22] for more in-depth knowledge about several aspects of IoT enabling technologies, its current development progress as well as their major issues and challenges. Furthermore, they can refer to [11]-[12], [23] to gain insights about CC technology and to [24]-[25] for FMEC technologies, their typical application scenarios, various challenges that occur when implementing CC and FMEC computing systems. Also, readers can refer to [16], [26]-[27] for the IoT and cloud technologies-eHealth integration, for Big Data-eHealth integration to [28], for Blockchain-eHealth integration to [29]- [30], for AI-eHealth integration [31]-[32] and for 5G-eHealth integration to [33].

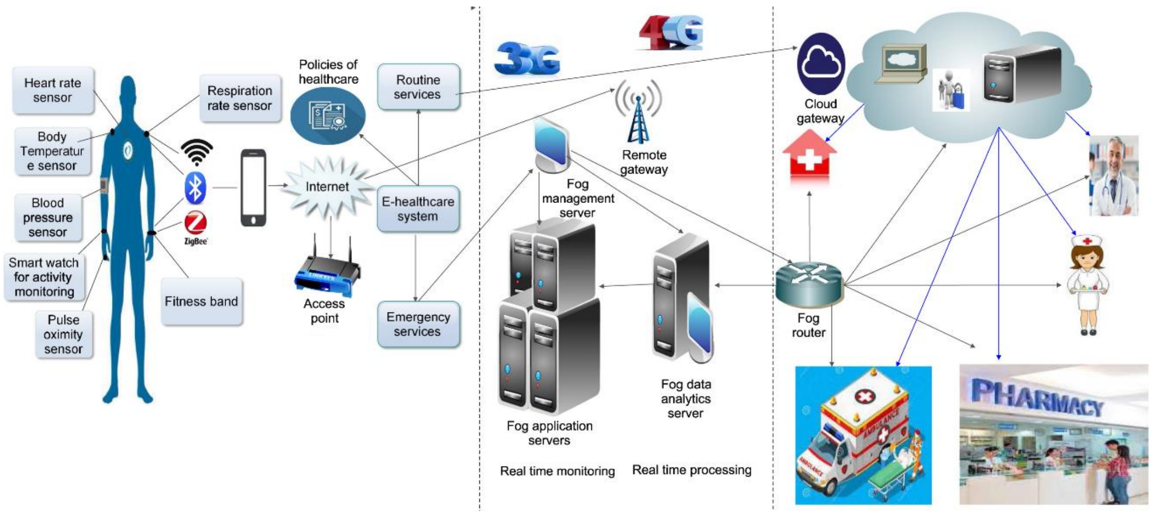


Figure 10. The basic architecture of Healthcare 4.0. [21]

A view of the main healthcare application scenarios shown in Figure 11.

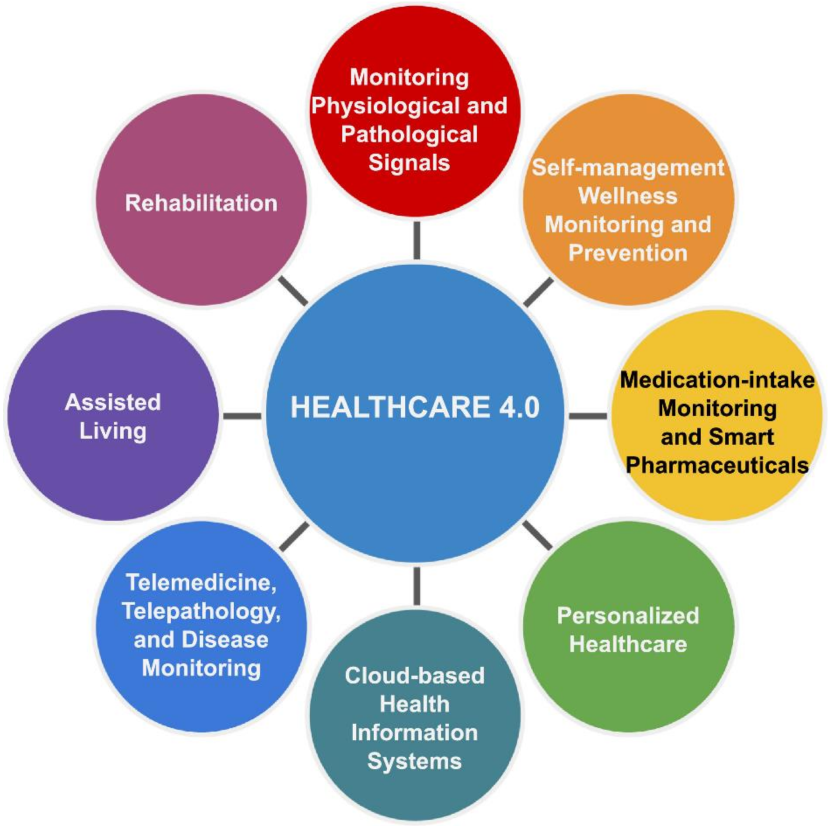

Monitoring Physiological and Pathological Signals
Self-management Wellness Monitoring and Prevention
Medication-intake Monitoring and Smart Pharmaceuticals
Personalized Healthcare
Cloud-based Health Information Systems
Telemedicine, Telepathology, and Disease Monitoring
Assisted Living
Rehabilitation
HEALTHCARE 4.0

Figure 11. Main healthcare application scenarios. [20]

3 Security and Privacy

Security and privacy presenting the greatest challenges for all ICTs. Essentially, these factors determine how much acceptable, and therefore successful, will be a technology by the vast majority of users. In eHealth sector, security and privacy requirements are growing rapidly as the main subject of eHealth is the data of users. eHealth challenges lie in the fact that eHealth is required to meet all the security challenges of its related ICTs and their components, e.g. hardware and software. Solving a security problem usually creates a new need for security and privacy. Although it seems like a "vicious circle", but this is that creates the need for continuous development and improvement of the sector.

First of all, we need a closer look in security, cybersecurity and privacy-related terms, concepts and cybersecurity relevant standards and services.

3.1 Terms and concepts

In every situation, it is very important to provide the terminology that we will use at work. First, we must disambiguate the terms that apply when it comes to security: Information Security and Cybersecurity.

Information Security [34]: "*the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability*." **Information System "***is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.*"[34].

The term Cybersecurity has its origins on the term cyberspace and was crafted and used to address security concerns in the cyberspace [35]. ENISA in [35] proposes that "***Cybersecurity** shall refer to security of cyberspace, where cyberspace itself refers to the set of links and relationships between objects that are accessible through a generalized telecommunications network, and to the set of objects themselves where they present interfaces allowing their remote control, remote access to data, or their participation in control actions within that Cyberspace. Cybersecurity shall therefore encompass the CIA paradigm for relationships and objects within cyberspace and extend that same CIA paradigm to address protection of privacy for legal entities (people and corporations), and to address resilience (recovery from attack)*."

According to the above-mentioned definition we depict the whole picture in Figure 12.

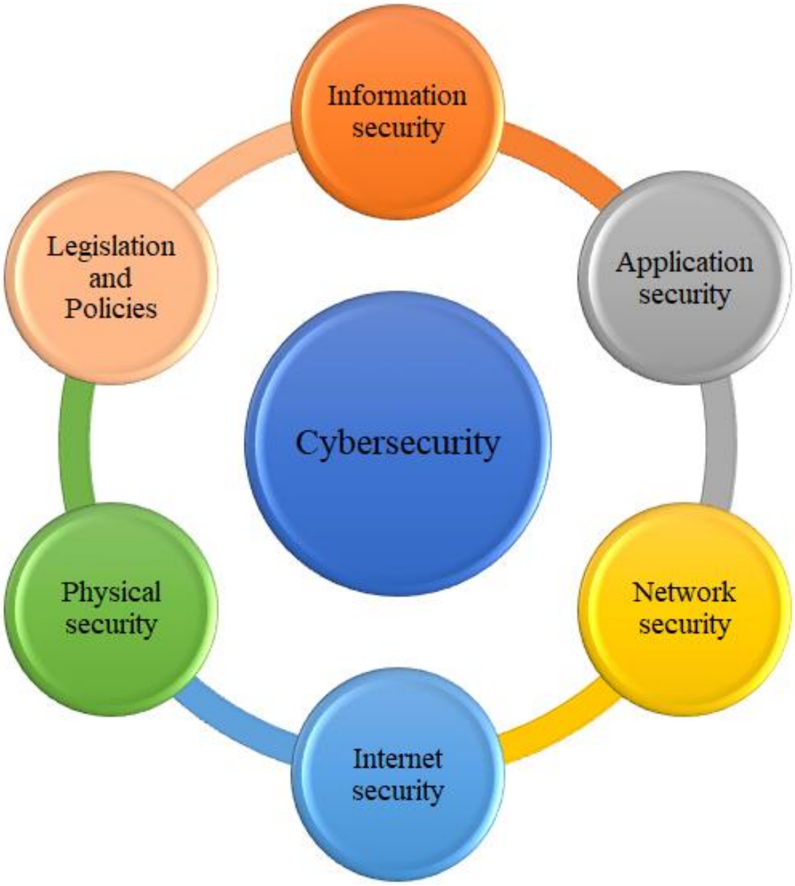


Figure 12. Logical-relationships between Cybersecurity and other security domains

The concepts **Confidentiality, Integrity and Availability form what is often referred to as the CIA paradigm or CIA triad**. The three concepts embody the fundamental security requirements for security of cyberspace. NIST Glossary [36] defines terms as follows:

- **Confidentiality**: "*preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.*" This term includes two concepts:
    - **Data confidentiality** which refers to the content of electronic documents or, in general, files and messages.
    - **Privacy** that assures protection of personal data.
- **Integrity**: "*guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity*." This term includes two concepts:
    - **Data Integrity** which refers to alteration of data in an unauthorized manner.

  - **System Integrity** which refers to unauthorized manipulation of the system intentional or accidental.

- **Availability**: "*ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.*"

CIA triad to define security objectives is well established and a fundamental basis to cybersecurity. To present a complete picture of security requirements, two more concepts are broadly defined. These concepts as defined in [36] are:

- **Authenticity:** "*the property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.*"
- **Accountability:** "*the security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.*" According [37] this supports:
  - non-repudiation
  - deterrence
  - fault isolation
  - intrusion detection and prevention
  - after-action recovery and legal action.

According to the above-mentioned definitions, the complete picture of cybersecurity requirements shown in Figure 13.

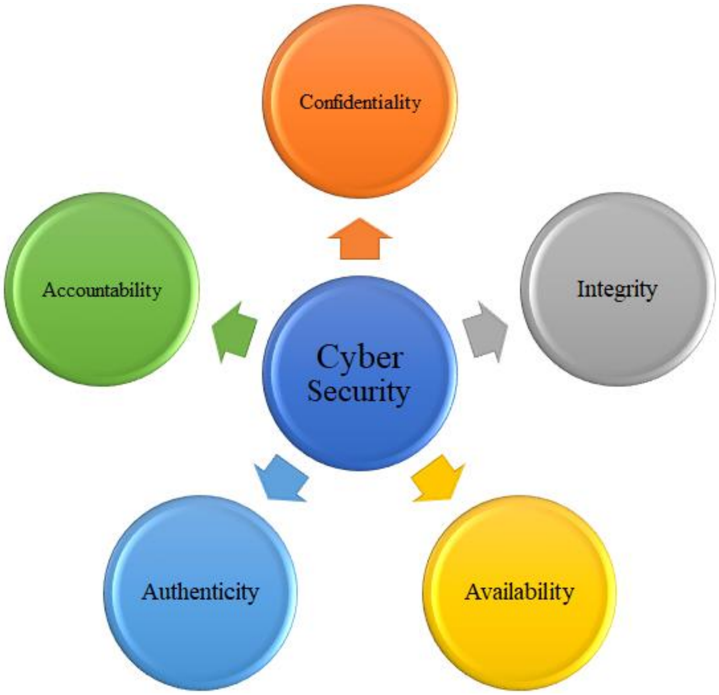


Figure 13. Essential Cybersecurity requirements

It is worth mentioning - and it is necessary – how the General Data Protection Regulation (GDPR) [38] defines personal data:

Personal data: “*any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*”

Further, the GDPR contains three additional important definitions that pertain to health data as follows:

Data concerning health: “*personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.*”

Genetic data: “*personal data relating to inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question*”.

Biometric data: “*personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data*”.

It is worth mentioning that “data concerning health,” “genetic data” and “biometric data” will be subject to a higher standard of protection than personal data in general.

NIST Glossary [36] defines terms related to threats and as follows:

Attack: “*Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.”*

Cyber Attack: “*An attack, via cyberspace, targeting an enterprise’s use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information*.”

Threat (synonym with Cyber threat): “*Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service (DoS).*” In the literature, the terms threat and attack are commonly used to mean more or less the same thing. Therefore, in work, these two terms used interchangeably.

In order to protect a system and to implement the most cost-effective security measures, we need to know and understand the vulnerabilities of the system and the threat sources that exploit the vulnerabilities. For that reason, the following terms are provided.

Threat “*The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability*.”

Vulnerability: “*Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source*.”

A threat source can be adversarial or non-adversarial [34]. As described in [34] “**adversarial threat sources** *are individuals, groups, organizations, or entities that seek to exploit an organization’s dependence on cyber resources.* ***Non-adversarial threat sources*** *refer to natural disasters or erroneous actions taken by individuals in the course of executing their everyday responsibilities*.” A simple common term used for adversarial threat sources is **threat actor** or **threat agent** [39]. At work it is obvious that we will deal with adversarial threat sources.

If in a system exist vulnerabilities, threat sources can lead to threat events. These events could potentially cause undesirable consequences or impacts and the damage that may cause on ICT systems varies, as described in the next chapters. In order to provide effective Cybersecurity requires a comprehensive approach that considers a variety of areas both within and outside of the Cybersecurity field. In order to protect information systems from threats, multi-layered security countermeasures implemented. **Countermeasures** defined in [36] as “*protective measures prescribed to meet the security objectives (i.e., confidentiality, integrity, and availability) specified for an information system.*”.

Another term to mention is attack vector [39]**. Attack Vector** “*is a path or means by which a threat agent can gain access to a computer or network server, abuse weaknesses or vulnerability on assets (including human) in order to achieve a specific outcome*.”

3.2 Cybersecurity Standards

Generally, ICT specifications help ensure that devices, systems and, services retain the ability to connect and interoperate with each other, enhancing innovation, and keeping ICT markets open and competitive. Specifications are used to maximize interoperability (the ability for systems to work together). Standards are developed to hide management practices and therefore the overall architecture of security mechanisms and services. Standards are the tool to make things work together, as shown in Figure 8. The process by which specifications are set covered by the term standardization.

Figure 14. ICT Standards as a tool. [40]

Globally exist thousands of industry or sector-based standards organizations that develop and publish industry-specific standards. The term Standards Developing Organization (SDO) refers to these organizations. The foremost important SDOs that are involved within the development or promotion of standards that are being developed for various aspects of Cybersecurity presented in [41] as follows:

- The International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) and the International Telecommunication Union (ITU), under UN governance are recognized by the standardization community as SDO. These organizations are potentially addressing all domains.
- In the EU the recognized standardization bodies are the European Telecommunications Standards Institute (ETSI), the European Committee for Electrotechnical Standardisation (CENELEC) and, the Comité Européen de Normalisation (CEN).
- Other entities working in specific and focused domains, for example, industrial fora like 3GPP, IEEE, IETF, AIOTI, etc. These industrial bodies have different ways of functioning depending on their scope, participation and coverage, but they intend to cover specific requirements from. However, they do not have the official recognition that the international SDOs have.
- National standardization bodies are also producing high-value standards, like for example the US National Institute of Standards and Technology NIST.

A full list of organizations that are involved within the development or promotion of standards that are being developed for various aspects of cybersecurity in standardization related to cybersecurity presented in [35] and [41].

The foremost important of these organizations are as follows:

- ITU-T[7]: The International Telecommunication Union (ITU) is an international organization within the United Nations System. The ITU Telecommunication Standardisation Sector (ITU-T) is one of the three sectors of the ITU. ITU-T's mission is the development of technical standards covering all fields of telecommunications. ITU-T standards are referred to as Recommendations.
- ISO[8]: The International Organization for Standardisation (ISO) is a worldwide federation of national standards bodies from more than 140 countries, one from each country. ISO is a nongovernmental organization that promotes the development of standardisation and related activities. ISO's work results in international agreements that are published as International Standards.
- ETSI[9]: The European Telecommunications Standards Institute (ETSI) is an independent, not-for-profit, SDO in the telecommunications industry (equipment makers and network operators) in Europe, with worldwide projection. ETSI produces globally-applicable standards for ICTs, related to telecommunications. ETSI supports European regulations and legislation through the creation of Harmonized European Standards.
- NIST[10]: National Institute of Standards and Technology (NIST) is a U.S.A. federal agency. NIST provides a specific set of Federal Information Processing Standards (FIPS) and NIST Special Publications (SPs) related to information security and risk management. Even if NIST is a national organization, its standards are recognized worldwide by international organizations such as ISO.

At this point, it is worth mentioning the European Union Agency for Network and Information Security (ENISA)[11] founded in 2004 and it is located in Greece. ENISA is a center of network and information security expertise for the EU, its member states, the private sector, and Europe's citizens and works with these groups to develop advice and recommendations on good practice in cybersecurity.

Also, we mention the Health Level Seven[12] International (HL7)[13] which is a not-for-profit, ANSI-accredited SDO. HL7 provides a framework and related standards for eHealth information that supports health services.

---

[7] https://www.itu.int/en/ITU-T/Pages/default.aspx

[8] https://iso.org/

[9] https://www.etsi.org/

[10] https://www.nist.gov/

[11] https://www.enisa.europa.eu/

[12] "Level Seven" refers to the seventh level of the ISO seven-layer communications model for Open Systems Interconnection (OSI) - the application level

[13] https://www.hl7.org/index.cfm

3.3 Security Services and Mechanisms

To assess effectively the security needs of a system that provides services and to evaluate and choose various security products and policies, we need some systematic way of defining the requirements for Cybersecurity and describing the methods to satisfying those requirements. Several systematics approaches from important SDOs are provided. One of the most important and fundamental approaches, which was the basis for other approaches (which we will present in next chapters) is the ITU-T Recommendation X.800, "*Security Architecture for OSI*" [42], which covers the model for Open Systems Interconnection (OSI)[14] to cover security aspects. As mentioned in [42], the services are proposed to counter security attacks, and they use security mechanisms for the service provision.

In [36] **security service** defined as "*a capability that supports one, or more, of the security requirements (Confidentiality, Integrity, Availability - CIA)*". We could say that security services set goals to meet basic security requirements, that is CIA. **Security mechanism** defined as "*device or function designed to provide one or more security services usually rated in terms of strength of service and assurance of the design*". We could say that security mechanisms determine the ways in how security goals can be achieved.

The security mechanisms are divided into those that are implemented in a specific protocol layer, an application-layer protocol, and those that are not specific to any particular protocol layer or security service. These mechanisms will be covered in appropriate chapters at work.

The most common security services are the following [37]:

- **Authentication service:** The function of the authentication service is to assure that communication is authentic either in the case of a user, process, or device sending a single message, either in the case of an ongoing interaction i.e. connection of a terminal to a host. In both cases the service assures that entities are authentic, that is, that each is the entity that it claims to be. Also, two specific authentication services are defined: peer entity authentication and data origin authentication. Two entities are considered peers if they implement to same communication protocol in different communication systems. At the establishment of, or at times during the data transfer phase of, a connection peer entity authentication is provided for use. Data origin authentication provisions applications like email, where there are no prior interactions between the communicating entities.

---

[14] Recommendation X.200 (https://www.itu.int/rec/T-REC-X.200-199407-I) describes the Reference Model for open systems interconnection (OSI). It establishes a framework for coordinating the development of existing and future Recommendations for the interconnection of systems. The objective of OSI is to permit the interconnection of heterogeneous computer systems so that useful communication between application processes may be achieved.

- **Access Control:** To limit and control access to systems and applications via communications links access control service must be applied. To attain this, each user, process, or device trying to gain access must first be identified or authenticated, so that access rights can be tailored to the entity. Therefore, there are to aspects of this service: authentication and authorization.
- **Data Confidentiality:** Confidentiality is the protection of transmitted data and the protection of traffic flow from analysis. This requires that an adversary not be able to observe the other characteristics of the traffic of a communication channel.
- **Data Integrity:** There are two cases of data integrity service and depends on the type of connection, that is if it is connection-oriented or connectionless. In the first case integrity service assures first that, messages are received as sent with no duplication, insertion, modification, reordering, or replays and second, there's no destruction of data. In the second case, integrity service protects against message modification only.
- **Nonrepudiation:** Nonrepudiation prevents communicating entities from denying a transmitted message. When a message is sent, the receiver can attest that the assumed sender, in fact, sent the message. Correspondingly, when a message is received, the sender can attest that the assumed receiver, in fact, received the message.
- **Availability Service:** A system or a system resource is available if it provides services according to the system design whenever authorized system users request them. Availability is reliant on suitable management and control of system resources and thus depends on access control service and other security services.

4 Common Cyber Threats in eHealth

Nowadays threat events occurring in eHealth systems that affect their availability and individual's privacy and data integrity are common. eHealth systems and networks can be affected as every other network and affecting operations in an eHealth system is a common phenomenon. Malicious physical attacks can compromise data integrity and availability and affect privacy. In 2019, 15% of data breaches involving healthcare organizations and holds the highest percentage of the total [43]. Sophisticated and highly organized cybercriminals target healthcare organizations showing every day how vulnerable the eHealth systems are. And the situation keeps getting more difficult, so first, we must defend. In general, to defend oneself, one must know who is a threat source, why he is threatening ("who and/or why?"), what is his purpose ("what?"), and how he uses these means ("how?") [44]. In this chapter, we present common eHealth-related threats. To achieve this we must identify the types of attacks, the "who and/or why?" a.k.a. threat actors and their motivation, the "what?" a.k.a their target and the "how?" a.k.a. their tools and methods (Tactics, Techniques, and Procedures - TTP). To provide the necessary background, we will present taxonomy[15] of threat actors, taxonomy of attacks, and common threat-related concepts. The holistic view of our classification depicted in Figure 15. Understanding how the adversary operates is essential to effective cybersecurity, so attack methodology is presented. Also, we present briefly a timeline of security incidents, threats landscape, and trends.

4.1 Taxonomy of Security Threats and Attacks in General

As mentioned in paragraph 2.1, *threat* and *attack* are commonly used to mean more or less the same thing and these two terms in the literature (and in work also) used interchangeably. In a nutshell, a threat is a possible danger that might exploit vulnerability and an attack is an assault on system security that derives from a threat. A successful attack has as result, a security incident and/or data breach.

There are several categories of threats that can affect IT systems in general and eHealth ecosystems particularly, which in fact consist of various elements and technologies. Taxonomy can be used as a rich and relevant knowledge-management tool to understand in detail the threats. Generally, creating threat taxonomy is a complex task. When dealing

---

[15] Taxonomy is the practice and science of classification of things or concepts, so, the terms taxonomy and classification in work used interchangeably

with topics like security, there can be different ways in which to classify threats, and it is not always easy or possible to determine which the best or correct classification is.

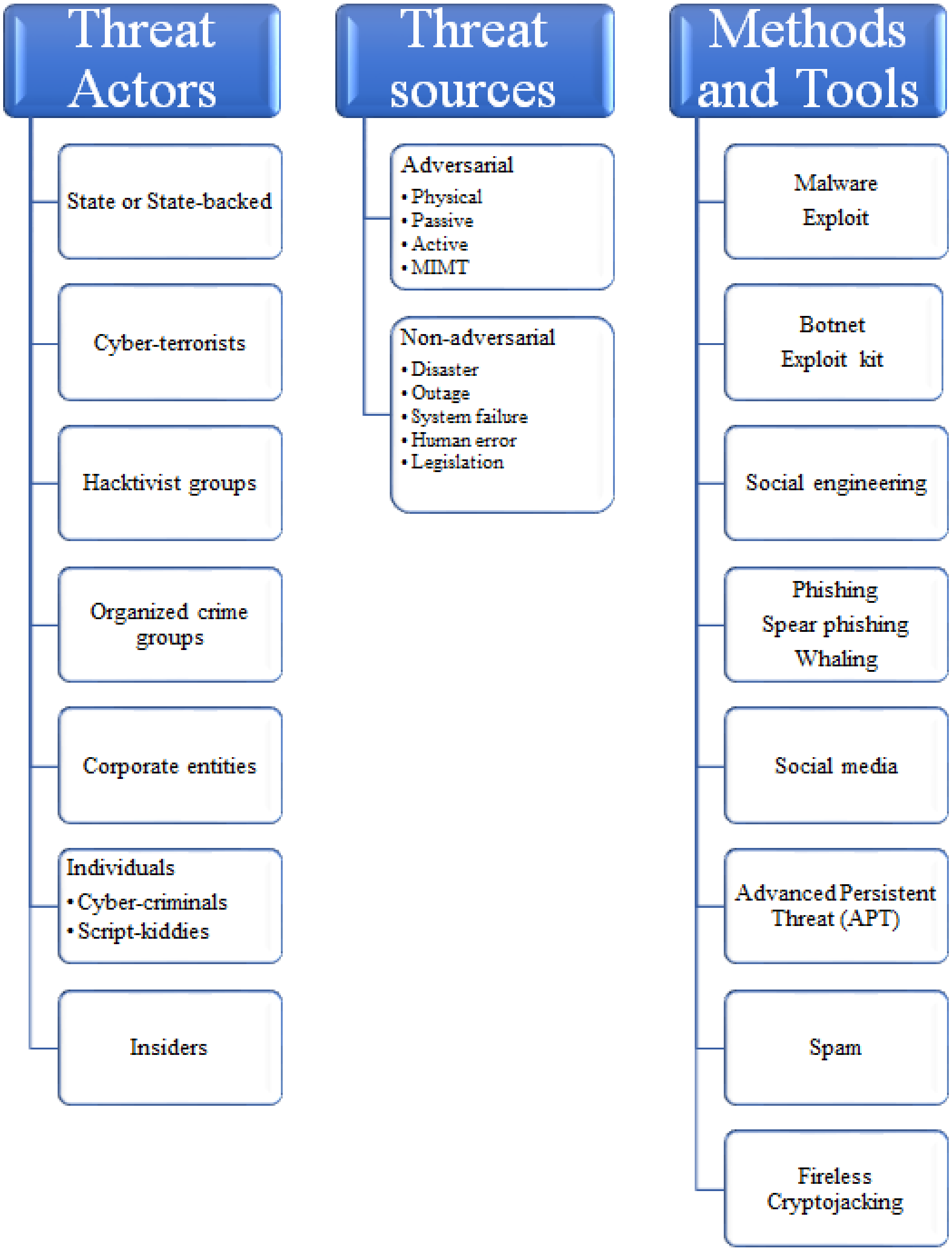


Figure 15. Classification of treat actors, threat sources and, methods and tools

Important SDOs (i.e. ITU-T in [45], ETSI in [44], NIST in [34]), organizations (e.g. ENISA in [39], [46]) and, surveys [47]- [48], provide proposals related to threat actors and sources taxonomy. In work, first, we classify threat actors, then threats and, finally, methods and tools.

It should be mentioned that, if we take a holistic view of the security of a system, as mentioned in paragraph 2.1, we have to take in account not only adversarial but also non-adversarial threats which include (a) natural and environmental disasters, (b) outages, (c) system failures and human errors (unintentional or accidental damages) [46]. For now, our goal is to classify adversarial threats resulting in attacks that are the intentional threats. These include (a) physical attacks, (b) eavesdropping, interception, and hijacking widely known as passive attacks and (c) malicious (or nefarious) activities widely known as active attacks [45], which are been discussed in next paragraph.

However, it is worth mentioning that system failures and human errors account equally for the majority of security incidents in the eHealth domain [49], as depicted in Figure 16. Also, human error is the primary root cause of the personal data breach as reported in [50] and depicted in Figure 17. It is worth noting that, according to [Verizon], 51% of data breaches in the eHealth sector are due to sending messages to the wrong recipient, which is a human error. The human factor is related to malicious actions, from the perspective of causing system holes by negligence or oversights, which could lead to system inefficiencies and thus make the infrastructures vulnerable to possible attacks. We will discuss this in detail in chapter 4.

Another category is legal threats, that is, threats of financial or legal penalty or loss of trust of customers and collaborators due to legislation, such as (a) violation of laws or regulations and breach of legislation and (b) failure to meet contractual requirements [46].

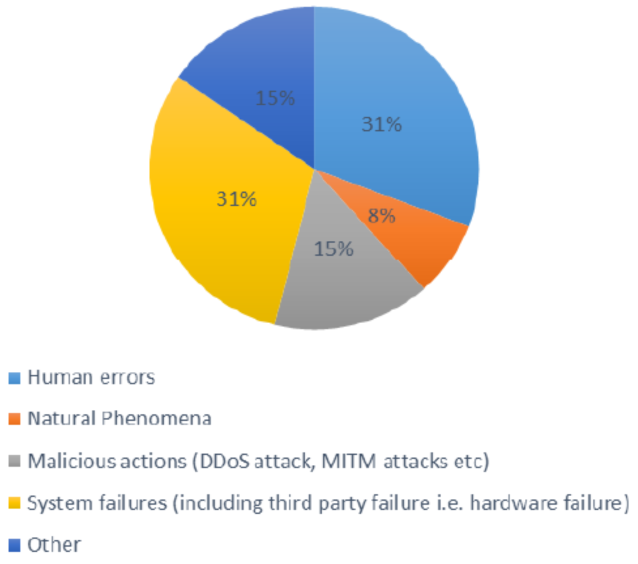


Figure 16. Common root causes of security incidents in healthcare. [49]

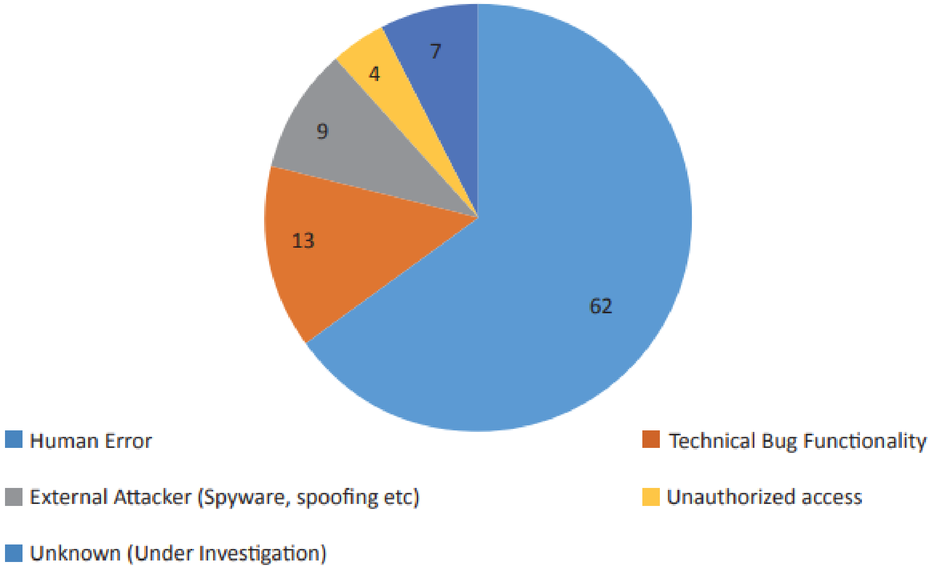


Figure 17. Root cause for the personal data breach. [49]

4.2 Threat Actors

The major threat actors can be categorized as follows [39], [44]:

- **State or state-backed threat actors:** they desire a sovereign state to control its security and safety and their motivations are primarily political.
- **Terrorists and cyber-terrorists:** they are organized criminal groups and motivated by political aims.
- **Hacktivist groups:** they are little organized groups, such as Anonymous, have a political agenda and wishing to make public knowledge negative (distribute propaganda) or cause damage to organizations.
- **Organized crime groups**: these threat actors are motivated by financial gain
- **Corporate entities**: these threat actors may seek to gain competitive advantage in the technological area through, theft of sensitive commercial data or by causing reputational or operational damage to their global competitors.
- **Isolated individuals (hackers)**: individuals have various motivations such fraud, need of recognition, revenge, extreme curiosity, fun, or personal glory. Usually hackers that have as motivation fun or personal glory named script-kiddies and the rest of them as cyber-criminals.
- **Insiders (internals):** this category refers to an insider working within an organization or partners of an organization (e.g. digital service providers). They

may work for other threat actors organized crime groups, a hacktivist group, a state actor or could be a hacker.

To have an idea of the evolution of leaks in recent years by category of intruders, we can take a look in Figures 18 and 19 [43]. It should be emphasized that, the main sector of data breaches is the eHealth sector and the main threat actors are insiders/internals [39], [43].

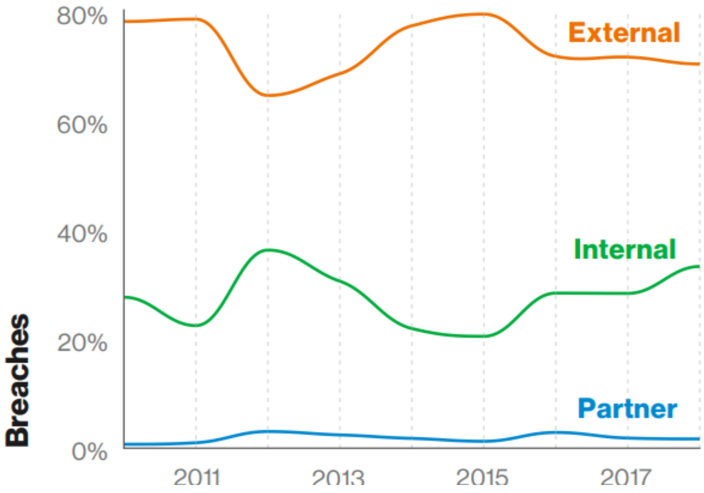


Figure 18. Threat actor in breaches over time. [43]

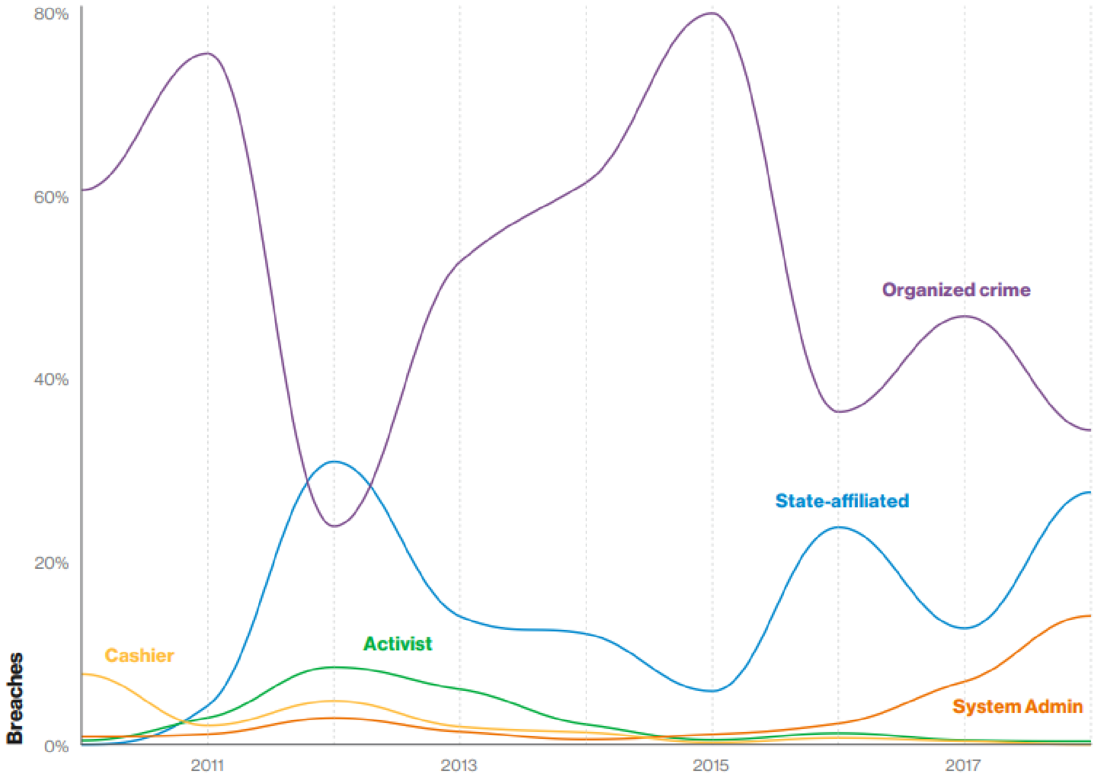


Figure 19. Select threat actors in breaches over time. [43]

To fight against threat actors, first, we must have an accurate idea of their motivation and rationale. Therefore, we tend to should examine "what?" the activities square measure before examining the forms of attacks. The possible actions of the attackers can generally be described as follows [44]:

- personal or organization disturbance,
- physical intrusion or illegal action,
- installation of unauthorized software or code on a system without the owner's consent,
- unauthorized access and actions on the system hardware and software components,
- information system remote disturbance,
- an illegal activity carried out on the public communication networks

The target of all the above-mentioned actions is obviously the breach of one or more of the security objectives, which described in section 3.1.

4.3 Intentional (Adversarial) Attacks

We classify intentional attacks in four categories: (a) physical, (b) passive, (c) active and, (d) Man-in-The-Middle attacks, as shown in Figure 20.

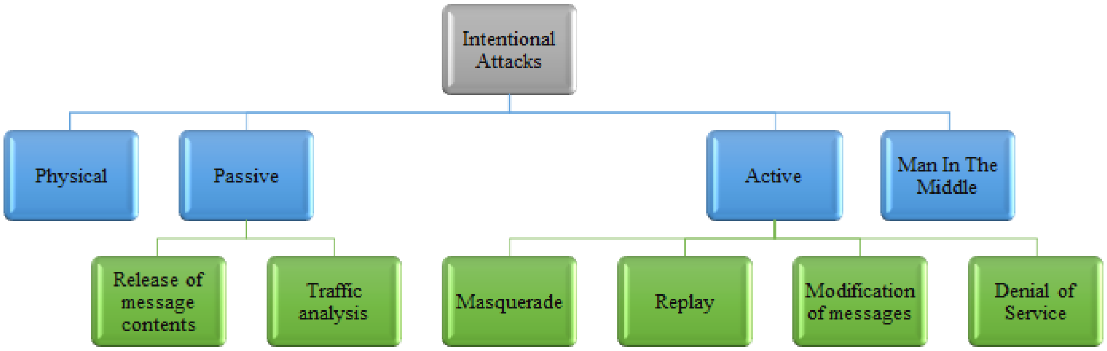


Figure 20. Classification of intentional attacks

4.3.1 Physical attacks

This category of threats contains threats that stem from intentional hostile human actions. Physical attacks include the following [46]:

- Fraud made by human
- Sabotage
- Vandalism
- Theft of devices, storage media and, documents
- Information leakage/sharing
- Unauthorized physical access/Unauthorized entry to premises
- Coercion, extortion or corruption
- Damage from the warfare
- Terrorists attack

4.3.2 Passive Attacks

Passive attack relay on the alters of communication between two parties. These attacks do not require installing additional tools/software on victims' site and it doesn't affect system resources. In a passive attack, the attacker aims at system information either by seeking or using the information. Passive attacks are within the nature of eavesdropping, hijacking, or monitoring transmissions using network sniffers and are essentially actions that precede another attack, as the information collected by the attacker through them will be exploited to carry out his main attack. The release of message contents and traffic analysis are the two kinds of passive attacks [37]. A more detailed description is the following:

- **Release of message contents:** Messages, i.e. email messages or transferred files, may contain sensitive or confidential information. It’s necessary to prevent an adversary from learning the contents of these transmissions.
- **Traffic analysis:** The attacker can collect important information that is transferred into the packages that the victim system exchanges. Even if the information exchanged is masked (encrypted) and the attacker albeit captured the message could not extract any information from the message, if the attacker has the means to gather information then he can apply various techniques to extract the information he needs. The term **sniffing** is used to represent the interception of data by employing a sniffer, which is an application aimed at capturing the network traffic (i.e. Wireshark[16]).

4.3.3 Active attacks

Threats of malicious activities required the use of tools by the attacker. These attacks required to install additional tools and/or software or do some additional steps on the victim's IT infrastructure and/or software. In an active attack, in contrast with a passive attack, the attacker attempts to modify system resources or disturb their operation. These can be subdivided primarily into four categories: masquerade, replay, modification of messages, and denial of service [37]. A more detailed description is the following:

- **Masquerade:** A type of attack where the attacker pretends to be a different authorized entity. A masquerade attack is a complex attack and usually includes one of the other forms of active attack. For example, if a masquerading can captured and replayed authentication sequences and gains the ability to pretend an authorized entity, then could gain greater privileges by impersonating an entity that has those privileges. Also, the term **spoofing** is used to represent behavior that involves an attacker that masquerades. Among the most widely-used spoofing attacks, is IP address spoofing that aimed at a network, DNS spoofing that aimed to corrupt Domain Name System (DNS) data and website spoofing that aimed at a browser.
- **Replay:** Includes the passive capture of a message and its subsequent retransmission to produce an unauthorized outcome.
- **Modification of messages:** Modification includes reordering or delay of messages exchanged or alteration of some portion of a legitimate message, to yield an unauthorized result.
- **The Denial of Service (DoS):** DoS prevents or inhibits the normal use or management of systems facilities and may have a specific target. For example, an entity may withhold all messages directed to a particular destination. Also, an attacker by disabling the network or by overloading it with messages could

---

[16] https://www.wireshark.org/

materialize another form of DoS, which is the disruption of an entire network. A **Distributed Denial of Service (DDoS) attack** is a DoS technique that uses multiple compromised hosts to perform the attack through the bombardment of simultaneous data requests to a central server. In doing so, the attacker intents to exhaust the target’s resources, for example, network bandwidth.

- **The Man In The Middle attack:** A well-known kind of attack is the Man In The Middle (MITM) attack. In this attack, an attacker secretly takes control of the communication channel between two or more endpoints. The difference between the MITM attacker from a simple eavesdropper is that a MIMT can intercept, modify, change, or replace victims’ communication traffic [51].

In Common Attack Pattern Enumeration and Classification (CAPEC) reference framework[17] security events related to malicious activities are provided.

4.4 Attack Methodology

To understand how an attacker operates, that is, what is its methodology is essential. A common tool to examine an attack methodology is the cyber kill chain. This is a common attack cycle model and is a series of steps that trace stages of a cyberattack from the early reconnaissance stages to the exfiltration of data [52] . The kill chain framework helps us to better anticipate, recognize and, combat cyberthreats [53]. The stages defined are as follows, and depicted in Figure 21:

- Planning the attack
    - Reconnaissance: Deep research and analysis was made on the target
    - Weaponization: Payload or attack tools were built
    - Delivery: Attackers delivers the payload or the tools to the target
- Compromising the target
    - Exploitation: Making use of existing vulnerabilities to exploit the target
    - Installation: Installing malicious code in the target
- Executing the attack
    - Command and Control (C2): Command and Control the compromised targets
    - Actions on Objectives: Collect of corrupt target’s data by using lateral movement onto a network

---

[17] https://capec.mitre.org/

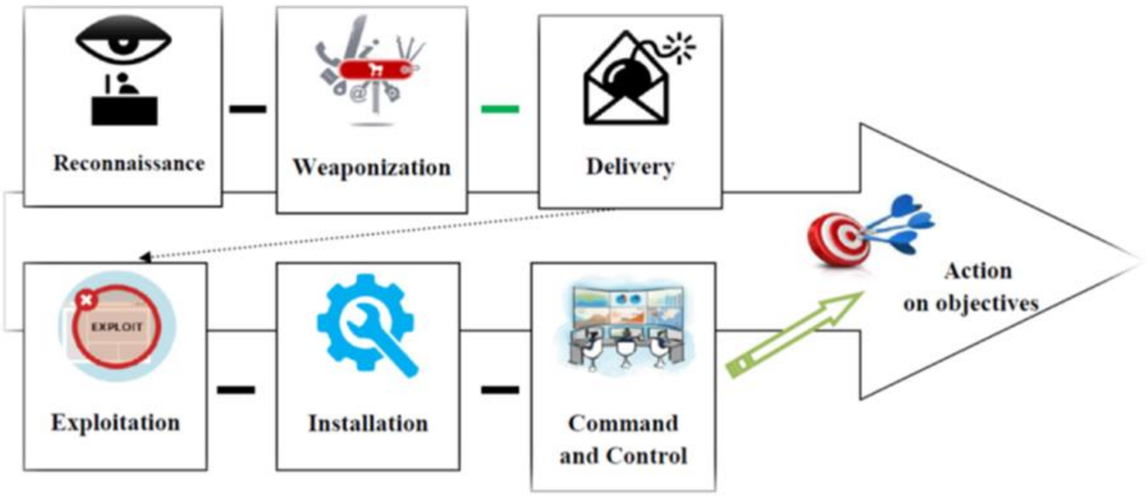


Figure 21. Cyber kill chain stages. [53]

4.5 Tools and Techniques

As mentioned, for each "what?" possibility, we must examine “how?”, which means examining the tools and techniques employed by threat actors.

4.5.1 Malware and Exploit

Malware and exploit can be used separately or in combination with multiple types of attacks. These terms usually used interchangeably, however, bear several clear distinctions, which are been discussed in succeeding paragraphs, where we define them and their purposes.

Malware, also known as ‘malicious software’, is a term that refers to any kind of code, script or application with a mischievous intention with a purpose to hamper the functionality of a system that is to attack and render devices, systems, operations and networks inoperable without user’s knowledge [34]. So, attackers by activating malware can take full or partial control of the operations. Malware is the top threat globally from 2014 until today [48]. 30% of all data breach which is theft and/or alters data resulting in a violation of privacy and/or integrity reported in 2018 involve malware [39]. The position of malware in the kill chain depicted in Figure 22.

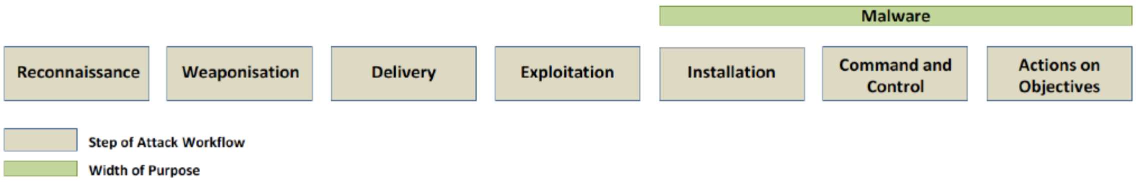


Figure 22. Position of malware in the kill chain. [39]

There are several types of malware. Well-known types are the following, as shown in Figure 23:

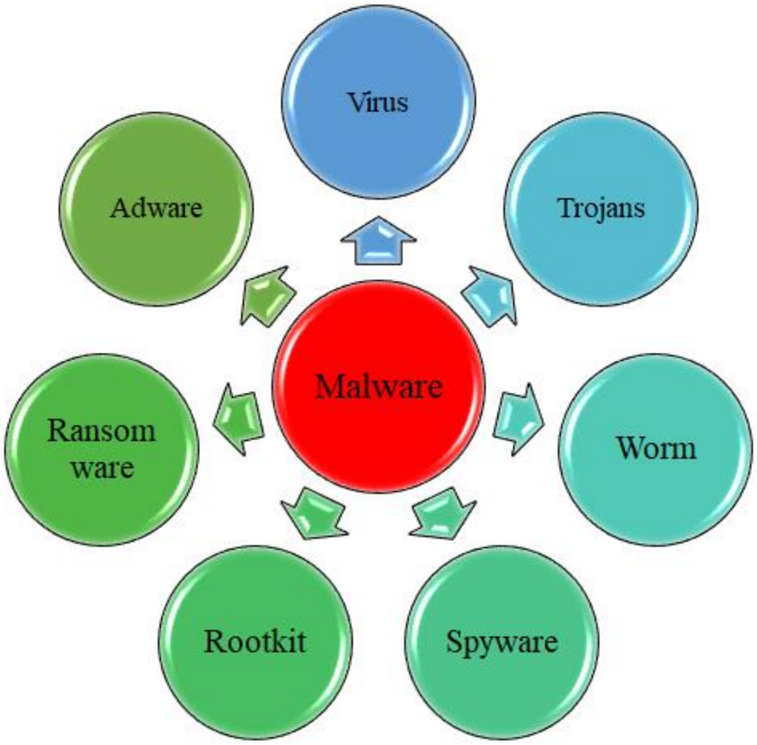


Figure 23. Main types of malware

- **Virus:** Malware that coexists with an executable file and is activated with its execution. Enabling the virus causes the code to run and play, infecting other system files [36]. For a system to be infected with a virus, the file that contains the virus must first somehow enter the system and run to infect other systems files. That could be done, for example, from vulnerabilities in web applications [54].
- **Trojan horse (Trojans):** Malware that appears as a useful program, but also has a hidden and potentially malicious function that escapes security mechanisms, usually by exploiting legitimate authorizations of a system entity that invokes the program [36]. Because trojans have the ability to coexist with other programs in the system, they can change their operation when they are executed [54]. During the years 2018 and 2019, the eHealth sector primarily targeted by trojans, and the two most dangerous of them are the ones with the names Emotet and TrickBot [55].
- **Worm (Write Once, Read Many):** A self-replicating, self-propagating, self-contained malware that uses networking mechanisms to spread itself [36]. Worms reproduce automatically and no one is required to execute their code. Worms can

contain payloads. Payloads could create bots, damage host devices or, destroy host networks [54].

- **Bot:** Short for “robot,” the term “bot” at the beginning had a positive meaning, but soon after the initial useful bots started to appear on **I**nternet **R**elay **C**hat, so did others, that could exploit vulnerabilities, steal passwords and log keystrokes. Bot is a software program created to give an attacker remote access and control over the operations of the infected computer resources. Also a bot can be a computer that has been compromised through a malware infection and can be controlled remotely by a cybercriminal. The cybercriminal can then use the bot to launch more attacks, or to bring it into a collection of controlled computers, known as a botnet. [56].
- **Spyware:** Malware that is installed into a system without user knowledge to gather information on individuals or organizations. Spyware secretly monitors user activities such as key logs and screen watching, so that attacker can make use of this information. Spyware attaches themselves with trojans to exploit vulnerabilities [54].
- **Rootkit:** Set of malware that the attacker installs on a victim system. To install a rootkit, the attacker previously gained access to a victim’s system. The main function of a rootkit is to enable the attacker to be able to enter the victim system in the future without being noticed by installing a backdoor, usually trojans used for remote system access. Another technique used by rootkits to hide the traces of the attacker is to use some functions that change the system's log files [54].
- **Ransomware:** Ransomware acquires data from computer resources through malware [57]. Malware may be locker where the whole system is locked or it may encrypt some files, thus rendering them inaccessible and leads to locking dedicated computers and access is denied. Attacker display messages to force victims to pay money as ransom to release the lock or access denial. In case the victim does not pay the ransom, the attacker may extend ransom amount or proceeds to destroy files on the devices [58]. It is worth noting that, a ransomware cryptoworm, the WannaCry, is one of the most harmful and infamous attacks in eHealth sector [59].
- **Adware:** Advertising-supported malware that is specifically designed to deliver the advertisement to users spontaneously. Adware consists of advertisements and pops up ads that show on websites. By clicking on ads, adware activates and steals information or track user activities [54].

Exploit is a piece of code or a program to exploit a vulnerability that will be used in an attack [60]. Vulnerabilities arise from defects in various software due to programming errors, from errors in system configuration, from software design imperfections, or insufficient security measures. Exploits are not inherently malicious, but they are likely to be used for malicious actions. Malware and exploits are used in combination with multiple types of malicious actions. After the vulnerability is exploited a malicious action may occur such DoS, data breach, arbitrary code execution, etc. Web based attacks and Web application attacks based mainly on exploits [39].

Exploits may be categorized into known and unknown exploits. Zero-day exploits take advantage of unknown vulnerabilities for which no software patch yet is available [52], [61].

4.5.2 Botnet and Exploit kit

Two terms closely related to the spread of malware are the terms (a) botnet and (b) exploit kit. Both belong to the Command and Control stage in the kill chain. Before examining these terms, its essential to present two more common concepts: backdoor and drive-by download.

A **backdoor** is a method used by threat actors to bypass security measures in any system hardware or software component, such user's device, network, or application, to gain access to system component[18]. Once access gained, the threat actor through the backdoor has the ability to install malware or to realize several types of malicious actions. It worth notice that a backdoor can also be installed by software or hardware providers as a means of gaining access to their products in order to support their customers or to resolve software issues. For example, a provider could be installed a backdoor to help a user to unlock his device.

A **drive-by download** is a method used by threat actors to install malware on users' devices without any action from the user. It could happen when a victim simply visiting an insecure compromised web page. If the device is vulnerable, it's infected automatically [39].

A **botnet** is a network of malware-infected computers that attackers use to perform tasks online without the user's permission. Bots become part of botnets, which consist of the network to be controlled by the botmaster [56]. It is evolving to become a severe security threat because botnets launch DDoS attacks, hack web servers data, malware masquerading on websites and, spam bots that gather information [62]. Figure 24 depicts the position of botnets in the kill chain.

---

[18] https://www.malwarebytes.com/backdoor/

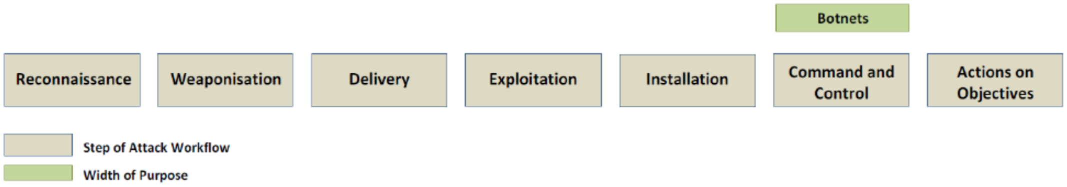


Figure 24. Position of botnets in the kill chain. [39]

The largest DoS attack in history was an IoT botnet, the Mirai [48]. An example of architecture of an IoT botnet is shown in Figure 25. The botnet includes a Command and Control Server (CCS) that controls the bots, a Reporting Server that compiles the data about vulnerable IoT devices and, forwards it to the Loader module, which is the basis to log into the victim devices. Once the Loader logs into the victim device, it instructs the victim device to contact the Malware Distributor (MD), a server in the botnet, to download additional malware payload. The infected IoT devices such as sensing nodes are then used to launch DDoS attacks [62].

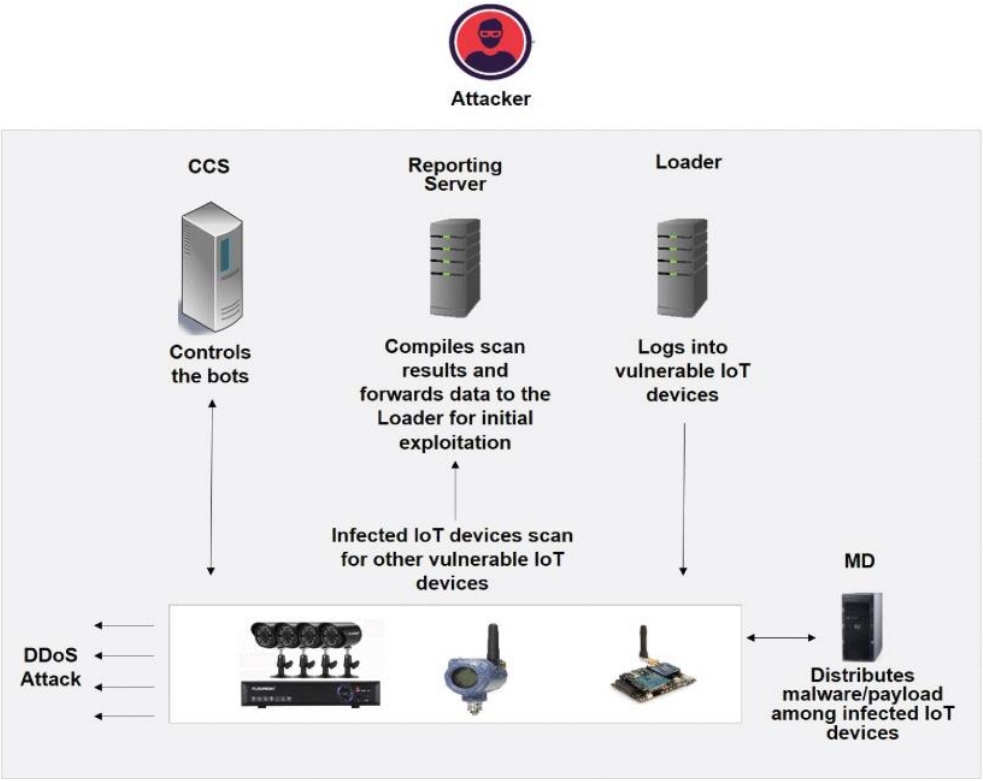

Attacker
CCS
Reporting Server
Loader
Controls the bots
Compiles scan results and forwards data to the Loader for initial exploitation
Logs into vulnerable IoT devices
Infected IoT devices scan for other vulnerable IoT devices
MD
DDoS Attack
Distributes malware/payload among infected IoT devices

Figure 25. Architecture of an IoT botnet controlled by an attacker. [62]

An **exploit kit** is a toolkit based on the drive-by download method used by an attacker to install malicious payload on victim devices based on the exploits vulnerabilities found on those devices [60]. The exploit kit is hidden on invisible web pages or hosted on advertisement networks and has the ability to scan the victim's device to find out information about the device’s operating system, the programs running and, the software-related vulnerabilities. Depending on the vulnerability, the exploit kit uses the suitable code and installs the malware. Exploit kits targets commonly installed software such as Adobe Flash and Java [60]. An example of how an exploit kit can work depicted in Figure 26.

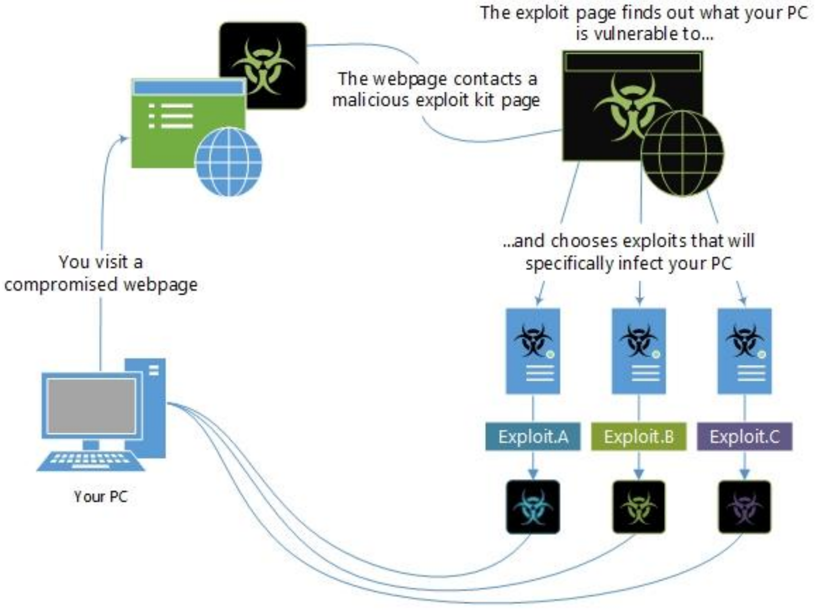

The exploit page finds out what your PC is vulnerable to...
The webpage contacts a malicious exploit kit page
You visit a compromised webpage
...and chooses exploits that will specifically infect your PC
Your PC
Exploit.A
Exploit.B
Exploit.C

Figure 26. Example of how an exploit kit works. [60]

4.5.3 Techniques Based on Human weaknesses

The attackers have discovered several techniques, also called client-side attacks [63], based on human weaknesses that can use to gather the information they would otherwise not have had access to. The most common of these techniques include:

Social Engineering*:* Social engineering is a general term for a technique that relies deeply on human interaction. Attackers try to influence an individual and encourage him to reveal confidential information (e.g., a password). This information can be used to attack any component of system infrastructure. A social engineering attack could be a complicated multi-phase attack that “employs either direct communication or indirect communication, and incorporates a social engineer, a target, a medium, a goal, one or additional compliance principles and one or additional techniques” [64]. Authors in [64] present a model of the attack, as shown in Figure 27. According to this model, the attack splits into phases and each of them is handled as a new attack.

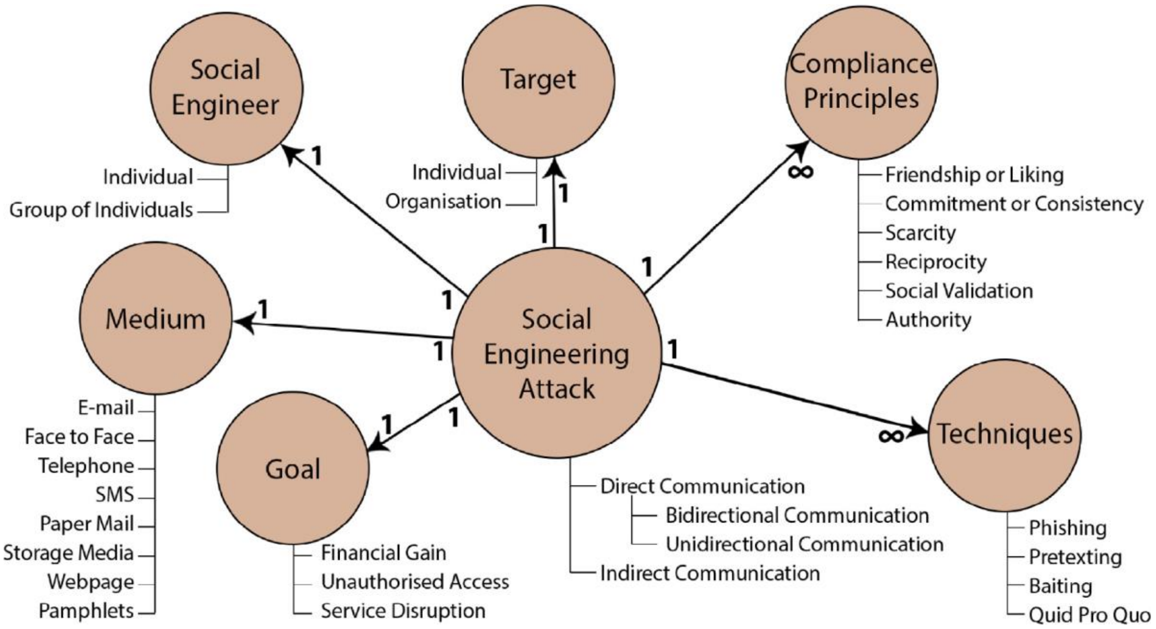


Figure 27. A model of a social engineering attack. [64]

Phishing: Phishing is a spoofing technique in which the threat actor masquerades as a reputable source through crafting messages using social engineering and spreading malware. The goal of phishers is to trick their victims through emails and messages to open an attachment, click on an URL, etc. into giving away sensitive data or to install the malware in the form of spyware on the victim's system [65] - [66]. Harm from the phishing attacks continues to grow every year[19] due to their diversity [67]. It is worth noting that 90% of malware infections and 72% of data breaches in organizations originate from phishing attacks [39]. Figure 28 depicts the position of phishing in the kill chain.

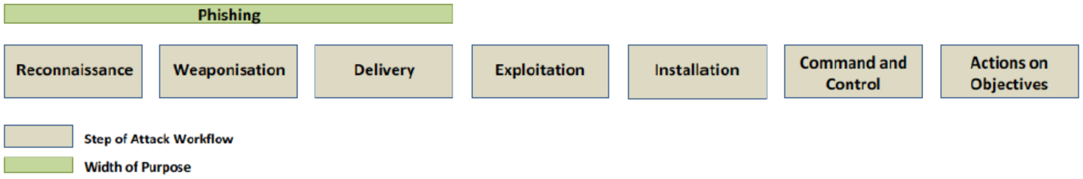


Figure 28. Position of phishing in the kill chain. [39]

Major types of phishing attacks shown in Figure 29:

---

[19] For more information on CSV Feed and Overall phishing statistics online: https://phishstats.info/

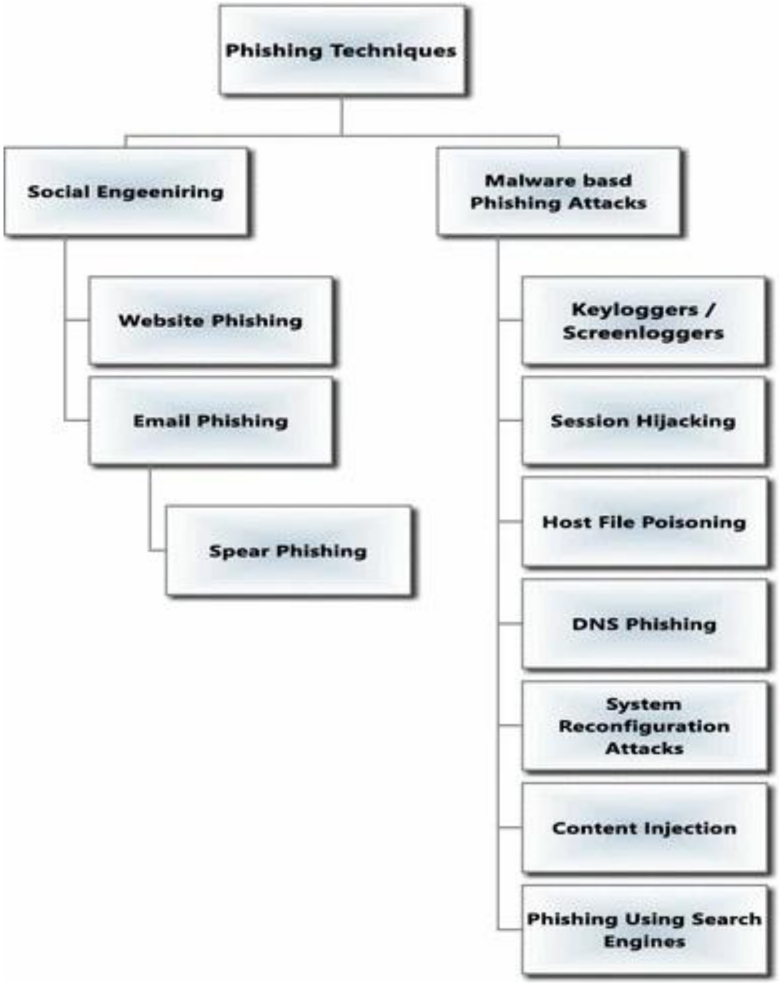


Figure 29. Types of phishing attacks. [65]

Spear phishing is a form of phishing that targets a specific group and usually includes highly customized scam content [66]. The term whaling refers to phishing attacks that target a particular individual. Spear phishing emails are a widely used technique to transfer malware to an end-user [66]. Also, we met the term vishing that refers to phishing over the phone and smishing that refers to phishing over SMS [67]. Especially in 2020, email phishing attacks have spiked over 600% since the end of February 2020 due to COVID-19 pandemic [68].

Social Media*:* Attackers exploit platforms of social media such as Facebook, Instagram, Twitter, LinkedIn, etc. to materialize targeted attacks. Social media accounts offer a method of gathering contact data, interests, and private connections of a targeted individual that successively may be wont to conduct a social engineering attack. Using fake social media accounts, adversaries can impersonate trusted individuals (i.e. coworkers) in order to send links to malicious code that steal personal or organizational information [68] - [69]. Also, as mentioned in [39], these platforms used to run and install IoT botnets.

4.5.4 Advanced Persistent Threat (APT)

Advanced Persistent Threat (APT) is an attack in which some specific threat actors use highly sophisticated techniques of multiple different attack vectors and have significant resources to establish persistent footholds within the victim's system to surveillance the system and exact valuable and critical information by multiple ways from time to time. The victim is usually unsuspecting of the intrusion. Threat actor works in several steps to achieve his objectives and in an APT included all stages of the kill chain and therefore is very complex [61]. Figure 30 depicts analytically the phases commonly observed in an APT. The attack usually begins with the social engineering technique, usually with the spear-phishing used by 71% of APT groups [39]. Physical media (i.e. USB) and remote exploitation (i.e. smartphone exploitation) also can be used and, the next treat events follow [61].

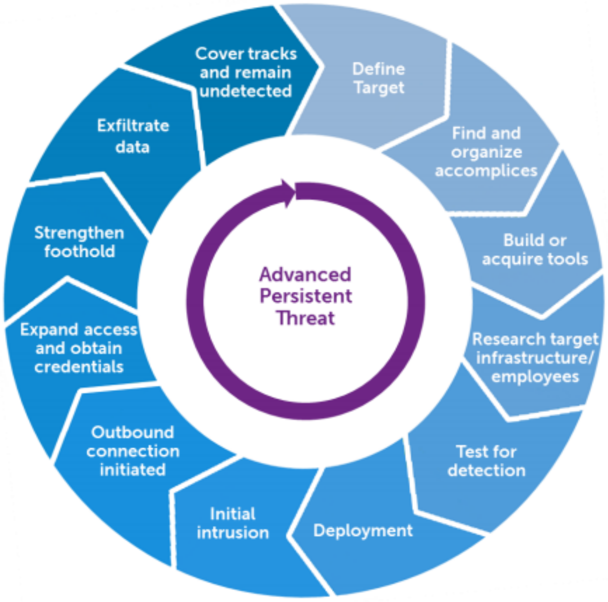

Advanced Persistent Threat
Define Target
Find and organize accomplices
Build or acquire tools
Research target infrastructure/ employees
Test for detection
Deployment
Initial intrusion
Outbound connection initiated
Expand access and obtain credentials
Strengthen foothold
Exfiltrate data
Cover tracks and remain undetected

Figure 30. Lifecycle of an Advanced Persistent Threat. [65]

APT attacks targeted Critical Information Infrastructures (CII) as eHealth infrastructures. Healthcare organizations are a common target because they host valuable personal and medical data. APT form a serious threat because APT's threat actors mostly perform zero- day attacks to compromise their target [52].

In 2020, the coronavirus (COVID-19) has become a global pandemic. The pandemic makes healthcare organizations a prime target because APTs try to obtain information for domestic research into COVID-19-related medicine [70]. On the other hand, attackers take advantage of collective fear to perform phishing campaigns using coronavirus as a trap [71]. Threat actors like hackers and state-backed have been using an APT technique to gain a foothold on victim machines and launch several types of malware attacks.

4.5.5 Spam

Spam is an unsolicited message or email sent out in bulk to a comprehensive recipient list urge users to open a malicious attachment or a malicious link. Spam usually sent by botnets and is related tightly to social engineering [64]. 26,6% is comprised of health-related spam [39]. The position of spam in the kill chain depicted in Figure 31.

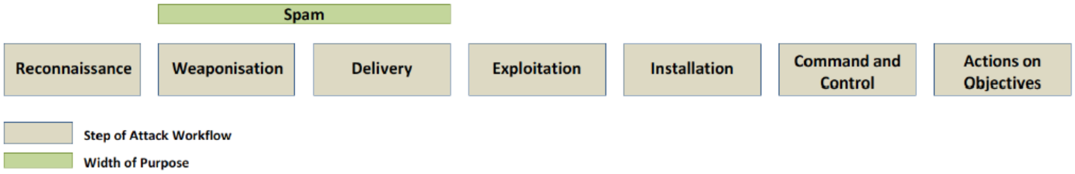


Figure 31. Position of spam in the kill chain. [39]

It is worthwhile to give an example in which it is shown how malware spreads through a spam email, as depicted in Figure 32. A trojan (the TrickBot[20]) which could come hand in hand with another trojan (the Emotet) reaches out to the botnet, so both malware spread.

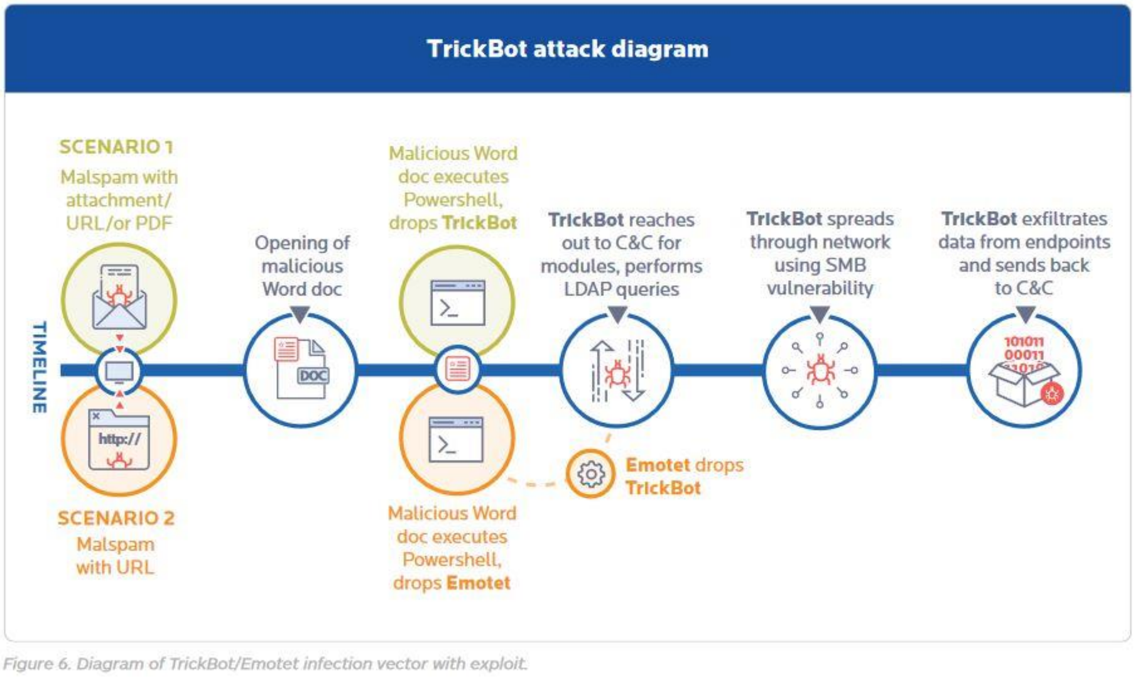

TrickBot attack diagram
SCENARIO 1
Malspam with attachment/ URL/or PDF
TIMELINE
http://
SCENARIO 2
Malspam with URL
Opening of malicious Word doc
DOC
Malicious Word doc executes Powershell, drops TrickBot
Malicious Word doc executes Powershell, drops Emotet
TrickBot reaches out to C&C for modules, performs LDAP queries
Emotet drops TrickBot
TrickBot spreads through network using SMB vulnerability
TrickBot exfiltrates data from endpoints and sends back to C&C
101011
00011
Figure 6. Diagram of TrickBot/Emotet infection vector with exploit.

Figure 32. Example of spread malware with exploit via spam. [72]

---

[20] https://blog.f-secure.com/what-is-trickbot/

4.5.6 Recent Types of Attacks

Fileless or memory-based attack, also known as “living-off-the-land”[73], is one in which an attacker uses existing software, allowed applications and authorized protocols. Attackers are capable of gaining control of devices without downloading any malware [39].

Cryptojacking is a new term to describe a specific attack that refers to the programs (cryptomining software) that use the victim's computing resources (i.e. CPU) to mine cryptocurrencies This processing power is used to solve cryptographic puzzles that are recorded in the blockchain. Crypto mining software considered as malware and unlike ransomware has as target to assume the control of the computational power of devices and this may affect device performance that is become critical when we refer to medical devices. The target may be any internet-connected device containing a CPU. Cryptojaking is a growing threat.

4.6 Cyberthreat Landscape

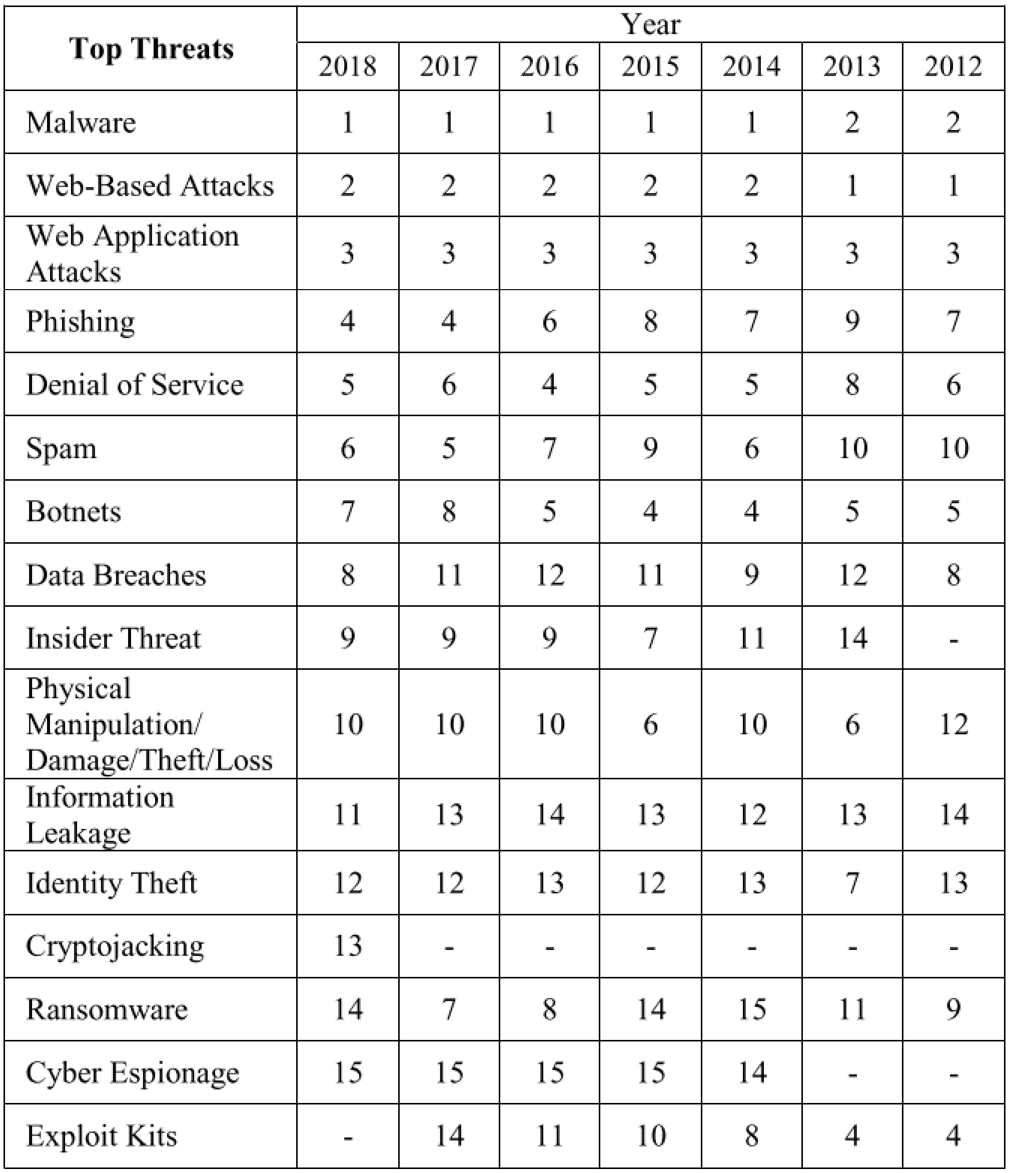
Until this point, we identify threat actors, their motivations levels and of the potential technical means available to them. There is no doubt that we need to look at what threats are predominant, what are the threat trends. Since 2012 ENISA provides annual Threat Landscape reports (ETL)[21] that contain the fifteen top cyber threats for the corresponding year. The information collected from publicly available sources (Open source intelligence - OSINT[22]), references from giant industries that provide cybersecurity solutions globally (i.e. Cisco[23], Fortinet[24], Kaspersky[25]) Verizon and websites (i.e. ZDNet[26]). In our humble opinion, these publications are a first-class source for outlining the threat landscape.

In this section we select to summarize the threat landscape through figures that shown:

- The annual change in ranking of the top fifteen cyber threats (Figure 33),
- The involvement of threat agents in the top cyber threats (Figure 34),
- The timeline of security attacks on healthcare data (Figure 35) and,
- The data breach statistics in 2019 related to healthcare (Figure 36)

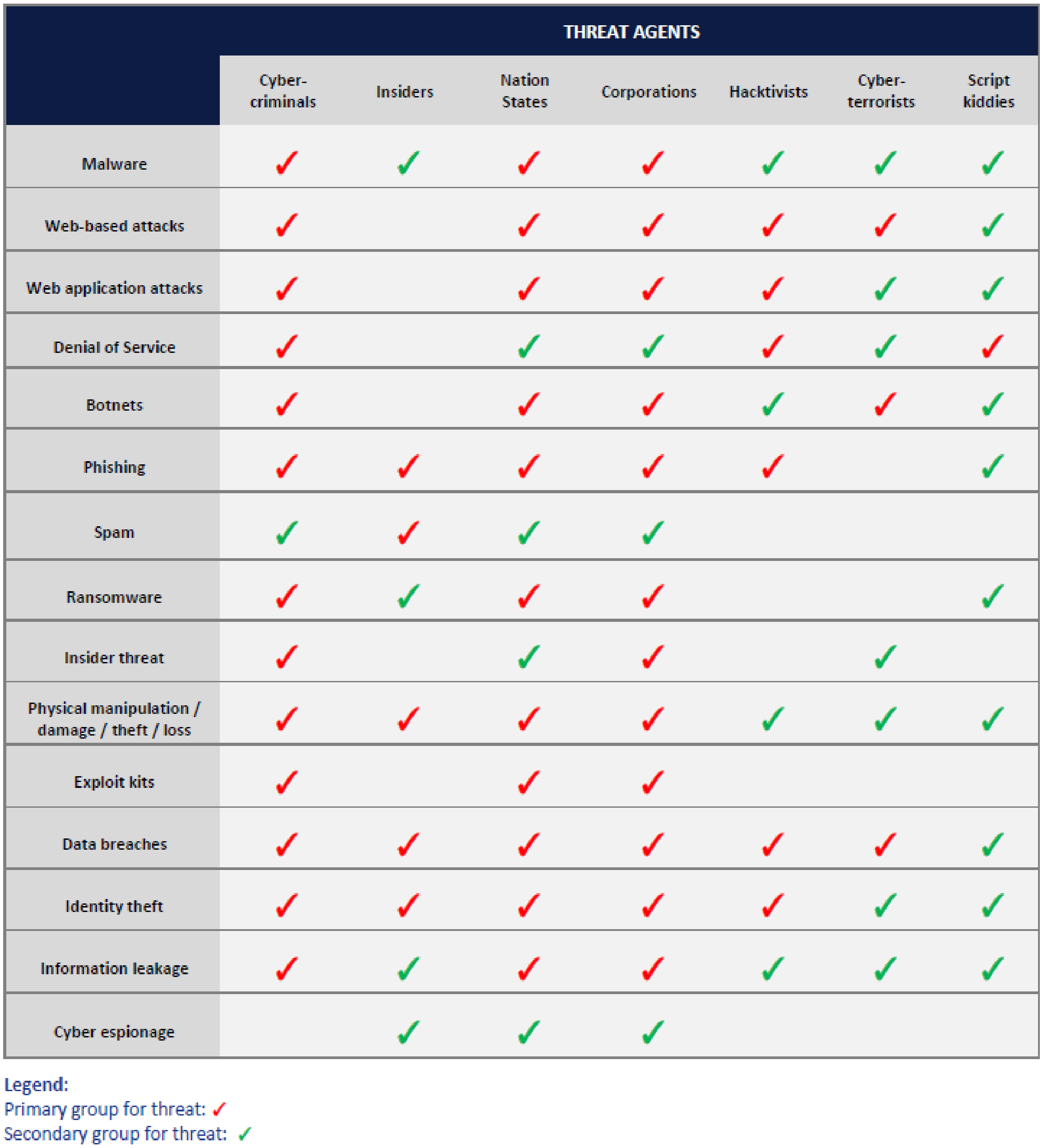
---

[21] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape
[22] https://osintframework.com/
[23] https://www.cisco.com/
[24] https://www.fortinet.com/
[25] https://www.kaspersky.com/
[26] https://www.zdnet.com/



Top Threats	Year						
	2018	2017	2016	2015	2014	2013	2012
Malware	1	1	1	1	1	2	2
Web-Based Attacks	2	2	2	2	2	1	1
Web Application Attacks	3	3	3	3	3	3	3
Phishing	4	4	6	8	7	9	7
Denial of Service	5	6	4	5	5	8	6
Spam	6	5	7	9	6	10	10
Botnets	7	8	5	4	4	5	5
Data Breaches	8	11	12	11	9	12	8
Insider Threat	9	9	9	7	11	14	-
Physical Manipulation/ Damage/Theft/Loss	10	10	10	6	10	6	12
Information Leakage	11	13	14	13	12	13	14
Identity Theft	12	12	13	12	13	7	13
Cryptojacking	13	-	-	-	-	-	-
Ransomware	14	7	8	14	15	11	9
Cyber Espionage	15	15	15	15	14	-	-
Exploit Kits	-	14	11	10	8	4	4

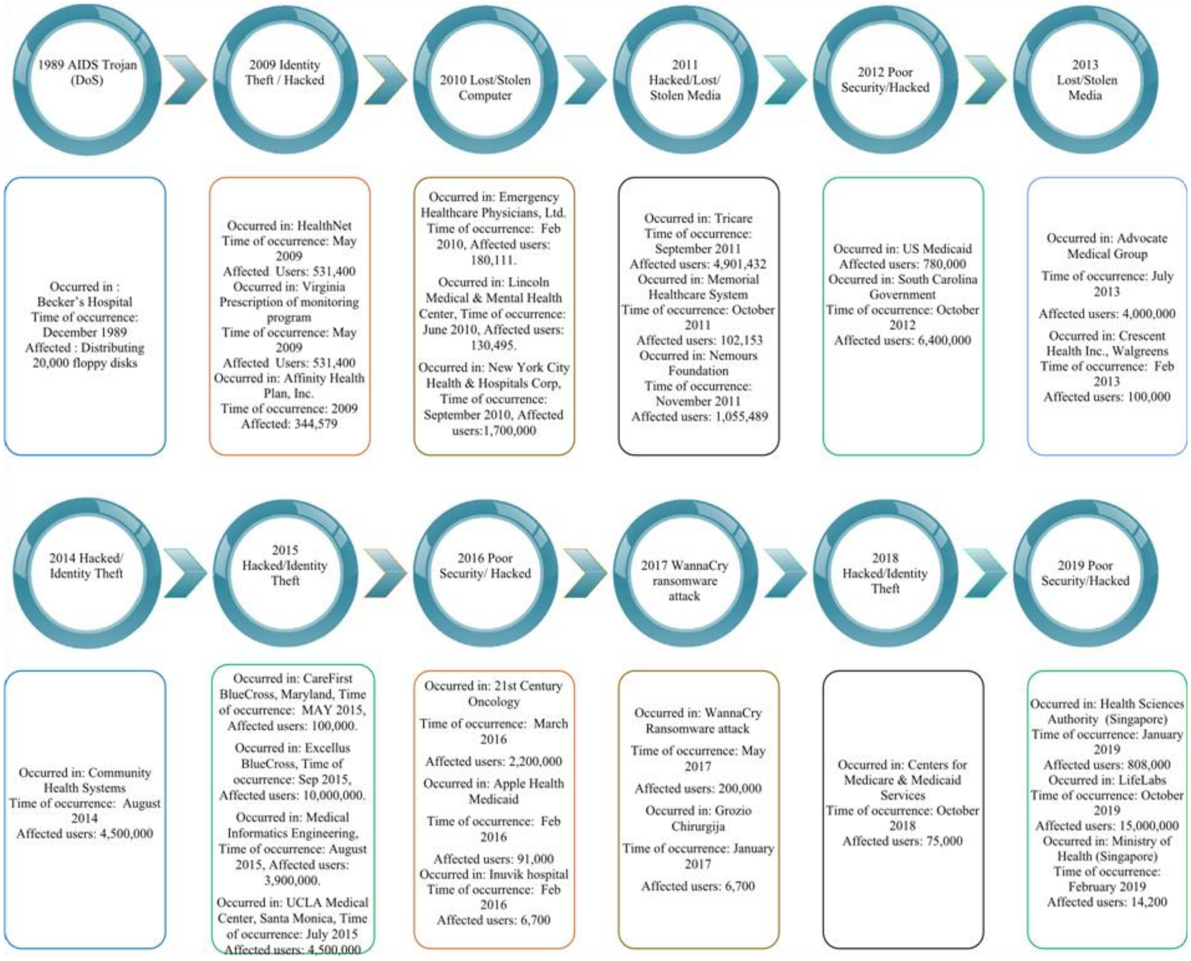
Figure 33. Annual change in ranking of the top fifteen threats according to ENISA reports (ETL: ENISA Threat Landscapes) [48]



	THREAT AGENTS						
	Cyber-criminals	Insiders	Nation States	Corporations	Hacktivists	Cyber-terrorists	Script kiddies
Malware	✔	✓	✔	✔	✓	✓	✓
Web-based attacks	✔		✔	✔	✔	✔	✓
Web application attacks	✔		✔	✔	✔	✓	✓
Denial of Service	✔		✓	✓	✔	✓	✔
Botnets	✔		✔	✔	✓	✔	✓
Phishing	✔	✔	✔	✔	✔		✓
Spam	✓	✔	✓	✓			
Ransomware	✔	✓	✔	✔			✓
Insider threat	✔		✓	✔		✓	
Physical manipulation / damage / theft / loss	✔	✔	✔	✔	✓	✓	✓
Exploit kits	✔		✔	✔			
Data breaches	✔	✔	✔	✔	✔	✔	✓
Identity theft	✔	✔	✔	✔	✔	✓	✓
Information leakage	✔	✓	✔	✔	✓	✓	✓
Cyber espionage		✓	✓	✓			

Legend:
Primary group for threat: ✔
Secondary group for threat: ✓

Figure 34. Involvement of threat agents in the top cyber threats. [39]



1989 AIDS Trojan (DoS)

Occurred in : Becker's Hospital
Time of occurrence: December 1989
Affected : Distributing 20,000 floppy disks

2009 Identity Theft / Hacked

Occurred in: HealthNet
Time of occurrence: May 2009
Affected Users: 531,400
Occurred in: Virginia Prescription of monitoring program
Time of occurrence: May 2009
Affected Users: 531,400
Occurred in: Affinity Health Plan, Inc.
Time of occurrence: 2009
Affected: 344,579

2010 Lost/Stolen Computer

Occurred in: Emergency Healthcare Physicians, Ltd. Time of occurrence: Feb 2010, Affected users: 180,111.

Occurred in: Lincoln Medical & Mental Health Center, Time of occurrence: June 2010, Affected users: 130,495.

Occurred in: New York City Health & Hospitals Corp, Time of occurrence: September 2010, Affected users:1,700,000

2011 Hacked/Lost/ Stolen Media

Occurred in: Tricare
Time of occurrence: September 2011
Affected users: 4,901,432
Occurred in: Memorial Healthcare System
Time of occurrence: October 2011
Affected users: 102,153
Occurred in: Nemours Foundation
Time of occurrence: November 2011
Affected users: 1,055,489

2012 Poor Security/Hacked

Occurred in: US Medicaid
Affected users: 780,000
Occurred in: South Carolina Government
Time of occurrence: October 2012
Affected users: 6,400,000

2013 Lost/Stolen Media

Occurred in: Advocate Medical Group

Time of occurrence: July 2013

Affected users: 4,000,000

Occurred in: Crescent Health Inc., Walgreens
Time of occurrence: Feb 2013
Affected users: 100,000

2014 Hacked/ Identity Theft

Occurred in: Community Health Systems
Time of occurrence: August 2014
Affected users: 4,500,000

2015 Hacked/Identity Theft

Occurred in: CareFirst BlueCross, Maryland, Time of occurrence: MAY 2015, Affected users: 100,000.

Occurred in: Excellus BlueCross, Time of occurrence: Sep 2015, Affected users: 10,000,000.

Occurred in: Medical Informatics Engineering, Time of occurrence: August 2015, Affected users: 3,900,000.

Occurred in: UCLA Medical Center, Santa Monica, Time of occurrence: July 2015 Affected users: 4,500,000

2016 Poor Security/ Hacked

Occurred in: 21st Century Oncology

Time of occurrence: March 2016

Affected users: 2,200,000

Occurred in: Apple Health Medicaid

Time of occurrence: Feb 2016

Affected users: 91,000
Occurred in: Inuvik hospital
Time of occurrence: Feb 2016
Affected users: 6,700

2017 WannaCry ransomware attack

Occurred in: WannaCry Ransomware attack

Time of occurrence: May 2017

Affected users: 200,000

Occurred in: Grozio Chirurgija

Time of occurrence: January 2017

Affected users: 6,700

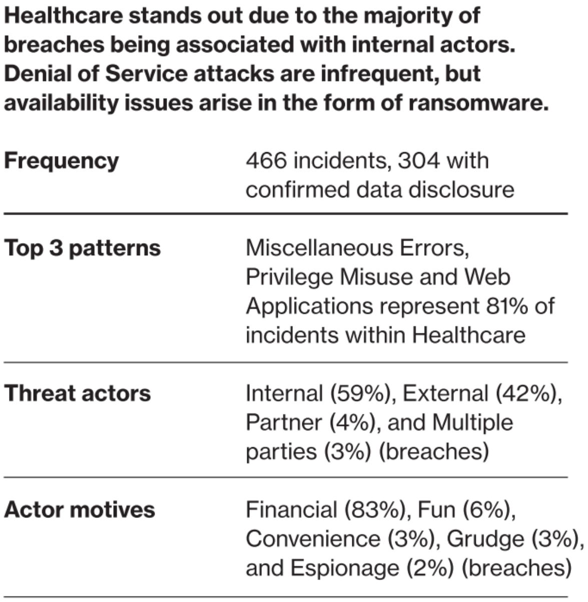
2018 Hacked/Identity Theft

Occurred in: Centers for Medicare & Medicaid Services
Time of occurrence: October 2018
Affected users: 75,000

2019 Poor Security/Hacked

Occurred in: Health Sciences Authority (Singapore)
Time of occurrence: January 2019
Affected users: 808,000
Occurred in: LifeLabs
Time of occurrence: October 2019
Affected users: 15,000,000
Occurred in: Ministry of Health (Singapore)
Time of occurrence: February 2019
Affected users: 14,200

Figure 35. Timeline of security attacks on healthcare data. [21]



Healthcare stands out due to the majority of breaches being associated with internal actors. Denial of Service attacks are infrequent, but availability issues arise in the form of ransomware.

Frequency	466 incidents, 304 with confirmed data disclosure
Top 3 patterns	Miscellaneous Errors, Privilege Misuse and Web Applications represent 81% of incidents within Healthcare
Threat actors	Internal (59%), External (42%), Partner (4%), and Multiple parties (3%) (breaches)
Actor motives	Financial (83%), Fun (6%), Convenience (3%), Grudge (3%), and Espionage (2%) (breaches)

Figure 36. Data breach statistics in 2019 related to healthcare. [43]

5 eHealth Specific Issues on Security and Privacy

The Health sector recognized by the EU through the NIS directive (the directive on security of network and information systems) [74] as a critical sector[27], so, we should always keep in mind that the majority of eHealth services are critical and therefore the eHealth infrastructure that supports them is critical. The NIS Directive defines as health subsectors, health care settings, including hospitals and private clinics that offer their services outside of their environment, as shown in Figure 37. Threat events occurring in eHealth systems that affect their availability and individual's privacy and data integrity are common. Generally speaking, every digital system has vulnerabilities and attracts threat actors to carry out an attack and an eHealth system is no exception. For all individuals and healthcare stakeholders to trust eHealth services, systems that support these services must cover security requirements. As mentioned in previous chapters, security services set goals to meet the basic security requirements and security mechanisms determine the ways in how these goals can be achieved. So, it is crucial to implement security mechanisms that are security measures, which means applying a collection of policies and actions to prevent any attraction from threat actors. In any case, a systematic approach is needed to determine the security measures that will be applied to each system.

In this chapter, first, we present the eHealth sector special issues. Then, the differences between security and privacy are discussed. Subsequently, the need for security guidelines for a systematic approach is emphasized and briefly, the NIST core framework is presented.

5.1 eHealth Special Issues

eHealth improves and innovates the operations, the quality and, the financial efficiency of the healthcare sector through the use of ICTs that support the eHealth services and management of their system components. As we mentioned in chapter 2, eHealth services, in general, include services that (a) support the collection and storage of individuals health data- this implies i.e. the existence of the medical records systems; (b) enable healthcare providers to communicate and share information with other providers in order to provide care- this implies, for example, the existence of access to medical records and scheduling programs; (c) support healthcare providers to diagnosis and treatment and delivery of care to individuals- this implies, for example, the existence of infrastructures to provide mHealth and telehealth services; (d) enable individuals and

---

[27] The NIS Directive defines as critical sectors Energy, Transport, Banking, Financial market infrastructures, Drinking water supply and distribution and Digital Infrastructure.

healthcare providers to access health information- this implies, for example, the existence of knowledge; (e) enable healthcare managers and administrators to manage the delivery of care- this implies the existence of health policy development and, of course, the assurance of security and resilience for all the above-mentioned eHealth services. Security is one of the main concerns regarding eHealth, which needs to be addressed along with the paramount need for safety.

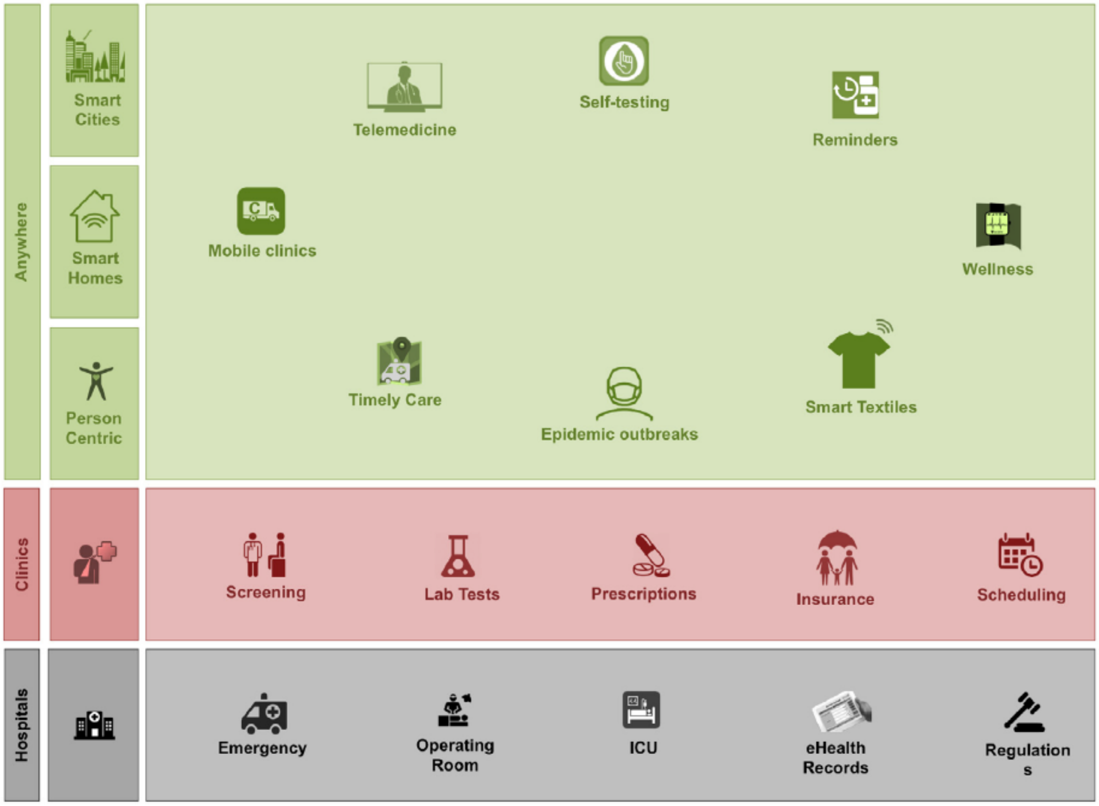


Figure 37. eHealth services in the context of stakeholders, operations, and application. [75]

From the above-described services resulting from that eHealth is not simply include healthcare professionals (doctors, nurses, etc.) and individuals as healthcare stakeholders, but also Standards Developing Organizations (SDOs), manufacturers, regulators and governments, and of course medical sensors and intervention devices. Also, administrators of medical facilities, research analysts, and others can require access to health data.

The purpose of access to eHealth data and services is not simple to categorize. For example, in addition to diagnostic medicine, maybe it is also necessary to provide treatment and access to medical records and so on. The consequence is that the set of actors in eHealth both by role and by name has to be mutable over the lifetime of the system and poses specific security requirements and implementation of specific security mechanisms. The examination of specialized forms of eHealth professionals and patients is expanded to examine the role of medical things in the eHealth sector [76]. For example, let's look at a diagnostic eHealth use case. The actors involved are the patient, the diagnostic sensor, and the health provider that, in a smart healthcare environment may be a machine. In this case, the possible required security services are entity authentication, infrastructure authentication, data integrity and confidentiality, service authorization, and key management [76].

Also, eHealth services that supporting diagnosis and treatment decisions and managing the delivery of care such as telehealth and mHealth requires access to valid and accurate records of patient health for as long as required. Thus whilst it may be argued that medical devices are critical, they are only critical if the readings they take are recorded, they are accurate and are available whenever necessary [76].

After the above discussion, we can understand why the main ICTs that considered for the eHealth ecosystem is Health Information Technology (HIT) systems and the Internet of Medical Things (IoMT) [77]. Among the types of medical things, which can be connected through the network, we can distinguish [77] - [78] (more information on types of medical things is provided in [2]-[79]-[80]-[81] and specifically on medical devices in [17]) :

- Smart wearable devices such as monitors of heart rate, perspiration levels.
- Hospital-use and home-use medical devices such as glucose monitors, blood pressure meters, insulin pumps.
- Implantable devices such as heart pacemakers
- Point-of-care kits such as diagnostic tests and analyzers
- Emergency response systems that react to alerts
- Virtual home assistants such as monitors of adherence to prescriptions
- Kiosks that dispensing medical products
- RFID tags such as tags in pharmaceutical packages
- Mobile devices such as smartphones, tablets, laptops

Nowadays HIT and IoMT is directly connected and coexist at least with wired and wireless communication, CC, FMEC, and BD technologies as shown in Figure 38. The landscape is complemented by the involvement of AI and BC technologies. All these ICTs are revolutionizing the eHealth ecosystem, moving it towards Healthcare 4.0, and considered their main pillars and building blocks [20]. eHealth ecosystem points to the eHealth with its all applications and eHealth system refers to a typical eHealth application. There are many eHealth services, applications that support the respective service and therefore the respective system that supports them. Security and privacy requirements and the related measures should be considered for any ICT implemented in an eHealth system.

In recent years, for the reasons mentioned above, there has been a particular interest from the academic community in the use of emerging Information and Communications Technologies (ICTs) for eHealth services.

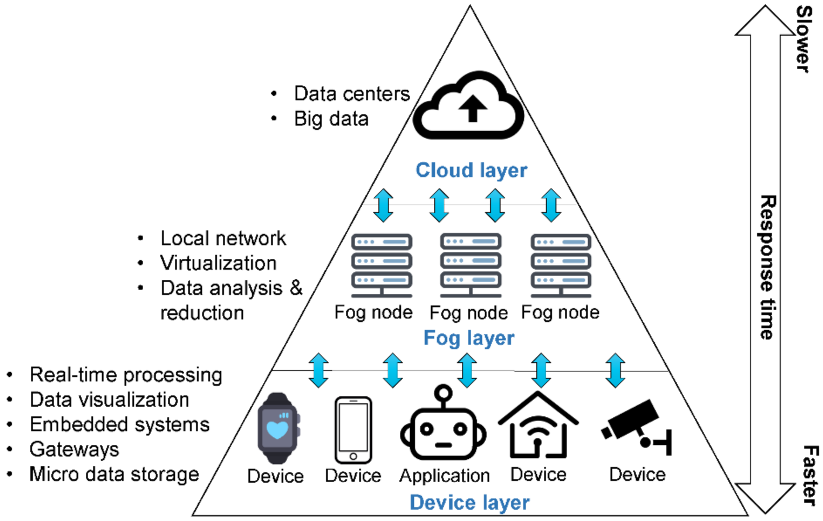


Figure 38. FMEC technology for IoMT. [16]

The Table 2 includes the most interesting papers since 2018 that cover almost the whole range of eHealth services.

Table 2. Papers related to eHealth in the last 3 years

Reference	**Year**	**Internet of Things**	**Cloud Computing**	**Fog and Multi-Access Edge Computing**	**5G**	**Big Data**	**Artificial Intelligence**	**Blockchain**
[82]	2020							✓
[20]	2020	✓	✓			✓		
[83]	2019	✓						
[84]	2019				✓			
[85]	2019	✓						
[86]	2019	✓			✓		✓	
[29]	2019							✓
[30]	2019							✓
[87]	2019	✓		✓				
[88]	2019	✓				✓		

Reference	Year	Internet of Things	Cloud Computing	Fog and Multi-Access Edge Computing	5G	Big Data	Artificial Intelligence	Blockchain
[16]	2019	✓	✓	✓		✓		
[80]	2019			✓		✓		
[31]	2018						✓	
[89]	2018					✓		✓
[90]	2018			✓				
[91]	2018	✓		✓		✓		
[2]	2018	✓				✓	✓	
[75]	2018			✓		✓	✓	

The ICT landscape in healthcare has completely changed organizations worldwide due to the proliferation of mobile and medical technology solutions. For example, medical technology companies manufacture more than 500,000 different types of medical devices (i.e. wearables, implantable, and stationary medical devices) [17]. In order to deliver patient care, all these devices which are made by different manufacturers must effectively communicate with each other. The increasing interconnection of medical things, the need to continuously monitor the patients, the huge amount of data that produced from medical things, the extended use of emails, the use of smartphones to access health information along with the possible inability of information technology (IT) professionals to apply cybersecurity services and solutions, make the eHealth ecosystem especially vulnerable. As mentioned in Chapter 4, while the complex eHealth ecosystem has vulnerabilities to exploit, it offers a wide range of malicious activities for threat actors.

On the other hand, data from medical records are multidimensional and consequently valuable. For example, an EHR of an EU citizen is a composite document and contain demographic information, personal data (e.g., name, birth date, gender, etc.), clinical data (e.g., allergies, current medical problems, medical implants, or major surgical procedures during the last six months), list of the current medication including all prescribed medication that the patient is taking, etc. [92]. Medical records information attracts threat actors which have financial or political motivations [93]. Also, it worth mentioning that, according to [94] the average total cost in 2019 of a data breach in the healthcare industry is $429 and it is 65% percent higher than the average total cost of a data breach which is $150. Primary factors that increase the total cost of a data breach are the extensive cloud migration, the system complexity, the extensive use of mobile platforms, and loss or stolen devices. On the contrary, primary factors that decrease the cost are the security measures [94], which are been discussed in succeeding sections.

In the healthcare sector, security issues prevail over ICT security. The convergence of safety and security is important, especially where human lives are endangered. For example, while in other areas an IoT device in front of critical fault can just shut down, a heart pacemaker has to enter safe mode, in the frame of fail-safe operation. However, manufacturers of medical devices should conform security by default rules security that means security should be built-in. Functional security requirements have to be collected for all building blocks (component level, device level, etc.) – as pieces of a puzzle. Identifying them properly is very important; predicting possible misuse cases is necessary[77].

As eHealth services become increasingly reliant on intelligent, interconnected medical things and health ITs, the related are the target of threat actors that could jeopardize patients’ data and threaten their lives. Therefore, security is one of the main concerns regarding eHealth, which needs to be addressed along with the paramount need for safety.

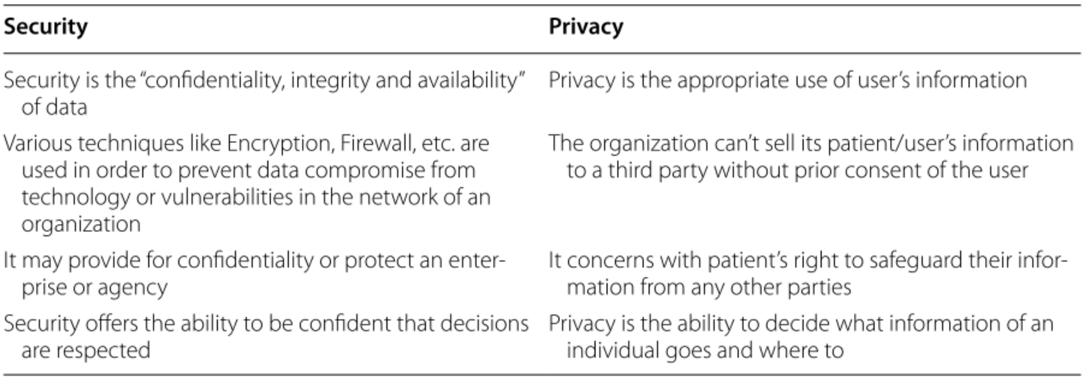
Combining the information we have drawn from Chapter 4 on the eHealth threat landscape and the information set out in this paragraph, we conclude at several issues that need attention in the eHealth sector as follows:

- The concurrent use of many emerging ICTs which have in fact developed in the last decade and each of them presents its own security issues
- The billions of people who benefit from the eHealth services
- The multidimensional information contained in medical records
- The proliferation of mobile devices, especially smartphones, which mainly results in the heavy use of wireless networks for myriads of mobile applications and, in some circumstances functioned as fog nodes.
- The extended use of web services such as email and, also, of web applications.
- The plethora of medical things

5.2 Differences between Security and Privacy

First of all, we consider it necessary to clarify the terms of security and privacy. Security focuses on protecting data from malicious attacks and theft of data. Security measures (based on cryptographic algorithms) are extensively used to address data confidentiality and integrity that is protection of data, but it’s insufficient for addressing the protection of sensitive personal data that is privacy. Personal and health-related data protection requirements and tools are examined under low enforcements such Health Insurance and

Portability and Accountability Act[28] (HIPAA) in USA and the General Data Protection Regulation (GDPR) in Europe [95] which is the most comprehensive data privacy standard to date [96]. Particularly, GDPR focuses on the use and governance of an individual's personal data like making policies and establishing authorization requirements to ensure that individuals' personal information is being collected, shared and utilized in the right ways. It is referenced as both a security and data by design protection mechanism. Figure 39 depicts the differences between security and privacy.



Security	Privacy
Security is the "confidentiality, integrity and availability" of data	Privacy is the appropriate use of user's information
Various techniques like Encryption, Firewall, etc. are used in order to prevent data compromise from technology or vulnerabilities in the network of an organization	The organization can't sell its patient/user's information to a third party without prior consent of the user
It may provide for confidentiality or protect an enterprise or agency	It concerns with patient's right to safeguard their information from any other parties
Security offers the ability to be confident that decisions are respected	Privacy is the ability to decide what information of an individual goes and where to

Figure 39. Differences between security and privacy. [96]

At this point, it's necessary to provide the following terms that are often used when it comes to cybersecurity:

- Security by design that is [77]: "*the product, service or process has been conceived, designed and implemented to ensure the key security properties are maintained: availability, confidentiality, integrity and accountability*".
- Security by default that is [77]: "*the product, service or process is supplied with the confirmed capability to support these security properties at installation*".
- Data protection by design that is [95]: "*implement appropriate technical and organizational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects*".
- Data protection by default that is [95]: "*implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons*."

---

[28] https://www.hhs.gov/hipaa/index.html

5.3 The Need of Security Guidelines

The characteristics of the eHealth ecosystem present new security challenges, threats, and risks that are manifold and evolve rapidly because, in parallel with the evolution of relevant ICTs, the attackers are evolving in the same way. There is not a one-size-fits-all security solution for any eHealth system infrastructure because every particular system faces different threats, different vulnerabilities, and different risk tolerances. It worth mentioning that, an eHealth system can be very simple, such as a mobile application for dietary advice to a patient suffering from diabetes or very complex, such a national EHR ecosystem that is a repository of individuals' health records. The security of any eHealth system requires a systematic proactive approach towards the security of each component, whether is software or hardware to achieve end-to-end security of the system as much as possible. Therefore, we need guidelines for edifying the eHealth ecosystem security. The ISO/IEC JTC 1/SC 27 standardization subcommittee[29] which has as scope "*the development of standards for the protection of information and ICT*" provides the 27xxx family of standards [97] known as the Information Security Management system (ISMS) standards which cover all the spectrum of cybersecurity for organizations that support critical infrastructures. The NIST provides the "*Framework for improving critical infrastructure cybersecurity*" [98]. Examining in-depth these kinds of standards and frameworks and their implementation in an organization is beyond the scope of work. Our goal is to examine the security measures to address the most common eHealth threats by identifying the common attack vectors that need special attention. However, through these sources, we can extract a guideline for a systematic approach to the security issues of any eHealth service. Depending on the use case and the needs of the resulting users, through these guidelines, we can identify the points related to the security of the individual system and select the appropriate security measures.

The NIST Framework[30] is one the foremost used guidelines within the private sector, public sector and academia because is written in common and accessible language, it's adaptable to several technologies, lifecycle phases, sectors, and uses, it's risk-based, it's supported international standards, it's a living and open document and, guided by many perspectives. The framework core is a set of cybersecurity activities and describes the desired outcomes. It's understandable by everyone, applies to any kind of risk management, and defines the whole breadth of cybersecurity. For these reasons, we select the NIST core framework as the main guideline. In summary, it consists of 5 functions to prepare basic cybersecurity activities at their highest level: Identify, Protect, Detect,

---

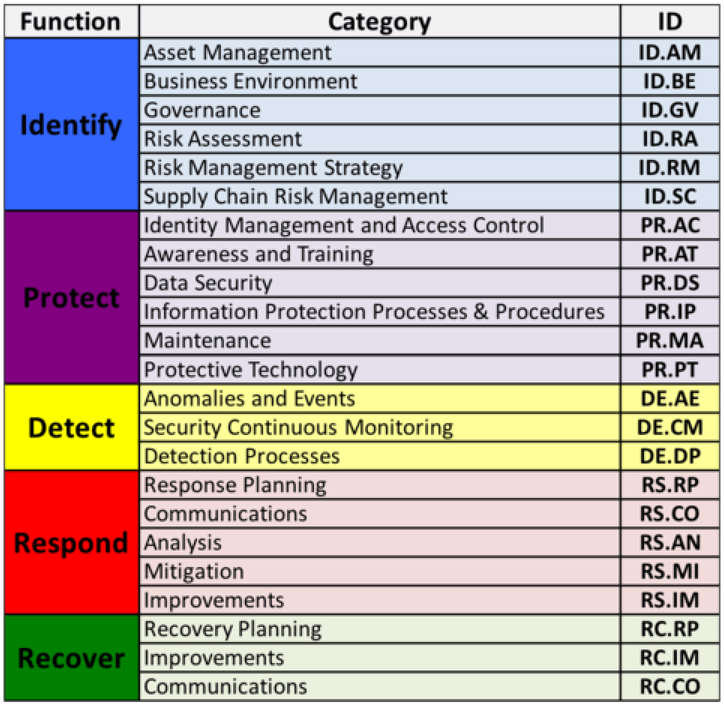
[29] https://www.iso.org/committee/45306.html

[30] The NIST Framework consists of three parts: the framework core, the implementation tiers, and the framework profiles.

Respond, and Recover, and provided as extracted from the original document [98] in Table 3. Every function identifies the key categories as depicted in Figure 40. The discrete outcomes identified by the underlying core framework subcategories which are the deepest level of abstraction. For every subcategory, the core provides example informative references like existing standards, guidelines, and practices as depicted, for example, in Figure 41.

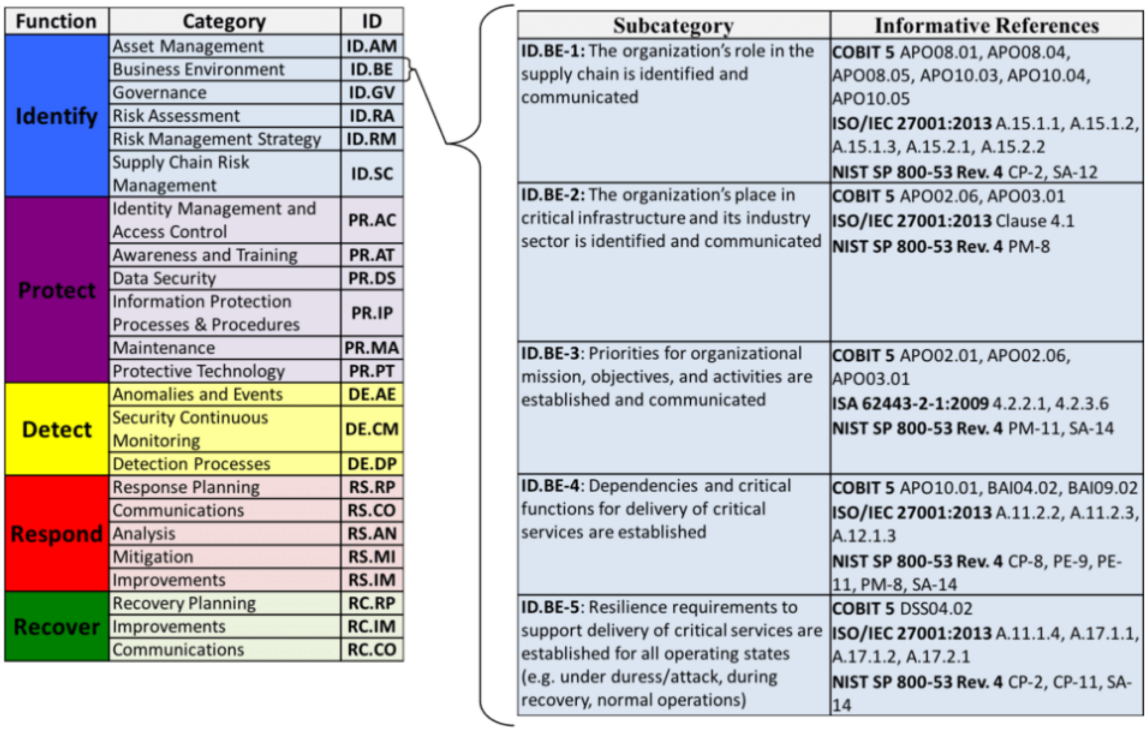
Table 3. The NIST Core Framework Functions. [98]

Function	**Purpose**	**Description**
Identify	Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.	The activities in the Identify function are foundational for effective use of the framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs
Protect	Develop and implement appropriate safeguards to ensure delivery of critical services.	Supports the ability to limit or contain the impact of a potential cybersecurity event. Information protection processes and procedures, maintenance, and protective technology.
Detect	Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.	Enables timely discovery of cybersecurity events.
Respond	Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.	Supports the ability to contain the impact of a potential cybersecurity incident.
Recover	Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.	Supports timely recovery to normal operations to reduce the impact from a cybersecurity incident.



Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Figure 40. The NIST Core Framework Functions and Categories with their IDs. [98]



Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

Figure 41 The NIST Core Framework [98]

It worth mentioning that, globally giant industries, such as IBM[31], Cisco[32], and Broadcom[33], etc., provide guidelines related to cybersecurity in general and to eHealth cybersecurity particularly. Also, useful and powerful eHealth-related guidelines from NIST Special Publications (SPs) and ENISA publications are provided. In order to achieve the goal of work, we'll draw information from the above-mentioned guidelines and academia, depending on the issue at hand.

As a first step, we will use the NIST framework core and the ENISA publications through the isolation of the parts of interest and analyze them in the following sections and chapters. From the NIST core framework functions of interest are the Identify, Protect and Detect function. Obviously, we start from the Identify function which is been discussed in succeeding paragraphs.

5.4 eHealth Assets Identification and Mapping to Potential Threats

According to [49] the criticality of an eHealth infrastructure is identified through three different perspectives: (a) healthcare business continuity, (b) data security and integrity and, (c) availability, and described as follows:

- Healthcare business continuity: examines which assets (infrastructures and services) are required to ensure the baseline functionality of the entire eHealth system. Central components and services that comprise the backbone of the eHealth system are considered as critical.
- Data security and integrity: It refers to data storage components, network infrastructure components for exchanging patient data and Identity and Access Management Systems (IAM).
- Availability: A service is crucial if, due to its unavailability, even one human life is threatened. For example, EHR systems are critical, but network availability is crucial. Also if an eHealth system or service is directly linked to the patient's care, for example, an eHealth diagnostic system is considered as critical.

Because of a lack of homogeneity of healthcare information technology systems, consisting of many functional and technical parts, developing a concise set of security technical and organizational (or/and individual) measures needs a look into all building blocks [77]. The protection of a system depends on the protection of any asset associated with infrastructure, software, systems, that is the protection of the devices themselves, cloud backend and services, applications, maintenance, diagnostic tools, etc. Cybersecurity starts with identifying the assets groups and assets to be protected in an eHealth system. The level of protection for a given asset will vary depending on the use

---

[31] https://www.ibm.com/security

[32] https://www.cisco.com/c/en/us/products/security/index.html

[33] https://www.broadcom.com/products/cyber-security

case, the application used and the use scenario of said eHealth system. **Security and privacy should be addressed for any asset in designing eHealth systems.** With mapping critical assets and relevant threats, we can assess possible attacks and identify security measures and, potential good practices to use to protect systems.

To depict the critical assets in eHealth systems, first, the eHealth service is identified based on specific criteria. Then it is broken down into applications supporting the core functions, which are in turn broken down into infrastructure assets that support the relevant application. This is a common approach in order to decide focus when classifying eHealth infrastructures [49] and depicted in Figure 42.

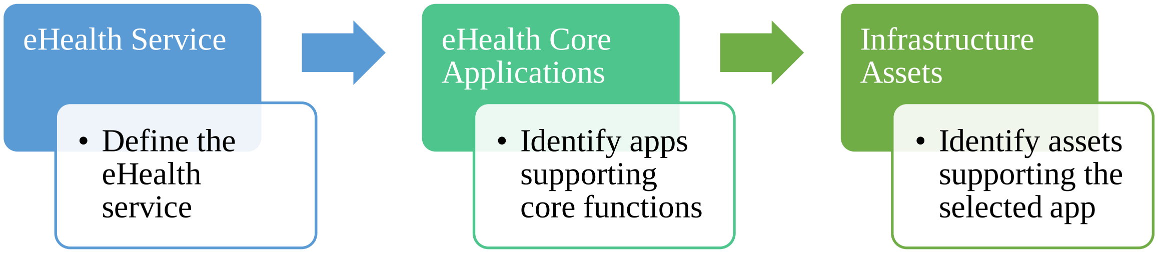

eHealth Service
• Define the eHealth service
eHealth Core Applications
• Identify apps supporting core functions
Infrastructure Assets
• Identify assets supporting the selected app

Figure 42. The common approach to identify assets

5.4.1 Methodology to Identify Assets

To identify assets we need a basis. Using an architectural model is a common approach in both industry and research. In general, two types of models widely used: (a) the basic horizontal model and, (b) the multilayered vertical model. Since eHealth services are developed with specific technologies and focus on specific applications result in fragmented and heterogeneous architectures laying down a common architectural basis for eHealth ecosystem in a horizontal high-level reference model as depicted, for example, in Figure 43 for FMEC and in Figure 44 for IoMT [91] and in Figure 10 for Healthcare 4.0 in general.

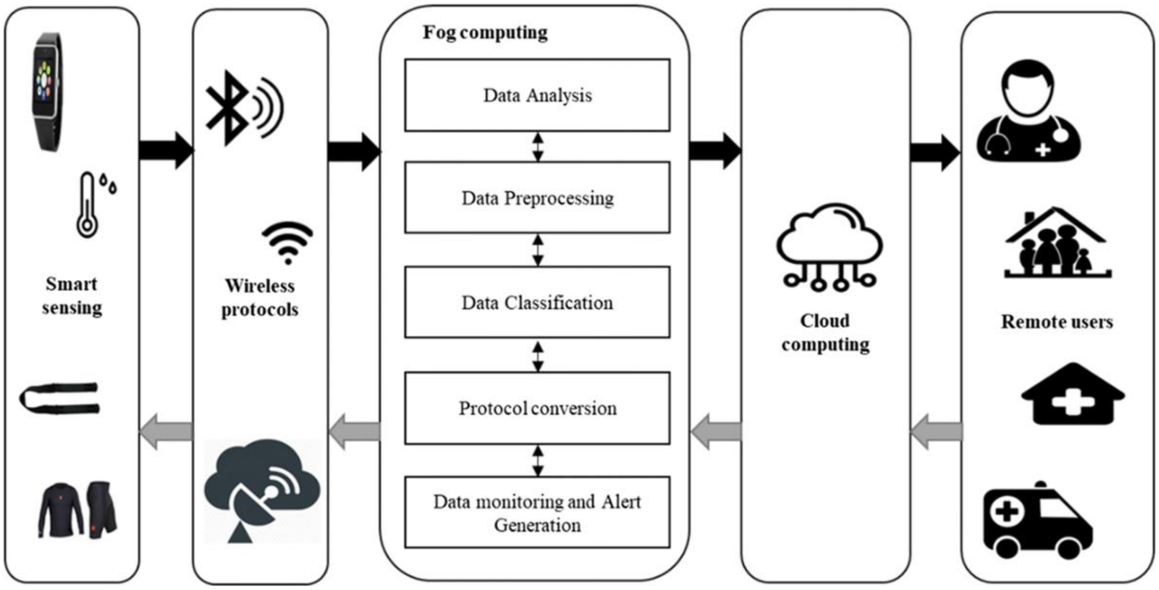


Figure 43. A high-level basic horizontal model for FMEC. [91]

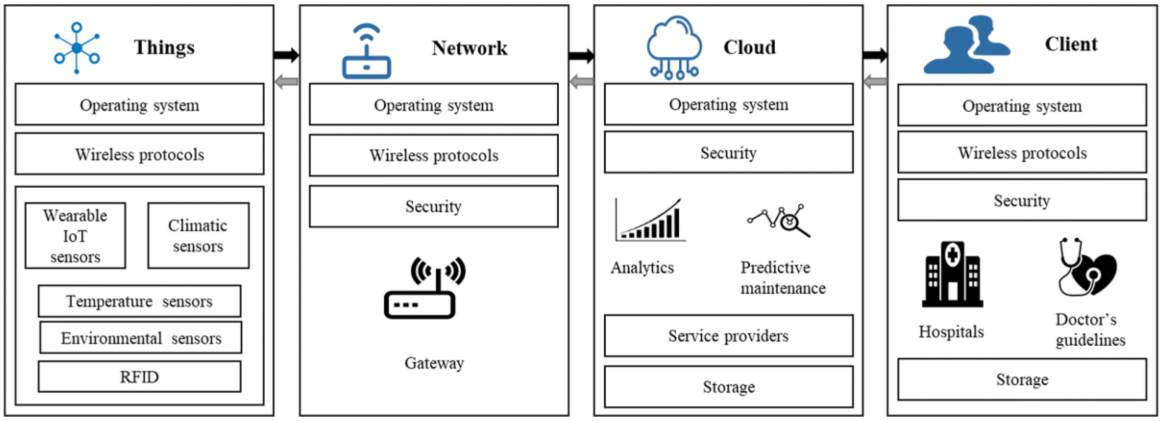


Figure 44. A high-level basic horizontal model for IoMT. [91]

From the horizontal model, we can extract the vertical model as depicted, for example, in Figure Figure 45. A vertical architectural model for IoMT. [62] from [62] which also depicts the protocol stack for IoMT. The vertical model aims to a particular vertical layered approach that allows representing technologies associated with each layer and the related protocols. Through a layered stack model, we can analyze the vulnerabilities in the particular system assets and suggested security measures around it because any system asset constitutes an attack surface.

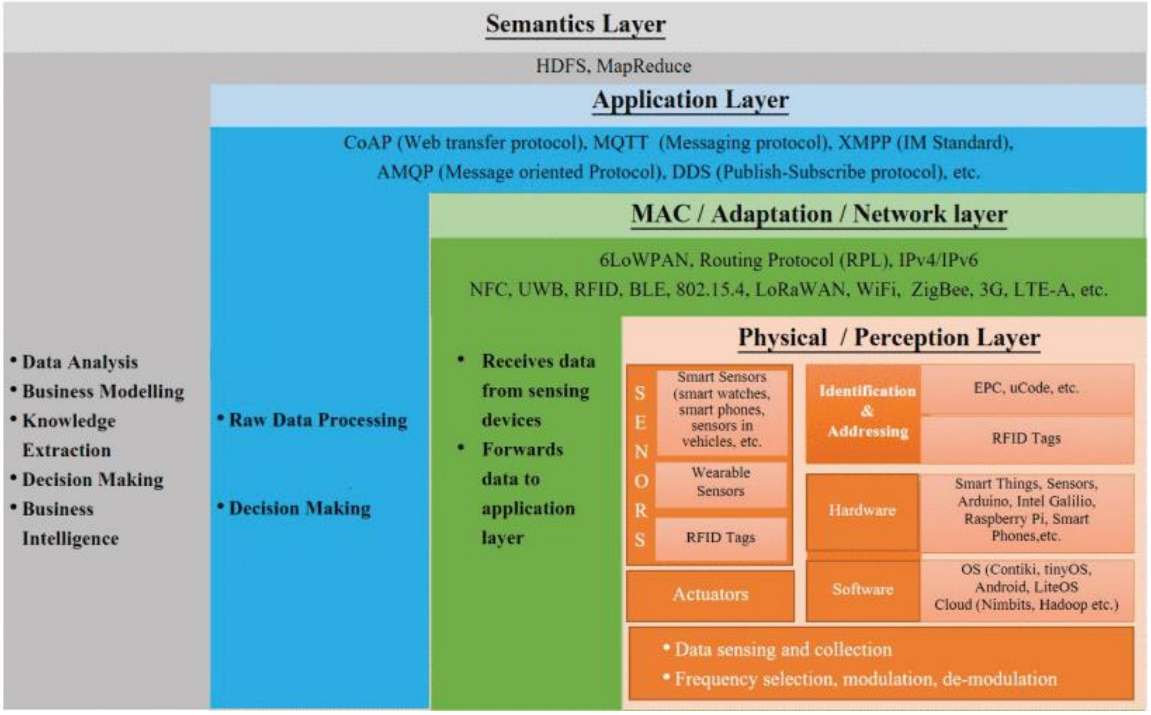

Semantics Layer
HDFS, MapReduce
Application Layer
CoAP (Web transfer protocol), MQTT (Messaging protocol), XMPP (IM Standard),
AMQP (Message oriented Protocol), DDS (Publish-Subscribe protocol), etc.
MAC / Adaptation / Network layer
6LoWPAN, Routing Protocol (RPL), IPv4/IPv6
NFC, UWB, RFID, BLE, 802.15.4, LoRaWAN, WiFi, ZigBee, 3G, LTE-A, etc.
Physical / Perception Layer
• Data Analysis
• Business Modelling
• Knowledge Extraction
• Decision Making
• Business Intelligence
• Raw Data Processing
• Decision Making
• Receives data from sensing devices
• Forwards data to application layer
SENSORS
Smart Sensors (smart watches, smart phones, sensors in vehicles, etc.
Wearable Sensors
RFID Tags
Actuators
Identification & Addressing
EPC, uCode, etc.
RFID Tags
Hardware
Smart Things, Sensors, Arduino, Intel Galilio, Raspberry Pi, Smart Phones,etc.
Software
OS (Contiki, tinyOS, Android, LiteOS Cloud (Nimbits, Hadoop etc.)
• Data sensing and collection
• Frequency selection, modulation, de-modulation

Figure 45. A vertical architectural model for IoMT. [62]

Application is the top level in a layered model which means that run on top of networks in a layered fashion. Different assets are implemented at each distinct layer depending on the particular eHealth system and its use cases. For example, in Figure 46 from [27] the basic scenarios are depicted resulting from the implementation of the predominant FMEC technology to eHealth. In the figure devices and infrastructure owned or controlled by the health providers depicted in gray, and devices and infrastructure owned or controlled by the patient in white.

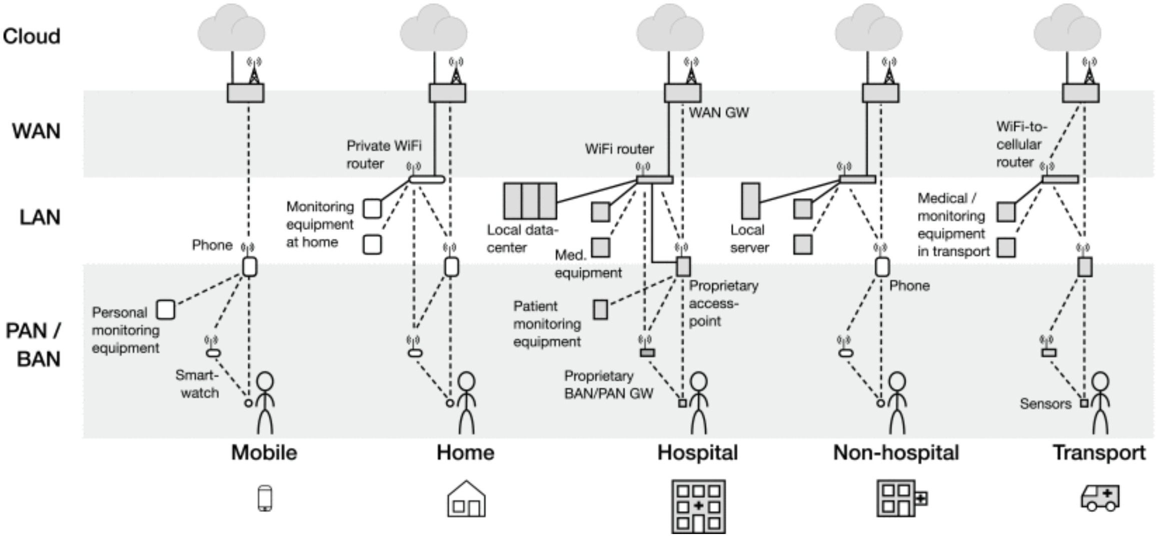


Figure 46. Basic eHealth-FMEC scenarios. [27]

Obviously, in the depicted scenarios there is the differentiation of involved individuals and stakeholders, devices, connectivity, criticality and, complexity. Depending on the functional and non-functional requirements of the particular eHealth system and scenario, we can use the multilayered model to select the devices, the type of networks, the communication protocols, the network infrastructure components, the required platforms and backend (web-based services, cloud infrastructure, and services), the possible ICTs for decision making (BD-Big Data and AI-Artificial Intelligence) and finally identify the system-related assets.

All of the above-mentioned assets organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the asset named information, that is **data**.

5.4.2 A High-level Categorization of eHealth Ecosystem Assets

For the categorization of the eHealth ecosystem assets, the information provided by the references mentioned in Table 4 as well as two remarkable references [62] and [99] is used. eHealth assets can be categorized in a high-level as follows[34]:

a) Medical things

- Hardware: The various physical components -except sensors and actuators- from which the medical things can be built. These include microcontrollers, microprocessors, the physical ports of the thing, the motherboard, etc.
- Software: Software includes the medical things' OS, its firmware, and therefore the programs and applications installed.
- Sensors: The subsystems whose purpose is to measure events from their environment and send the data to other electronics so as to be processed.
- Actuators: These are medical things' output units, which execute decisions supported previously processed data.

b) FMEC devices[35]

- Devices to interface with medical things: Their purpose is to serve as an interface or as an aggregator between other medical things of a given system. Moreover, devices employed by users to interface and interact with medical things.

---

[34] Laptops and workstations may be included in medical things for Health IT systems and in devices to interface with medical things and gateways for IoMT systems.

[35] Because FMEC is the predominant technology in the innovative eHealth services we use the term "FMEC devices" to include other devices related to the eHealth ecosystem

- Devices to manage Things: Devices specially designed to manage other medical things, networks, etc.
- Embedded systems: Systems that supported a processing unit that permits them to process data on their own. They include embedded sensors and/or actuators, network capabilities to connect directly to the FMEC or the cloud, a memory footprint, and the ability to run the software.

c) Communications

- Networks: They permit the different nodes of the system to exchange data with one another, via a data link. There are different sorts of networks consistent with their spatial range, which include (W)LANs, (W)BANs, (W)PANs, and (W)WANs, among others.
- Protocols: They define the set of rules on how communication between two or more medical things must be performed through a given channel. There are many communication protocols in eHealth systems, which may be either wireless or wired. Examples of such wireless communication protocols are the short-range protocols such as ZigBee, Near Field Communication (NFC) and Wi-Fi at OSI datalink layer, long-range mobile networks such as 4G and 5G, long-range IoT protocols such as LoRaWAN at OSI network layer, protocols such MQTT and CoAP at OSI session layer, etc.

d) Infrastructure

- Routers: The networking components that forward data packets between the different networks of the system.
- Gateways: The network nodes used for interfacing with another network from the environment that uses different protocols. Gateways may provide protocol translators, fault isolators, etc., with the aim of achieving system interoperability.
- Power supply: It supplies electrical power to a medical thing and to its internal components. The power source is often wired or supplied by a battery integrated within the device.
- Security assets: This group comprises the assets specifically focused on the security of medical things, networks, and data. These include firewalls, Web Application Firewalls (WAF), Cloud Access Security Brokers (CASB) for protecting the cloud, Intrusion Detective Systems (IDS), Intrusion Preventive Systems (IPS) and Authentication and Authorization (AA) systems. We will discuss them thoroughly further down.

e) Platform and Backend

- Web-based services: services within the World Wide Web, which give a web-based interface to web users or to web-connected applications. Web technologies may be also used for Human-to-Machine (H2M) communications and for M2M communications.
- Cloud infrastructure and services: The cloud infrastructure is employed to aggregate and process data from medical things, and it also provides computing capabilities, storage, applications, services, etc.

f) Decision making

- Data mining: algorithms and services to process collected data and transform it into a defined structure for further use, using BD technologies for discovering patterns in very large data sets.
- Data processing and computing: Services facilitating the processing of gathered data to obtain useful information, which may be used to apply rules and logic, to form decisions and to automate processes. AI and particularly Machine Learning (ML) are often employed to “learn” from the utilization of data.

g) Application and services

- Data analytics and visualization: Once the data has been collected and processed, the resulting information can be analyzed and visualized in order to identify new patterns, improve operational efficiency, etc.
- Medical things and network management: That includes the software updates of the OS, firmware, and applications. It also encompasses the tracking and monitoring of the medical things and networks, collecting and storing logs that can later be used for diagnostics.
- Medical things usage: The contextualization of the system medical things and networks, so as to understand the present status, performance, etc.

h) Data

- Data at rest (data storage): Includes the data stored in a database in the cloud backend or the medical things themselves.
- Data in transit (network traffic): Includes the data sent or exchanged through the network between two or more system components.
- Data in use (endpoint actions): Includes the data used by an application, service, or system element.

For the sake of consistency Figure 47 from [27] is provided as an example that depicts how the above-mentioned assets actually deployed.

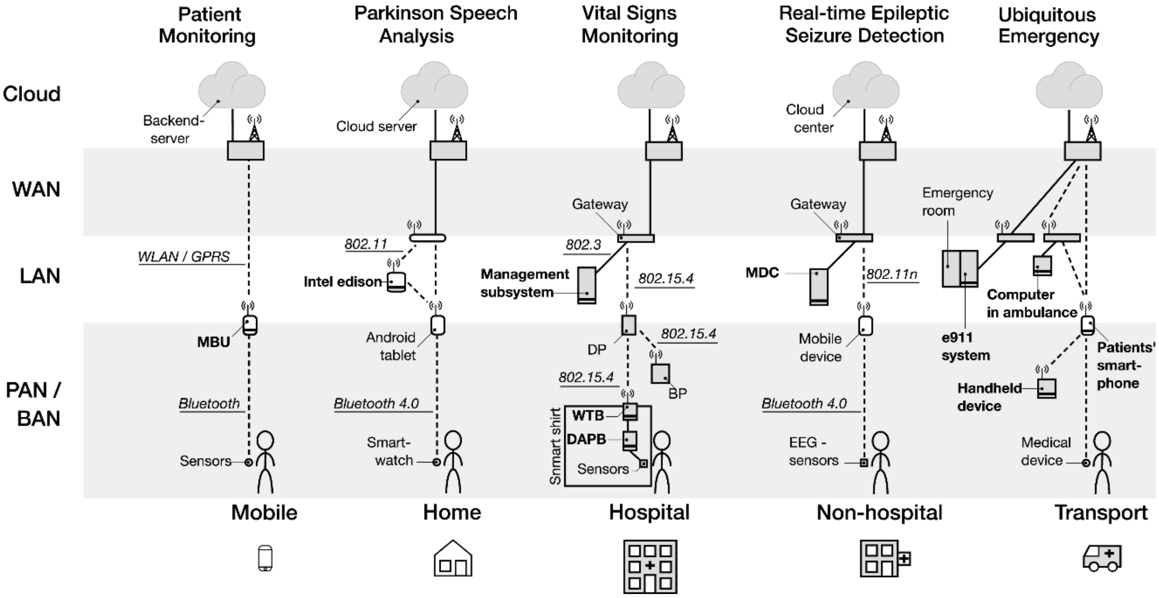


Figure 47. Examples of actual deployment in eHealth-FMEC. [27]

5.4.3 Origin of Attack Vectors

Attack vectors in an eHealth system assets could have as origin:

- **Physical interaction with system assets**: Physically present threat actors can directly interact with medical things that they have access to.
- **Wireless communication with assets**: Attacks within range of wireless technologies.
- **Wired communication with IT assets**: Threat actors with access to the Internet can interact with related assets including cloud backend, and online healthcare information systems. Also, threat actors with physical presence may have direct access to network infrastructure, that they can connect to in order to communicate with other connected devices.
- **Interaction with individuals**: One of the most common threats in eHealth is the social engineering threat. Instead of targeting the system directly, threat actors focus on users with privileged access.

5.4.4 Mapping Threats to Assets

Security and privacy should be addressed for any asset in designing eHealth systems. With mapping critical assets and relevant threats, we can assess possible attacks and identify security measures and, potential good practices to use to protect systems. In Table 4, we present in summary an indicative mapping and discuss the role of each asset category in data security and privacy. We don’t include the decision making asset category because they are usually implemented in the cloud backend. Also, at the moment we don’t include the application and services asset category which are been discussed later.

The role of medical things security. Medical things played as active participants at different layers of a system so that even a small portion of compromised medical things could lead to harmful results for the whole system. For example, if a threat actor manipulates a device that became a botnet has the ability to proceed with any malicious activities. In addition, compromised devices can manipulate services in some particular scenarios, where the threat actor has gained the control privilege of one of these devices [79].

The role of FMEC devices security. Several FMEC devices which deployed usually for real-time services (for example, in cases when an alarm to a healthcare provider is needed) are in charge of the virtualized services and several management services by deploying FMEC devices in a specific geographical location, for example in a hospital environment. In this case, threat actors can access the FMEC devices and may steal or tamper the data in rest. If the threat actors have gained enough control privilege of the FMEC device, then they can abuse their privileges as a legitimate administrator or can manipulate the services. As a consequence, the threat actors can perform several types of attacks, such as MIMT, DoS, DdoS, etc. Moreover, there is a situation that threat actor can control the FMEC device or can forge a false infrastructure, so can completely control data in transit [100].

The role of communications and infrastructure security. The interconnection of medical things by the integration of multiple communications cause many security challenges of these communications infrastructures [16]. Threat actors can launch passive attacks to control the communication infrastructure. Particularly, the MIMT attack highly possible to affect all the functional elements of a network by hijacking the data in transit. Another network security challenge is the rogue gateway deployed by malicious adversaries. In this type of attack, the entire network infrastructure is injected with traffic, and the output the same result as the MIMT threat [100].

The role of platform and backend security. Web-based services and cloud infrastructure and services assets address the general security issues concerning each category. For example, a remarkable recent survey for CC is [23]. In the eHealth ecosystem, the difference lies in the criticality and the sensitivity of personal data. It is worth mentioning that, all FMEC deployments may be supported by several core infrastructures, such as centralized cloud service and the management systems, these core infrastructures may be managed by the same third party suppliers, such as mobile network operators. This would raise enormous challenges, such as privacy leakage, data tampering, DoS attacks and service manipulation, because of these core infrastructure may be semi-trusted or completely untrusted. Firstly, the user's data could be accessed or theft by unauthorized entities or honest but curious threat actors. This will lead to the challenges of data breach or data altering. Also, FMEC allows exchanging information directly between FMEC devices and FMEC data centers which may bypass the cloud. In this case, there is a possibility for provision and exchanging false data when the services are hijacked, which may cause attacks such as DoS [100].

In any of the above-mentioned situations, we must take into account the physical attacks on devices of all asset categories in the case that the physical protection is careless or even not included. Also, a very important factor is human errors that come from either awareness or lack of training [79], [21].

Finally, we must take into account the software vulnerabilities which may exist in medical things, in the FMEC devices, in platform and backend, in infrastructure, and in application and services assets. This threat is considered crucial because it is connected to exploit kits and consequently to malware.

Table 4. Mapping common threats to eHealth assets

Category	**Threat**	**Assets affected**
Active threats	Malware	Medical things FMEC devices Platform and backend
	Data leakage	Medical things FMEC devices Platform and Backend Data
	Botnets	Medical things

Category	**Threat**	**Assets affected**
		FMEC devices Infrastructure
	APT	Infrastructure Platform & Backend Data
	DoS and DDoS	Medical things FMEC devices Platform and Backend Infrastructure
	Exploit Kits	Medical things FMEC devices Infrastructure
Passive threats	Traffic Analysis	Medical things Infrastructure Communications Platform and Backend Data
	Replay of messages	Medical things Platform & Backend Data
Man in the middle		Medical things Communications Data
Physical attacks	Devices theft	Medical things FMEC devices Infrastructure

Category	Threat	Assets affected
Data breach and Identity theft		Personal Data Data concerning health Genetic Data Biometric data

5.4.5 Selected Parts from the NIST Core Framework

The parts that isolated so far at work from the NIST framework and adapted to our needs (regardless of the order of presentation and discussion) are presented in Table 5 as they provided originally from the NIST [98].

Table 5. Selected parts of Identify Function of NIST core framework [102]

Function	Category	Subcategory
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried
		ID.AM-2: Software platforms and applications within the organization are inventoried
		ID.AM-3: Organizational communication and data flows are mapped
		ID.AM-4: External information systems are catalogued
		ID.AM-5: Resources (e.g., hardware, devices,

Function	Category	Subcategory
		data, time, personnel, and software) are prioritized based on their classification, criticality, and business value
	Business Environment (ID.BE): The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization’s role in the supply chain is identified and communicated
		ID.BE-2: The organization’s place in critical infrastructure and its industry sector is identified and communicated
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented
		ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources
		ID.RA-3: Threats, both internal and external, are identified and documented

6 State-of-the-art Cybersecurity Measures and Solutions

Healthcare organizations must take additional steps to achieve security requirements by implement stronger defenses and good practices which means applying a collection of security solutions to prevent any attraction from threat actors, as it turned out during the COVID-19 pandemic and the crisis that followed. Sophisticated and highly organized cybercriminals target healthcare organizations showing every day how vulnerable the eHealth systems are. And the situation keeps getting more difficult, so, there is a need of keeping one step ahead form threat actors.

Nevertheless, there is not a one-size-fits-all security solution for any eHealth system and it is not feasible to address every cybersecurity challenge because every particular system faces different threats, different vulnerabilities, and different risk tolerances. No matter how much we shield a system, human errors and weaknesses will always be a threat. Also, unpredictable situations, such as the COVID-19 crisis will create new challenges. In essence, the goal of security measures is to reduce the risk of cyber-attacks and data breaches.

So far we have examined the eHealth threat landscape to define threat actors and the most common threats, we presented the eHealth sector special issues and we identified the critical eHealth assets and their mapping to common eHealth security threats. Also, the need for guidelines explained.

In this chapter, we focus on the most prevalent cybersecurity measures and solutions for a broad range of organizations within the eHealth sector. First, guidelines related to eHealth which consist of the base of work are presented. Next, the security measures are presented in general and a brief description of operational measures is provided. An analysis of technical measures, based on selected guidelines follows, and finally, we present the common eHealth security measures and the required solutions to defend against the prevalent threats. In Appendix A useful websites for security tools are provided.

6.1 Guidelines Related to eHealth

The challenge of the proper application of security measures[36] to an eHealth system is gradually becoming a highly debated topic in many different communities, ranging from

---

[36] Security measures in literature also referred to as security controls or security safeguards

research and academia to industry and standards enforcement, and compliance management in the case of personal data protection laws. Therefore, nowadays we have access to an excellent range of security technology and tools, vulnerability databases, catalogs of security measures, and countless recommendations. Also, there is an emergence of threat information feeds, tools and reports, security requirements, compliance rules, regulatory mandates, and so forth. Based on the analysis so far, we indent to explore further the technical solutions that can support implementation in practice. Although all known security measures have their own, well-understood, intrinsic properties, this does not render the choice of the proper technique a trivial task in practice.

The work does not “reinvent the wheel” but answering the prevailing question, “Where to start and how to determine a set of certain cybersecurity measures and identify technical solutions that mitigate the most common threats in eHealth sector?”. To answer this question we perform an extensive analysis for the good practices proposed in literature to identify and analyze existing security guidelines and research in the area of eHealth security.

Guidelines provide good practices, that is the recommendation of security measures, and give directions for choosing the appropriate cybersecurity solutions to implement these measures. After research and analysis, we identify the following resources that provide concrete and useful information on eHealth cybersecurity. More specifically our research focused on existing publications from the Cybersecurity Act of 2015, Section 405(d) Task Group[37], from NIST Special Publications series 1800-x that documented by the National Cybersecurity Center of Excellence[38] (NCCoE), from ENISA[39], as well from global giant technology companies focused at eHealth security such as IBM[40], Cisco[41], Symantec (acquired from Broadcom[42]) and, Microsoft[43]. Also, we searched websites and digital libraries, such as IEEE, ACM, Springer, Google Scholar for proposals and solutions from academia.

Our criteria for the selection of companies based on the study and exploration of the literature so far and is indicative. It worth mentioning that, there is a vendor overload on cybersecurity solutions and tools. Multiple vendors in a solution space have different approaches and many tools may duplicate others. Also, there exist free and open-source tools that may not provide a replacement of industrial tools, may not have the needed

---

[37] https://www.phe.gov/Preparedness/planning/405d/Pages/task-group.aspx
[38] https://www.nccoe.nist.gov/
[39] https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/health
[40] https://www.ibm.com/security/industry/healthcare
[41] https://www.cisco.com/c/en/us/solutions/industries/healthcare/security-and-compliance.html
[42] https://www.broadcom.com/solutions/integrated-cyber-defense/healthcare
[43] https://www.microsoft.com/en-us/microsoft-365/solutions/health

functionality and may not have support to standards and compliance needs of a healthcare organization. So, as a first step, we had to limit our research to several industries.

In general, the majority of academic papers present scientific research on evolving ICTs in the eHealth sector, which we referred to in previous chapters, such as Blockchain, AI, FMEC and traditional technologies such as cryptography to support the implementation solutions, for example in [21]. Also, proposals in academia researchers hold a layered approach (as described in Chapter 5), for example in [101], [102].

The initial basis for our work is [103], [78] (and the related tool [104]). In [103] the NIST Framework is adopted and, ENISA's publications refer to NIST's work and acknowledge its important contribution to the field of research concerning cybersecurity. Also, we mention that [103] and [78] based their proposals after analyzing threats which are prevalent in the eHealth sector and we thoroughly presented them in Chapter 4 such as social engineering and phishing (which have as primary attack vector the email), ransomware, device and data theft, data loss caused by human errors and insiders and medical device tampering, as depicted simply by Figure 48.

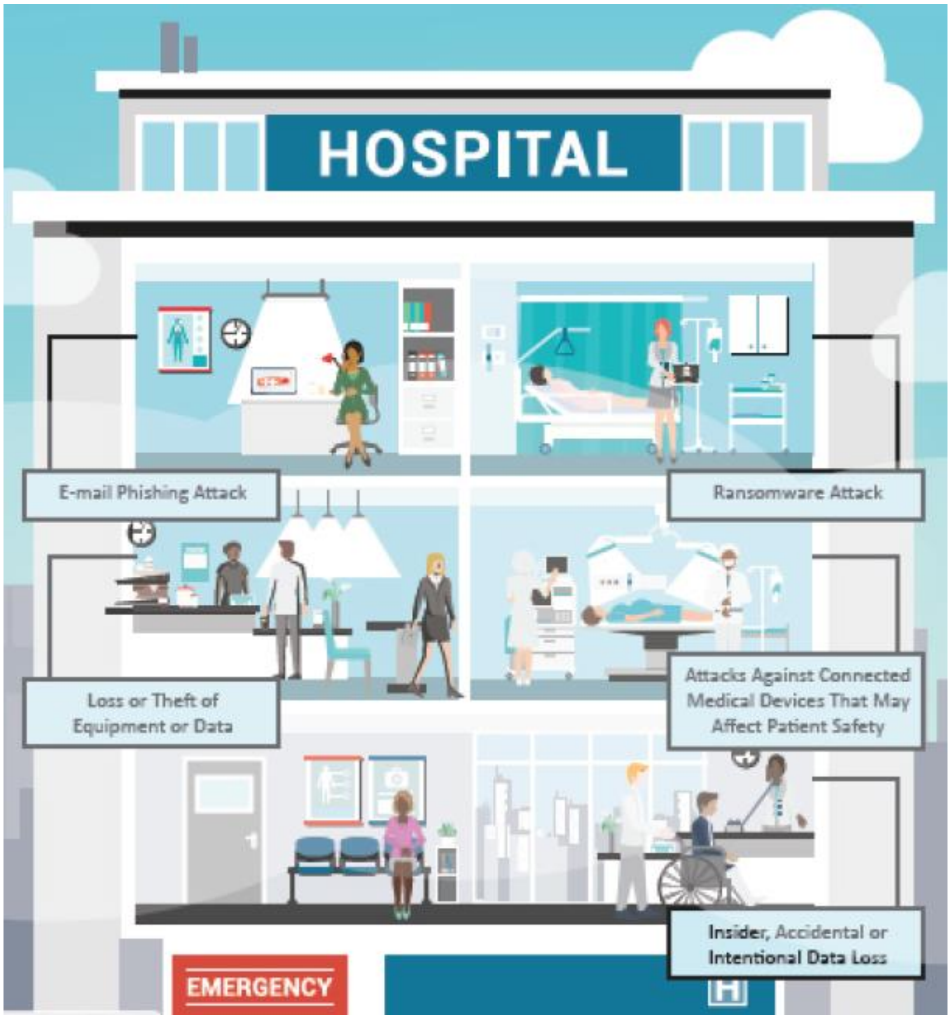
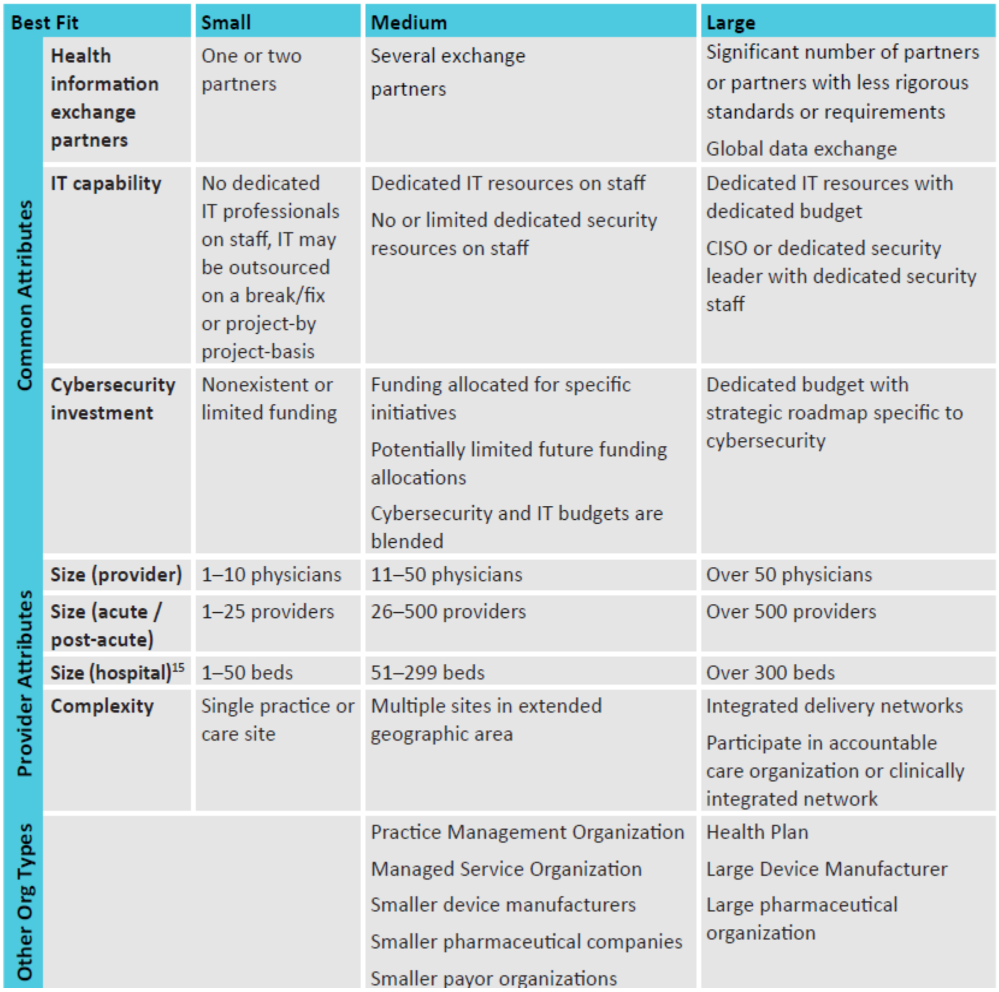

HOSPITAL
E-mail Phishing Attack
Ransomware Attack
Loss or Theft of Equipment or Data
Attacks Against Connected Medical Devices That May Affect Patient Safety
Insider, Accidental or Intentional Data Loss
EMERGENCY

Figure 48. The most prevalent attacks in a healthcare organization. [103]

In [103], there is a separation of proposed measures according to the size of the organization, as depicted in Figure 49. For this reason, two more publications are provided [105]- [106]. In contrast, ENISA in [78] which refers in general to smart hospitals. Regarding the identification of assets, [78] and [106] are almost identical.



Best Fit		Small	Medium	Large
Common Attributes	**Health information exchange partners**	One or two partners	Several exchange partners	Significant number of partners or partners with less rigorous standards or requirements Global data exchange
	IT capability	No dedicated IT professionals on staff, IT may be outsourced on a break/fix or project-by project-basis	Dedicated IT resources on staff No or limited dedicated security resources on staff	Dedicated IT resources with dedicated budget CISO or dedicated security leader with dedicated security staff
	Cybersecurity investment	Nonexistent or limited funding	Funding allocated for specific initiatives Potentially limited future funding allocations Cybersecurity and IT budgets are blended	Dedicated budget with strategic roadmap specific to cybersecurity
Provider Attributes	**Size (provider)**	1–10 physicians	11–50 physicians	Over 50 physicians
	Size (acute / post-acute)	1–25 providers	26–500 providers	Over 500 providers
	Size (hospital)[15]	1–50 beds	51–299 beds	Over 300 beds
	Complexity	Single practice or care site	Multiple sites in extended geographic area	Integrated delivery networks Participate in accountable care organization or clinically integrated network
Other Org Types			Practice Management Organization Managed Service Organization Smaller device manufacturers Smaller pharmaceutical companies Smaller payor organizations	Health Plan Large Device Manufacturer Large pharmaceutical organization

Figure 49. Guide to identify best practices according to an organization size. [103]

It worth mentioning that ENISA provides [107], [77] which are related to smart hospitals and also [99], [108] which are related to IoT and can be used as complementary guidelines for IoMT issues. Also, there is a lot of work from ENISA related to technology for privacy, to support the implementation, monitoring and, enforcing the GDPR[44]. ENISA focuses especially on the concept of privacy by design[45] as the *"fundamental principle of embedding data protection measures at new electronic products and services"*. In this context, ENISA study Privacy Enhancing Technologies (PETs)[46] that support privacy integration in systems and services. The usefulness of PETs is undeniable, especially for individuals and this was evident during the COVID-19 crisis. Also, the security of personal data, which is the protection of CIA of personal data, is a field in which it focuses and proposes security measures for the protection of

---

[44] https://www.enisa.europa.eu/topics/data-protection

[45] https://www.enisa.europa.eu/topics/data-protection/privacy-by-design

[46] https://www.enisa.europa.eu/topics/data-protection/privacy-enhancing-technologies

personal data[47].To support the practical implementation for the security of personal data processing, an online useful tool is provided[48].

Having reviewed and thoroughly analyzed the aforementioned work and ongoing activities, we will compare their proposals and we’ll extract several of them to define baseline security measures to be adopted which are been discussed thoroughly in succeeding paragraphs.

6.2 Common Security Tools to Cover Security Measures

The implementation of security measures concern the selection and the deployment of a set of systems, technologies, and tools (i.e., applications, appliances, processes, compliance programs, etc.) to cover security requirements. The selection of suitable tools is not a trivial task, due to the plethora of available tools that are commercial or free and open-source.

In the context of this work, we do not intend to make a benchmarking of commercial and free open-source tools. We only comment on the fact that, if there is no funds for commercial tools, the implementation of free open-source tools is required, which has been proven during the COVID-19 crisis.

Depending on its size and the resources (budget and human) it has to implement the measures, a healthcare organization has the ability to choose either individual tools that will compose the security solution, or integrated tools that cover the security measures. For example, a solution for data protection may consist of separate tools, for example, a DPL tool, an encryption tool, an MFA (Multi-Factor Authentication) tool, or maybe an integrated tool that offers all these capabilities. Also, a security company may be specialized for example, in antimalware and antivirus or data loss protection, or maybe cover the whole range of security tools.

In any case, in addition to the financial cost, other factors should be considered for the evaluation and selection of a tool such as the capabilities, functionality, support, and interoperability to name a few. Indicatively, in [109] the top cybersecurity companies are presented.

After the study and analysis of best practices for healthcare organisations, we conclude, in general, the requirements and the related security tools as follows:

a. Threat actors constantly change methods to attack, so we must protect the system and the data from advanced threats. There are options for tools that offer:

---

[47] https://www.enisa.europa.eu/topics/data-protection/security-of-personal-data/security-measures

[48] https://www.enisa.europa.eu/risk-level-tool/

- Protection against advanced threats across endpoints, networks, and email (advanced threat protection tool)
- Protection for endpoints and virtual desktops to block all known and unknown threats (endpoint protection tool and cloud workload protection tool)
- Protection against email-based attacks including spam, spear phishing, and advanced malware (email protection tool)
- Protection against complex web-based attacks (secure web gateway tool and vulnerability management tool)
- Management and tracking of medical devices (endpoint management tool)

b. Mobile devices are one of the most common end-user endpoints, so there is a need to protect sensitive data against mobile attacks by secure Corporately Owned, Personally Enabled (**COPE**) and Bring Your Own Device (**BYOD**) mobile devices, that is a mobile device management tool [110].

c. Data breaches are a major threat, so we must manage and protect patient records and sensitive data on the premises or in the cloud. There are options for tools -individual or unified- that offer:

- Monitoring and protection of confidential data at rest and in use (data loss prevention tool and cloud access security broker tool)
- Protection of confidential data wherever it goes (encryption tool)
- Identity and access management (IAM tool)
- Visibility into risky behaviors and risky users (user and entity behavioral analytics tool)

There is a need to comply with regulations such as GDPR [95] and HIPAA (Health Insurance Portability and Accountability Act) [111]. So, there is a need for a compliance tool and a data prevention loss tool. Such a tool, for example, provided by Symantec [112] - [113] and the capabilities shown in Figure 50. A useful guide for the GDPR compliance provided in [114].

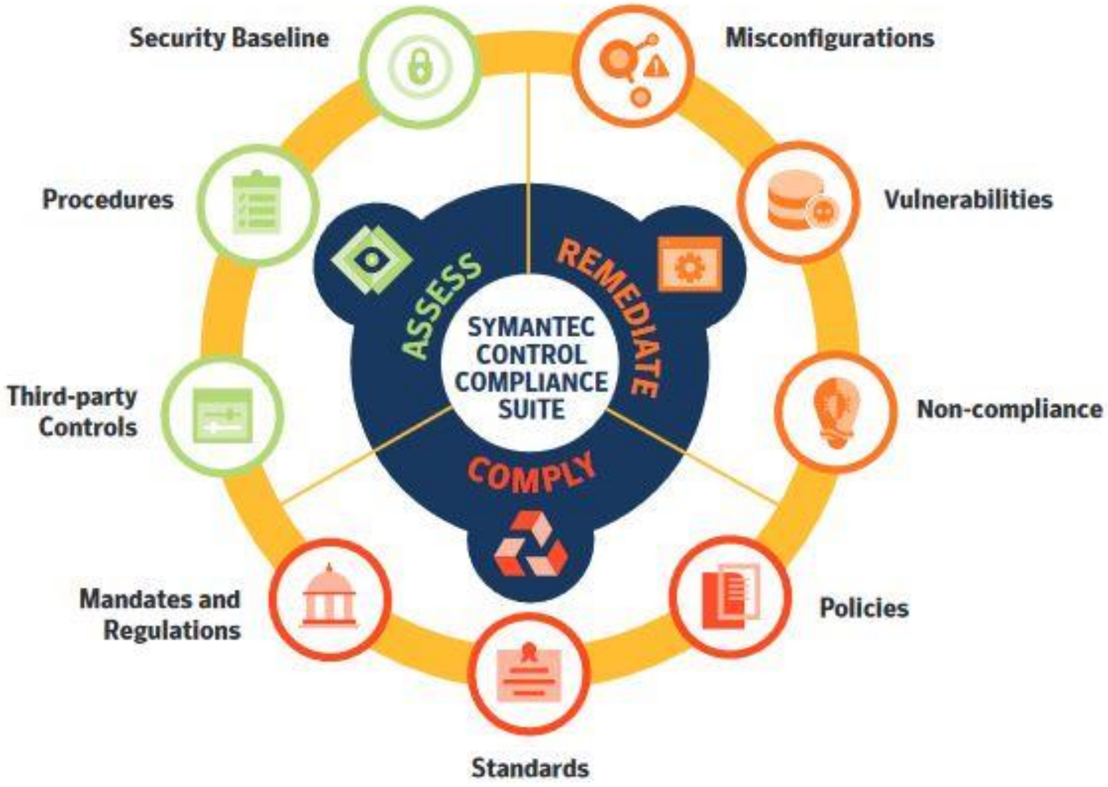
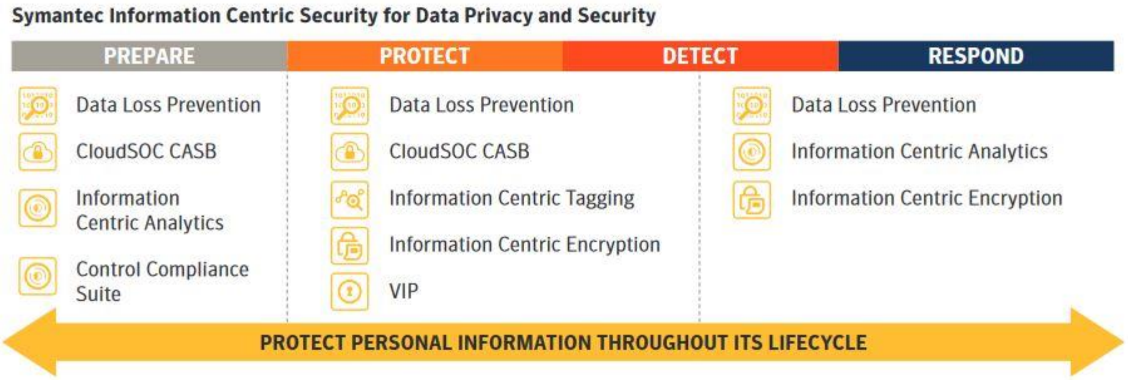


Figure 50. A Compliance Tool. [112]

It worth mentioning that, to cover the data protection challenges including the requirements of the GDPR, an information protection strategy that focuses especially on the data (not the endpoints, network or users) and consist of a set of tools is required [115], as depicted, for example, in Figure 51.


Symantec Information Centric Security for Data Privacy and Security

PREPARE | **PROTECT** | **DETECT** | **RESPOND**

Data Loss Prevention
CloudSOC CASB
Information Centric Analytics
Control Compliance Suite

Data Loss Prevention
CloudSOC CASB
Information Centric Tagging
Information Centric Encryption
VIP

Data Loss Prevention
Information Centric Analytics
Information Centric Encryption

PROTECT PERSONAL INFORMATION THROUGHOUT ITS LIFECYCLE

Figure 51. An Information-Centric Security for Data Privacy and Security. [115]

d. Last, but not least, there is a need for network management, which includes both hardware and software technologies. Traditional tools and technologies, such as firewalls and VPNs, are not enough to defend against sophisticated and resourceful threat actors and there is an imperative need to deploy additional tools. There are options for tools that offer:

- Network intrusion detection and prevention (NIDP Systems tool)
- Anomalous network monitoring and analytics (SIEM-Security Information and Event Management tool)
- Sandboxing (network sandboxing tool)
- The implementation of policies for controlling devices and user access to organization’s network (network access control tool)

Obviously, we can't cover the full range of security tools and suites available. In the following paragraphs, we present the most important of them. Where required, we quote or even supplement terms and concepts that not covered so far.

6.2.1 Tools for email protection

The most common tool that continues to be the front line of defence for the email attack vector is the Secure Email Gateway (SEG). SEG is software that runs on the email server or on a separate server, a gateway appliance, or included in email server software products themselves. An increasing number of organizations move the email out of on-premises servers to cloud-based systems to gain benefits such as low maintenance, high productivity, and access to up to date tools [116]. Cloud-based systems are such as Microsoft Office 365[49] and Google G Suite[50] that have their built-in security. For example, Microsoft Office 365 includes an antispam, anti-phishing and anti-malware service. Also, additionally offers Advanced Threat Protection (ATP), data loss prevention (DLP), email encryption and enterprise digital rights management (EDRM). According to [117] “*email security refers collectively to the prediction, prevention, detection and response framework used to provide attack protection and access protection for email*” and the capabilities that offer Office 365 and G Suite cannot fully protect against email threats. Therefore, there is a need to add additional layers of security and leading industries on security to develop cloud-based tools that supplement the cloud email security and provide additional capabilities. Also, several industries provide tools for on-premises email systems (such as Microsoft Exchange). Capabilities of such a tool, that covers Office 365, G Suite and also on-premises email systems, provided by Symantec shown in Figure 52.

---

[49] https://www.microsoft.com/en-us/microsoft-365

[50] https://gsuite.google.com/

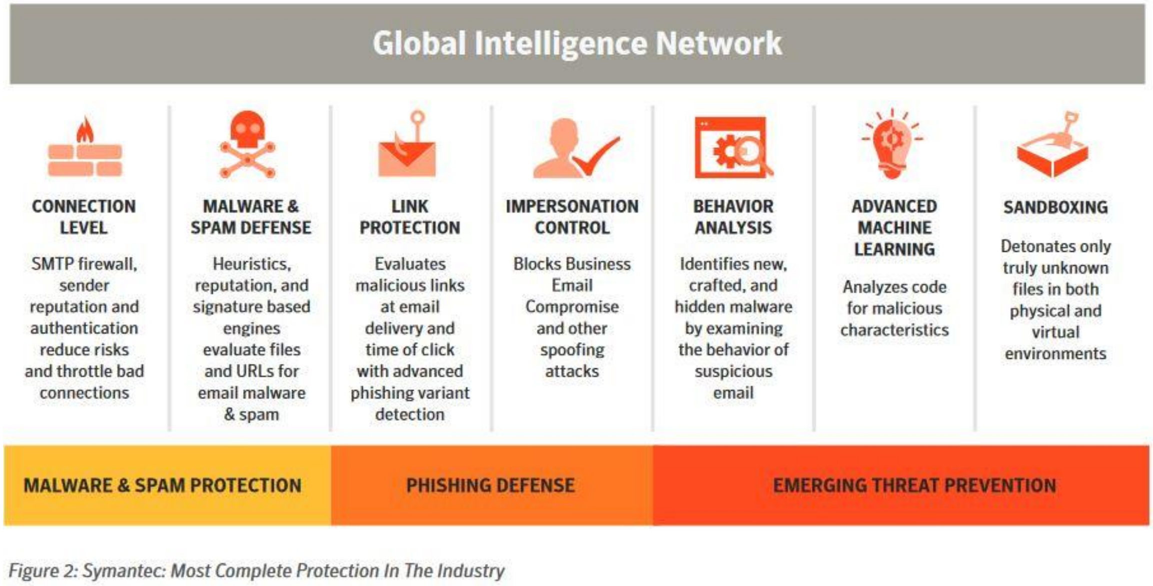

Global Intelligence Network
CONNECTION LEVEL
SMTP firewall, sender reputation and authentication reduce risks and throttle bad connections
MALWARE & SPAM DEFENSE
Heuristics, reputation, and signature based engines evaluate files and URLs for email malware & spam
LINK PROTECTION
Evaluates malicious links at email delivery and time of click with advanced phishing variant detection
IMPERSONATION CONTROL
Blocks Business Email Compromise and other spoofing attacks
BEHAVIOR ANALYSIS
Identifies new, crafted, and hidden malware by examining the behavior of suspicious email
ADVANCED MACHINE LEARNING
Analyzes code for malicious characteristics
SANDBOXING
Detonates only truly unknown files in both physical and virtual environments
MALWARE & SPAM PROTECTION
PHISHING DEFENSE
EMERGING THREAT PREVENTION
Figure 2: Symantec: Most Complete Protection In The Industry

Figure 52. An Example of an Integrated Cloud-based Email Protection Tool. [118]

6.2.2 Tools for endpoint protection

According to [117] an Endpoint Protection Platform (EPP) *“is a solution deployed on endpoint devices to prevent file-based malware, to detect and block malicious activity from trusted and untrusted applications, and to provide the investigation and remediation capabilities needed to dynamically respond to security incidents and alerts.”*

EPP tools offered as client agents managed by an on-premises management server and also, existing tools that utilize a cloud-native architecture. EPP tools maybe include data protection tools such as data loss prevention (DLP) and encryption. To protect endpoints from advanced threats, there is a need for extra capabilities such as detection, investigation and remediation. Nowadays, several vendors offer the EPP capabilities in extended tools, the Endpoint Detection and Response (EDR) tools, that additionally can address and respond to advanced threats [117].

As we mentioned, there is a shift from hardware servers to Virtual Machines (VMs), containers and private or public cloud infrastructure. This shift suggests different security requirements compared to end-user endpoints. As a result, specialized tools to address both the cloud and on-premises deployments are diverging into a new family of tools, the Cloud Workload Protection (CWP) tools [117].

Another family of automation tools related to endpoint protection is the Client Management Tools (CMTs) to automate endpoint management tasks. CMTs perform the following technical functions [117]:

- OS deployment

- Hardware and software inventory
- Software distribution
- Patch management
- Configuration management
- Security configuration management
- Remote control

There are tools that support the control over any type of an end-user device and IoMT endpoints, the Enterprise Mobility Management (EMM) tools that are an improvement of the Mobile Device Management (MDM) tools.

Also, there is another category of tools, the Unified Endpoint Management (UEM) that supports the convergence of enterprise mobility management (EMM) and CMT functionality [117]. UEM support also the Bring Your Own Device (BYOD) policy.

Unified endpoint management (UEM) tools combine the management of multiple endpoint types in a single platform. UEM tools perform the following functions [117]:

- Configuration, management and monitoring endpoint's OS, and management IoMT endpoints.
- Combine the application of configurations, the management of profiles, device compliance, and data protection.
- Provide a unified view of multidevice users, improving the effectiveness of end-user support and gathering detailed data in the workplace.
- Function as a coordination point for the orchestration of activities of relevant endpoint solutions such as identity services and security infrastructure.

6.2.3 Tools for Identity Management and Access Control

There are separate tools for Identity Management (IM), Access Control (AC), Authentication and Authorization (AA), Federated Identity Management (FIM), and tools that unify these measures, that is IAM (Identity and Access Management tools). IAM tools can be based in the cloud, on-premises, or a hybrid of both. Cloud-based IAM solutions continue to increase, as in general there is a shift to cloud-based solutions. Also, several vendors offer IAM as a Service (IDaaS – Identity-as-a-Service), for example, Amazon[51].

There is a trend to implement IAM zero-trust tools. As mentioned in previous paragraphs, the dramatic increase in the number of perimeters that are no longer around the organisation's data center, but around users, devices, and applications [119]. Zero-trust solutions offer the capability to decouple logical application access from the physical perimeter and maintain policy-based controls. More information about zero-trust security provided in [120].

---

[51] https://aws.amazon.com/iam/

6.2.4 Tools for Data Protection and Loss Prevention

Tools usually used for data protection are the Data Loss Prevention (DLP) tools, the Cloud Access Security Broker (CASB) tools, the encryption tools, and authentication and authorization tools.

Cloud services are being adopted at an increased rate. Users access cloud services within and outside the traditional organization perimeter. Therefore there is a need to secure cloud services and a Cloud Access Security Broker (CASB) tool is the solution to address the security issues. Figure 53 depicts what is CASB.

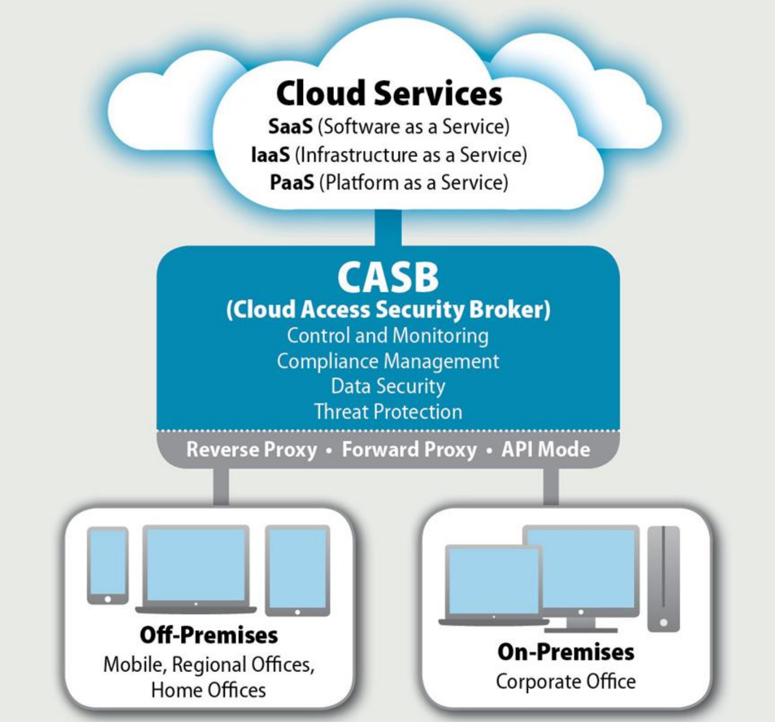

Cloud Services
SaaS (Software as a Service)
IaaS (Infrastructure as a Service)
PaaS (Platform as a Service)
CASB
(Cloud Access Security Broker)
Control and Monitoring
Compliance Management
Data Security
Threat Protection
Reverse Proxy • Forward Proxy • API Mode
Off-Premises
Mobile, Regional Offices, Home Offices
On-Premises
Corporate Office

Figure 53. What is a CASB. [121]

Industries offer tools that unify several technologies to monitor, protect, and control sensitive data. For example, Symantec offers such a tool, the Information-Centric Security (ICS) [122] that provides:

- Data Loss Prevention (DLP)
- Cloud Access Security Broker (CASB)
- Encryption
- Multi-Factor Authentication
- User and Entity Behavior Analytics (UEBA)

Loss prevention achieved through the implementation of data backup and recovery tools. This tool is essential to recover in the case of a ransomware attack.

It worth mentioning that, the emerging technology to protect data and prevent data loss, is Blockchain technology. Research in this field is a particular topic and we intend to carry it out in future work. In the current phase, we cite as an example of such a tool available as free and open-source from IBM [123].

6.2.5 Tools for Asset Management

For the asset management of an organization, several vendors offer ITAM tools (IT Asset Management) separately for the hardware and the software management (for example, Symantec[52]), unified tools (for example, IBM[53]) or offer asset management as a service for their products (for example, Cisco[54]).

6.2.6 Tools for Network Management

Secure web gateways (SWGs) are hardware or virtual tools that apply URL filtering, advanced threat defence, and malware protection to defend against web-based threats. SWG tools are implemented as on-premises or cloud-based services, or in hybrid mode. The SWG tool which Cisco offers and suggests as cloud service for the healthcare sector is a tool named Umbrella (Figure 54).

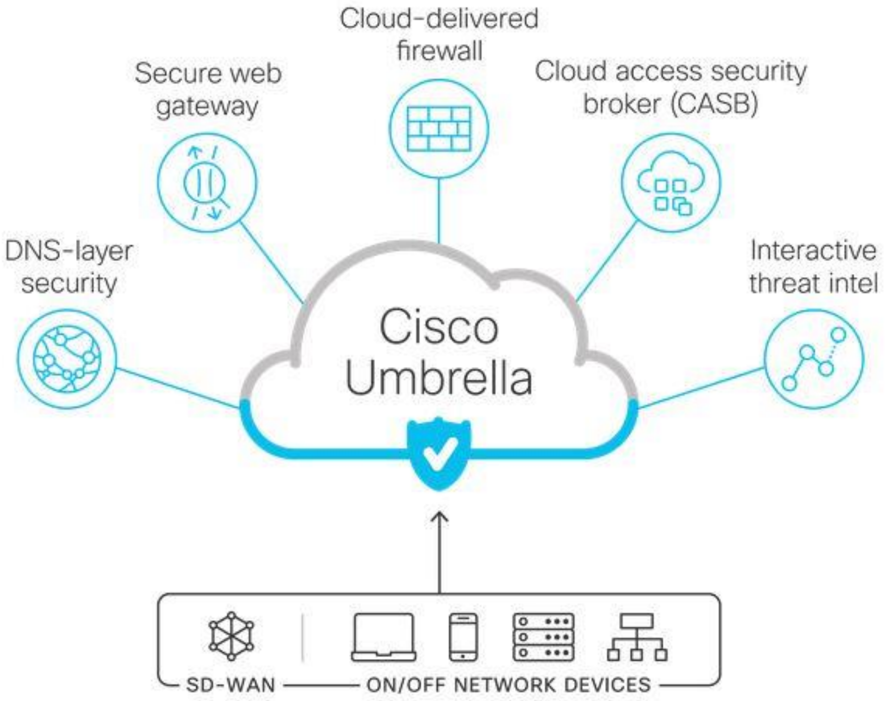


Figure 54. Cisco Umbrella Capabilities. [124]

---

[52] https://docs.broadcom.com/doc/the-symantec-approach-to-software-asset-management-en
[53] https://www.ibm.com/products/maximo
[54] https://www.cisco.com/c/dam/global/shared/assets/pdf/smart-net-total-care/at-a-glance-c45-735476.pdf

Also, Symantec offers a similar cloud security service, as depicted in Figure 55.

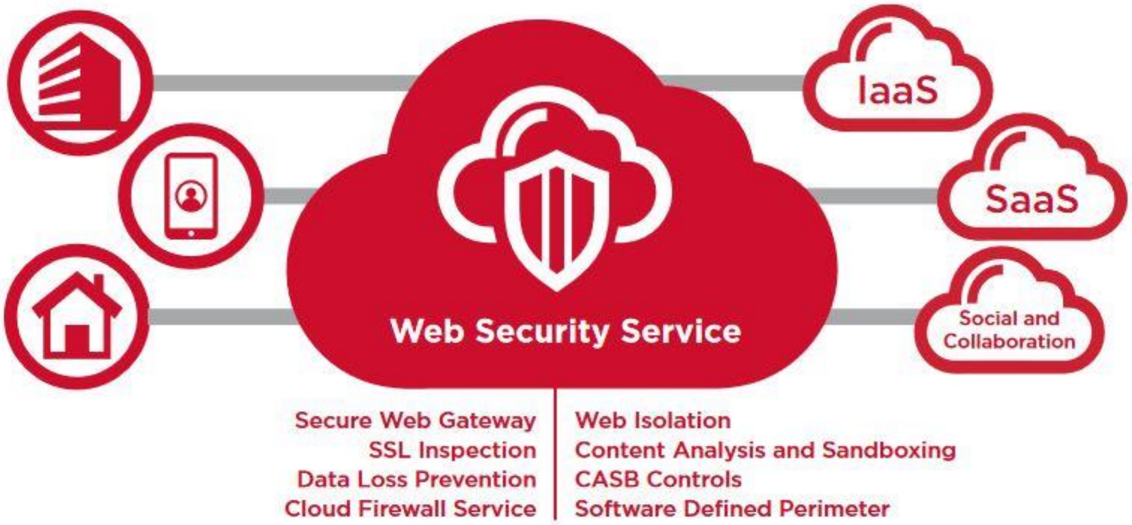


Figure 55. Symantec Web Security Service [125]

Network-based sandboxing is a technique for detecting malware and targeted attacks and vendors offer tools that provide this capability. As described in [117] *"network sandboxes monitor network traffic for suspicious objects and automatically submit them to the sandbox environment, where they are analysed and assigned malware probability scores and severity ratings."*

The Network Intrusion Detection and Prevention system (NIDPS) tools are stand-alone physical and virtual appliances that inspect network traffic on-premises or in the cloud. They are located in the network to inspect traffic that has passed through perimeter security devices, such as firewalls, SWGs and SEGs. It worth mentioning that exist two well-known and widespread free open-source tools, that used also in many universities for learning purposes, the **Suricata**[55] and the **Snort**[56].

Network Access Control (NAC) are technologies that enable organizations to implement policies for controlling access to corporate infrastructure by both user-oriented devices and IoT (therefore for IoMT) devices [117].

According to [117], the minimum capabilities of NAC are:

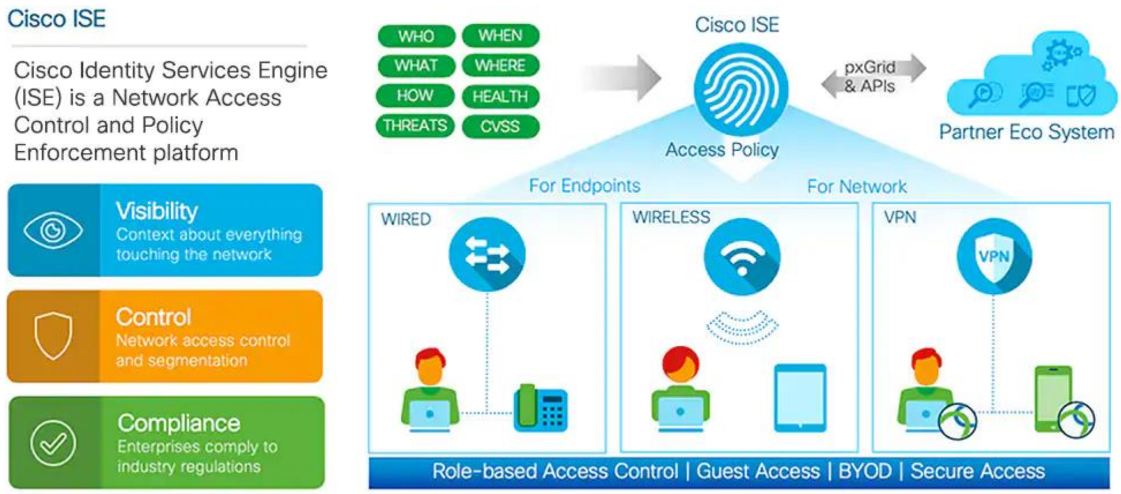
- Dedicated policy management
- Determination of the suitable level of access for any endpoint attempting to connect

---

[55] https://suricata-ids.org/
[56] https://www.snort.org/

- Access control to block, isolation, or grant varying degrees of access.
- Management guest access
- An engine to discover, identify and monitor endpoints
- Integration with other security applications and components

Network Access Control tools (NAC) are among the zero-trust solutions. Such a tool provided by Cisco and shown in Figure 56.


Cisco Identity Services Engine (ISE) is a Network Access Control and Policy Enforcement platform

Cisco ISE
Visibility
Context about everything touching the network
Control
Network access control and segmentation
Compliance
Enterprises comply to industry regulations
WHO
WHEN
WHAT
WHERE
HOW
HEALTH
THREATS
CVSS
Cisco ISE
Access Policy
pxGrid & APIs
Partner Eco System
For Endpoints
For Network
WIRED
WIRELESS
VPN
Role-based Access Control | Guest Access | BYOD | Secure Access

Figure 56. Cisco Identity Service Engine. [126]

Organizations need to analyse event data in real-time to detect targeted attacks and data breaches and to collect, store, investigate and report on log data[57] for incident response, forensics, and regulatory compliance [117]. Security Incident and Event Management (SIEM) is a security management tool, which combines functions of Security Information Management (SIM), that focuses on automating the collection of log data, events and flows from security appliances on a network and Security Event Management (SEM) that is for real-time monitoring and alerts. Therefore, a SIEM tool offers real-time collection and analysis of security alerts and correlation of events to deduce it to detect incidents and malicious patterns of behaviours [127].

The implementation of a SIEM tool aims at the following:

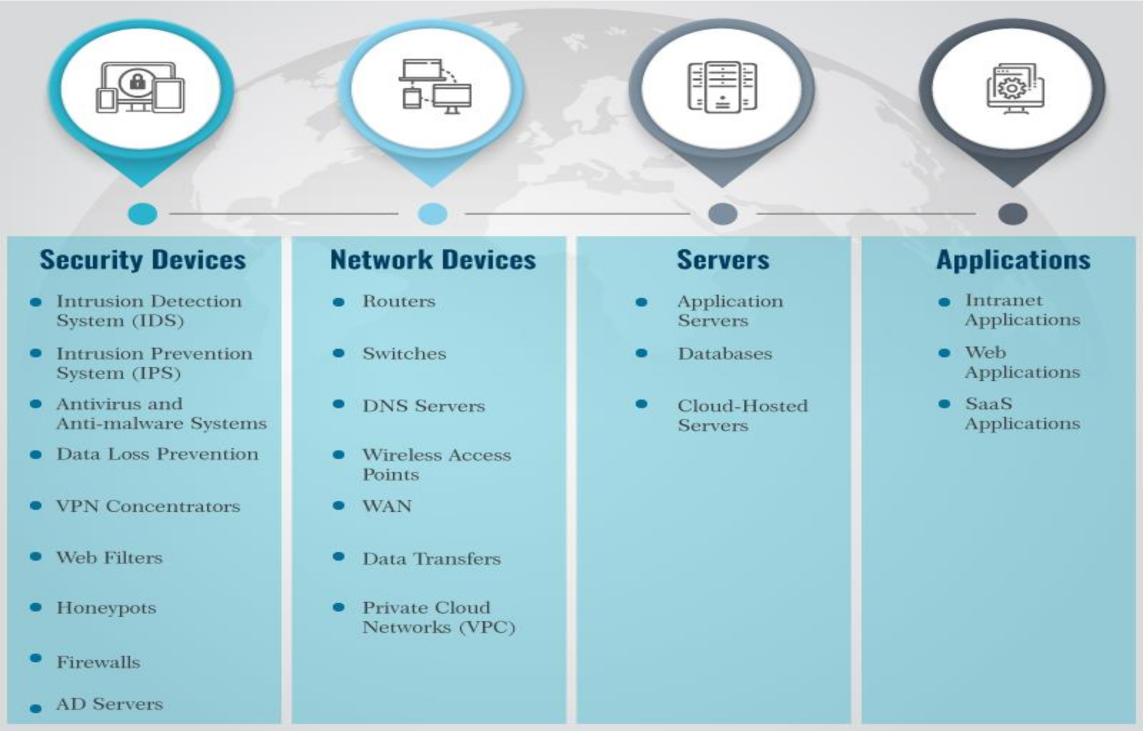
- To reveal potential known and unknown threats
- To monitor the activities of authorized users and also the privileged access to resources
- To compile a regular report

---

[57] A log is a record left behind by each activity performed by the application (for example, open the browser) or the operating system (for example, create a folder).

- Backs up incident response (IR)

SIEM makes the work of IT workforce easier by collecting log data and security incidents from various components of a system, as shown in Figure 57.



Security Devices

- Intrusion Detection System (IDS)
- Intrusion Prevention System (IPS)
- Antivirus and Anti-malware Systems
- Data Loss Prevention
- VPN Concentrators
- Web Filters
- Honeypots
- Firewalls
- AD Servers

Network Devices

- Routers
- Switches
- DNS Servers
- Wireless Access Points
- WAN
- Data Transfers
- Private Cloud Networks (VPC)

Servers

- Application Servers
- Databases
- Cloud-Hosted Servers

Applications

- Intranet Applications
- Web Applications
- SaaS Applications

Figure 57. SIEM Logging Sources. [127]

The typical architecture of a SIEM depicted in Figure 58.

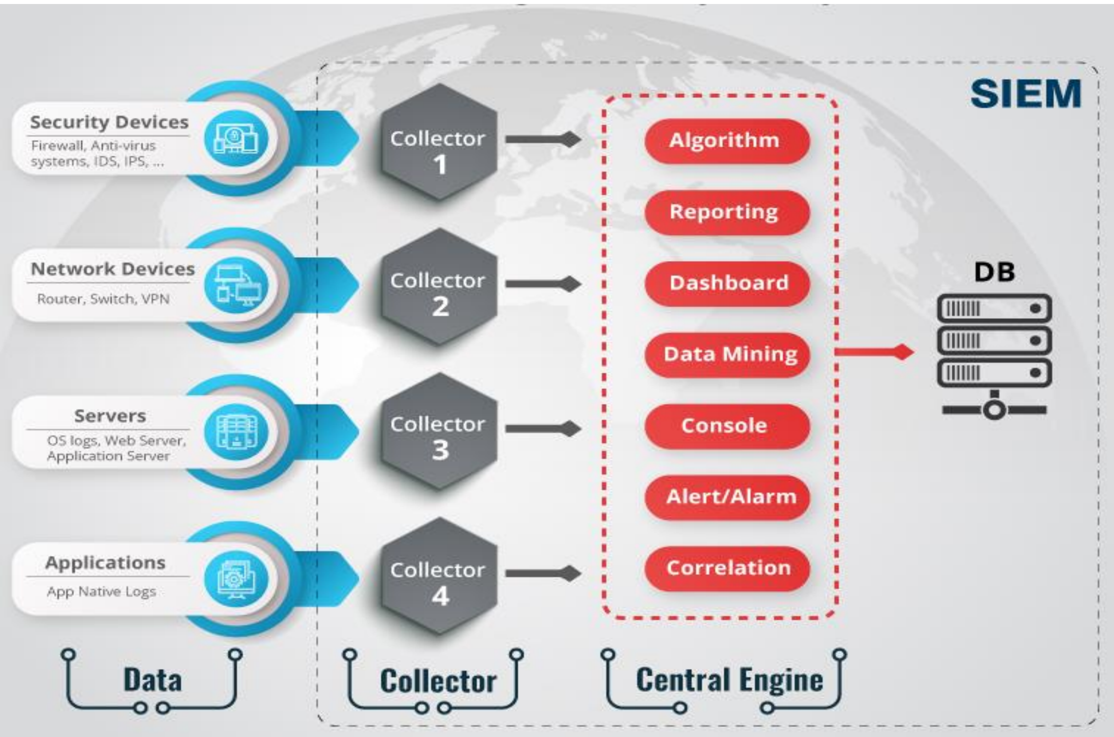


Figure 58. Typical Architecture of a SIEM. [127]

6.2.7 Tools for Vulnerability Management

According to [117] tools for vulnerability management belong to the category of vulnerability assessment tools that provide capabilities to identify, categorize, and manage vulnerabilities. Patch management tools and vulnerability scanners also included in this category.

7 eHealth Cybersecurity and Privacy Issues Associated with the COVID-19

“The coronavirus pandemic has brought many changes. It has forced us all to find new ways of working, interacting and living. It has raised questions about how our societies are ordered, and about where we want and need to invest for the future. It has shown us our strengths and highlighted our weaknesses. It has set us new challenges, not the least of which is to try to find a cure. Digital technology is a key component of our collective effort to tackle the virus and support our new ways of living and working reality during this exceptional time.”

With these words begins the European Commission to emphasize the role of digital technologies in tackling the COVID-19 crisis [128]. The dramatic experience of several countries such as Italy, Spain, and recently in USA with COVID-19 has highlighted the importance of the health facilities systems and hospitals in the first place and has made the need for effective eHealth cybersecurity even more urgent. Since there is evidence of viral assaults possible repetitiveness in the foreseeable future, prevention and preparedness are more essential than ever [129].

The COVID-19 situation also triggered a profound change. The crisis has a result in the increase of various remote activities such as teleworking, remote governance, e-education, and e-commerce. Nevertheless, security and privacy management on these activities have not evolved in terms of user’s awareness and cyberspace knowledge. Also, most of the security and privacy technologies available nowadays have been developed to protect the assets of systems and networks. There is a question if security solutions raise to the challenge, or there is a need to approach the problem differently [130].

COVID-19 crisis raised and brought up a unique paradox in ICT (Information and Communication Technologies), which hadn’t been predicted in most business continuity plans. Instead of non-available ICT infrastructure, there was a non-availability of ICT staff, because of lockdown, special purpose sickness leave, and measures of protection. This caused a deficient oversight and management of server rooms, in a moment that their constant service was necessary and crucial more than ever, in order to support telework, e-services, e-shops and generally the business continuity of companies and organizations.

Also, the issue of data protection and ethics is becoming of pivotal importance, due to the required medical research to treat the disease and the measures deemed necessary to prevent its contagion [131], [132].

In this chapter, the issues in eHealth cybersecurity, data protection and ethics, are presented in summary. Also, COVID-19-related information for the security of systems and people's privacy is provided in Appendix B. Finally, we present a summary of the National Cyber Security Strategy (NCSS) in Greece.

7.1 The Issue for Healthcare Cybersecurity in the era of COVID-19

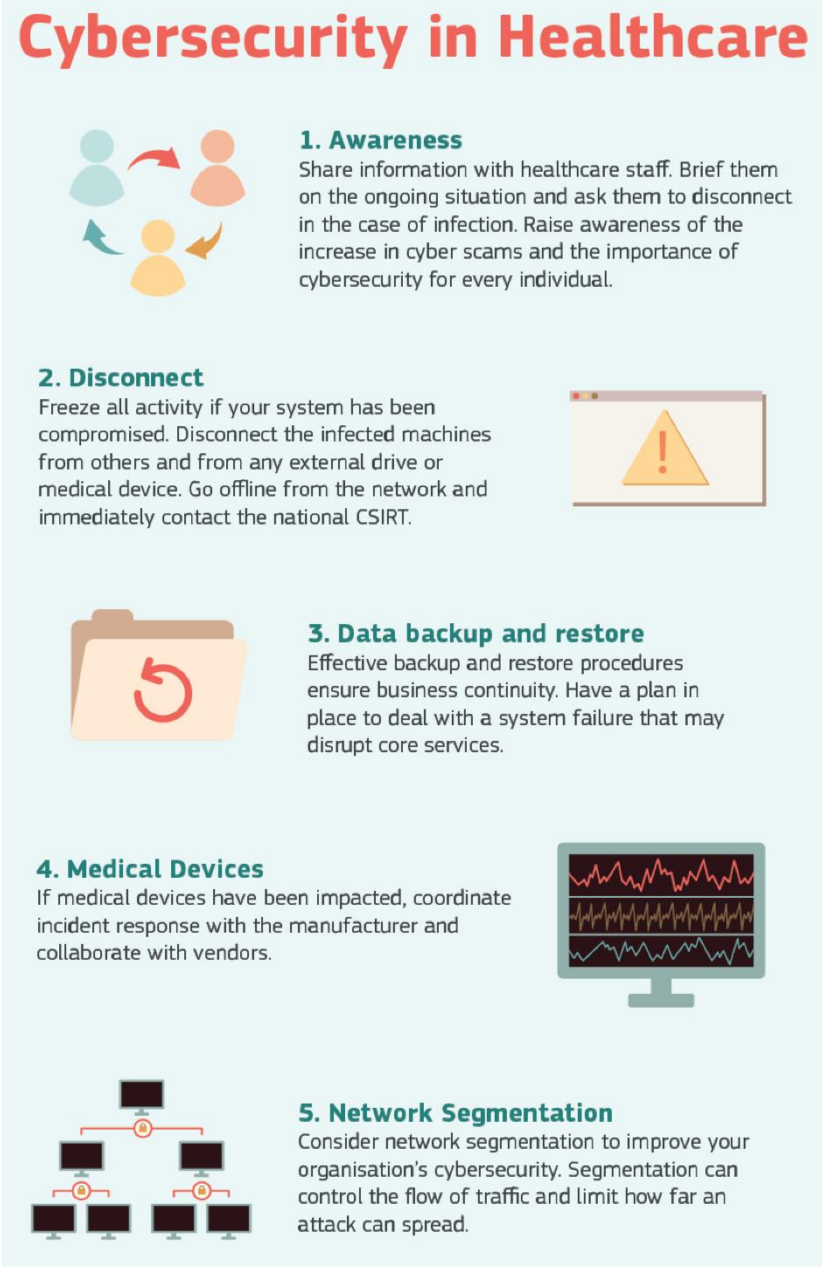
The dramatic experience of several countries such as Italy and Spain with COVID-19 has highlighted the importance of the health facilities systems and hospitals in the first place and has made the need for effective eHealth cybersecurity even more urgent. Since there is evidence of viral assaults possible repetitiveness in the foreseeable future, prevention and preparedness are more essential than ever.

We have already analysed the threat landscape and, the security measures and solutions that a health care organisation must implement to defend against the prevalent threats that increased dramatically during the COVID-19 crisis. However, successful attacks highlighted weaknesses and omissions in eHealth security.

The ENISA's director, Juhan Lepassaar in [129], explains the body's contribution in the field of eHealth-related cybersecurity, and claimed that it emerged that ENISA's whole work and especially [107] would be valuable to support IT professionals in hospitals in order to build a strong cybersecurity. To face a new reality, there is a need to take proper and permanent security measures, also considering the increase in telehealth and telemedicine deployment that is now of paramount importance to society and before the COVID-19 crisis the security of these services had been overlooked compared to other eHealth related services. Therefore, there is a need to focus on ensuring cybersecurity for telehealth and telemedicine, and, also need for security and data protection measures that vendors and providers (i.e. cloud services providers) should take to meet heavy demand from society while ensuring the cybersecurity of the services.

Due to the widespread attacks by threat actors that take advantage of the COVID-19 pandemic and target healthcare organizations, ENISA, along with European Institutions, supported cybersecurity in the essential systems in hospitals and of healthcare organizations and proposed some recommendations targeting healthcare IT professionals, as depicted in Figure 59.

Given that less is better than nothing, organizations need to implement these measures and incorporate a security strategy into their goals. eHealth systems security is an issue that can no longer be questioned, excuses, and delays. No one knows if similar tragic situations will arise in the future and the problems that have arisen should be taught to eHealth stakeholders and to humanity in general.



Cybersecurity in Healthcare

1. Awareness
Share information with healthcare staff. Brief them on the ongoing situation and ask them to disconnect in the case of infection. Raise awareness of the increase in cyber scams and the importance of cybersecurity for every individual.

2. Disconnect
Freeze all activity if your system has been compromised. Disconnect the infected machines from others and from any external drive or medical device. Go offline from the network and immediately contact the national CSIRT.

3. Data backup and restore
Effective backup and restore procedures ensure business continuity. Have a plan in place to deal with a system failure that may disrupt core services.

4. Medical Devices
If medical devices have been impacted, coordinate incident response with the manufacturer and collaborate with vendors.

5. Network Segmentation
Consider network segmentation to improve your organisation's cybersecurity. Segmentation can control the flow of traffic and limit how far an attack can spread.

Figure 59. ENISA's Recommendations Targeting Healthcare IT Professionals. [133]

7.2 GDPR Personal Data Protection and Ethics in the era of COVID-19

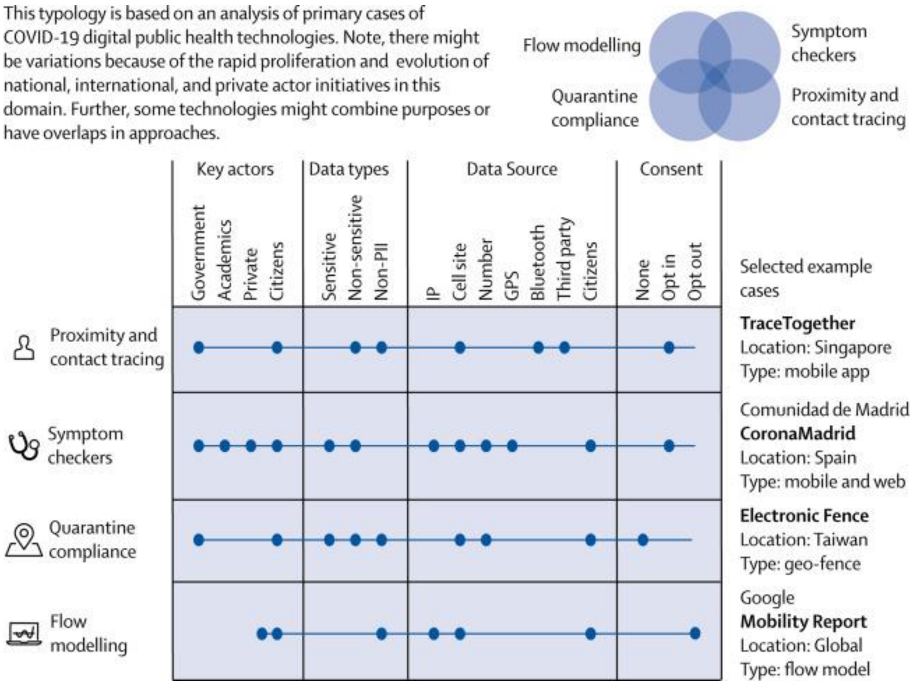
The situation during the COVID-19 pandemic triggered a series of campaigns due to conditions such as high demands for certain goods (such as protective masks and household products), increasing reliance on teleworking remote governance, e-education, and e-commerce, increasing fear, uncertainty and, doubt in the general population, which exploited making the situation even more vulnerable [134]. Threat actors look at crisis as an opportunity and use COVID-related themes to launch widespread attacks such as phishing. On the other hand, the issue of data protection and ethics is becoming of pivotal importance, due to the required medical research to treat the disease and the measures deemed necessary to prevent its contagion [131], [132]. As expected, various security and privacy challenges and issues became more urgent and new questions arose. We will briefly mention several of them.

A. Security and privacy management on remote activities have not evolved in terms of user's awareness and cyberspace knowledge. Also, most of the security and privacy technologies available nowadays have been developed to protect the assets of systems and networks. There is a question if security solutions raise to the challenge, or there is a need to approach the problem differently [130].

B. The use of digital technologies for the treatment of the disease and to prevent its contagion presupposes the collection and processing of a large volume of personal data. The issue of personal data protection in the field of research covered by GDPR [95], as the author explains in [131]. Although, as the author recognizes, questions related to data protection that are unsolved are the following:

- How can the notion of "research" be delimited avoiding abuses of such terms as a legal ground for data processing?
- How to sufficiently protect research subjects, especially the sensitive data subjects?
- Consent should be considered as an adequate legal basis for processing data for research purposes or, to the contrary, it is highly unlikely that research subjects might give a really "free" and impartial consent?
- How transparency can be enhanced in practice?
- What is the role of the accountability principle when dealing with data processing in research and how such a principle should interact with the principle of "ethics in research"?

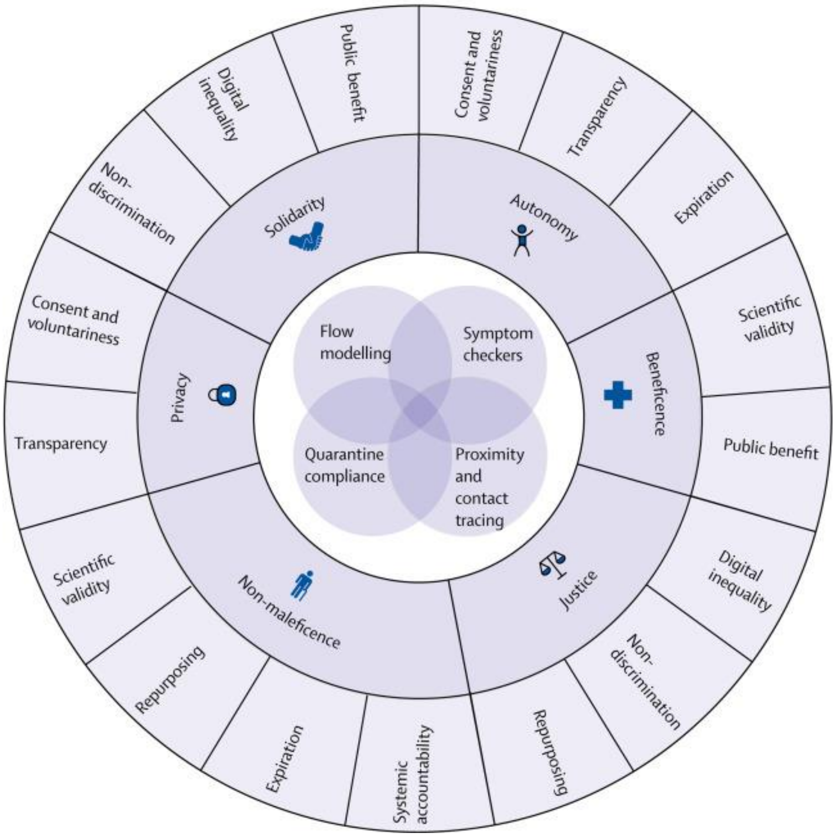
C. A series of campaigns worldwide from governments and organisations took place to mitigate the COVID-19 pandemic and loosening lockdown measures. The majority of them were based on the collection and processing of data through digital technologies and related applications. The ethical and legal boundaries of deploying digital technologies for disease surveillance and control purposes are unclear, so, a discussion has emerged globally around the promises and risks of mobilising digital technologies for public health. A presentation of a typology of the primary digital public health applications that used during campaigns is provided in [132] and depicted in Figure 11. Also, authors provide the context-specific risks, cross-sectional issues, and ethical concerns, as depicted in Figure 60. Finally, authors proposed practical guidance to aid policymakers and other decision-makers for the ethical development and use of digital public health tools, as depicted in Figure 61.



This typology is based on an analysis of primary cases of COVID-19 digital public health technologies. Note, there might be variations because of the rapid proliferation and evolution of national, international, and private actor initiatives in this domain. Further, some technologies might combine purposes or have overlaps in approaches.

	Key actors				Data types			Data Source							Consent			
	Government	Academics	Private	Citizens	Sensitive	Non-sensitive	Non-PII	IP	Cell site	Number	GPS	Bluetooth	Third party	Citizens	None	Opt in	Opt out	Selected example cases
Proximity and contact tracing	●			●		●	●		●			●	●			●		**TraceTogether** Location: Singapore Type: mobile app
Symptom checkers	●	●	●	●	●	●		●	●	●	●			●		●		Comunidad de Madrid **CoronaMadrid** Location: Spain Type: mobile and web
Quarantine compliance	●			●	●	●	●		●	●				●	●			**Electronic Fence** Location: Taiwan Type: geo-fence
Flow modelling			●	●			●	●	●					●			●	Google **Mobility Report** Location: Global Type: flow model

Figure 60. Typology of digital public health technologies against COVID-19. [132]



This sunburst diagram presents how the six ethical principles raise ethical and legal issues when considered in relation to digital public health technologies against COVID-19. As shown by the intersecting circles at the centre, these principles apply equally to symptom checkers, proximity and contact tracing, quarantine compliance, and flow modelling.

Figure 61. Ethical and legal issues raised by applying ethical principles to COVID-19 digital technologies. [132]

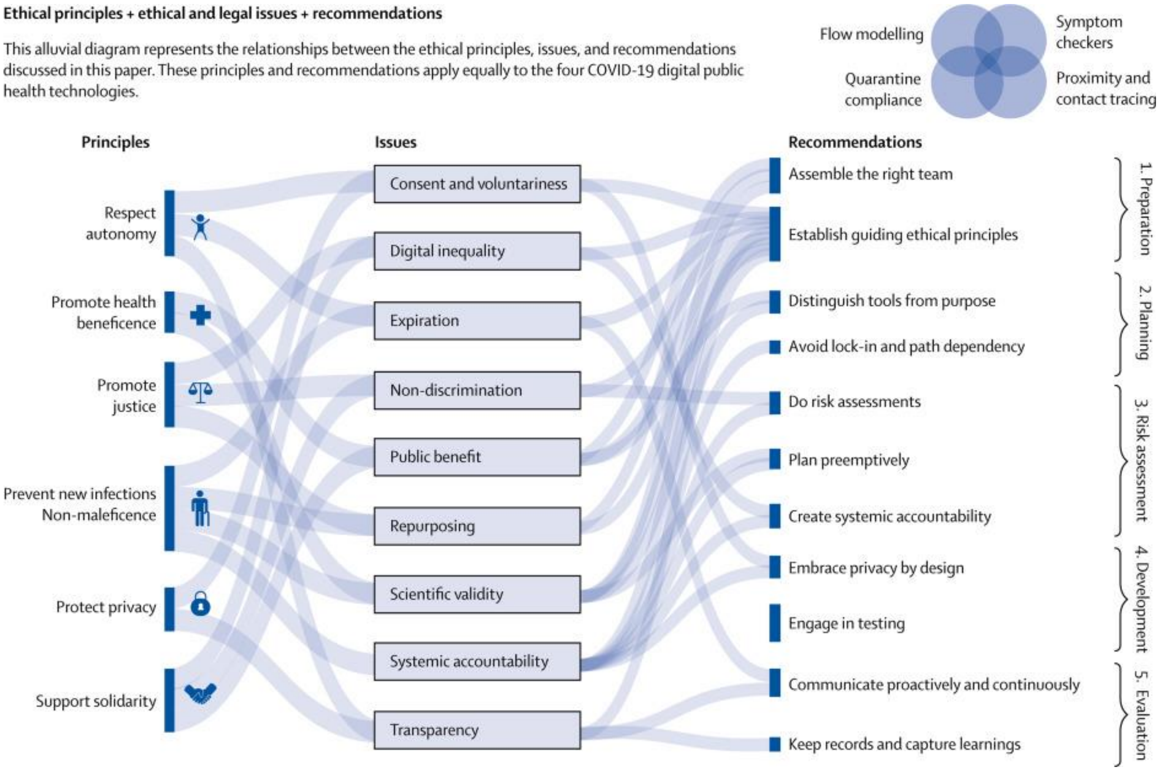

Ethical principles + ethical and legal issues + recommendations
This alluvial diagram represents the relationships between the ethical principles, issues, and recommendations discussed in this paper. These principles and recommendations apply equally to the four COVID-19 digital public health technologies.
Flow modelling
Symptom checkers
Quarantine compliance
Proximity and contact tracing
Principles
Respect autonomy
Promote health beneficence
Promote justice
Prevent new infections Non-maleficence
Protect privacy
Support solidarity
Issues
Consent and voluntariness
Digital inequality
Expiration
Non-discrimination
Public benefit
Repurposing
Scientific validity
Systemic accountability
Transparency
Recommendations
Assemble the right team
Establish guiding ethical principles
Distinguish tools from purpose
Avoid lock-in and path dependency
Do risk assessments
Plan preemptively
Create systemic accountability
Embrace privacy by design
Engage in testing
Communicate proactively and continuously
Keep records and capture learnings
1. Preparation
2. Planning
3. Risk assessment
4. Development
5. Evaluation

Figure 62. The relationship between ethical principles, ethical and legal issues, and recommendations. [132]

7.4 National Cyber Security Strategy (NCSS) in Greece

We consider it important and appropriate to dedicate a paragraph on the National Cyber Security Strategy (NCSS) in Greece. It worth mentioning that, Greece transposed and implemented the NIS Directive into national laws and identified operators of essential services [128]. The successful response to the COVID-19 related issues in our country – hitherto- is mainly due to the coordinated efforts of the related actors. We provide a summary of the objectives of the strategy and in Appendix C the national cybersecurity organizations, as exactly provided by [135], [136].

A. Objectives of NCSS

- Address cyber crime
- Balance security with privacy
- Citizen's awareness
- Critical Information Infrastructure Protection
- Develop national cyber contingency plans
- Engage in international cooperation
- Establish a public-private partnership

- Establish an incident response capability
- Establish an institutionalised form of cooperation between public agencies
- Establish and implement policies and regulation capabilities
- Establish baseline security requirements
- Establish incident reporting mechanisms
- Establish trusted information-sharing mechanisms
- Foster R&D
- Organise cyber security exercises
- Risk assessment approach
- Set a clear governance structure
- Strengthen training and educational programmes

7.5 Changes in the Threat Landscape Due to the COVID-19

There is not a surprise, that during the COVID-19 pandemic and the crisis that followed, the threat actors took advantage of the vulnerable situation in which healthcare organizations placed because they focused on their primary role, that is the care of patients. On the other hand, the situation in Europe and worldwide triggered a series of campaigns due to conditions such as high demands for certain goods (such as protective masks and household products), increasing reliance on teleworking, increasing fear, uncertainty and, doubt in the general population, which exploited making the situation even more vulnerable [134]. Threat actors look at crisis as an opportunity and use COVID-related themes to launch widespread attacks such as phishing that target society overall, and attacks such ransomware that target healthcare organizations.

According to [137] until mid-April 2020 news report several attacks targeting healthcare organizations worldwide, such as Brno University Hospital in the Czech Republic, Paris' hospital system, the computer systems of Spain's hospitals, hospitals in Thailand, medical clinics and a healthcare agency in the U.S. state of Illinois to name a few. More sophisticated intrusion methods employed by threat actors and Advanced Persistent Threat (APT) groups have been using COVID-19 for malware spreading, as reported in [138]. The Figure 63 shows the top ten cyber threats from January 2020 to March 2020, taking advantage of COVID-19:

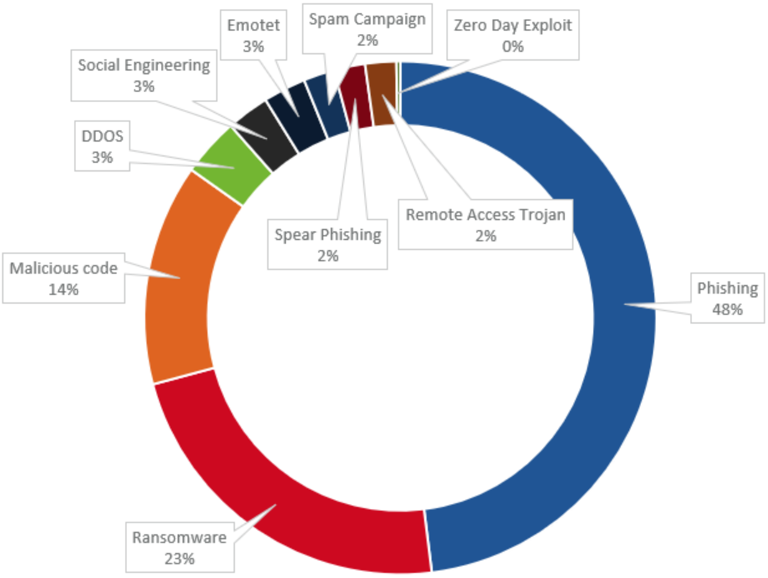


Figure 63. The Top Ten Cyber Threats from January 2020 to March 2020. [139]

Acronis reported that ransomware detections in Europe increased up to 7% in the last week of February 2020, and 10% the week after [140].

The threat analysis specialized team of Google (Google's Threat Analysis Group -TAG) that work to identify new vulnerabilities and threats for his products, detected 18 million malware and phishing Gmail messages, and more than 240 million spam messages related to COVID-19 daily [141]. Particularly, the TAG reported that over a dozen state-backed threat actors used COVID-19 themes as bait for phishing through emails. For example, TAG discovered a campain that target personal accounts of U.S. government employees using American fast-food franchises and messages that offered free meals and coupons in response to COVID-19. By clicking on the emails, presented phishing pages designed to trick users into providing their Google account credentials.

Also, TAG found that several threat actors tried to fake users by impersonating health organizations. For example, TAG found an activity, with emails that linked to a domain spoofing the World Health Organization's (WHO) login page. A similar attack reported on Microsoft Office 365 platform [142].

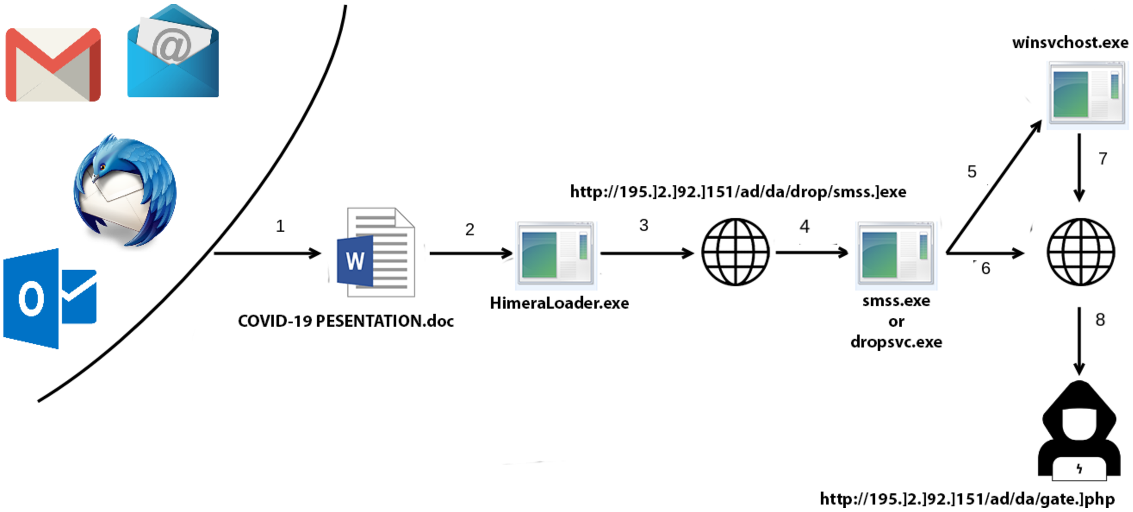


Figure 64. Infection Chain of an Email Attack. [143]

The Yoroi[58] threat intelligence team intercepted incoming emails directed to their customers and realized that the messages were leveraging FMLA (Family and Medical Leave Act) requests related to the COVID-19 pandemics and also, discover the cyber-criminal tools that used [143]. The infection chain of this attack, provided by Yoroi depicted in Figure 64.

ENISA in [139] analysed the exploitation by threat actors of the COVID-19 pandemic and provided an instructive, explanatory infographic, as depicted in Figure 65. This infographic captures the sources used by attackers to deliver the payloads or the tools to the target in order to execute attacks. From the aforementioned analysis, two essentials emerge and these concern the sources and the prevalent attacks. Concerning the sources, it is evident that email phishing remains a primary attack vector.

Finally, RiskIQ[59], a leading company on digital threat management, since March 2020, began compiling disparate data and intelligence related to COVID-19 into weekly reports that combine major updates around COVID-19 and its impacts on society, and also essential and cybercrime data to raise the situational awareness of cybersecurity IT teams [144].

---

[58] https://yoroi.company/

[59] https://www.riskiq.com/

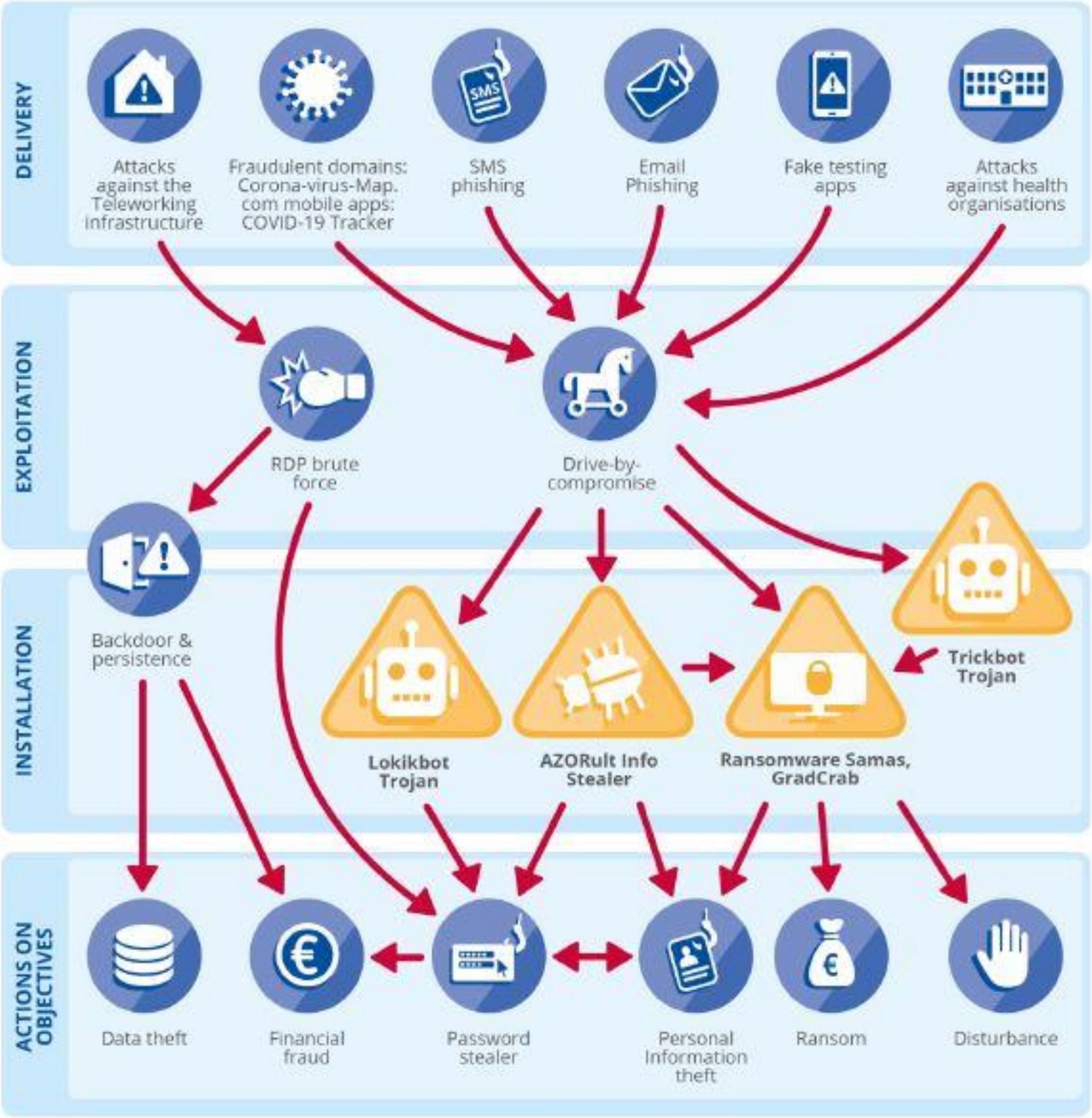


Figure 65. Exploitation by Cybercriminals and APT Groups of the COVID-19 pandemic. [139]

8 Conclusions

The role of eHealth is vital in promoting universal health coverage in a variety of ways. eHealth helps provide services to people and communities through telehealth and mHealth, simplifies the training of the health workforce through the use of e-learning, and makes education more widely accessible especially for those who are isolated and enhances diagnosis and treatment by providing accurate and timely patient information through health records. eHealth through the use of ICT improves the operations and financial efficiency of healthcare systems.

The use of ICTs such as the IoMT, Cloud, Fog and MEC, Big Data, Blockchain and, AI technologies are revolutionizing eHealth and its whole ecosystem, moving it towards Healthcare 4.0, and considered their main pillars and building blocks. eHealth ecosystem points to the eHealth with its all applications and eHealth system refers to a typical eHealth application. There are many eHealth services, applications that support the respective service and therefore the respective system that supports them.

Security and privacy presenting the greatest challenges for all ICTs. Essentially, these factors determine how much acceptable, and therefore successful, will be a technology by the vast majority of users. In the eHealth sector, security and privacy requirements are growing rapidly as the main subject of eHealth is the data of users. eHealth challenges lie in the fact that eHealth is required to meet all the security challenges of its related ICTs and their components, e.g. hardware and software. Solving a security problem usually creates a new need for security and privacy. Although it seems like a “vicious circle”, but this is that creates the need for continuous development and improvement of the sector.

The health sector recognized by the EU through the NIS directive as a critical sector, so, we should always keep in mind that the majority of eHealth services are critical and therefore the eHealth infrastructure that supports them is critical, as it turned out during the COVID-19 pandemic and the global crisis that followed. Threat events occurring in eHealth systems that affect their availability and individual’s privacy and data integrity are common. Generally speaking, every digital system has vulnerabilities and attracts threat actors to carry out an attack and an eHealth system is no exception. For all individuals and healthcare stakeholders to trust eHealth services, systems that support these services must cover security requirements. It is crucial to implement security mechanisms that are security measures, which means applying a collection of policies and actions to prevent any attraction from threat actors. In any case, a systematic approach is needed to determine the security measures that will be applied to each system.

Several issues that need attention in the eHealth sector as follows:

- The concurrent use of many emerging ICTs which have in fact developed in the last decade and each of them presents its own security issues
- The billions of people who benefit from the eHealth services
- The multidimensional information contained in medical records
- The proliferation of mobile devices, especially smartphones, which mainly results in the heavy use of wireless networks for myriads of mobile applications and, in many circumstances functioned as fog nodes.
- The extended use of web services such as email and, also, of web applications.
- The plethora of medical things

Considering the aforementioned issues, the following are generic challenges identified that hinder the integration of secure eHealth ecosystem:

- **Very large attack surface:** The threats and risks related to eHealth are manifold and evolve rapidly. eHealth is heavily based on the gathering, exchange, storing, and processing of large amounts of data from a variety of actors. Considering their impact on individuals' health, safety, and privacy the threat landscape concerning eHealth is extremely wide.
- **Resource-constraint devices:** The majority of medical things are resource-constraint, e.g. processing, memory, and power, and therefore advanced security mechanisms, such security algorithms, cannot be effectively applied, neither malware nor anti-virus protection. A weak security mechanism in an IoMT device is susceptible to attacks and can effectively draft the device to a large IoT botnet.
- **Complex ecosystem:** eHealth ecosystem should not be seen as a collection of independent devices, but a rich, diverse, and wide ecosystem involving aspects such as devices, communications, interfaces, and people.
- **Disappear of network perimeter:** The evolution of connected IoMT devices, the emergence of cloud and mobile computing and, the federation of multiple stakeholders in the eHealth ecosystem results in the single network perimeter disappearing around applications and users. Traditional security methods to securely delivering applications to end-users over any channel, anytime, anyplace security methods are insufficient, so, new methods required.
- **Fragmentation of standards and regulations in IoMT:** The fragmented adoption of standards and regulations to guide the adoption of IoMT security measures and good practices, as well as the continuous evolution of ICTs, further complicate relevant concerns.
- **Security integration:** This is a very challenging task, due to the presence of possibly contradicting viewpoints and requirements from all involved actors. For example, different IoMT devices and systems may be based on different

authentication solutions, because they have different operating systems (OS) or even lack of OS.

- **Communication media:** IoMT devices mostly are mobile and connect to the Internet or gateways through less secure wireless communication media compared to the end devices that connect through more secure media wired or wireless. Also, cellular technologies, i.e. 3G, 4G, and even the evolving 5G suffer from security issues.
- **Safety aspects:** They are very relevant in the IoMT context because of the presence of actuators, which act on the physical world. Security threats can cost human lives as, for example, an interception on a biomedical sensor network that alerts in case of a heart attack.
- **Low cost:** The wide penetration of IoMT and the advanced functionalities it offers in the eHealth sector represents the potential for significant cost savings by exploiting features such as remote monitoring of patients. The low cost of IoMT devices and systems will have implications in terms of security. Many manufacturers do not prioritize security and safety but system functionality at the lowest possible cost and thus product security might not be able to protect against certain types of threats.
- **Security updates:** Applying security updates to medical devices is extremely challenging since the particularity of the user interfaces available to users does not allow traditional update mechanisms. Since a medical device is the enabler of an attack, threat actors can discover and exploit vulnerabilities associated with software to succeed.

Healthcare organizations must take additional steps to achieve security requirements by implement stronger defenses and good practices which means applying a collection of security solutions to prevent any attraction from threat actors, as it turned out during the COVID-19 pandemic and the crisis that followed. Nevertheless, there is not a one-size-fits-all security solution for any eHealth system and it is not feasible to address every cybersecurity challenge because every particular system faces different threats, different vulnerabilities, and different risk tolerances. No matter how much we shield a system, human errors and weaknesses will always be a threat. Also, unpredictable situations, such as the COVID-19 crisis highlighted weaknesses that have as a result failures to effective cybersecurity implementation of security measures in healthcare organizations and will create new challenges.

The following are the most significant factors that have as a result failures to effective cybersecurity implementation of security measures in healthcare organizations:

- **Low priority**: In healthcare organizations, cybersecurity is undeniably not a priority.

- **The human factor:** Human error is the most common risk in the eHealth sector.
- **Lack of education:** Workforce is not appropriately trained to address phishing attacks.
- **Lack of resources:** There is a lack of financial and human resources for the IT department and consequently this leads to the lack of security experts, but also the implementation of limited security measures.
- **Medical device manufacturers:** There is limited flexibility from the medical device manufacturers and a lack of contractual obligations related to cybersecurity.

There is a lot of research from nations, organisations, academia and industry related to security measures, solutions and tools that could be implemented in eHealth systems to defend against prevalent threats such as phishing and ransomware that increased dramatically during the COVID-19 crisis and highlighted the weaknesses and the omissions in eHealth security. No one knows if similar tragic situations, such as created during the COVID-19 pandemic, will arise in the future. The provision of healthcare must be permanent and the digital technologies that support it must be resilient to any situation.

The COVID-19 crisis has made the need for prevention urgent and the lessons that humanity has learned are hopefully enough to highlight the role of security and privacy.in the whole eHealth ecosystem.

9 Contribution and Future Work

The primary goal of the work is the investigation of common eHealth-related cybersecurity and privacy issues. In the context of this goal we investigated:

- The eHealth ecosystem and the related digital technologies
- The eHealth threat landscape
- The eHealth specific issues on cybersecurity and privacy
- The eHealth-related state-of-the-art cybersecurity measures and solutions
- The eHealth Cybersecurity and Privacy issues associated with the COVID-19

During the elaboration of the work the humanity experienced the COVID-19 pandemic. We thought, it would be useful and helpful to dedicate a section of the work to the COVID-19 crisis, even if it was still in progress.

Although we believe that we have achieved our goal, it is certain that there are many directions for a future work which may concern the following:

- Research on cybersecurity measures in Greek hospitals before or/and after the COVID-19
- Research on cybersecurity maturity in Greece in terms of the eHealth sector in general
- Research on the implementation of emerging technologies such as blockchain and FMEC technology regarding eHealth security and privacy
- Cyber-security research covering all steps of the defense-in-depth strategy

References

[1] World Health Organization, “Global diffusion of eHealth: Making universal health coverage achievable,” *Report of the third global survey on eHealth Global Observatory for eHealth*, 2016. [Online]. Available: http://who.int/goe/publications/global_diffusion/en/. [Accessed: 07-Apr-2020].

[2] P. Sundaravadivel, E. Kougianos, S. P. Mohanty, and M. K. Ganapathiraju, “Everything you Wanted to Know About Smart Health Care,” *IEEE Consum. Electron. Mag.*, vol. 7, no. 1, pp. 18–28, 2018.

[3] World Health Organization, “National eHealth Strategy Toolkit,” 2012. [Online]. Available: https://www.who.int/ehealth/publications/en/. [Accessed: 16-May-2020].

[4] L. H. Iwaya, “Engineering Privacy for Mobile Health Data Collection Systems in the Primary Care,” 2019.

[5] C. Lee Ventola, “Social media and health care professionals: Benefits, risks, and best practices,” *P T*, vol. 39, no. 7, pp. 491–500, 2014.

[6] European Commission, “ICT Standardisation Priorities for the Digital Single Market. COM(2016) 176 final,” 2016. [Online]. Available: https://ec.europa.eu/digital-single-market/en/news/communication-ict-standardisation-priorities-digital-single-market. [Accessed: 06-Apr-2020].

[7] M. Agiwal, A. Roy, and N. Saxena, “Next generation 5G wireless networks: A comprehensive survey,” *IEEE Commun. Surv. Tutorials*, vol. 18, no. 3, pp. 1617–1655, 2016.

[8] P. Mell and T. Grance, “The NIST-National Institute of Standars and Technology-Definition of Cloud Computing,” *NIST Spec. Publ. 800-145*, p. 7, 2011.

[9] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” *Comput. Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[10] M. Marjani *et al.*, “Big IoT Data Analytics: Architecture, Opportunities, and Open Research Challenges,” *IEEE Access*, vol. 5, pp. 5247–5261, 2017.

[11] B. Varghese and R. Buyya, “Next generation cloud computing: New trends and research directions,” *Futur. Gener. Comput. Syst.*, vol. 79, pp. 849–861, 2018.

[12] R. Buyya *et al.*, “A manifesto for future generation cloud computing: Research directions for the next decade,” *ACM Comput. Surv.*, vol. 51, no. 5, pp. 1–51, 2019.

[13] Y. Lu, “The blockchain: State-of-the-art and research challenges,” *J. Ind. Inf.*

Integr., vol. 15, no. January, pp. 80–90, 2019.

[14] G. Aceto, V. Persico, and A. Pescapé, “The role of Information and Communication Technologies in healthcare: taxonomies, perspectives, and challenges,” *Journal of Network and Computer Applications*, vol. 107, no. July 2017. Elsevier, pp. 125–154, 2018.

[15] L. Atzori, A. Iera, and G. Morabito, “Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm,” *Ad Hoc Networks*, vol. 56, pp. 122–140, 2017.

[16] L. Minh Dang, M. J. Piran, D. Han, K. Min, and H. Moon, “A survey on internet of things and cloud computing for healthcare,” *Electron.*, vol. 8, no. 7, pp. 1–49, 2019.

[17] K. Taylor, A. Sanghera, M. Steedman, and M. Thaxter, “Medtech and the Internet of Medical Things: How connected medical devices are transforming health care,” *Deloitte*, 2018. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Life-Sciences-Health-Care/gx-lshc-medtech-iomt-brochure.pdf. [Accessed: 05-May-2020].

[18] C. Puliafito, E. Mingozzi, F. Longo, A. Puliafito, and O. Rana, “Fog computing for the Internet of Things: A survey,” *ACM Trans. Internet Technol.*, vol. 19, no. 2, 2019.

[19] Y. C. Hu, M. Patel, D. Sabella, N. Sprecher, and V. Young, “ETSI White Paper #11 Mobile Edge Computing - A key technology towards 5G,” *ETSI White Pap. No. 11 Mob.*, no. 11, pp. 1–16, 2015.

[20] G. Aceto, V. Persico, and A. Pescapé, “Industry 4.0 and Health: Internet of Things, Big Data, and Cloud Computing for Healthcare 4.0,” *Journal of Industrial Information Integration*, vol. 18, no. February. Elsevier, p. 100129, 2020.

[21] J. J. Hathaliya and S. Tanwar, “An exhaustive survey on security and privacy issues in Healthcare 4.0,” *Comput. Commun.*, vol. 153, no. February, pp. 311–335, 2020.

[22] I. Ud Din *et al.*, “The Internet of Things: A Review of Enabled Technologies and Future Challenges,” *IEEE Access*, vol. 7, pp. 7606–7640, 2019.

[23] R. Kumar and R. Goyal, “On cloud security requirements, threats, vulnerabilities and countermeasures: A survey,” *Comput. Sci. Rev.*, vol. 33, pp. 1–48, 2019.

[24] A. Yousefpour *et al.*, “All one needs to know about fog computing and related edge computing paradigms: A complete survey,” *J. Syst. Archit.*, vol. 98, no. December 2018, pp. 289–330, 2019.

[25] P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, and T. Taleb, “Survey on

Multi-Access Edge Computing for Internet of Things Realization," *IEEE Commun. Surv. Tutorials*, vol. 20, no. 4, pp. 2961–2991, 2018.

[26] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. S. Kwak, "The internet of things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, 2015.

[27] F. A. Kraemer, A. E. Braten, N. Tamkittikhun, and D. Palma, "Fog Computing in Healthcare-A Review and Discussion," *IEEE Access*, vol. 5, pp. 9206–9222, 2017.

[28] D. V. Dimitrov, "Medical internet of things and big data in healthcare," *Healthc. Inform. Res.*, vol. 22, no. 3, pp. 156–163, 2016.

[29] C. Agbo, Q. Mahmoud, and J. Eklund, "Blockchain Technology in Healthcare: A Systematic Review," *Healthcare*, vol. 7, no. 2, p. 56, 2019.

[30] A. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G. Soursou, "Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives," *Cryptography*, vol. 3, no. 1, p. 3, 2019.

[31] J. Cabestany, D. Rodriguez-Martin, C. Perez, and A. Sama, "Artificial Intelligence Contribution to eHealth Application," *Proc. 25th Int. Conf. Mix. Des. Integr. Circuits Syst. Mix. 2018*, no. July, pp. 15–21, 2018.

[32] F. Jiang *et al.*, "Artificial intelligence in healthcare: Past, present and future," *Stroke Vasc. Neurol.*, vol. 2, no. 4, pp. 230–243, 2017.

[33] H. Magsi, A. H. Sodhro, F. A. Chachar, S. A. K. Abro, G. H. Sodhro, and S. Pirbhulal, "Evolution of 5G in Internet of medical things," *2018 Int. Conf. Comput. Math. Eng. Technol. Inven. Innov. Integr. Socioecon. Dev. iCoMET 2018 - Proc.*, vol. 2018-Janua, pp. 1–7, 2018.

[34] M. Nieles, K. Dempsey, and V. Y. Pillitteri, "NIST SP800-12 Revision 1 : An introduction to information security," *NIST Spec. Publ.*, no. 800–12 (draft) revision 1, 2017.

[35] European Union Agency for Network and Information Security, "Definition of Cybersecurity | Gaps and overlaps in standardisation," *European Union Agency For Network And Information Security*, 2015. [Online]. Available: https://www.enisa.europa.eu/publications/definition-of-cybersecurity. [Accessed: 06-Apr-2020].

[36] "National Institute of Standards and Technology, COMPUTER SECURITY RESOURCE CENTER, Glossary." [Online]. Available: https://csrc.nist.gov/glossary. [Accessed: 07-Apr-2020].

[37] W. Stallings, *Network Security Cryptography and Principles and Practice 7th Edition*. Pearson Education, 2017.

[38] European Parliament, “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da.” [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj. [Accessed: 13-Jun-2020].

[39] European Union Agency for Network and Information Security, *ENISA Threat Landscape Report 2018 15 Top Cyberthreats and Trends*, no. January. European Union Agency for Network and Information Security (ENISA), 2019.

[40] “Standards” [Online]. Available: https://ec.europa.eu/digital-single-market/en/standards-digitising-european-industry. [Accessed: 15-May-2020].

[41] J. Fernandez and M. Schaffer, *STANDARDISATION IN SUPPORT OF THE Recommendations for European standardisation in relation to the Cybersecurity Act*, no. December. European Union Agency for Network and Information Security (ENISA), 2019.

[42] I. T. U. (ITU), “Recommendation X.800 (03/91) : Security architecture for Open Systems Interconnection for CCITT applications,” 1991. [Online]. Available: https://www.itu.int/rec/T-REC-X.800-199103-I/en. [Accessed: 01-Apr-2020].

[43] Verizon, “2019 Data Breach Investigations,” 2019. [Online]. Available: https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf. [Accessed: 23-May-2020].

[44] E. T. S. I. (ETSI), “GS ISI 002 - V1.2.1 - Information Security Indicators (ISI); Event Model A security event classification model and taxonomy,” 2015. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/ISI/001_099/002/01.02.01_60/gs_isi002v010201p.pdf. [Accessed: 15-Apr-2020].

[45] International Telecommunication Union, “Series X: Data Networks, Open System Communications and Security: Telecommunication security - Overview of cybersecurity,” *ITU-T X.1205 Recommendation*, 2008. [Online]. Available: https://www.itu.int/rec/T-REC-X.1205-200804-I. [Accessed: 01-Apr-2020].

[46] European Union Agency for Cybersecurity (ENISA), “Threat Taxonomy.” [Online]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view. [Accessed: 10-May-2020].

[47] A. M. Shabut, K. T. Lwin, and M. A. Hossain, “Cyber attacks, countermeasures, and protection schemes - A state of the art survey,” *Ski. 2016 - 2016 10th Int. Conf. Software, Knowledge, Inf. Manag. Appl.*, pp. 37–44, 2017.

[48] H. Kettani and P. Wainwright, “On the top threats to cyber systems,” *2019 IEEE 2nd Int. Conf. Inf. Comput. Technol. ICICT 2019*, pp. 175–179, 2019.

[49] D. Liveri, A. Sarri, and C. Skouloudi, “Security and Resilience in eHealth,” *Enisa*, 2015. [Online]. Available: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/ehealth_sec/security-and-resilience-in-ehealth-infrastructures-and-services. [Accessed: 20-Jun-2020].

[50] European Data Protection Supervisor, “2019 Annual Report.” [Online]. Available: https://edps.europa.eu/sites/edp/files/publication/2020-03-17_annual_report_2020_en.pdf. [Accessed: 16-May-2020].

[51] M. Conti, N. Dragoni, and V. Lesyk, “A Survey of Man in the Middle Attacks,” *IEEE Commun. Surv. Tutorials*, vol. 18, no. 3, pp. 2027–2051, 2016.

[52] W. Tounsi and H. Rais, “A survey on technical threat intelligence in the age of sophisticated cyber attacks,” *Comput. Secur.*, vol. 72, pp. 212–233, 2018.

[53] J. M. Spring and E. Hatleback, “Thinking about intrusion kill chains as mechanisms,” *J. Cybersecurity*, vol. 3, no. 3, pp. 185–197, 2017.

[54] A. Qamar, A. Karim, and V. Chang, “Mobile malware attacks: Review, taxonomy & future directions,” *Futur. Gener. Comput. Syst.*, vol. 97, pp. 887–909, 2019.

[55] Malewarebytes, “CYBERCRIME TACTICS AND TECHNIQUES: the 2019 state of healthcare.” [Online]. Available: https://resources.malwarebytes.com/files/2019/11/191028-MWB-CTNT_2019_Healthcare_FINAL.pdf. [Accessed: 28-May-2020].

[56] IBM security, “The inside story on botnets.” [Online]. Available: https://www.ibm.com/downloads/cas/V3YJVYZX. [Accessed: 27-May-2020].

[57] T. Manikandan, B. Balamurugan, C. Senthilkumar, R. R. A. Harinarayan, and R. R. Subramanian, “Cyberwar is Coming,” in *Cyber Security in Parallel and Distributed Computing*, John Wiley & Sons, Ltd, 2019, pp. 79–89.

[58] I. Yaqoob *et al.*, “The rise of ransomware and emerging security challenges in the Internet of Things,” *Comput. Networks*, vol. 129, no. 2017, pp. 444–458, 2017.

[59] G. Martin, P. Martin, C. Hankin, A. Darzi, and J. Kinross, “Cybersecurity and healthcare: How safe are we?,” *BMJ*, vol. 358, pp. 4–7, 2017.

[60] Microsoft, “Exploits and exploit kits.” [Online]. Available: https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/exploits-malware. [Accessed: 31-May-2020].

[61] S. Sibi Chakkaravarthy, D. Sangeetha, and V. Vaidehi, “A Survey on malware analysis and mitigation techniques,” *Comput. Sci. Rev.*, vol. 32, pp. 1–23, 2019.

[62] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, “Anatomy of Threats to the Internet of Things,” *IEEE Commun. Surv. Tutorials*, vol. 21, no. 2,

pp. 1636–1675, 2019.

[63] J. Faircloth, “Client-side attacks and social engineering,” in *Penetration Tester’s Open Source Toolkit (Fourth Edition)*, Fourth Edi., J. Faircloth, Ed. Boston: Syngress, 2017, pp. 273–318.

[64] F. Mouton, L. Leenen, and H. S. Venter, “Social engineering attack examples, templates and scenarios,” *Comput. Secur.*, vol. 59, pp. 186–209, 2016.

[65] B. B. Gupta, A. Tewari, A. K. Jain, and D. P. Agrawal, “Fighting against phishing attacks: state of the art and future challenges,” *Neural Comput. Appl.*, vol. 28, no. 12, pp. 3629–3654, 2017.

[66] A. Das, S. Baki, A. El Aassal, R. Verma, and A. Dunbar, “SoK: A Comprehensive Reexamination of Phishing Research from the Security Perspective,” *IEEE Commun. Surv. Tutorials*, vol. 22, no. 1, pp. 671–708, 2020.

[67] G. Park and J. Rayz, “Ontological Detection of Phishing Emails,” *Proc. - 2018 IEEE Int. Conf. Syst. Man, Cybern. SMC 2018*, pp. 2858–2863, 2019.

[68] R. S. Kunwar and P. Sharma, “Social media: A new vector for cyber attack,” *Proc. - 2016 Int. Conf. Adv. Comput. Commun. Autom. ICACCA 2016*, pp. 1–5, 2016.

[69] B. F. Alrashidi, A. M. Almuhana, and A. M. Aljedaie, “The Effects of the Property of Access Possibilities and Cybersecurity Awareness on Social Media Application,” in *Advances in Data Science, Cyber Security and IT Applications*, 2019, pp. 57–68.

[70] Cybersecurity and Infrastructure Security Agency (CISA), “COVID-19 Exploited by Malicious Cyber Actors.” [Online]. Available: https://www.us-cert.gov/ncas/alerts/aa20-099a. [Accessed: 30-May-2020].

[71] Malwarebytes, “APTs and COVID-19: How advanced persistent threats use the coronavirus as a lure.” [Online]. Available: https://blog.malwarebytes.com/threat-analysis/2020/04/apts-and-covid-19-how-advanced-persistent-threats-use-the-coronavirus-as-a-lure/. [Accessed: 01-Jun-2020].

[72] Malwarebytes, “CYBERCRIME TACTICS AND TECHNIQUES: the 2019 state of healthcare”, [Online]. Available: https://resources.malwarebytes.com/files/2019/11/191028-MWB-CTNT_2019_Healthcare_FINAL.pdf. [Accessed: 07-June-2020].

[73] P. Gralla, “Your Next Big Security Worry: Fileless Attacks.” [Online]. Available: https://www.symantec.com/blogs/feature-stories/your-next-big-security-worry-fileless-attacks. [Accessed: 05-Jun-2020].

[74] European Parliament, “Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of

security of network and information systems across the Union." [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC. [Accessed: 13-Jun-2020].

[75] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant, and K. Mankodiya, "Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare," *Futur. Gener. Comput. Syst.*, vol. 78, pp. 659–676, 2018.

[76] E. T. S. I. (ETSI), "TR 103 477 - V1.1.1 - eHEALTH; Standardization use cases for eHealth," 2019.

[77] European Union Agency for Cybersecurity (ENISA), *ICT security certification opportunities in the healthcare sector*, no. December. European Union Agency for Network and Information Security (ENISA), 2018.

[78] ENISA, "Smart Hospitals: Security and Resilience for Smart Health Service and Infrastructures," 2016. [Online]. Available: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals. [Accessed: 19-Jul-2020].

[79] J. P. A. Yaacoub *et al.*, "Securing internet of medical things systems: Limitations, issues and recommendations," *Futur. Gener. Comput. Syst.*, vol. 105, pp. 581–606, 2020.

[80] X. Wang and Z. Jin, "An Overview of Mobile Cloud Computing for Pervasive Healthcare," *IEEE Access*, vol. 7, pp. 66774–66791, 2019.

[81] S. B. Baker, W. Xiang, and I. Atkinson, "Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities," *IEEE Access*, vol. 5, pp. 26521–26544, 2017.

[82] E. Chukwu and L. Garg, "A systematic review of blockchain in healthcare: Frameworks, prototypes, and implementations," *IEEE Access*, vol. 8, pp. 21196–21214, 2020.

[83] G. Marques, R. Pitarma, N. M. Garcia, and N. Pombo, "Internet of things architectures, technologies, applications, challenges, and future directions for enhanced living environments and healthcare systems: A review," *Electron.*, vol. 8, no. 10, pp. 1–27, 2019.

[84] A. Ahad, M. Tahir, and K. L. A. Yau, "5G-based smart healthcare network: Architecture, taxonomy, challenges and future research directions," *IEEE Access*, vol. 7, pp. 100747–100762, 2019.

[85] M. M. Dhanvijay and S. C. Patil, "Internet of Things: A survey of enabling technologies in healthcare and its applications," *Comput. Networks*, vol. 153, pp. 113–131, 2019.

[86] B. Mohanta, P. Das, and S. Patnaik, “Healthcare 5.0: A paradigm shift in digital healthcare system using artificial intelligence, IOT and 5G communication,” *Proc. - 2019 Int. Conf. Appl. Mach. Learn. ICAML 2019*, pp. 191–196, 2019.

[87] P. P. Ray, D. Dash, and D. De, “Edge computing for Internet of Things: A survey, e-healthcare case study and future direction,” *J. Netw. Comput. Appl.*, vol. 140, no. May, pp. 1–22, 2019.

[88] G. Ntehelang, B. Isong, N. Dladlu, and F. Lugayizi, “IoT-based big data analytics issues in healthcare,” *ACM Int. Conf. Proceeding Ser.*, pp. 16–21, 2019.

[89] M. Z. Alam Bhuiyan, G. Wang, A. Zaman, H. Tao, T. Wang, and M. M. Hassan, “Blockchain and big data to transform the healthcare,” *ACM Int. Conf. Proceeding Ser.*, pp. 62–68, 2018.

[90] A. M. Rahmani *et al.*, “Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach,” *Futur. Gener. Comput. Syst.*, vol. 78, pp. 641–658, 2018.

[91] V. Jagadeeswari, V. Subramaniyaswamy, R. Logesh, and V. Vijayakumar, “A study on medical Internet of Things and Big Data in personalized healthcare system,” *Heal. Inf. Sci. Syst.*, vol. 6, no. 1, pp. 1–20, 2018.

[92] E. C. Schiza, T. C. Kyprianou, N. Petkov, and C. N. Schizas, “Proposal for an eHealth Based Ecosystem Serving National Healthcare,” *IEEE J. Biomed. Heal. Informatics*, vol. 23, no. 3, pp. 1346–1357, 2019.

[93] L. Coventry and D. Branley, “Cybersecurity in healthcare: A narrative review of trends, threats and ways forward,” *Maturitas*, vol. 113, no. April, pp. 48–52, 2018.

[94] Ponemon Institute, “Cost of a data breach report,” *IBM Secur.*, p. 76, 2019.

[95] European Union, “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da.” [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504. [Accessed: 15-May-2020].

[96] K. Abouelmehdi, A. Beni-Hessane, and H. Khaloufi, “Big healthcare data: preserving security and privacy,” *J. Big Data*, vol. 5, no. 1, pp. 1–18, 2018.

[97] ISO/IEC, “INTERNATIONAL STANDARD ISO/IEC 27000:2018(E) Information technology — Security techniques — Information security management systems — Overview and vocabulary,” 2018. [Online]. Available: https://www.iso.org/standard/73906.html. [Accessed: 13-Jun-2020].

[98] National Institute of Standards and Technology, “Framework for improving critical infrastructure cybersecurity.” [Online]. Available: https://www.nist.gov/cyberframework/framework. [Accessed: 17-Jul-2020].

[99] European Union Agency for Cybersecurity (ENISA), *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures*, no. November. European Union Agency for Network and Information Security (ENISA), 2017.

[100] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, “Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues,” *IEEE Access*, vol. 6, no. Idc, pp. 18209–18237, 2018.

[101] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, “A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services,” *IEEE Commun. Surv. Tutorials*, vol. 20, no. 4, pp. 3453–3495, 2018.

[102] H. A. Abdul-Ghani and D. Konstantas, “A comprehensive study of security and privacy guidelines, threats, and countermeasures: An IoT perspective,” *J. Sens. Actuator Networks*, vol. 8, no. 2, 2019.

[103] “Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP),” *Cybersecurity Act of 2015, Section 405(d) Task Group*. [Online]. Available: https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf. [Accessed: 16-Jul-2020].

[104] ENISA European Union Agency For Network and Information Security, “ENISA Good practices for IoT and Smart Infrastructures Tool,” *ENISA Website*. [Online]. Available: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool/results#Smart Hospitals. [Accessed: 16-Jul-2020].

[105] “Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations,” *Cybersecurity Act of 2015, Section 405(d) Task Group*. [Online]. Available: https://www.phe.gov/Preparedness/planning/405d/Documents/tech-vol1-508.pdf. [Accessed: 16-Jul-2020].

[106] “Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations,” *Cybersecurity Act of 2015, Section 405(d) Task Group*. [Online]. Available: https://www.phe.gov/Preparedness/planning/405d/Documents/tech-vol2-508.pdf. [Accessed: 16-Jul-2020].

[107] ENISA, *PROCUREMENT GUIDELINES FOR CYBERSECURITY IN HOSPITALS Good practices for the security of Healthcare services FEBRUARY 2020*, no. February. 2020.

[108] European Union Agency for Cybersecurity, *Good practices for security of IoT*, no. November. European Union Agency for Network and Information Security

(ENISA), 2019.

[109] D. Robb, “Top Cybersecurity Companies.” [Online]. Available: https://www.esecurityplanet.com/products/top-cybersecurity-companies.html. [Accessed: 30-Jul-2020].

[110] J. Franklin *et al.*, “NIST SPECIAL PUBLICATION 1800-4 - Mobile device security,” *NIST Spec. Publ.*, no. C, 2019.

[111] “HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996.” [Online]. Available: https://aspe.hhs.gov/report/health-insurance-portability-and-accountability-act-1996. [Accessed: 05-Aug-2020].

[112] “Symantec Control Compliance Suite”, *Symantec*. [Online]. Available: https://docs.broadcom.com/doc/control-compliance-suite-en. [Accessed: 30-Jul-2020].

[113] “Control Compliance Suite and GDPR,” *Symantec*. [Online]. Available: https://docs.broadcom.com/doc/ccs-gdpr-allregion-but-germany. [Accessed: 20-Jul-2020].

[114] P. Rubens, “How to Comply with GDPR.” [Online]. Available: https://www.esecurityplanet.com/network-security/how-to-comply-with-gdpr.html. [Accessed: 05-Jul-2020].

[115] “Why you need an Information Centric Security model for the GDPR”, *Symantec*. [Online]. Available: https://docs.broadcom.com/doc/why-you-need-an-information-centric-security-model-for-the-gdpr-en. [Accessed: 20-Jul-2020].

[116] Cisco, “Introducing Cloud Mailbox Defense.” [Online]. Available: https://www.cisco.com/c/dam/en/us/products/collateral/security/email-security/cmd-newsletter-partner-with-gartner.pdf. [Accessed: 30-Jul-2020].

[117] “IT Solutions Reviews Organized by Markets,” *Gartner*. [Online]. Available: https://www.gartner.com/reviews/markets/. [Accessed: 30-Jul-2020].

[118] “Symantec Email Security.cloud”, [Online]. Available: https://docs.broadcom.com/doc/email-security-cloud-en. [Accessed: 15-Jul-2020].

[119] V. Lander, “The Evolution of Digital Identity,” *Symantec*. [Online]. Available: https://docs.broadcom.com/doc/the-evolution-of-digital-identity. [Accessed: 30-Jul-2020].

[120] K. DelBene, M. Medin, and R. Murray, “The Road to Zero Trust (Security).” [Online]. Available: https://media.defense.gov/2019/Jul/09/2002155219/-1/-1/0/DIB_THE_ROAD_TO_ZERO_TRUST_(SECURITY)_07.08.2019.PDF. [Accessed: 30-Jul-2020].

[121] "CASB 101: How Cloud Access Security Brokers Can Make Your Data More Secure." [Online]. Available: https://www.esecurityplanet.com/mobile-security/casb.html.

[122] "Symantec Information Center Security," *Symantec*. [Online]. Available: https://docs.broadcom.com/doc/information-centric-security-brief-en. [Accessed: 30-Jul-2020].

[123] "Store private healthcare data off-chain and manage medical data using blockchain." [Online]. Available: https://github.com/IBM/Medical-Blockchain. [Accessed: 05-Jul-2020].

[124] "Cloud security for the future of your business", [Online]. Available: https://umbrella.cisco.com/products/cloud-security-service, [Accessed: 15-Jul-2020].

[125] "Web Security Service" [Online]. Available: https://docs.broadcom.com/doc/web-security-service-at-a-glance-en. [Accessed: 14-Sep-2020].

[126] "Cisco Identity Services Engine Administrator Guide, Release 2.7." [Online]. Available: https://www.cisco.com/c/en/us/td/docs/security/ise/2-7/admin_guide/b_ise_27_admin_guide/b_ISE_admin_27_overview.html. [Accessed: 15-Jul-2020].

[127] "WHAT IS SECURITY INCIDENT AND EVENT MANAGEMENT (SIEM)?," *EC-Council*. [Online]. Available: https://blog.eccouncil.org/what-is-security-incident-and-event-management-siem/. [Accessed: 05-Jul-2020].

[128] "Implementation of the NIS Directive in Greece," *EUROPEAN COMMISSION Shaping Europe's digital future Policies*. [Online]. Available: https://ec.europa.eu/digital-single-market/en/implementation-nis-directive-greece. [Accessed: 05-Jul-2020].

[129] J. Lepassaar, "Healthcare Cybersecurity in the Time of COVID-19," *HealthManagement, Volume 20 - Issue 4, 2020*. [Online]. Available: https://healthmanagement.org/c/healthmanagement/issuearticle/healthcare-cybersecurity-in-the-time-of-covid-19. [Accessed: 30-Jul-2020].

[130] "GHOST: A user-friendly application to improve security and privacy." [Online]. Available: https://www.ghost-iot.eu/ghost-project. [Accessed: 05-Aug-2020].

[131] G. Malgieri, "Data protection and research: A vital challenge in the era of COVID-19 pandemic," *Comput. Law Secur. Rev.*, vol. 37, no. March, pp. 30–33, 2020.

[132] U. Gasser, M. Ienca, J. Scheibner, J. Sleigh, and E. Vayena, "Health Policy Digital tools against COVID-19: taxonomy, ethical challenges, and navigation aid," *Lancet*, vol. 7500, no. figure 1, 2020.

[133] “Cybersecurity in Healthcare.” [Online]. Available: https://www.enisa.europa.eu/topics/wfh-covid19/media/infographic-cybersecurity-in-healthcare/download. [Accessed: 15-Jul-2020].

[134] ENISA European Union Agency For Network and Information Security, “Cybersecurity in the healthcare sector during COVID-19 pandemic.” [Online]. Available: https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-healthcare-sector-during-covid-19-pandemic. [Accessed: 12-Jul-2020].

[135] “NATIONAL CYBER SECURITY STRATEGY - Version 3.0 -,” *European Union Agency for Cybersecurity (ENISA)*. [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-greece/@@download_version/50cded9109d442e7839649f42055da60/file_en. [Accessed: 27-Jul-2020].

[136] “National Cyber Security Strategies - Interactive Map,” *European Union Agency for Cybersecurity (ENISA)*. [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.

[137] T. Burt, “Protecting healthcare and human rights organizations from cyberattacks.” [Online]. Available: https://blogs.microsoft.com/on-the-issues/2020/04/14/accountguard-cyberattacks-healthcare-covid-19/. [Accessed: 20-Jul-2020].

[138] “COVID-19 RELATED CYBER ATTACKS,” *ITC secure*. [Online]. Available: https://itcsecure.com/covid-19-related-cyber-attacks/. [Accessed: 05-Aug-2020].

[139] “Threat Landscape Mapping,” *ENISA Website*. [Online]. Available: https://www.enisa.europa.eu/topics/wfh-covid19/resources/eu-institutions-and-bodies/threat-landscape-mapping-infographic. [Accessed: 30-Jul-2020].

[140] R. McArthur, “Cyber-attacks on healthcare facilities ‘growing threat’ during coronavirus pandemic.” [Online]. Available: https://www.healthcareitnews.com/news/europe/cyber-attacks-healthcare-facilities-growing-threat-during-coronavirus-pandemic. [Accessed: 05-Aug-2020].

[141] S. Huntley, “Findings on COVID-19 and online security threats.” [Online]. Available: https://blog.google/technology/safety-security/threat-analysis-group/findings-covid-19-and-online-security-threats/. [Accessed: 20-Aug-2020].

[142] “Abnormal Attack Stories: WHO Impersonation,” *Abnormal Security*. [Online]. Available: https://abnormalsecurity.com/blog/abnormal-attack-stories-who-impersonation/. [Accessed: 20-Aug-2020].

[143] “Himera and AbSent-Loader Leverage Covid19 Themes,” *Yoroi Company*.

[Online]. Available: https://yoroi.company/research/himera-and-absent-loader-leverage-covid19-themes/. [Accessed: 10-Sep-2020].

[144] “COVID-19 Cybercrime Weekly Update,” *RiskIQ*. [Online]. Available: https://www.riskiq.com/blog/analyst/covid19-cybercrime-update/. [Accessed: 30-Aug-2020].

Appendix A

Useful websites for security tools

In Table 1, we provide several useful links for more information concerning the good practices and the related tools.

Table 1: Resources related to available tools for implementing security solutions

Practice	Websites for industrial security tools	Related tools
Email protection	https://www.gartner.com/reviews/market/email-security https://www.esecurityplanet.com/applications/email-security.html https://www.cisco.com/c/en/us/products/security/email-security/competitive-comparison.html	SEG
Endpoint protection	https://www.gartner.com/doc/reprints?id=1-1OCBC1P5&ct=190731&st=sb https://www.gartner.com/reviews/market/endpoint-protection-platforms https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions https://www.gartner.com/reviews/market/cloud-workload-protection-platforms https://www.gartner.com/reviews/market/client-management-tools https://www.gartner.com/reviews/market/unified-endpoint-management-tools https://www.esecurityplanet.com/products/top-emm-solutions.html	EPP EDR CWP HIDPS UEM EEM MDM
Identity management and Access control	https://www.gartner.com/reviews/market/access-management https://www.gartner.com/reviews/market/privileged-access-management https://www.gartner.com/reviews/market/identity-governance-administration https://www.gartner.com/reviews/market/user-authentication https://solutionsreview.com/identity-management/the-10-best-free-and-open-source-identity-management-tools/ https://www.esecurityplanet.com/products/top-iam-products.html	IM AC AA FIO IAM
Data protection and loss prevention	https://www.gartner.com/reviews/market/cloud-access-security-brokers https://www.gartner.com/reviews/market/enterprise-data-loss-prevention https://www.esecurityplanet.com/compliance/gdpr-solutions.html	DLP CASB Encryption MFA Compliance Backup

Practice	Websites for industrial security tools	Related tools
	https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions	UEBA
Asset Management	https://www.softwaretestinghelp.com/asset-discovery-tools/ https://www.gartner.com/reviews/market/software-asset-management-tools https://www.gartner.com/reviews/market/enterprise-asset-management-software	ITAM
Network management	https://www.gartner.com/reviews/market/intrusion-prevention-systems https://www.gartner.com/reviews/market/network-firewalls https://www.gartner.com/reviews/market/network-sandboxing https://www.gartner.com/reviews/market/secure-web-gateways https://www.gartner.com/reviews/market/network-access-control https://www.esecurityplanet.com/products/top-network-access-control-solutions.html https://www.gartner.com/reviews/market/security-information-event-management https://www.esecurityplanet.com/products/top-siem-products.html	Firewall VPN SWG NIDPS NAC SIEM
Vulnerability Management	https://www.gartner.com/reviews/market/vulnerability-assessment https://www.dnsstuff.com/network-vulnerability-scanner https://www.esecurityplanet.com/products/top-patch-management-solutions.html	Scanners Patch mngmt

Appendix B

COVID-19-related Information for Cybersecurity and Privacy

The importance of research and information sharing always is important, but during the global COVID-19 crisis, it has become foundational and essential. Nations, healthcare organizations, industry, press, research and academia, individuals offer their services, recommendations, warnings, guidance, and advice to battle with the pandemic and the threat actors that see the crisis an opportunity to jeopardize once again organizations security and people’s privacy. In the following tables, we provide several initiatives related to COVID-19. The two columns of each table list the description and the corresponding link

A. EU Institutions and bodies initiatives

a. European Parliament	
Covid-19 tracing apps: ensuring privacy and data protection	https://www.europarl.europa.eu/news/en/headlines/society/20200429STO78174/covid-19-tracing-apps-ensuring-privacy-and-data-protection
COVID-19 tracing apps: MEPs[60] stress the need to preserve citizens' privacy	https://www.europarl.europa.eu/news/en/press-room/20200512IPR78915/covid-19-tracing-apps-meps-stress-the-need-to-preserve-citizens-privacy
COVID-19: fundamental rights must be upheld, warn MEPs	https://www.europarl.europa.eu/news/en/headlines/priorities/eu-response-to-coronavirus/20200423STO77706/covid-19-fundamental-rights-must-be-upheld-warn-meps
European Parliament resolution of 17 April 2020 on EU coordinated action to combat the COVID-19 pandemic and its consequences (2020/2616(RSP))	https://www.europarl.europa.eu/doceo/document/TA-9-2020-0054_EN.html
Use of smartphone data to manage COVID-19 must respect EU data protection rules	https://www.europarl.europa.eu/news/en/press-room/20200406IPR76604/use-of-smartphone-data-to-manage-covid-19-must-respect-eu-data-protection-rules
b. European Commission (EC)	
Joint statement ahead of the 2nd year anniversary of the General Data Protection Regulation	https://ec.europa.eu/commission/presscorner/detail/en/statement_20_913
Tourism and transport: Commission's guidance on how to safely resume travel and reboot Europe's tourism in 2020 and beyond*	https://ec.europa.eu/commission/presscorner/detail/en/ip_20_854
Coronavirus: a common approach for safe and efficient mobile tracing apps across the EU	https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_869
Guidance on Apps supporting the fight against	https://eur-lex.europa.eu/legal-

---

[60] Smartphone apps used to manage the spread of the pandemic named MEPs.

COVID-19 pandemic in relation to data protection	content/EN/TXT/?qid=1587141168991&uri=CELEX%3A52020XC0417%2808%29
Recommendation on apps for contact tracing	https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1587153139410&uri=CELEX%3A32020H0518
c. eHealth Network	
Interoperability guidelines for approved contact tracing mobile applications in the EU Common EU Toolbox for Member States Version 1.0	https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf
Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States Version 1.0	https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf
d. European Union Agency for Fundamental Rights	
Tech answers to COVID-19 should also safeguard fundamental rights	https://fra.europa.eu/en/news/2020/tech-answers-covid-19-should-also-safeguard-fundamental-rights
Protect human rights and public health in fighting COVID-19	https://fra.europa.eu/en/news/2020/protect-human-rights-and-public-health-fighting-covid-19
e. European Data Protection Board (EDPB)	
Guidance on the use of location data and contact tracking tools	https://www.enisa.europa.eu/topics/wfh-covid19/resources/eu-institutions-and-bodies/guidance-on-the-use-of-location-data-and-contact-tracking-tools
Statement for the processing of personal data in the context of covid-19 outbreak	https://www.enisa.europa.eu/topics/wfh-covid19/resources/eu-institutions-and-bodies/statement-for-the-processing-of-personal-data-in-the-context-of-covid-19-outbreak
Guidance on the processing of health data for the purpose of scientific research in the context of the COVID-19 outbreak	https://www.enisa.europa.eu/topics/wfh-covid19/resources/eu-institutions-and-bodies/guidance-on-the-processing-of-health-data-for-the-purpose-of-scientific-research-in-the-context-of-the-covid-19-outbreak
f. ENISA	
Cybersecurity recommendations on a variety of topics including working remotely, shopping online, and eHealth to face COVID-19 security issues	https://www.enisa.europa.eu/topics/wfh-covid19?tab=details
Record of all news produced during COVID-19 crisis	https://www.enisa.europa.eu/topics/wfh-covid19?tab=articles
Additional resources for COVID-19	https://www.enisa.europa.eu/topics/wfh-covid19/?tab=resources
g. EUROPOL	
Staying safe during COVID-19: what you need to know	https://www.enisa.europa.eu/topics/wfh-covid19/resources/eu-institutions-and-bodies/europol-staying-safe-during-covid-19-what-you-need-to-know

B. Business

F-Secure - Cybersecurity Guidance for COVID-19	https://blog.f-secure.com/cyber-security-guidance-for-covid-19/
Symantec - Stepping Up to Meet the COVID-19 Crisis	https://symantec-enterprise-blogs.security.com/blogs/product-insights/symantec-identity-stepping-meet-covid-19-crisis
Cisco - Keeping You Connected During the COVID-19 Crisis	https://www.cisco.com/c/m/en_sg/covid19.html
The Register - UK snubs Apple-Google coronavirus app API	https://www.theregister.com/2020/04/28/uk_coronavirus_google_apple_api/
Flypig - Google/Apple's “privacy-safe contact tracing“, a summary	https://www.enisa.europa.eu/topics/wfh-covid19/resources/business/flypig-google-apples-201cprivacy-safe-contact-tracing201c-a-summary
CISOMAG - Underbelly of COVID-19: Malware and Ransomware Ramp Up	https://www.enisa.europa.eu/topics/wfh-covid19/resources/business/cisomag-underbelly-of-covid-19-malware-and-ransomware-ramp-up
Cyber security 101: Protect your privacy from hackers, spies, and the government	https://www.zdnet.com/article/online-security-101-how-to-protect-your-privacy-from-hackers-spies-and-the-government/

C. International

Tech UK - COVID-19: Cyber Security Guidance and Advice Repository	https://www.enisa.europa.eu/topics/wfh-covid19/resources/international/tech-uk-covid-19-cyber-security-guidance-and-advice-repository
INTERPOL - COVID-19 cyberthreats	https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats
United Nations - Fighting the Industrialization of Cyber Crime	https://www.un.org/en/chronicle/article/fighting-industrialization-cyber-crime
ActionFraud - COVID-19 related scams - news and resources	https://www.actionfraud.police.uk/covid19

D. In Greece

a. Initiative from the GR CSIRT Network	
GR CSIRT - Cybersecurity in a remote workplace: A joint effort	https://csirt.cd.mil.gr/announcement/cybersecurity-remote-workplace-joint-effort
b.Guidance from Hellenic Data Protection Authority (DPA)	
Guidance for security measures in the context of teleworking	https://www.dpa.gr/APDPXPortlets/htdocs/documentSDisplay.jsp?docid=135,127,231,131,72,198,37,128
Guidance for the processing of personal data in the context of the management of COVID-19	https://www.dpa.gr/APDPXPortlets/htdocs/documentSDisplay.jsp?docid=163,39,44,101,194,223,3,99

Appendix C

A. National Cybersecurity Organizations

a. Authorities

- Hellenic Data Protection Authority (DPA) | GDPR
- Hellenic Police - Cyber Crime | Cyber Crime
- Ministry of Digital Policy, Telecommunications and Media - Directorate of Cyber Security | NIS
- Ministry of National Defence (MOD) - Hellenic National Defence General Staff | CSIRT for NIS
- Telecommunications & Post Commission (EETT) | National regulator for electronic communications
- “ADAE” Hellenic Authority for Communication Security and Privacy | Authority for Communication Security and Privacy
- “EYP” National Intelligence Service - National CERT | National CERT

b. Centres

- "ATHENA RC" Research & Innovation Information Technologies
- "DEMOKRITOS" National Centre for Scientific Research
- "FORTH-ICS" Foundation for Research and Technology- Hellas Institute of Computer Science
- “CERTH/ITI” Center for Research and Technology HELLAS Information Technologies Institute
- “DIOFANTOS”

B. National Information Sharing and Analysis Centers (ISACs)

- EYP – National Intelligence Service – National CERT
- Ministry of National Defence (MOD) – Hellenic National Defence General

C. Research & Development (R&D) and Innovation

a. Universities focusing on NIS (Network and Information Security)

- Athens University of Economics and Business (AUEB)
- University of Piraeus (UNIPI)

- University of the Aegean
- University of Macedonia
- University of Patras

b. National Public Institutions

- General Secretariat for Digital Policy (GSDP)
- General Secretariat for Research and Technology (GSRT)

c. R&D Programmes (H2020: Horizon 2020, is a funding work programme of European Commission about Research and Innovation, available over 7 years, from 2014 to 2020)

- H2020: CONCORDIA
- H2020: CYBERSANE
- H2020: CYBERSURE
- H2020: CrowdHEALTH
- H2020: Curex
- H2020: FutureTPM
- H2020: GUARD
- H2020: INCOGNITO
- H2020: RESIST
- H2020: SAFERtec
- H2020: SECONDO
- H2020: SEMIoTICS
- H2020: SMESEC
- H2020: SPEAR
- H2020: SPIDER
- H2020: THREAT-ARREST
- H2020: YAKSHA
- H2020: sealedGRID

D. Major players in NIS (Network and Information Security)

General Secretariat for Digital Policy (GSDP)