Chapter 8

Security Challenges for the Critical Infrastructures of the Healthcare Sector

By Eva Maia, Isabel Praça, Vasiliki Mantzana, Ilias Gkotsis, Paolo Petrucci, Elisabetta Biasin, Erik Kamenjasevic and Nadira Lammari

DOI: 10.1561/9781680836875.ch8

Published in *Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures* by John Soldatos, James Philpot and Gabriele Giunta (eds.). 2020. ISBN 978-1-68083-686-8. E-ISBN 978-1-68083-687-5.

Suggested citation: Eva Maia *et al.* 2020. "Security Challenges for the Critical Infrastructures of the Healthcare Sector" in *Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures*. Edited by John Soldatos, James Philpot and Gabriele Giunta. pp. 142–165. Now Publishers. DOI: 10.1561/9781680836875.ch8.

now
the essence of knowledge

Healthcare organizations are an easy target for cybercrime due to their critical and vulnerable infrastructure. Increasing digitalization has led to the emergence of several security challenges. It is crucial to identify these critical challenges, not only from a technical point of view but also from a legal and management perspective. Recognition of the threats that may arise is also important to be able to fight cybercrime. Not just physical and/or cyber threats are relevant but also the combination of both. It is important to understand how they can impact and destabilize health services, and how they are being used by attackers to achieve their aims. This chapter provides a brief introduction to the critical challenges in the healthcare sector and a list of recent security incidents. Five main groups of threats and a critical assets categorization are also presented. Finally, the EBIOS methodology is introduced and used to describe two relevant cyber-physical scenarios of threat.

8.1 Introduction

Over the last decade, cybercrime has been the greatest threat to every sector in the world. Due to its critical and vulnerable infrastructure, the health sector is an easy target for hackers. Moreover, healthcare organizations are highly trusted entities that hold valuable and personal information, meaning that exploiting its vulnerabilities brings huge potential financial and political gain.

Several security challenges emerge from the needs of the healthcare sector. It is important to ensure the security of data without impacting the availability of the healthcare services, as they are crucial to human life. The increasing interconnection of physical and cyber assets of the hospital brings new threats that should be considered to ensure patient safety. Also, legal requirements like GDPR in Europe need to be taken into account to ensure patient data protection and compliance with the regulations.

Being aware of security incidents that have occurred is very important for understanding the risks that healthcare facilities can face. It is also important to know which critical assets are present and their impact on the availability of systems. Only then is it possible to identify and design scenarios that can help recognize threats that a security solution for a healthcare facility must cover. These scenarios should exploit combined physical and cyber threats in the context of cascading attacks, since they are the most complex and interesting threats to cope with.

8.2 Challenges in Healthcare Sector

Nowadays, healthcare structures are equipped with common perimeter precautions and active and predictive cybersecurity solutions. With these cybersecurity systems, the possibility of successfully carrying out an attack on critical assets (for example, on the main IT systems, HIS hospital information system, PACS picture archiving and communication system, LIS laboratory information systems, and other vertical software like for ER-ED) remains very low.

There is no other possibility of breaking the perimeter defenses, even using a physical attack, since it is necessary to connect directly to servers and networks sections that are not accessible from the outside. In this case, access with violence, theft, or other fraudulent access should only be seen as complementary action of a cyberattack.

It is known that hospital or healthcare structures do not work properly without IT systems, in particular the PACS and the LIS, without which it is very difficult to work with radiological images and laboratory tests, making diagnosis and therefore

treatment of patients difficult, or extremely slow. This could be considered an attack damage "multiplier effect."

Therefore, it is essential to face the risk of attacks on hospital IT systems in order to decrease the functioning capacity of hospitals and to absorb patients in the emergency department, in the event of a terrorist attack and consequent maxi-inflow of wounded people. For that, threats can no longer be analyzed solely as physical or cyber. It is critical to develop an integrated approach in order to fight against such combination of threats.

8.2.1 The Protection of Critical Assets—the Point of View of Healthcare Structures Management

The management of Healthcare structures are used to facing complex challenges, such as the typical complexities of the healthcare sector, and a number of internal and external emergencies that may occur and have actually occurred; but the challenge of cybersecurity and physical security is something that in most European hospitals and Healthcare structures there is not yet full knowledge of and is not yet being considered; or perhaps, better expressed, that we are only now beginning to consider as an emerging problem, but are still lacking widespread and shared solutions.

Certainly, the IT sectors of Healthcare structures have, in recent years, had to face a number of malware attack campaigns (the most famous being Wannacry, NotPetya and CryptoLocker) that are not specifically directed to a particular type of structure.

For some hospitals, the damage was greater than expected (for countless causes, such as the diffusion of computer clients of different management and origin), but this had the benefit of putting the structures and management on alert, and considering the problem as a possible threat, like any other.

Only in recent years (mainly in USA and Asia) have attacks specifically targeting healthcare facilities been reported (like orangeworm, kwampirs, medjack). This confirmed a certainty: *Hospitals* are no stranger to malware and ransomware cyber*attacks.*

In some cases, vulnerabilities of medical device systems have been exploited; medical devices, something that was not considered a possibility, likely for cultural reasons, coupled with the fact that the medical device suppliers themselves did not consider an attack possible and were not prepared to deal with the possibility. Indeed, it is necessary to consider the particular market of medical devices:

- Productions in small series, sometimes very small series (for example, in Radiotherapy);

- Highly complex and innovative systems and therefore high costs for research and development;
- Complex sector regulations (MDD, MDR, IVD, IVR), with the need to certify every different model;
- The consequent difficulty of keeping operating systems and antivirus updated.

In recent years, there have been reported numerous local health structures affected by massive ransomware attacks, with the consequence of the total blockade of some departments, such as the emergency room and hospitalizations (!), with the sole exclusion of the "most critical" patients not diverted elsewhere (in danger of life, in other words, negotiable without the help of a computer system). A criminal attack with the explicit request for cash ransom, an operation organized on a larger scale than the typical ransomware already widespread at the level of individual personal computers, more organized as entire networks and computer servers are affected, making entire hospital systems unavailable.

Of course, we do not know the full consequences of the attacks, only what was reported to the press—in some cases, it has been reported that the very few infected computers have been reformatted, and restored, without significant loss of data; in others, the administration admitted that it preferred to pay the ransom after several days. But many operators are convinced that the cases disclosed are only a part of those actually verified and never spread for obvious reasons of bad publicity.

The latest attacks that have been reported in the news took place in October 2019 (USA and Australia). Again, with reference to the world of the United States, the analysis lead experts to believe that hackers are increasingly concentrated on the portals, patients that are increasingly popular, as they are connected with EMR/EHR (Electronic Medical/Health Record). At the same time in Europe, in recent years (at least after the serious attacks on crowded and critical structures like railways, undergrounds, airports), all critical structures are expected to be prepared to be hit by attacks. Until now, attacks using explosives on hospital are documented only in East and Middle East (Egypt, Afghanistan, Pakistan).

In short, there is a need for European structures to be prepared for the worst, in order to deal systematically with these threats, simply because of the obvious consideration that these threats will, sooner rather than later, hit the old continent as well. Without forgetting the considerable latency due to finding suitable solutions and the time necessary to spread them in the structures.

- To understand the reference context (and consequent difficulties and facilities), it is important to consider the particular situation of typical European healthcare structure: Entrances and access control—unlike public offices or

other public buildings, no hospital or healthcare structure has the possibility to restrict access to one or two "single point of entry," nor is the commissioning of check points at a visitor control desk, with the control and filing of identity documents, possible.

The reasons can be many and among these certainly is the fact of not having so far hypothesized the need to protect these buildings from specific attacks (a cultural aspect that is certainly erroneous). We cannot ignore also:

- The considerable inflows—many thousands of people for some European hospital districts;
- The dimensions (hectares) of hospital enclosures, within the urban fabric context, sometimes in historical contexts and historical buildings;
- The simultaneous presence of different organizations—such as universities, with consequent additional inflows of students and various attending people.

- Critical assets—hospital structures are characterized by the presence of a very large number of critical assets, probably of a small size when compared to industrial plants, but with the contemporaneity of a huge number of different types of implants and different specific safety systems (idem—when compared to industrial plants). For example: cryogenic systems, RX systems, handling radioactive isotopes, big magnetic field systems, gas tanks, hyperbaric systems and so on, And with the greatest difficulties deriving from the co-presence of large number of people: patients, visitors, students (the largest being some 10–20 thousand people);
- Separate management of IT assets (IT department) and medical devices assets (clinical engineering department), for cultural and historical reasons; this separation was culturally motivated in the last century for the absence of networked medical devices systems, at least those few who were computerized. Nowadays, the opposite happens: very few medical devices are not computerized and not connected to the IT network. Without denying the specific skills of the two staff (IT and CE), there is a strong need for coordination in management for cybersecurity aspects;
- Emergency Plans—all the hospital structures have a well-established habit of confidence and have long established various emergency plans, maxi-influx of patients, evacuation of patients, etc; the staff is therefore trained for even disastrous events and can therefore also face the consequences caused by attacks;
- Provision of video surveillance systems—due to the difficulties of inserting access controls, many hospital structures are equipped with several video surveillance systems, videocameras and a videoserver, mainly for crime prevention purposes (only with video-recording).

8.2.2 The Protection of Critical Infrastructures for the Healthcare Sector in Europe: Legal Challenges

8.2.2.1 The EU legal framework for the protection of critical infrastructures

The legal framework concerning security and the protection of critical infrastructures in Europe is characterized by its complexity. This is due to the presence of heterogeneous laws differing in scope (applicable at national or EU level) and matter (ranging from civil protection law, security laws, privacy laws, etc.) applicable to the subject matter. Moreover, the protection of critical infrastructures encompasses two parallel aspects, the physical and the cyber. Each aspect corresponds to what is commonly referred to as "Critical Infrastructure Protection" (CIP) and "Critical Information Infrastructure Protection" (CIIP) (1). This parallel is also evident in the EU legislation concerned with the topic[1] [1]. CIP and CIIP are regulated by respective directives (legislative acts setting out only a goal that all MS must achieve via national laws). The most important piece of legislation concerning CIP is the ECI Directive [2] dealing with the 'European Critical Infrastructures' (ECI). The most relevant legislation dealing with CIIP is the NIS Directive [3] the aim of which is to set up measures for a high common level of security of network and information systems across the Union.[2]

8.2.2.2 Challenges originating from the EU legal framework

With regard to the CIP, the status of protection of national healthcare critical infrastructure results to be "disparate" [4] among the MS, which is due to the regulation of security by national laws. As a consequence, some MS (e.g., the Netherlands [5]) do not explicitly mention "healthcare" as a sector worthy of protection under national CIP legislations.[3]

---

1. The outline of the legislative developments of CIP and CIIP legislation in Europe falls outside the purposes of the present article. For an overview of the main pieces of legislation and policy-making instruments in the EU, see A. Kasper, A. Antonov, "Towards Conceptualizing EU Cybersecurity Law" (2018).

2. The ECI Directive has been approved in 2008 and, although devoted to CIP, it applies only to CI that fall under the definition of 'European Critical Infrastructures. Member States' national Critical Infrastructures fall outside the scope of the ECI Directive. The ECI Directive remains, however, a key reference within the EU CIP framework as it provides meaningful legal definitions on CI (such as, the definition of Critical Infrastructure, under art. 2). Furthermore, the ECI Directive does not consider the healthcare sector as worthy of being protected, while, the NIS Directive considers the healthcare sector as falling within the scope of the legislation.

3. France is an example of a Member State that has included the healthcare within CIP legislation. The French Defence Code ("Code de la Défense") considers critical infrastructures as the ones that are vital for the maintenance of the social and economic progress. It considers 12 sectors for critical infrastructures and includes healthcare.

With regard to the CIIP, the NIS Directive represents an important step towards reaching a common level of cyber resilience across the EU as it has set, among others, security and notification requirements for operators of essential services (OES) (i.e., "healthcare providers" for the healthcare sector) [6]. Nonetheless, many challenges—concerning the implementation and the interpretation of the law by the EU MS—await to be addressed. For example, many MS have not respected the deadline (9 May 2018) for the adoption of national laws implementing the NIS Directive [7]. This has implied uncertainty for many stakeholders willing to put in place the necessary measures foreseen by the EU law and national law. Furthermore, in order to identify the OES (such as hospitals, clinics, etc.) [8]. MS have adopted methodologies that have proven to be heterogeneous. [9] For instance, some MS have identified a very high number of OES (for instance, Finland) [9], whereas others have identified less.[4] Such difference in numbers may have a negative impact on the coherent application of the NIS Directive within the Union, with possible consequences for the whole internal market and the effective handling of cyber-dependencies [9]. Moreover, the Directive states that OES have to notify incidents "having a significant impact to the continuity of the essential services they provide" [10]. Since the purpose of the Directive is to provide a level of minimum harmonization [11], the body of the text does not specify what "significant impact" means—leaving MS to provide their own definition. This may consequently lead to fragmentation among operators across Europe who will have to follow their respective national approaches with regard to incident notification.[5] Similarly, the Directive does not granularly define the security measures that OES must adopt "to prevent and minimize the impact of incidents affecting the security of the network and information

4. To give an example, according to the data provided by the EC Report [8], Finland has identified 10.897 OES for all NISD sectors—due to the high number of OES identified for the healthcare sectors (see [9], p. 27, footnote 8). This number appears to be very high, considering that the sum of all OES identified by all the other MS for all the NISD sectors is 4.925. To give a comparative example with another MS, Italy has identified 553 OES for all NISD sectors [9]. Furthermore, according to the preliminary documentation available, Italy has identified 326 OES for the healthcare sector—see Presidenza del Consiglio dei Ministri. Intesa ai sensi dell'articolo 4 del decreto legislative 18 maggio 2018, n. 65, recante attuazione della direttiva (UE) 2016/1148 del Parlamento Europeo e del Consiglio, 6 luglio 2016: misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi dell'Unione, tra il Governo e le Regioni e Province autonome di Trento e Bolzano, sullo schema di decreto del Ministero della salute (version of 7 November 2018, available at: www.statoregioni.it).

5. While this problem remains, for the sake of completeness it is also true that the European Commission is putting in place also coordinative efforts to tackle this kind of issues. As an example, see the European Commission guidelines on Incident Reporting, which have been drafted within the framework of a Cooperation Group composed by Member States' experts. European Commission, Reference document on Incident Notification for Operators of Essential Services. Circumstances of notification, CG Publication (February 2018). To be noted that the document is not binding.

systems" [12]. This may bring further fragmentation among healthcare operators in Europe.

Although the challenges mentioned above might appear copious, it should also be stressed that during recent years, the EU has put in place several legislative measures to increase the level of CIP in Europe [13]. While there is still enough room for improvement, legislative instruments such as the ECI Directive and the NIS Directive have served as a catalyst in many Member States to pave the way for real change in the institutional and regulatory landscape of critical infrastructures. Further non-binding guidance at an EU level and the already established coordinative mechanisms between Member States (most importantly the recently established NIS Cooperation Group [14]) could be beneficial to achieve a higher degree of coherence for CIP, and especially CIIP, in Europe.

8.3 Recent Security Incidents

According to the World Health Organization (WHO) definition "Hospitals complement and amplify the effectiveness of many parts of the health system, providing continuous availability of services for acute and complex conditions" [15]. They are an essential element to health systems as they support care coordination and integration and play a key role in supporting other healthcare providers, such as primary health care, community outreach and home-based services. For these reasons, cyber and physical attacks against hospitals, patients, healthcare workers, and facilities have been on the rise worldwide [16].

More specifically, in terms of cyberattacks, it has been reported that 81% of 223 healthcare organizations surveyed and >110 million patients in the US had their data compromised in 2015, with only 50% of the providers thinking that they could protect themselves from cyberattacks [17]. In addition, between 2009 and 2018, there have been 2.546 healthcare data breaches that resulted in theft/exposure of 189,945,874 records [18]. In the healthcare sector, hacking and malware (including ransomware) are the leading attack type of health data breaches [19]. These data breaches result in large financial losses, but also in loss of reputation and reduced patient safety.

Several cyberattacks in the healthcare sector have been reported and some examples of such incidents are presented below:

- 2017 WannaCry attack infected more than 300,000 computers across the world demanding that users pay bitcoin ransoms. The WannaCry cyberattack targeted the UK's National Health Service (NHS). By exploiting a Windows vulnerability, the hackers managed to infect at least 16 health centers and

200,000 computers, which led to the cancellation of nearly 20,000 appointments and paralyzed more than 1,200 pieces of diagnostic equipment [20]. Moreover, according to US media, the Presbyterian Medical Centre shut down for 10 days until it paid a $17,000 ransom [21].

- Medical Device Hijack (Medjack) is another known attack that injects malware into unprotected medical devices to move laterally across the hospital network [22]. Between the first detection of Medjack in 2015 and now, there have been many variations of the attack with several hospitals' medical devices, including X-ray equipment, Picture Archive and Communications Systems (PACS), and Blood Gas Analyzers (BGA), etc., having been attacked. The attacker establishes a backdoor within the medical device, and almost any form of manipulation of the unencrypted data stored and flowing through the device is possible.
- It was reported in the press that in January 2019 hackers performed a ransom attack in a heart specialist clinic in Melbourne, where the hackers hit patient files [23]. As a result, staff was unable to access some patient files for more than three weeks. The Clinic could have mitigated the impact if data was properly and fully backed and if they were investing consistently in IT security.
- A billing company based in the USA, which operates the online payment system used by a network of 44 hospitals in the USA, discovered that some of its databases that contained 2,652,537 patients' records had been compromised in 2018. Upon discovery of the breach, access to data was terminated and forensic specialists were hired to review the incident, secure affected databases, and improve security controls (HIPAA, 2018).
- In 2019, it was revealed that a billing services vendor American Medical Collection Agency was hacked for eight months between August 1, 2018, and March 30, 2019. Since the breach was revealed, at least six covered entities have come forward to report their patient data was compromised by the hack. So far, up to 25 million patients from were affected [24].
- 128,400 records were affected by a sophisticated phishing incident that happened at New York oncology and hematology clinic. More specifically, fourteen employee email accounts clicked on phishing emails, which exposed health information in the email accounts. The clinic hired forensic specialists to assess the breach and types of data affected. Moreover, improvements to data security following the incident included active monitoring of affected systems, regular password resets, additional employee training, and new email protocols [19].

On a similar line, in the USA, the U.S. Department of Health and Human Services has developed a breach portal, the aim of which is to gather information

on healthcare sector physical and cyber breaches. According to this portal, in 2019, 407 entities have been attacked and 40.267.487,00 individuals have been affected. In addition, there have been identified four main types of breaches hacking/IT incident (61%), improper disposal (1%), loss (3%), theft (8%), and unauthorized access/disclosure (28%), with the hacking/IT incidents affecting a total of 35.381.048,00 individuals and the unauthorized access/disclosure affecting 4.551.487,00 individuals [25].

In addition, physical attacks deprive people of urgently needed care, endanger healthcare providers, and undermine health systems. The WHO created the Attacks on Health Care initiative to systematically collect evidence on attacks on healthcare, to advocate for the end of such attacks, and to promote best practices for safeguarding healthcare from attacks [26]. The initiative is global, but its main geographic focus is at the country level. According to this initiative, in 2018 the healthcare sector (19 countries) was attacked 388 times and this caused 322 deaths and 425 injuries. The attacks were mainly bombings (51%), shootings (14%), threats of violence (9%), etc. Several physical attacks, such as violence against physicians (including hostage taking), fires, shootings, bombings against infrastructures, have been reported all around the world and some examples of such incidents are described below:

- While a nurse was examining a female patient, the accompanying Roma (gypsies) group attacked her and injured her face. The incident happened at the Salamina Island Health Center, Greece (POEDIN, 2018). Similar incidents have been reported to other countries, such as Cyprus [27], Louisiana [28], Kolkata [29], Australia [30], etc.
- A UK A&E registrar was held hostage when she had gone to check on a young patient, who was having a mental health episode after taking drugs. Unfortunately, the patient had managed to hide a pair of scissors, which she pulled out before backing the doctor into a corner. The police were eventually called and restrained the patient [31].
- A woman opened fire at a flat opposite a Catholic Hospital and then inside the hospital in the south-western town of Lorrach in Baden-Wuerttemberg, Germany, killing at least three, including one child, and wounding several patients before police shot her dead [32].
- A gunman killed six patients in a hospital waiting room in the Czech city of Ostrava and drove off. Police launched two helicopters to search for him, once they had obtained pictures of the suspect from security cameras. When one of the helicopters was flying over the car, the man shot himself in the head and later died of his injuries [33]. It has been reported that shooting rates in hospitals, increased from 9 per year from 2000 to 2005 to 17 per year

from 2006 to 2011, according to a study published in 2012 in the Annals of Emergency Medicine [34].

Physical or cyber incidents like the above could affect the healthcare services provision and could cause overwhelming pressure, such as loss of infrastructure or a massive patient surge. Hospitals not only provide care services but they are also the last resort for disaster victims seeking care and represent an icon of social security, connectivity, and community trust [35]. Thus, in this context, it is fundamental for a hospital to remain resilient, maintain the level of provided care, and be able to scale up its service delivery in any given emergency situation.

8.4 Threat and Risk Analysis

Threats are actions that can negatively impact valuable resources of an organization. Typically, threats exploit vulnerabilities of the system, i.e., take advantage of some weaknesses in the system to trigger an undesired outcome, as damage or loss of an asset.

To guarantee the safety of the systems, it is very important to determine the possible root causes of threats. According to ENISA [36], we can identify five main groups of threats faced by healthcare organizations:

- **Malicious actions** that are deliberate acts performed by an internal or external person or organization to destroy or steal data or sabotage the system. Malware (e.g., virus, ransomware), hijacking, social engineering, medical device tampering, device and data theft are examples of malicious actions;
- **Human errors** that are related with misconfiguration or improper use of devices and information systems, and incorrect execution of processes;
- **System failures;**
- **Supply chain failures** that are responsibility of third-party suppliers, for example, power suppliers, medical device manufacturers, etc.;
- **Natural phenomena.**

The person or entity who is responsible for conducting these threats (threat actor) can also be classified according to its role:

- **Insider threat actor:** this category is composed of the hospital staff (physicians, nurses, administrative staff, etc.);
- **Malicious patients and guests;**
- **Remote attackers:** actors who are not physically in the hospital;
- **Other causes:** such as environmental or accidental equipment failure.

Table 8.1. Asset categories.

Category	Example
Specialist personnel	Employees, Persons with special functions, etc.
Buildings and Facilities	Main and ancillary buildings, Technical buildings, Power and climate regulation systems, temperature sensors, medical gas supply, room operation, automated door lock system, etc.
Identification Systems	Tags, bracelets, badges, biometric scanners, CCTV (video surveillance), RFID services, etc.
Networked Medical Devices	Mobile devices (e.g., glucose measuring devices), wearable external devices (e.g., portable insulin pumps), implantable devices (e.g., cardiac pacemakers), stationary devices [e.g., computed tomography (CT) scanners], support devices (e.g., assistive robots), etc.
Networking Equipment	Transmission media, network interface cards, network devices (e.g., hubs, switches, routers, etc.), telephone system, etc.
Interconnected Clinical Information Systems	Hospital information system (HIS), Laboratory information system (LIS), Pharmacy information system (PIS), Picture archiving and communication system (PACS), blood bank system, etc.
Mobile Client Devices	Mobile clients (e.g., laptops, tablets, smartphones), mobile applications for smartphones and tablets, alarm, and emergency communication applications for mobile devices, etc.
Remote Care System Assets	Medical equipment for tele-monitoring and tele-diagnosis, medical equipment for distribution of drugs and telehealth equipment (cameras, sensors, telehealth computer system for patients to register their physiological measurements themselves, etc.)
Data and records	Clinical and administrative patient data, financial, organizational and other hospital data, staff data, vendor details, tracking logs, etc.
Operating resources	Medicinal products, medical consumables, Laundry supply, Sterile supply, Food supply, etc.

Organizations have a wide range of entities, the assets, which are essential for their operation. Thus, it is crucial to identify the critical assets in the hospital to ensure the patients' safety. Table 8.1 presents the list of critical asset categories.

A cyber-physical attack scenario is a combination of threats, vulnerabilities, and assets. In the next section, we will describe nine different relevant attack scenarios against critical health infrastructures.

8.5 Scenarios of Threat

The definition of the cyber-physical scenarios of threat, to be clearer, should follow a methodology. Several methodologies for risk assessment exist, such as ISO 31000:2018, IEC 31010: 2019, ISO27005, etc. EBIOS methodology is compliant with the standards, as ISO3100, ISO/IEC 27001, ISO/IEC 15408, etc., and it is commonly used to describe the scenarios of threat. EBIOS [37] is a French acronym meaning Expression of Needs and Identification of Security Objectives (Expression des Besoins et Identification des Objectifs de Sécurité) and was developed by the French Central Information Systems Security Division. EBIOS is used to assess and treat risks related to information systems security (ISS). It can also be used to communicate this information within the organization and to partners and therefore assists in the ISS risk management process since it is compliant with major IT security standards. EBIOS can be employed in different fields (using the appropriate techniques and knowledge bases) [38], even if it was initially designed for information security. To apply EBIOS in a specific field, it is generally sufficient to adapt the terminology and exploit the techniques and the knowledge bases specific to that field concerned if the knowledge does not seem to be applicable or understood (primary assets, considered criteria, potential impacts, etc.).

EBIOS uses a progressive risk management approach (see Figure 8.1): it starts in the major missions of the object under study (highest level) and goes to the business functions and techniques (lowest level), studying possible risk scenarios [39]. It aims to obtain a synergy between compliance and scenarios, positioning these two complementary concepts in the best way, i.e., where they bring the highest value. The compliance approach is used to determine the security base of the scenarios,

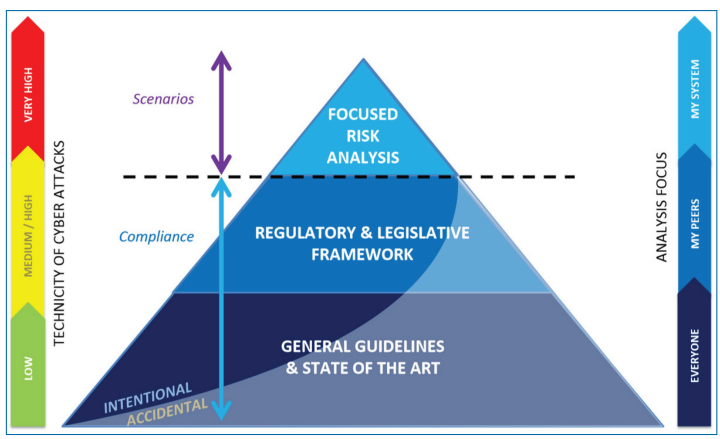

Figure 8.1. Digital risk management pyramid.

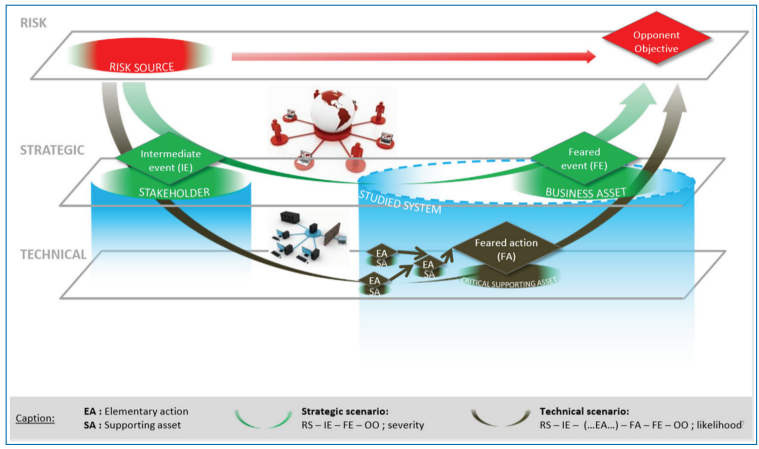

Figure 8.2. Cyber risk scenario.

particularly to develop targeted or sophisticated scenarios. This assumes that accidental and environmental risks are treated a priori by the compliance approach. Thus, scenario risk assessment focuses on intentional threats.

The EBIOS method consists of five iterative workshops (Figure 8.2):

- **Scope and Security Baseline:** the first workshop aims to identify the scope of the study, the workshop participants and the time frame. During this workshop, essential and support assets and business values should be listed. Threat events and their impact should be identified at this stage. The security baseline should also be defined. This first workshop follows the compliance approach: it corresponds to the first two stages of the digital risk management pyramid.
- **Risk Sources:** in the second workshop, the risk sources and their high-level objectives should be identified and characterized.
- **Strategic Scenarios:** in this workshop, it is possible to have a clear vision of the ecosystem, which allows to build high-level scenarios of threat. They represent the paths of attack that a risk source can take to achieve its objective. These scenarios are conceived taking into account the ecosystem and the business values of the object, and they are evaluated in terms of severity. At the end of the workshop, it is already possible to define security measures on the ecosystem.
- **Technical Scenarios:** the purpose of this workshop is to build scenarios containing the technical procedures that can be used by the risk sources to carry out the strategic scenarios. This workshop adopts a similar approach of the previous one but focuses on the critical assets. Then, the likelihood of the technical scenarios should be evaluated.

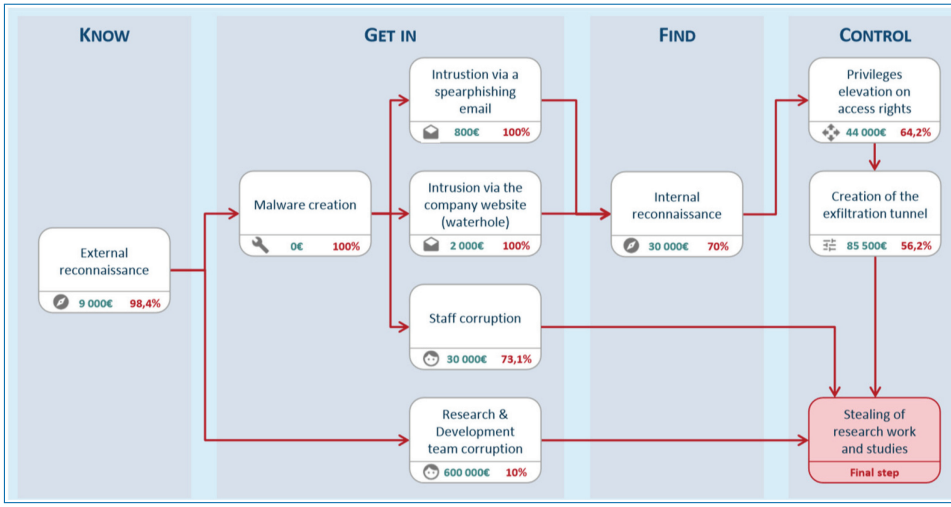

Figure 8.3. Example of a technical scenario description using attack graphs.

- **Risk Treatment:** in the last workshop, all the risks studied in the previous workshops are considered to define the risk treatment strategy. Then, a set of safety measures are defined and included in a continuous improvement plan. In this workshop the residual risks are also summarized and the risk monitoring framework is defined.

Therefore, we can summarize the construction of a cyber risk scenario as described in Figure 8.3.

A technical scenario can be represented in the form of an attack graph to visualize the operational modes planned by the attacker to achieve its objective. An example of an operational scenario is given in Figure 8.3.

The proposed model consists of 4 phases:

- **KNOW:** set of targeting, reconnaissance, and external discovery activities conducted by the attacker to prepare his attack and to increase his chances of success (ecosystem mapping, information on key people and systems, search and evaluation of vulnerabilities, etc.). Such information shall be collected according to the determination and resources of the attacker: intelligence, economic intelligence, exploitation of socio-professional networks, direct approaches, specialized meetings for information inaccessible in open source, etc.
- **GET IN:** all activities carried out by the attacker to digitally or physically introduce either directly and frontally into the target information system or in its ecosystem for a rebound attack. The intrusion is usually carried out

through "border" goods that serve as the entry points due to their exposure, for example, user post connected to the Internet, maintenance tablet of a provider, TV-maintained printer, etc.
- **FIND:** internal recognition of networks and systems, localization, elevation, and persistence, which allows the attacker to locate the desired data and material. During this phase, the attacker usually seeks to remain discreet and erase his traces.
- **CONTROL:** all the data and media activities found in the previous stage. For example, in the case of sabotage, this phase includes the activation of the active load, for example, ransom; in the case of an espionage operation aimed at ex-filtering emails, it may be necessary to establish and maintain discrete capacity for data collection and exfiltration.

After the definition of the technical scenario, it is important to evaluate its overall likelihood, which reflects its probability of success or feasibility. To begin, the elemental likelihood of each action in the scenario should be assessed. This can be estimated by the judgment of an expert or using metrics. Then, the overall likelihood of the scenario is evaluated from the elementary likelihoods.

Three different approaches can be considered to rate the likelihood of the operational scenarios:

- **Express method:** direct quotation of the likelihood of the scenario;
- **Standard method:** rating of the "probability of success" of each elemental action of the scenario, from the point of view of the attacker;
- **Advanced method:** in addition to the "probability of success," rating of the "technical difficulty" of each elementary action of the scenario, from the point of view of the attacker.

We will consider the standard method. The following scale will be used to determine the probability of success of each elementary actions (Pr(EA)) [40]:

- **4 – Almost certain:** Probability of near-certainty >90%;
- **3 – Very High:** Very high probability of success >60%;
- **2 – Significant:** Probability of significant success >20%;
- **1 – Low:** Success probability low <20%;
- **0 – Very Low:** Success probability very low <3%.

The overall likelihood score of the scenario can be evaluated using the following rule:

$$Index\_\Pr(EA_n) = Min\{Pr(EA_n),\ Max(Index\_Pr(EA_{n-1}))\}$$

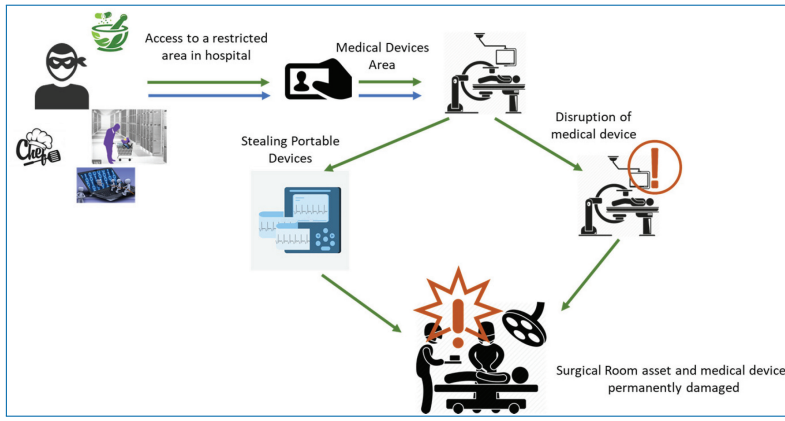

Figure 8.4. Medical devices attack: sketch.

The idea is to evaluate step by step an intermediate cumulative probability index from the elementary action "EA_n" of a node n and the cumulative indices of the previous node n−1. The overall probability of success index (final step) is obtained by taking the highest intermediate cumulative probability index among the procedures that lead to the final step. It corresponds to the mode(s) operating(s) whose chance of success seems the highest.

8.5.1 Scenario Example 1: Cyber-physical Attack to on Medical Devices

Medical devices are an important asset in healthcare infrastructure. They improve the quality of life of the patients, but they are also a source of threat due to the increasing connectivity to all parts of the hospital. Several attacks on medical devices have been reported during the last years. For example, in 2018, security researchers demonstrated that they have founded security weaknesses in Medtronic pacemakers that leaves the life-saving device vulnerable to hackers and puts patients at risk.[6] Figure 8.4 shows an example of medical devices attack.

An attacker, in order to influence treatment outcome or for financial gain, can obtain physical or remote access to medical device and use reverse engineering to identify a vulnerability and exploits it. Then, the attacker can take advantage of the exploit of the medical device to alter its software and/or cause a disruption in health systems, which can potentially harm patients and/or staff (see Figure 8.5).

Thus, in this case, after the vulnerability scanning, the medical device system is changed or a denial of service is launched to interrupt the health system (Figure 8.6).

6. https://www.cnbc.com/2018/08/17/security-researchers-say-they-can-hack-medtronic-pacemakers.html

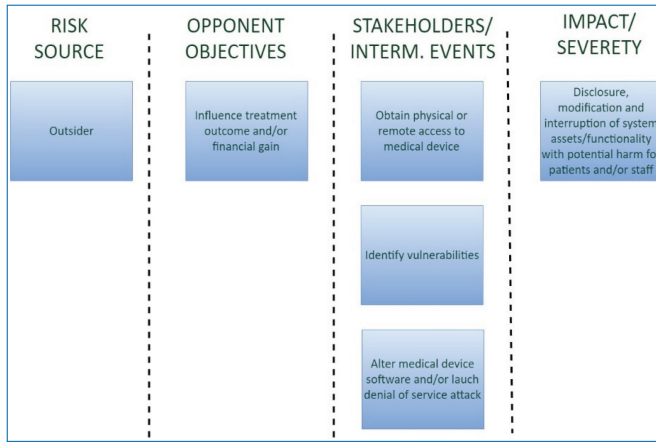

Figure 8.5. Medical devices attack: strategic scenario.

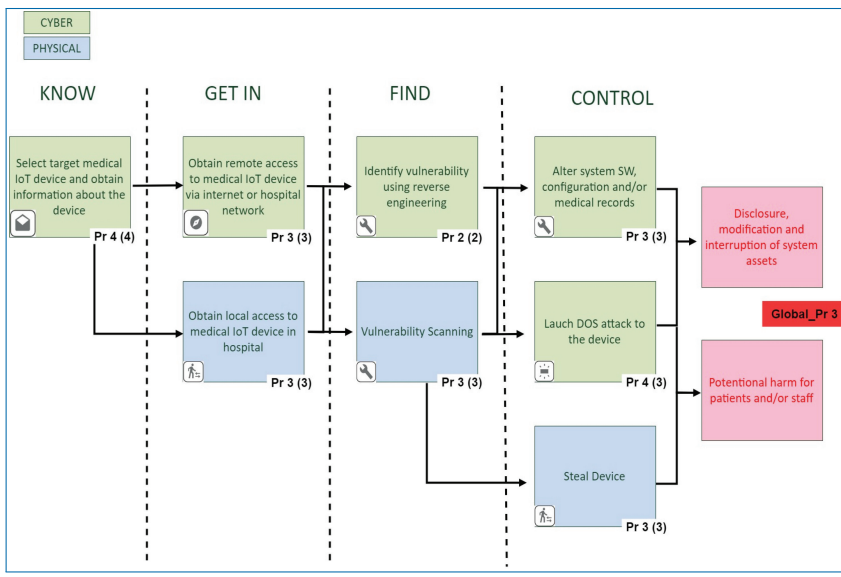

Figure 8.6. Medical devices attack: technical scenario.

The attacker can also steal the device. This will cause a disclosure, modification, and/or disruption of the medical device which will impact patient and/or staff safety. This attack has a very high probability of success (Pr 3).

Several assets are compromised in this type of scenario, for example: Buildings and Facilities, e.g., technical room; Identification Systems, e.g., badge (physical), credentials (cyber); Networked Medical Devices, e.g., Wearable Medical IoT; Networking Equipment, e.g., Router; Interconnected Clinical Information Systems, e.g., PACS; and Data and records, e.g., patient data.

Some practices can be considered to minimize the impact of this attack, which are:

- Establish and maintain communication with vendors security teams;
- Implement access controls for vendor support staff;
- Implement security operations practices for devices;
- Develop and implement security measures for a devices network.

8.5.2 Scenario Example 2: Cyber-physical Attack to Cause a Hardware Fault

As any critical infrastructure, the interruption of services in healthcare facilities has a huge impact on patients. Attackers can take advantage of this feature of hospitals for financial gain, or for attention or other motives. A sketch of an attack that can cause a hardware fault is represented in Figure 8.7.

The usual aims of this kind of attack are extortion, sabotage, or even intimidation. Therefore, the attacker is only concerned with finding a way to cause system unavailability, damaging the system permanently (or not) and without worrying whether the patient will be at risk or not (Figure 8.8).

The attacker can use social engineering to obtain information about the hospital infrastructure. With this knowledge, he/she could exploit the system's vulnerability, gain administrator privileges, and cause a hardware failure (Figure 8.9). The unavailability of the healthcare system can cause death or serious injury to patients, because the assistance services cannot work properly with hardware failures.

Some of the affected assets in this scenario are: Networked Medical Devices, e.g., medical devices that communicate with central system; Networking Equipment, e.g., externally accessible server; Interconnected Clinical Information Systems,

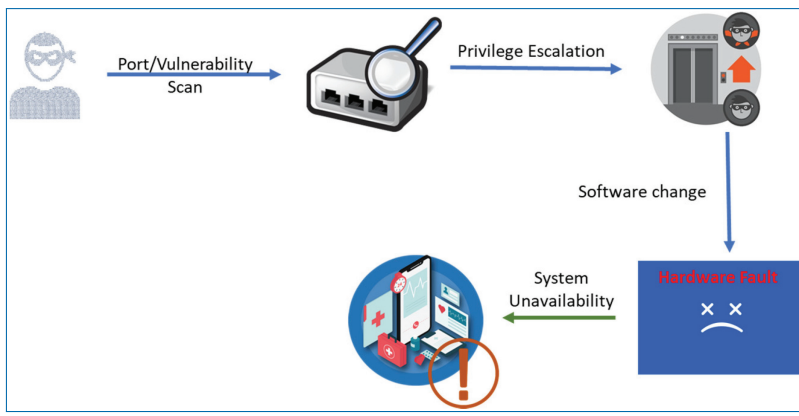

Figure 8.7. Hardware fault attack: sketch.

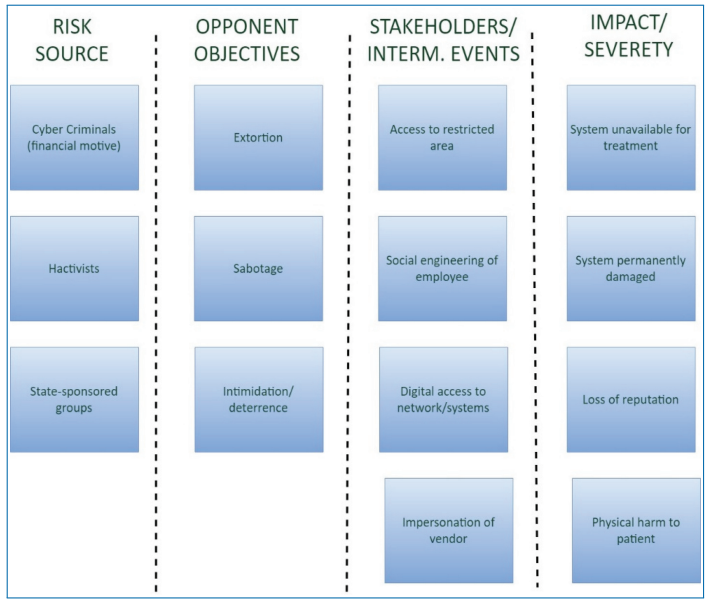

Figure 8.8. Hardware fault attack: strategic scenario.

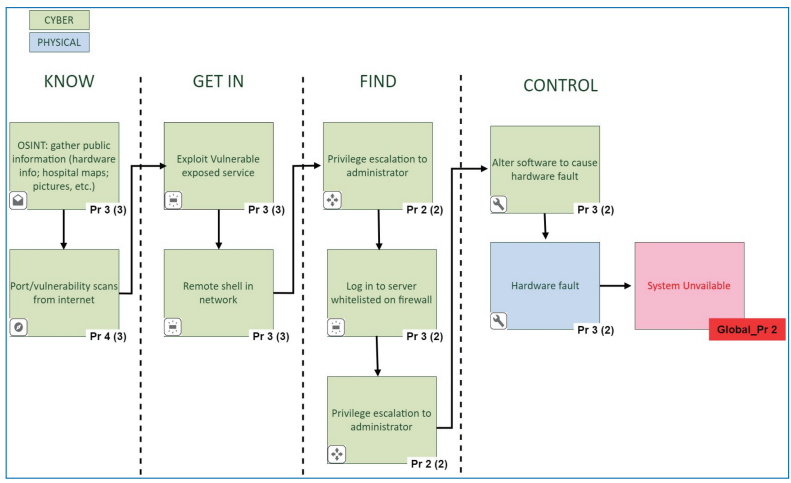

Figure 8.9. Hardware fault attack: technical scenario.

e.g., PACS; Mobile Client Devices, e.g., mobile applications for smartphones and tablets; Remote Care System Assets, e.g., medical equipment for tele-monitoring; Data and records, e.g., health records.

It is important to note this attack could be, at least partially, mitigated if:

- An appropriate intrusion detection system had been deployed to detect early the attack;

- Exists an endpoint security system that prevents the connection of unknown devices;
- The staff had been trained to understand the threat, recognize suspicious emails, and never open email attachments from unknown senders;
- Privileged access management tools to report access to critical infrastructures had been deployed;
- Devices have been patched after the patches have been validated and distributed by medical device manufacturer;
- A restricted and rigid access controls policy for clinical and vendor support staff (including remote access and monitoring of vendor access) had been implemented.

8.6 Conclusion

Healthcare organizations are a fruitful target for crime. The increasing integration of cyber and physical systems and connected devices in its environment brings new challenges to these organizations, especially from a security perspective. To combat the threats that emerge from this healthcare technology era, hospitals need to implement cyber and physical controls, reducing the risks that can cause harm to people, property, and environment.

In this chapter, we have presented the main security challenges in the healthcare environment, not only from a structure management point of view but also from a legal perspective. A survey about the recent security incidents was performed in order to understand the type of vulnerabilities exploited by the attackers in the health sector. Inspired by this research, five main groups of threats and a critical assets categorization were defined. Finally, using EBIOS methodology, that is also briefly described, two combined cyber and physical scenarios of threat are described. All this information should clarify and alert the reader to the security issues faced by healthcare facilities in this smart hospital's era.

Acknowledgments

This work has received funding from European Union's H2020 research and innovation programme under SAFECARE Project, grant agreement no. 787002.

References

[1] Dunn, M. Understanding Critical Information Infrastructures. [book auth.] M. Dunn and V. Mauer. International CIIP Handbook vol. 2. 2006.

[2] (Directive), Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [2008] L 345/75 (ECI.
[3] (Directive), 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 [2016] L 194/2 (NIS).
[4] THREATS. An Analysis of Critical Infrastructure Protection Measures Implemented within the European Union: Identifying which European Member States includes the Health Sector as part of Critical National Infrastructure and which facets of Health Infrastructes are. 2014.
[5] Biasin, E., *et al.* SAFECARE Deliverable 3.9 – Analysis of ethics, privacy, and confidentiality constraints. 2018.
[6] NIS Directive, Annex II.
[7] Howard, Casey. 20 EU Member States haven't implemented the NIS Directive. *itgovernance.eu.* [Online] 22 May 2018. [Cited: 3 January 2020.] https://www.itgovernance.eu/blog/en/20-eu-member-states-havent-implemented-the-nis-directive.
[8] Art 5 NISD.
[9] Commission, European. *Report from the Commission to the European Parliament and the Council Assessing the Consistency of the Approaches Taken by Member States in the Identification of Operators of Essential Services in Accordance with Article 23(1) of Directive 2016/1148/EU on.* 2019.
[10] NIS Directive, art 14(3).
[11] NIS Directive, art 3.
[12] NIS Directive, art 14(2).
[13] Kasper, A. and Antonov, A. Towards conceptualising EU cybersecurity law. 2018.
[14] NISD, art 11.
[15] World Health Organisation. [Online] 2019. [Cited: 15 09 2019.] https://www.who.int/hospitals/en/.
[16] International Committee of the Red Cross (ICRC). Health Care in Danger: Making the Case. *International Committee of the Red Cross (ICRC).* [Online] 2011. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi7i_XttvjlAhWXxcQBHbGNDpoQFjABegQIAxAC&url=https%3A%2F%2Fshop.icrc.org%2Ficrc%2Fpdf%2Fview%2Fid%2F2033&usg=AOvVaw2mlBEe7xYmGywa0Gea9edg.
[17] KPMG. Health care and cyber security: increasing threats require increased capabilities. [Online] 2015. https://assets.kpmg/content/dam/kpmg/pdf/2015/09/cyber-health-care-survey-kpmg-2015.pdf.

[18] HIPAA. HIPAA Journal. *Healthcare Data Breach Statistics.* [Online] 2018. https://www.hipaajournal.com/healthcare-data-breach-statistics/.

[19] —. HIPAA Journal. *Largest Healthcare Data Breaches of 2018.* [Online] 2018. https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2018/.

[20] Perlroth, N.; Sanger, D.E. The New York Times. [Online] 2017. https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html.

[21] Stormshield. Top 5 cyberattacks against the health care industry. [Online] 2019. https://www.stormshield.com/top-5-cyberattacks-against-the-healthcare-industry/.

[22] Hei X., Du X. Conclusion and Future Directions. In: Security for Wireless Implantable Medical Devices. *SpringerBriefs in Computer Science.* 2013.

[23] Martin L. The Guardian. [Online] 2019. https://www.theguardian.com/technology/2019/feb/21/hackers-scramble-patient-files-in-melbourne-heart-clinic-cyber-attack.

[24] Healthitsecurity. The 10 Biggest Healthcare Data Breaches of 2019, So Far. [Online] 2019. https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2019-so-far.

[25] U.S. Department of Health and Human Services. Breach Portal. [Online] 2019. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

[26] World Health Organisation. Health Systems. [Online] 2019. [Cited: 01 09 2019.] http://www.euro.who.int/en/health-topics/Health-systems/pages/health-systems.

[27] OFFSITE. OFFSITE. 27 χρονοςεπιτέ ϑηκε σε γιατρούς στο Νοσοκομείο Λάρνακας. [Online] 2017. https://www.offsite.com.cy/articles/eidiseis/topika/231890-27hronos-epitethike-se-giatroys-sto-nosokomeio-larnakas.

[28] Nurse. Nurse Dies After Being Attacked By Mental Health Patient – Manslaughter Charges. [Online] 2019. https://nurse.org/articles/nurse-attacked-by-patient-dies-manslaughter/.

[29] Times of India. Kolkata doctor beaten up after Garden Reach child's death. [Online] https://timesofindia.indiatimes.com/city/kolkata/doctor-beaten-up-after-garden-reach-childs-death/articleshow/69656632.cms.

[30] ZeroToleranceWorldwide. Patient charged with attempted murder after firing police officer's gun in Canberra Hospital. [Online] 2019. http://zerotoleranceworldwide.com/2018/07/19/patient-charged-with-attempted-murder-after-firing-police-officers-gun-in-canberra-hospital/.

[31] The Guardian. Violence in the NHS: staff face routine assault and intimidation. [Online] 2019. [Cited: 11 12 2019.] https://www.theguardian.com/society/2019/sep/04/violence-nhs-staff-face-routine-assault-intimidation.

[32] The Times. Woman kills 3 in hospital shooting spree. [Online] 2010. https://www.thetimes.co.uk/article/woman-kills-3-in-hospital-shooting-spree-n9q9nbhws9b.

[33] BBC. Czech shooting: Gunman kills six at hospital in Ostrava. [Online] 2019. https://www.bbc.com/news/world-europe-50725840.

[34] Kelen, Gabor D. *et al.* Hospital-Based Shootings in the United States: 2000 to 2011. 2012, vol. 60, 6, pp. 790–798.

[35] World Health Organization. Hospital Safety Index: Guide for Evaluators. [Online] 2015. [Cited: 10 09 2019.] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwi_tdq7n_kAhVE2aQKHVZfBbkQFjAAegQIAxAC&url=https%3A%2F%2Fwww.who.int%2Fhac%2Ftechguidance%2Fhospital_safety_index_evaluators.pdf&usg=AOvVaw3Jb3x3xUgBh-IK84EtnKD8.

[36] ENISA. Smart Hospitals: Security and Resilience for Smart Health Service and Infrastructures. [Online] 2016. [Cited: 23 April 2019.] https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals.

[37] —. EBIOS Risk Manager: Guide Method. [Online] 2018. [Cited: 23 April 2019.] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_ebios.html.

[38] EBIOS, Club. EBIOS: the risk management toolbox. [Online] 09 05, 2018. [Cited: January 23, 2020.] https://club-ebios.org/site/wp-content/uploads/productions/EBIOS-GenericApproach-2018-09-05-Approved.pdf.

[39] ANSSI. EBIOS risk manager. [Online] November 2019. [Cited: January 23, 2020.] https://www.ssi.gouv.fr/uploads/2019/11/anssi-guide-ebios_risk_manager-en-v1.0.pdf.

[40] ANSSI. EBIOS Risk Manager, Le Supplément. [Online] January 31, 2019. https://www.ssi.gouv.fr/uploads/2018/10/fiches-methodes-ebios_projet.pdf.