A Cybersecurity Threat Model for a Combined Cyberattack against Hospitals and Terrorist Attack in Spain

Oxford University – Universidad Autónoma de Madrid
Project Report

CONSULTANTS:

Lucas Kello (Principal Consultant)
Ivan Martinovic
Martin Strohmeier
Florian Egloff

Academic Coordinator (UAM): Raquel Galindo Dorado

1. INTRODUCTION

Hospital cybersecurity is a global concern. According to an investigation by Pulse magazine, health record security breaches in the United Kingdom's at National Health Service rose 20 percent in the last year. Data from 55 hospitals indicated breaches included records dumped in public places, records given to the wrong patient and patient data given to relatives without permission. In 2015 alone, more than 94 million U.S. health records were compromised, costing affected institutions approximately $46 billion. According to Experian's 2014 Data Breach Industry Forecast, the healthcare industry will be among the most susceptible industries to publicly disclosed and widely scrutinized data breaches.[1] The October 2013 security breach of the U.S. FDA's Center for Biologics Evaluation and Research compromised 14,000 accounts and demonstrated that competitive pharmaceutical trade secrets, which the federal government stores, represent an opportunity for foreign interests to benefit from new drug discoveries without having to invest in them.

Hospitals face significant cyber risks. Increasingly, hackers seek to exploit vulnerabilities in hospital computer systems and devices. Attackers' motives are diverse—ranging from stealing sensitive patient data to creating disruption and chaos in the delivery of services to the use of "ransomware" for criminal profit. With more hospital and patient data moving to the cloud and travelling across multiple national borders, the risk of complex international breaches increases. Devices with default passwords that are left unchanged, and outdated operating systems that are connected to the network, such as medical databases, are all too common in healthcare. Experts have already found flaws in a blood gas analyzer, a medical image system and radiology equipment.

Fundamentally, the question of cyber threats against hospitals is not whether investigative sites will suffer a data breach, but *when* this will occur, and *how serious* the consequences will be for the healthcare sector as a whole. There is no foolproof way to physically protect digital records that are frequently accessed, altered and shared, sometimes internationally. But it is possible to up the ante for hackers and malware by focusing on how you handle this data in the first place.

This report on cybersecurity in two Madrid hospitals, Moncloa and Fuenlabrada, investigates the current state of preparation against possible cyber attacks in these institutions. It will discuss possible vulnerabilities and generate recommendations which show a path towards improved security and resilience in the future.

This report is structured as follows: Section 2 will provide the necessary background on cybersecurity in the healthcare sector. Section 3 discusses the capabilities and motivations of different threat actors while Section 4 presents the analysis of potential vulnerabilities in the reviewed hospitals in Madrid. Section 5 compares the different IT infrastructure paradigms in terms of security and risk. In Section 6, a case study on large medical devices discusses the patching process. Finally, Section 7 provides recommendations and concludes this report.

2. BACKGROUND

This section will discuss the current cybersecurity environment in the healthcare sector. We will first review the reported breaches and systematize them into separate categories. Following this, we will survey the relevant academic literature on cybersecurity in hospitals.

2.1 Review of Reported Incidents

The Center for Internet Security reports that the "healthcare industry is plagued by a myriad of cybersecurity-related issues". The reported attacks can be systematized into four different major sectors:

2.1.1 Ransomware

Ransomware, a type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid, has become the most prominent reported type of attack, not only in the health care sector.

Recent reported incidents with regards to hospitals include:

1. "Infection with ransomware via outdated server software. In these cases, the attacker uploaded malware to the out-of-date server without any interaction from the victim, as opposed to infecting the hospitals through common workstations used by everyday staff. The Hollywood Presbyterian Hospital in California was one of the hospitals affected, in a case which delayed patient care and ultimately resulted in the hospital paying $17,000 to regain access to files and their network." [2]

2. "On June 14, 2017, the Pacific Alliance Medical learned its networked computer systems were affected by a cyber incident, which IT officials later determined to be ransomware. The medical center shut down its systems and initiated its response and recovery procedures. Officials were able to decrypt

1 See Experian, 2014 Data Breach Industry Forecast, https://www.oppinsurance.com/wp-content/uploads/2014/02/experian-2014-data-breach-industry-forecast.pdf

2 https://www.cisecurity.org/ransomware-in-the-healthcare-sector/

the infected files and have since taken action to restore the affected systems." [3]

3. "Atlanta-based Peachtree Neurological Clinic uncovered a 15-month breach to its computer system while investigating a separate ransomware attack. The clinic reported nearly **176,295** patient records were potentially affected." [4]

4. "Fayetteville-based Arkansas Oral & Facial Surgery Center notified **128,000** patients of a July ransomware attack on its computer network that may have compromised some patient names, dates of birth and Social Security numbers, among other data."[5]

5. The most publicized attack in Europe was the WannaCry attack on the UK National Health Services in May 2017. The UK National Audit Office reports: "The attack led to disruption in at least 34% of trusts in England although the Department and NHS England do not know the full extent of the disruption. On 12 May, NHS England initially identified 45 NHS organizations including 37 trusts that had been infected by the WannaCry ransomware. Over the following days, more organizations reported they had been affected. In total, at least 81 out of 236 trusts across England were affected." [6]

Not all ransomware attacks on hospitals have been publicly reported, however, just from the size of the known incidents we can deduce that ransomware has been the main active threat vector for attacks on hospitals in 2017.

2.1.2 Data Breaches

Data breaches are generally more difficult to detect compared to ransomware attacks or other active cybersecurity issues. In 2017, there have been many large cases where hospital security has been breached and data siphoned off by attackers with the intent to exploit or sell it. It is likely that many such attacks have not been noticed (yet) as they do not necessarily have a noticeable impact on day-to-day operations.

The U.S. Department of Health and Human Services provides a breach portal, that as of the time of writing lists 391 data breaches affecting 500 or more individuals within the past 24 months in the US alone.[7]

Reported major examples of such data breaches include:

1. "Banner Health is contacting 3.7 million individuals whose personal information may have been accessed in a cyberattack that began on systems that process credit card payments for food and beverage purchases at Banner locations. The breach then expanded to include patient and health plan information." [8]

2. On March 21, Bowling Green, Kentucky-based Med Center Health, which includes several hospitals, issued a public notification saying that on Jan. 4, 2017, "during the course of an internal investigation, we determined that [a] former Med Center Health employee had, on two past occasions during their employment, obtained certain billing information by creating the appearance that they needed the information to carry out their job duties for Med Center Health." This breach affected almost 700,000 individuals.[9]

3. "Peachtree Orthopedics has announced a hacker gained access to a patient database containing names, addresses, dates of birth, email addresses, treatment codes, prescription records, and Social Security numbers. The breach notification letters sent to patients on October 7, 2016 explain that the hacker potentially stole the contents of the database." [10]

These examples illustrate the severity of data breaches, which can be conducted both by outsiders and insiders. While they do not actively interfere with health care operations in a direct way, they can lead to serious consequences for patients in the long run (e.g., blackmail or fraud). In most industrialized countries laws exist which require public notification of data breaches concerning patient data, causing a potentially severe loss of reputation for the affected health care provider.

2.1.3 Distributed Denial of Service Attacks

Distributed denial of service (DDoS) attacks, which overpower and effectively disable network connections using numerous distributed clients, are extremely common against services connected to the global Internet, from popular websites to governments. For hospitals, this has been less of a concern compared to the previous threat vectors.

However, some examples exist:

> "In 2014, Anonymous (a well-known hacktivist group) targeted the Boston's Children's Hospital with a DDoS attack after the hospital recommended one of their

3 https://www.beckershospitalreview.com/healthcare-information-technology/266k-la-medical-center-patients-phi-compromised-in-ransomware-attack.html
4 https://www.beckershospitalreview.com/healthcare-information-technology/atlanta-clinic-discovers-15-month-breach-while-investigating-separate-ransomware-attack.html
5 https://www.beckershospitalreview.com/cybersecurity/arkansas-surgery-center-reports-128k-patients-impacted-by-ransomware.html
6 https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf
7 https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
8 http://www.modernhealthcare.com/article/20160803/NEWS/160809954
9 https://www.careersinfosecurity.com/breach-involving-encrypted-devices-raises-questions-a-9789
10 https://www.netsec.news/peachtree-orthopedics-discovers-patient-database-hacked/

patients, a 14-year-old girl, be admitted as a ward of the state and that custody be withdrawn from her parents. The doctors believed the child's ailment was actually a psychological disorder and that her parents were pushing for unnecessary treatments for a disorder the child did not have. The custody debate put Boston Children's Hospital in the middle of this controversial case, and some, including members of Anonymous, viewed this as an infringement on the girl's rights. Anonymous took action by conducting DDoS attacks against the hospital's network, which resulted in others on that network, including Harvard University and all its hospitals, to lose Internet access as well. The networks experienced outages for almost a week, and some medical patients and medical personnel could not use their online accounts to check appointments, test results, and other case information, according to the Boston Globe. As a result, the hospital spent more than $300,000 responding to and mitigating the damage from this attack, according to the attacker's arrest affidavit."[11]

DDoS attacks are notoriously difficult to defend against, even for the biggest players in the IT and defense business. Unsecured internet of things (IoT) devices have recently created botnets of unprecedented size and power, which will grow further in the future.

2.1.4 Phishing and Fraud Scams

As one of the largest business sectors in virtually every developed country, hospitals and other health care facilities are a natural victim for all types of targeted and non-targeted fraud scams. Phishing and spear phishing can be an entry point for ransomware and data breach attacks such as described above, but it can also be an attack vector on it's own.

As an example of the former:

1. "In 2013, nearly 90,000 patients at University of Washington Medicine had their personal information compromised as a result of phishing techniques. A hospital employee was sent an email that had a malicious link embedded into the content. The link was accessed in order to view an attachment. When opened, malware took over the computer and accessed the employee's computer, which contained files needed for billing patients. While it was quickly discovered and contained the following day, patient data such as names, addresses, phone numbers, Social Security numbers, and birth dates were already exposed." [12]

2. In an audit report by the Leeds Teaching Hospitals NHS Trust, 400 out of approximately 17,000 employees (around 2.3% of all staff) responded to a simulated phishing email and revealed confidential information like passwords or network credentials.[13]

For spear phishing attacks combined with engineering to elicit money from a hospital, in particular high-level employees are at risk of being targeted. Several thwarted incidents illustrate the danger in this type of attack:

1. "On Feb. 16, an employee received an e-mail, purportedly from the hospital's chief financial officer, asking for specific payroll information on Main Line Health workers. "The employee put together the information for what the employee thought was a legitimate request and forwarded the information back" to the e-mail sender, thinking it was the CFO." [14]

2. "Instead of an example of someone falling victim to this type of attack, I'll share an uplifting case. In 2015, a local medical center reported that they received a phone call from a pharmacy to confirm a large order of prescription drugs, over $500,000 worth. Upon investigation, it was determined the medical center had not placed that order, and it was in fact fraudulent. The pharmacy had only called to clarify because the shipping address for the medical center was different from that which they had on record, but all the other certificates and credentials checked out, including the Drug Enforcement Agency (DEA) ID number, doctor licenses, and pharmaceutical certificates. In this incident, a malicious actor had compromised the medical center's credentials and was attempting to take out a large line of credit with the pharmacy to purchase drugs. The pharmacy's act of calling the medical center to double check the order saved them from losing $500,000 in prescription drugs, and saved the medical center $500,000 being withdrawn from their account. The protocols in place were properly followed by the employee, (calling to confirm when there is a change on an account) and the scam was halted in its tracks." [15]

As can be deducted from these reports, (spear) phishing attacks on hospitals can not only lead to other cyber attacks such as ransomware attacks and data breaches. Instead, the attackers aim to extract money directly from the system by posing as a person authorized to conduct financial transactions.

11 https://www.cisecurity.org/ddos-attacks-in-the-healthcare-sector/
12 http://resources.infosecinstitute.com/the-5-most-visible-cyber-attacks-on-hospitals
13 http://www.leedsth.nhs.uk/assets/Board-Meetings/30-03-2017/Blue-Box-Documents/10.3i-Draft-Audit-Committee-Minutes-8-March-2017.pdf
14 http://www.modernhealthcare.com/article/20160317/NEWS/160319915
15 https://www.cisecurity.org/business-email-compromise-in-the-healthcare-sector/

2.2 Review of the Academic Literature

While there is much academic research and practical knowledge on the security of networked systems and business enterprises in general, the specific environment of hospitals and the health care sector necessitates research that goes beyond common solutions. It needs to take into account the particular requirements found in this area and examine solutions that are able to adapt to these circumstances.

In the academic literature, cybersecurity in hospitals has only recently started to become a topic of extended research, with a focus mostly on medical device software, in particular pacemakers and other personal and implantable medical devices (IMD).

Fu and Blum argue that the prevalence of medical device hacking is often overstated but that the flaws are real.[16] In their work, they suggest a new reporting system that captures security-related failures in such devices so the community can get an idea of how widespread such security problems are in practice. However, the vulnerabilities found in such devices do exist, illustrated by the story of former US Vice President Dick Cheney having the wireless telemetry interface on his implanted pacemaker disabled for fear of attacks on his life.[17] Rushanan et al. provide a comprehensive overview of the problem space in a 2014 survey, which identifies three security-relevant research areas for IMDs: the telemetry interface, the software, and the sensor interface layers. They find that the security of the telemetry interface has received much attention in academia, while the threats of software exploitation and the sensor interface layer deserve further attention.[18]

On the medical side of the academic literature, Perakslis discusses cybersecurity in the New England Journal of Medicine,[19] dividing cybercrime into four classes: data loss, monetary theft, attacks on medical devices, and attacks on infrastructure. The author also calls for a forum to share reports on security problems beyond the existing privacy and data security institutions. He further suggests that an "active learning approach is required to make prioritized cyber protection strategies and tactics focused and successful."

Kruse et al. further discuss the matter in their 2017 survey on cybersecurity in health care.[20] They analyse the trends in attacks and solutions with regards to cybersecurity in the sector and conclude that:

> "The two primary drivers exposing healthcare to cyber threats include rapid technological advancement and evolving federal policy. As healthcare IT infrastructure struggles with new technology and security protocols, the industry is a prime target for medical information theft. While security companies and the government have made progress to slow the prevalence of cyber attacks, the healthcare industry is lagging behind other leading industries in securing vital data. Healthcare must continuously adapt to the ever-changing cybersecurity trends and threats such as ransomware, where critical infrastructure is exploited and valuable patient data is extracted. It is imperative that time and funding is invested in maintaining and ensuring the protection of healthcare technology and the confidentiality of patient information from unauthorized access."

As an outlook for the future, Martin et al. note that until know practically all known attacks in the health care sector have been for financial gain of some sort and integrity of data has not been compromised.[21] They suggest that altering blood groups or test results could have devastating outcomes and outline commonly known enterprise network security steps that should be taken as a preventive measure, from malware prevention to use education.

3. THREAT MODEL

This section discusses the threat model that hospitals have to deal with in terms of cyber attacks. Understanding the different threat actors and their capabilities is a key proposition to improve the security of hospital systems in the future. In the second part of the section, we analyze potential insider threats which permeate the different threat actor classes.

3.1 Threat Actors

3.1.1 Nation State Actors

With sufficient knowledge and near-unlimited resources, it is possible to bypass standard checks and most traditional corporate network security defences. Against this most powerful attacker even the most critical of infrastructures such as parliament networks or crucial political decision making processes are difficult to protect and regularly breached. Ultimately, it is not possible to defend a network

16 Fu, K. and Blum, J., 2013. Controlling for cybersecurity risks of medical device software. *Communications of the ACM*, 56(10), pp.35-37.

17 Kolata, G., 2013. Of fact, fiction and Cheney's defibrillator. New York Times. http://www.nytimes.com/2013/10/29/science/of-fact-fiction-and-defibrillators.html

18 Rushanan, Michael, Aviel D. Rubin, Denis Foo Kune, and Colleen M. Swanson. "SoK: Security and privacy in implantable medical devices and body area networks." In S*ecurity and Privacy (S&P), 2014 IEEE Symposium on,* pp. 524-539. IEEE, 2014.

19 Perakslis, Eric D. "Cybersecurity in health care." N Engl J Med 371, no. 5 (2014): 395-397.

20 Kruse, Clemens Scott, Benjamin Frederick, Taylor Jacobson, and D. Kyle Monticone. "Cybersecurity in healthcare: A systematic review of modern threats and trends." Technology and Health Care 25, no. 1 (2017): 1-10.

21 Martin, Guy, Paul Martin, Chris Hankin, Ara Darzi, and James Kinross. "Cybersecurity and healthcare: how safe are we?." Bmj 358 (2017): j3179.

against a determined nation state actor for a prolonged period of time. Consequently, it is important to add *resilience* to the system, i.e. the ability to quickly detect attacks and be able to recover to a working state of the system in the least possible amount of time. Likewise, even successful attacks should not be able to bring the system down as a whole, thanks to redundancy and prepared offline procedures.

3.1.2 Script Kiddies

Script kiddies and hobbyists are the lowest active threat in our model based on their abilities considering both hardware and knowledge. Their aim is to exploit well-known security holes with existing, easy-to-use attacks with typically low sophistication. Their motivation is regularly not rational; instead any identifiable impact is sought for thrill and recognition, with hospitals providing a high-profile target. We assume a typical attack to be the following: using downloadable software they aim to create any noticeable effect on a website or hospital system. The objective of the attacker can range from a denial-of-service attack to defacing a website or see private data.

3.1.3 Cyber Crime

The cyber crime attacker class seeks to attack systems for monetary gain. Equipped with sufficient subject-matter knowledge, they use social engineering or software exploits to try and bypass current detection systems. Cyber crime attackers are typically interested in causing maximum damage and exerting credible threats, as a prerequisite for, e.g., blackmail or to take advantage of captured inside knowledge. Consequently, they are interested in exploiting any potential and effective way to attack systems in the healthcare sector.

3.1.4 Cyber Terrorists

Attacks on networked systems powering critical infrastructures such as hospitals are a natural target for terrorists and politically motivated attacks. Terrorists seek to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence. By exploiting vulnerabilities in hospital IT systems, terrorist groups, who traditionally act using physical force, could mount attacks from within safe distances. Existing preparatory scheme not normally consider scenarios in which a major cyberattack against hospital computer systems occurs in combination with a conventional terrorist attack (e.g., a bombing in a public space or damage to transportation infrastructures). In such a scenario, the hospitals' diminished lack of operational capacity would limit their ability to assist victims of the physical terrorist attack. Casualties would mount; public panic would be severe and widespread.

3.2 Terrorist Threat to Public Health in Spain: A Profile

The terrorist threat represents a serious national security concern to European nations -- including and especially Spain. The cyber threat is also a foremost danger. This section assesses the confluence of these two threats as they relate to the Spanish public health sector. First, the analysis examines the terrorist threat in Spain posed by different terrorist groups. The most direct threat to Spanish citizens and institutions stems from religious (particularly Islamist) terrorism, followed by separatist and anarchist terrorism.[22] Second, the report explains how the use of cyberspace to attack public health institutions matches (or could match) the aims of these groups. Third, the report evaluates the proven cyber capability of the actors and contextualizes this knowledge with the capabilities needed to realize a terrorist attack against public health institutions.

It is important to note that much of the discussion below is necessarily conjectural. The findings are based on inferences about past and current known capabilities from which we project possible future intent and capabilities.

3.2.1 Overview: The Terrorist Threat in Contemporary Spain

Terrorist activities in Europe are best categorized according to their varying motivations. These motivations fall within the following main categories:

- Ethno-nationalism and separatism
- Religious extremism
- Left wing activism and anarchism
- Right wing extremism
- Single-issue terrorism (e.g. animal rights and environmental extremism)

Ethno-nationalism and Separatism

Spain has a long history confronting domestic political violence beginning with the founding of the Basque separatist group Euskadi Ta Askatasuna (ETA) in July 1959. The group has inflicted the largest number, by far, of terrorist casualties in the country. Despite its extended campaign of violence, which in some instances achieved stunning results, the group is nearing a situation of total defeat. A low level of activity from the group seems to validate ETA's announcement in 2011 that it will end its armed campaign.[23]

But ETA is not alone. Other ethno-nationalists include latent groups such as Izquierda Abertzale and the Resistencia Galega in Galicia. It is possible, though highly unlikely, that

22 "Informe Anual de Seguridad Nacional 2016," Gobierno de España, 2017.

23 BBC, "Basque Group ETA Says Armed Campaign Is Over," BBC, 20. October, 2011, accessed 6. November, 2017, https://perma.cc/6CPP-W9DF.

Madrid's opposition to Catalonia's independence may give rise to extremist elements within the region -- for example, reviving the long defunct group Terra Lliure or a new version of it.

Left-wing Extremism and Anarchism

The extreme political Left presents a low-level threat to Spanish security. For example, reports suggest that members of Spanish communist groups have joined the Kurdish militias in Syria and Iraq.[24] In addition, there is a violent anarchist movement that displays a high level of ideological cohesion and commitment.[25]

Islamic Extremism

At present, a diverse range of groups using terrorist tactics actively operate against Spanish interests. Islamist extremist groups' protestations of reconquering the territory they refer to as "al-Andalus" confirms their continued intent to target Spain following the Madrid train bombings of March 2004.[26]

The most prominent contemporary manifestation of this threat is the Islamic State of Iraq and the Levant (ISIS). The group presents the gravest terrorist threat against Spain. Measured by its proven operational capacity, the extent of its media projection, its social media savviness, and its recruitment and leadership capacities, conclusive defeat of the group remains a significant challenge.

Since ISIS began to suffer significant losses of territory in Syria and Iraq, the danger posed by fighters returning to Europe and Spain has grown. The instability in the nearby Maghreb and the Sahel regions of Northern Africa serve as a training ground for new fighters to emerge.[27] The ISIS inspired vehicle attacks in Barcelona and Cambrils in August 2017 have confirmed that the risk level remains high.[28]

Besides ISIS, Al-Qaeda and its regional affiliates represent a significant threat against Spanish interests. In particular, Al-Qaeda in the Islamic Maghreb (AQIM), the Northern African branch of Al-Qaeda, has stated its intent to fight against the French and Spanish presence in the Is[29]lamic Maghreb. Spain's engagement in the military operation in Mali, therefore, serves as an ideological rallying point for Al-Qaeda's targeting.[30]

3.2.2 Terrorist Groups and Cyberspace

Intent to use cyberspace as a means of terror

For the purposes of this report, "cyber terrorism" denotes the use of computer code to produce *direct effects* harm against a computer system or network and/or an *indirect effects* against social, political, or economic interests beyond cyberspace for extremist political or ideological motives.[31] Importantly, the indirect effects may be more harmful than direct effects. Certainly, they will be the terrorists' primary concern; that is, they will likely prioritize the infliction of harm on humans and institutions than on the machines themselves.

To-date, no terrorist groups has prioritized cyberspace as an offensive domain of action.[32] However, UK national security officials assess ISIS to have the intent, but not the capability, to use cyberspace as a means of terror. Similarly, the Spanish annual national security report points to the possibility of disrupting critical infrastructures -- of which hospitals form a vital part -- via cyberspace.[33] These assessments are based mainly on classified evidence. Consequently, it is difficult to assess the true nature of motivations.

On this basis, some observers are sceptical of the terrorist

24 Europol, "European Union Terrorism Situation and Trend Report 2017," 43.

25 "Informe Anual De Seguridad Nacional 2016," 44.

26 "Spain: Extremism & Counter-Extremism," Counter Extremism Project, 2017, accessed 6. November, 2017, https://perma.cc/S6ES-JHJA. 1.

27 "Informe Anual De Seguridad Nacional 2016," 44-45.

28 "Islamist Terrorism in Catalonia Leaves the Spanish Wondering Why," The Economist, 18. August 2017. ISIS took credit for the attacks and announced its intent to continue targeting members of the Coalition against ISIS. See e.g. Al-Hayat Media Centre, "Rumiyah Magazine - Issue 13," 9. September, 2017. 5, 39.

29 "An Interview with Abdelmalek Droukdal," The New York Times, 1. July 2008.

30 "Terror Targets in the West: Where and Why," Counter Extremism Project, 2017, accessed 6. November, 2017, https://perma.cc/MV57-86VE. It is prudent to also keep other groups with more localized struggles, such as Boko Haram and Al-Shaabab, on the radar.

31 CCN-CERT, "Hacktivismo Y Ciberyihadismo - Informe Resumen 2016," 19. Translation by the author. Original assessment: "De este modo, el ciberyihadismo sería una forma de ciberterrorismo, entendido como la aplicación de la violencia por medios cibernéticos (ciberataques) para producir un daño directo contra un objetivo atacado y un efecto indirecto contra una audiencia más amplia (generación del terror en la sociedad, advertencia a las instituciones estatales). Durante 2016 puede afirmarse que el ciberyihadismo estrictamente como tal es una amenaza teórica que todavía no se ha manifestado. En las evaluaciones de ciberseguridad, el ciberyihadismo ha venido estando asociado al desarrollo de capacidades ciberterroristas por parte de grupos terroristas como 'Al Qaeda' o el 'Daesh', pero ese escenario todavía no se ha producido más allá del plano de las hipótesis." (p.19). For the additional detail provided in the definition and a detailed discussion, see Florian Egloff, "Intentions and Cyberterrorism," in Oxford Handbook of Cyber Security, ed. Paul Cornish (Oxford: Oxford University Press, 2018).

32 CCN-CERT, "Hacktivismo Y Ciberyihadismo - Informe Resumen 2016," 2017, 19. Sometimes, the media classifies the attack against the French broadcaster TV5 Monde, in which the station was modified to broadcast Islamist-extremist material, as a cyber terrorist attack. However, as of the evidence available today, the attack was perpetrated by APT28, a Russian offensive cyber outfit, as a false-flag attack. See Brian Bartholomew and Juan Andrés Guerrero-Saade, "Wave Your False Flags! Deception Tactics Muddying Attribution in Targeted Attacks" (paper presented at the Virus Bulletin Conference, Denver, CO, 5. October 2016), 6; Martin Untersinger, "Le Piratage De TV5 Monde Vu De l'Intérieur," Le Monde, 10. June 2017.

33 "Informe Anual De Seguridad Nacional 2016," 56.

intent to use cyberattacks as a means of terror.[34] Indeed, two of the most active terrorist groups, ISIS and al-Qaeda, in their public messaging have not emphasized cyber attacks. One analyst even suggests that cyberattacks may run counter to ISIS ideology, which emphasizes an even more traditionalist approach than al-Qaeda.[35] No statement of intent is known to directly target hospitals via cyber means. Rather, ISIS and al-Qaeda continue to call for physical attacks. However, in order to understand the terrorist threat profile, it is pertinent to assess how a terrorist intent may be realized in a cyber attack against a hospital.

Intent to target hospitals

Since 1981, terrorist attacks against hospitals have occurred mostly outside of Europe, including such committed by Islamist, ethno-nationalist, and communist/Marxist groups.[36] Most of the attacks involved explosives, followed by armed attacks, hostage takings, and mortar/grenade attacks.[37]

Hospitals are part of the strategic critical infrastructure of modern city life. Due to the easy access and the indiscriminate nature of people who end up there, as well as the symbolic value of killing already sick people, hospitals are lucrative targets to evoke moral outrage and disproportionate media coverage.[38]

Due to hospitals' involvement in the response to a conventional terrorist attack, the literature also identifies them as attractive secondary targets. However, secondary targeting has been found to be a rare phenomenon outside of the context of an armed conflict.[39]

ISIS demonstrated its intent to target hospitals by taking credit for the attack in August 2016 against a hospital in Quetta, Pakistan, in which over 70 people died and over 100 were wounded.[40] Since, it included hospitals in its targeting advice for arson attacks,[41] and repeatedly offered praise for attacks against a hospitals, both in Iraq and Afghanistan.[42] In February 2017, the US National Counterterrorism Center issued a warning against ISIS inspired arson attacks addressed specifically to hospitals and healthcare facilities.[43]

A cyberattack against hospitals as primary targets is unlikely to be restricted to the targeting of patients' personal information. Instead, the attack would likely attempt to interfere with the hospitals' operational activity in order to harm patients' health or even produce fatalities. Targets within hospitals can be the following:

- *primary attack surfaces*, whereby the attack targets patient health directly
- *secondary attack surface*, whereby an additional step is required before a patient is harmed
- *tertiary attack surfaces*, whereby generic IT infrastructure is attacked (e.g. servers, office installations, websites, basic web applications).[44]

ISE breaks down the hospital into four primary attack surfaces, interacting directly with the patient in a hospital setting: the physician, medicine, active medical devices, and surgery. All four, if attacked, directly affect a patient's health. The secondary attack surfaces, if targeted, have the potential to misdirect or influence a patient's health by altering or misdirecting a dependent process.

Cyber terrorist attacks against hospitals may involve both targeted attacks against specific patients, as well as attempts to indiscriminately harm patients. Furthermore, hospitals could also be targeted as a secondary target, to delay or denigrate an effective response to a conventional terrorist attack. Thus, terroristic intent could also target information linkages between the broader emergency response sector, for example, by misrepresenting information about the availability of trauma care units in hospitals, by altering geographic information systems (GIS) for emergency response, or by overloading the emergency response network with fake emergency telephone calls.[45]

34 See Rose Bernard, "These Are Not the Terrorist Groups You're Looking For: An Assessment of the Cyber Capabilities of Islamic State," Journal of Cyber Policy 2, no. 2 (2017); Egloff, "Intentions and Cyberterrorism."

35 Bernard, "These Are Not the Terrorist Groups You're Looking For: An Assessment of the Cyber Capabilities of Islamic State," 3.

36 Ganor Boaz and Miri Halperin Wernli, "Terrorist Attacks against Hospitals: Case Studies," The ICT Working Paper Series, no. 25 (2015), https://perma.cc/9XCK-AVUP. There have been some exceptions, for example, the 1991 Musgrave park (Belfast) hospital bombing by the PIRA.

37 Ibid., 9.

38 Ibid., 31. See also David J. Finucane, "Unhealthy Complacency: The Vulnerability of US Hospitals to Direct Terrorist Attacks," Journal of Healthcare Risk Management (2017); Harald De Cauwer et al., "Hospitals: Soft Target for Terrorism?," Prehospital and Disaster Medicine 32, no. 1 (2017); Denis Fischbacher-Smith and Moira Fischbacher-Smith, "The Vulnerability of Public Spaces: Challenges for UK Hospitals under the 'New' Terrorist Threat," Public Management Review 15, no. 3 (2013).

39 Julian Thompson et al., "Risks to Emergency Medical Responders at Terrorist Incidents: A Narrative Review of the Medical Literature," Critical Care 18, no. 5 (2014). But see the NCTC warning in NCTC, DHS, and ONI, "Worldwide: IED Targeting of First Response Personnel – Tactics and Indicators," NCTC Special Analysis Report - 2012-34a, 7. August 2012.

40 Gul Yousafzai, "Suicide Bomber Kills at Least 70 at Pakistan Hospital, IS Claims Responsibility," Reuters News, 8. August 2016.

41 Al-Hayat Media Centre, "Rumiyah Magazine - Issue 5," 6. January, 2017. 9-10.

42 "Rumiyah Magazine - Issue 6," 4. February, 2017. 27; "Rumiyah Magazine - Issue 8," 5. April, 2017. 27.

43 DHS, FBI, and NCTC, "Terrorists Call for Attacks on Hospitals, Healthcare Facilities," Fire Line, 8. February 2017.

44 Independent Security Evaluators, "Securing Hospitals," 2016, 27-40.

45 This happened in October 2016 denial of service attacks against the 911 network in 12 US states. See NCTC, DHS, and FBI, "Cyber Threats to First Responders Are a Persistent Concern," First Responder's Toolbox, 24. July 2017.

Finally, hospitals are also sites of interests for terrorists due to their access to specific materials and their function in the health supply chain. Thus, when assessing the exposure of the public health sector to terroristic activities, hospitals also should take note of terrorists' involvement in the illegal organ and drug trade, as well as their interest in special chemicals and radiological materials. Cyberattacks could facilitate these interests through circumvention of access controls, or through facilitating a subversion of the supply chain.[46]

Current capabilities

Current cyber capabilities of terrorist groups to commit harmful acts are assessed to be low. Various terrorist groups and their affiliates are using their low capabilities with great success in gaining publicity.

ISIS and ISIS-affiliated groups

ISIS featured large in media and cybersecurity reporting. They hold a large online footprint, particularly with regard to propaganda, recruitment, and attack coordination.[47] However, their offensive cyber capabilities are probably low. Analytically, one has to distinguish ISIS's own capabilities (i.e. people directly affiliated and recognized by ISIS's leadership) and pro-ISIS inspired hacking activities. The former is virtually non-existent. Most of ISIS's technical capability has been dedicated to building and maintaining the group's "operational security and resilience".[48] Even the two hackers ISIS had access to (Junaid Hussain and Ardit Ferizi) were not tasked with building a complex offensive terror campaign. Rather, their online skills were mostly used for propaganda and recruitment purposes.[49]

A different picture emerges from the analysis of the pro-ISIS inspired hacking activities with names such as "Islamic State Hacking Division, UCC, United Islamic Cyber Force, Cyber Kahilafah, and Islamic Cyber Army."[50] While these groups may claim to be officially aligned with ISIS, both their activities and official ISIS communication suggests independence from the ISIS core organization. The threat posed by these individual groups has, consequently, also to be judged on a group by group basis. Their hacking tactics, techniques, and procedures suggests a strong overlap with the cyber hacktivist community in various countries, including Tunisia, Pakistan, Egypt, and offshoots of Anonymous in South America.[51] They mostly employ website defacements and distributed denial of service (DDoS) attacks against a wide range of targets.

Beyond the web defacements and DDoS attacks, pro-ISIS groups have compiled and published so-called "kill lists" (also referred to as "doxing"), sometimes implying that they had had access to the information as a result of cyber intrusions.[52] The publication of lists feature the personally identifiable information of civilians, government officials, and military and law enforcement officials. The groups usually publish them in conjunction with a call for ISIS supporters to kill or injure the people on the lists. Analysis has shown that some of the lists were re-publishing previously public information. The source of private information was likely based on simple web application hacking techniques, such as the use of automated SQL injection attacks, and brute-forcing SSH.[53] The publication of kill-lists has been assessed by U.S. law enforcement as an aspirational threat, with the primary purpose to "heighten anxiety and a sense of vulnerability," and an actual physical follow-through is judged as unlikely.[54]

Thus, based on the defacements and the publication of kill-lists, one can assess ISIS's demonstrated capability as low. They use low sophistication hacking techniques against highly vulnerable sites to achieve their targets, which seems to be mainly an effort of propaganda and sowing fear. This assessment is further corroborated in online conversations, where some of the groups who previously voiced threats against national systems were found to display "little technical understanding."[55] For example, Cyber Kahilafah maintained a site claiming to distribute NSA cyber tools leaked by the Shadowbrokers group. However, this can be seen as an attempt to try to appear proficient, rather than

46 On radiological materials, consider the caesium-137 gained by Chechen rebels in attacks against the hospital in Budennovsk, Russia in 1995 Boaz and Halperin Wernli, "Terrorist Attacks against Hospitals: Case Studies". 19. On illegal drug trade, see Boaz Ganor and Miri Halperin Wernli, "The Infiltration of Terrorist Organizations into the Pharmaceutical Industry: Hezbollah as a Case Study," Studies in Conflict & Terrorism 36, no. 9 (2013). Re ISIS's involvement in the organ trade, see NCTC, DHS, and FBI, "International Partnerships among Public Health, Private Sector, and Law Enforcement Necessary to Mitigate Isis's Organ Harvesting for Terrorist Funding," First Responder's Toolbox, 11. May 2017.

47 John Mueller, "The Cybercoaching of Terrorists: Cause for Alarm," CTC Sentinel 10, no. 9 (2017); Seamus Hughes and Alexander Meleagrou-Hitchens, "The Threat to the United States from the Islamic State's Virtual Entrepreneurs," ibid., no. 3.

48 Bernard, "These Are Not the Terrorist Groups You're Looking For: An Assessment of the Cyber Capabilities of Islamic State," 2.

49 Egloff, "Intentions and Cyberterrorism." See also United States of America Vs. Ardit Ferizi, 1:16-cr-042 (2016).

50 Bernard, "These Are Not the Terrorist Groups You're Looking For: An Assessment of the Cyber Capabilities of Islamic State," 4.

51 Ibid., 5.

52 A timeline of kill-lists can be found in SITE Intelligence Group, "Special Report: Kill Lists from Pro-IS Hacking Groups," Bethesda, MD, 2016. See also CCN-CERT, "Hacktivismo Y Ciberyihadismo - Informe Resumen 2016," 22-24.

53 Bernard, "These Are Not the Terrorist Groups You're Looking For: An Assessment of the Cyber Capabilities of Islamic State," 7.

54 DHS and FBI, "Handling Threats to Private Citizens and Locations Named Online by Violent Extremists," September 2017, 1.

55 Bernard, "These Are Not the Terrorist Groups You're Looking For: An Assessment of the Cyber Capabilities of Islamic State," 7.

having the technical proficiency needed to undertake a complex destructive cyber campaign.[56] This judgement is further corroborated by the absence of any evidence of Islamist sourced attacks using the NSA toolset leaked in April 2017.

Other hacking groups with the potential to engage in terrorist activities in Spain

From a capabilities perspective, a larger problem may be the anarchist and extreme left-wing hacking community. Spain's National Cryptologic Centre notes several hacktivist activities undertaken in 2016, including some perpetrated by the anti-capitalist, anarchist 9th company (an off-shoot of Anonymous) and Phineas Fisher. The 9th company engages mostly in website defacements and exfiltration of information, relying on SQL-injection and misconfigured servers.

While the 9th company is judged to be Spanish local hackers, the offensive action claimed by Phineas Fisher is assessed to have taken place (or designed to appear to do so) from outside of Spain.[57] In 2016, the Police Union of the Mossos d'Esquadra was hacked, their social media accounts taken over, and the personal data of 5600 members published online. The moniker "Phineas Fisher" took credit for the attack and justified it as an action to demonstrate that "they are spying on activists and social and libertarian movements."[58]

Out of all the hacktivists active in Spain, the Phineas Fisher team has the highest demonstrated capability. They previously hacked the spyware companies Gamma Group and Hacking Team, and leaked their files online. For all three high-profile hacks (Gamma Group, Hacking Team, and Police Union of the Mossos d'Esquadra), Phineas Fisher published a step-by-step documentation of the operation.[59] Even if we do not know the veracity of the claims, the tutorials demonstrate an awareness of how a technically sophisticated operation would take place. Ideologically, however, it is unlikely that Phineas Fisher would target a hospital to induce harm. Rather, they expressed commitment to an anarchist ideology, supporting the Kurdish Rojava project, their previous targets falling in to the police and intelligence services spectrum. Furthermore, Phineas Fisher expressed no intent to undertake further political hacks in the near future to concentrate more on their criminal activities.[60]

Leak of NSA toolset and absence of attacks as indicator of low capability

The leaking of the NSA toolset can also be used as an analytic indicator for other groups' threat profile. For a moderately to highly sophisticated attacker group, the availability of the toolset in April 2017 would have been a prime opportunity to act upon intent. The fact that we have not witnessed attacks stemming from any of the terrorist groups mentioned above demonstrates either the low capability or the absence of an intent to use cyber means to terrorize. As outlined in this section, the pro-ISIS affiliated hacking groups fall in the category of low capability.

Capability needed to achieve significant effects in the health sector

Due to the generally low prioritization of information security practices in the health sector, the level of effort needed to opportunistically target a hospital is minimal. However, this judgement is reserved for the tertiary attack surface made up of generic information technologies. As soon as an attacker wants to achieve effects in more specific technologies and systems (e.g. active and passive medical devices, climate control of patient samples/bloodwork, medication inventory systems), the level of training and experience needed for the attacker to achieve a tailored effect rises.[61] However, in an environment with bad security practices, a moderately competent attacker can take the time to learn about the technologies and systems used in a hospital.[62]

A hospital should expect a targeted cyber terrorist threat to be able to draw not only on moderately competent technical abilities, but also on a close access capability. Especially if the cyberattack against a hospital is perpetrated in conjunction with a traditional terrorist attack, it is prudent to assume that terrorists will physically infiltrate into the hospital (e.g. as staff, patients, or suppliers). Importantly,

56 Ibid.

57 CCN-CERT, "Hacktivismo Y Ciberyihadismo - Informe Resumen 2016," 9-10.

58 Ibid., 10.

59 Gamma: "Hack Back! A DIY Guide for Those without the Patience to Wait for Whistleblowers," Pastebin, 8. August, 2014, accessed 7. November, 2017, https://perma.cc/B6VV-7A4D. Hacking Team: "Hack Back! A DIY Guide," Pastebin, 18. April, 2016, accessed 7. November, 2017, https://perma.cc/4UQ2-LJ83; "Hack Back! Una Guía DIY," Pastebin, 15. April, 2016, accessed 7. November, 2017, https://perma.cc/CWG8-96TB. Sindicat de Mossos d'Esquadra: HackBack, "Hacking Sindicat De Mossos D'esquadra (Catalan Police Union)," tune.pk, 2016, accessed 7. November, 2017, https://perma.cc/3BBZ-BW65.

60 "Hacking Team Hacker Phineas Fisher Is Taking a Break Because of Stress," Motherboard, 9. February, 2017, accessed 7. November, 2017, https://perma.cc/9TE3-MDRJ.

61 Those barriers are not insurmountable, however. Medical device insecurity is now an area of active research. See for example excellent work done by Eireann Leverett, Marie Moe, and Tony Naggs, "Medical Devices Vulnerabilities, Threats and Security," 4SICS Summit Workshop, 2016, accessed 7. November, 2017, https://perma.cc/VU3G-X7U8.

62 Useful guidance for good security practices in an environment with medical devices is available in: American Hospital Association, "Cybersecurity Resources," 2017, accessed 7. November, 2017, https://perma.cc/3CR2-MG5A; U.S. Food & Drug Administration, "Digital Health - Cybersecurity," U.S. Department of Health and Human Services, 2017, accessed 7. November, 2017, https://perma.cc/Y29H-GD66; Evaluators, "Securing Hospitals."

one can assume that they will be willing to use force to coerce hospital staff to comply. Hence, not only do health information systems have to be robust against external attacks, but mitigations have to be in place to limit the harm attainable by a malicious insider. Ideally, organizational processes are assessed for their contribution towards a system that can withstand coerced effects and limit their impact.

3.2.3 Lessons from the Past

Past cyber incidents can shed some light onto what could happen in an attack on the health sector. Since the leaking of NSA toolset in April 2017, we have witnessed several large campaigns using the toolset, including one with significant effects in the health sector. In particular, the so-called WannaCry incident of spring 2017 offers useful lessons.

In May 2017, a ransomware attack worm, referred to as WannaCry, spread globally, using one of the recently released NSA tools as a redistribution vector (EternalBlue SMBv1 exploit). As part of its spread, it also infected a large part of the United Kingdom's National Health Service (NHS). The worm can serve as a benchmark for an untargeted attack affecting the health sector, using a well-engineered propagation mechanism.

In the United Kingdom, before WannaCry occurred, out of the 88 trusts assessed (of a total of 236) in the domain of information security, none had passed.[63] Hence, their information security practices were of low quality, failing to implement minimal information security policies and procedures. As a result, the WannaCry worm could, in principle, inflict its maximum impact. However, this impact was mitigated by the unrelated activation of a kill switch by a security researcher.

A national audit of the incident assessed the actual and potential impact (without the kill switch): 81 out of 236 trusts (hospital care facilities) were affected, with a further 21 trusts attempting to contact the WannaCry domain, but not reporting locked out devices.[64] An additional 603 primary care facilities were infected, including 595 GP practices.[65]

The hospitals reported two major impacts. First, not being able to use their devices denied or delayed accessing and updating patient information, sending test results to doctors, and managing patient discharge and transfer.[66] Second, locked medical equipment and devices, or isolated devices meant departments that relied on them were disrupted in their diagnostic capability (e.g. radiology and pathology for imaging and testing blood and tissue samples).[67] Hospitals not infected by the ransomware were further disrupted by the, in absence of any central guidance, preventive measures of shutting down information systems. The disruptions resulted in cancelled appointments (estimated ca. 19'000) and further travel to accident and emergency facilities (five hospitals diverted their emergency services).[68] The incident deserves close study with regard to the prevention of a terrorist cyberattack against a healthcare system, as many of the preventative security measures that would have helped to mitigate the impact of an initial infection are also part of the baseline defence against targeted cyber attacks with a terroristic intent.

3.2.4 Conclusion

This section assessed the current and latent threat of a terrorist cyberattack against public health institutions in Spain. The current threat of cyberattack with terrorist intent is low, mainly due to the absence of a group with moderately sophisticated offensive capabilities. While hospitals are intended targets of terrorist groups for traditional attacks, specifically by ISIS, previous experience suggests that their cyber capability is insufficient to be deemed a credible risk to primary attack surfaces resulting in harm to patient health. Furthermore, conducting moderately sophisticated cyberattacks to induce terror has not been part of the main tactics of any terrorist group. Thus, it is unlikely that hospitals become strategically targeted by acts of cyber terrorism in the near future. Today, any risk of a cyber terrorist attack against a hospital stems solely from being an opportunistic target, where a terrorist group gains an entrepreneurial, moderately skilled attacker.

Nevertheless, hospitals, due to their critical function in the functioning of modern society (especially within large modern cities such as Madrid), remain prime targets for traditional terrorist attacks. Thus, when one of the active terrorist groups attains a moderate to advanced offensive cyber capability, hospitals could fall within the potentially targeted facilities.[69]

Previous untargeted cyberattacks affecting healthcare facilities have demonstrated some of the problems that can arise when hospital systems become unavailable. The mitigations against falling victim to untargeted attacks are also necessary not to fall prey to targeted attacks. As preventative mitigation strategy, hospitals would do well to assess the impact of a targeted attack on their critical assets and employ measures to contain the harm of an attack with terrorist intent.

63 "Investigation: WannaCry Cyber Attack and the NHS," London:National Audit Office, 2017, 4.
64 Possibly due to infection after the kill-switch domain had been activated. Ibid.
65 Ibid.
66 Ibid., 11.
67 Ibid.
68 Ibid., 13-14.
69 Analysts judge this to be unlikely, as it would "require a change in focus and deliberate recruiting and training efforts." Australian Cyber Security Centre 2017 Threat Report, Canberra: Australian Government, 2017. https://perma.cc/BHN7-E8FY. 52.

4. IDENTIFICATION OF VULNERABILITIES

In this section, we first describe the auditing process, which we used to identify potential security vulnerabilities. In the second part, we discuss the results obtained from this process, separately for the two hospitals, Fuenlabrada and Moncloa.

4.1 Description of Process

We broadly follow the standardized framework by the National Institute of Standards and Technology (NIST), which are widely considered the industry standard for best security practices.

4.1.1 General Overview

Figure 1 shows the general risk assessment process as outline by NIST Special Publication 800-30 Revision 1, Risk Management Guide for Information Technology Systems [1].

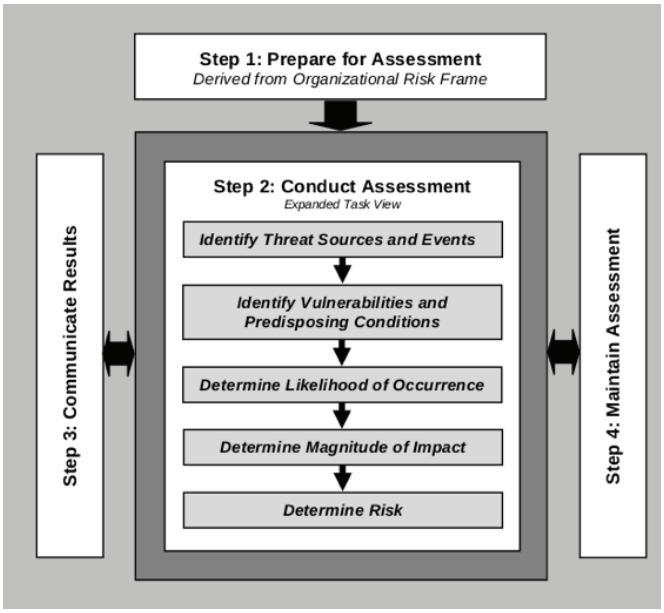


Figure 1: Risk Assessment process following NIST 800-30.

Step 1: Preparing the Assessment

We first identify the Identify purpose, scope, assumptions and constraints of the risk assessment. We further identify the possible information sources for the assessment.

Step 2: Conducting the Assessment

In the second step, we conduct the actual assessment. With the help of a second questionnaire, we identify the relevant threat sources and threat events, the vulnerabilities and finally determine the likelihood and the potential impact on the hospital infrastructure. In the following, we describe these different sub-steps taken in some more detail, for a more in-depth description, please refer to the original document [1].

a) Identify Threat Source
This step comprises the identification and characterization of threat sources, including capability, intent, and targeting characteristics for adversarial threats.

b) Identify Threat Events
This step comprises the identification of potential threat events, relevance of the events, and the threat sources that can initiate the events.

c) Identify Vulnerabilities
This step comprises the identification of vulnerabilities and predisposing conditions that affect the likelihood that threat events cause adverse impacts.

d) Determine Likelihood
This step comprises the determination of the likelihood that threat events cause adverse impacts. It considers the characteristics of the threat sources, the vulnerabilities/predisposing conditions and the implemented countermeasures.

e) Determine Impact
This step comprises the determination of the adverse impacts from threat events. It considers the same characteristics as the previous step.

f) Determine Risk
This step comprises the determination of the risk to the organization from threat events. It: considers the impact that would result from the events and the likelihood of the events occurring.

Step 3: Communicating the Results

We communicate the results in Sections 5 and 6. Please note that Step 4, maintaining the assessment, is out of the scope of this report.

4.1.2 Preparation: First Questionnaire

The purpose of the first questionnaire is to obtain important information used for the preparation stage of the risk assessment. The questionnaire serves to assess the scope and principal assumptions of the risk assessment exercise, the availability of relevant information sources, facts about known threat events, and knowledge of the predisposing conditions found in the target systems in the two hospitals under review: Hospital Universitario de Fuenlabrada and Hospital Universitario HLA Moncloa. The information collected herein set the stage for detailed operational assessments conducted in the next stage of the project.

4.1.3 Quantitative Assessment: Second Questionnaire

The purpose of the second questionnaire is to obtain important information required for the second stage of the risk assessment. The questionnaire is a follow up to the first survey, which was aimed at understanding the scope and principal assumptions of the risk assessment exercise, the availability of relevant information sources, facts about known threat events, and knowledge of the predisposing conditions found in the target systems in the reviewed hospitals. In the pursued top-down assessment approach, this next stage of the process is concerned with obtaining detailed operational data, after collecting high-level information in the first stage. It serves to identify concrete threats and vulnerabilities and their likelihood. Concretely, the survey contains 24 tangible threats across 7 different categories, which could impact the hospitals' networking systems and potentially have adverse effects on hospital operations, hospital assets, or individuals (patients or employees). For each threat vector, the impact on the hospitals' systems is to be identified. Then, it is examined how the existing security infrastructures are able to deal with each attack (or not).

The impact is defined as show in figure two.

4.1.4 Qualitative Assessment: Interviews / Additional Questions

Further to our quantitative assessment using structured questionnaires, we added a qualitative element to our approach. First, we conducted several unstructured interviews with employees of both hospitals who were either directly involved with the IT infrastructure and its security or working in the hospitals' management. We discuss these results in the next sections. Furthermore, we identified an additional area of investigation: the patching process of large medical devices. To evaluate this process, we have sent a follow-up request to Siemens Healthineers, a critical manufacturer of such devices used in Madrid hospitals. We discuss the results from this investigation in Section 6.

Figure 2: Definition of impact.

Critical	The threat event could be expected to have **multiple severe or catastrophic adverse effects** on hospital operations. hospital assets, or individuals (patients or employees).	See below
High	The threat event could be expected to have a **severe or catastrophic adverse effects** on hospital operations, hospital assets, or individuals (patients or employees).	A **severe or catastrophic adverse effect** means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) results in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.
Medium	The threat event could be expected to have **a serious adverse effect** on hospital operations hospital assets, or individuals (patients or employees).	A **serious adverse effect** means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) results in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals involving loss of life or serious life-threatening injuries.
Low	The threat event could be expected to have **limited to negligible adverse effects** on hospital operations hospital assets, or individuals (patients or employees).	A **limited adverse effect** means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) results in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
None	The threat event could be expected to have **no adverse effects** on hospital operations hospital assets, or individuals (patients or employees).	No discernible impact to any of the hospital networks, individuals, or affiliated systems.

4.2 Discussion of Results

We first discuss the results of the questionnaire, before we describe the qualitative results obtained from the interviews. Please note, that in the case of Moncloa, we have sent the questionnaire both to IT representatives from the hospital as well as TICH Consulting, who are the developers and maintainers of the Green Cube cloud software system that underlies most of the IT infrastructure used within Moncloa hospital.[70]

4.2.1 Questionnaire Results

Fuenlabrada

Fuenlabrada hospital maintains a traditional, non-cloud based, IT infrastructure that has organically grown over decades. The non-homogeneity and decentralization of this infrastructure, which is maintained in house, naturally has fundamental consequences with regards to its cybersecurity and maintenance compared to other solutions. This is discussed in detail in Section 5.

Previous threat events:

The key previous threat event for Fuenlabrada was the global attack of the WannaCry ransomware, which required IT services to cut off hospital connectivity to conduct comprehensive patching. This had an impact on hospitals staff as any service requiring internet connectivity was unavailable for this time.

The reported timeline was as follows: The ongoing attack was known on Friday; the hospital's access to the regional networks were taken offline on Sunday, no internet connection was available for two weeks. 90% of the hospital employees were able to work, for example all CT scanners are accessible locally and were not disrupted.

Most important potential threat events by risk:

From the second questionnaire we identify the following threat events as the most relevant for Fuenlabrada as defined by risk, e.g. the combination of likelihood and impact:

1. **Malware delivery**
   The key threat vector is the possible delivery of malware using different deployment methods. These range from USB sticks over targeted phishing attempts to exploitation of the WPA2 networks used by managers and medical devices. This threat vector is common to most large networks and institutions.
2. **Social engineering**
   The second major threat vector comprises attacks where an adversary induces authorized users within the hospital system to inadvertently expose, disclose, or mishandle critical/sensitive information, e.g. via targeted phishing emails or phone calls. This may also occur via instant messaging, or comparable means; often directing users to websites that appear to be legitimate sites, while actually stealing the entered information.
3. **Exploitation of software vulnerabilities**
   Thirdly, in a very heterogeneous environment with many legacy hosts and devices as it is found in Fuenlabrada, it is highly likely that a fraction of the systems contain exploitable vulnerabilities. Host devices range from large medical devices over ordinary networked computers to specialist software systems such as those used by the radiology and imaging units. This vector is available for all threat agents, more powerful actors have access to zero-day or custom exploits while less sophisticated actors exploit the window of opportunity between disclosure and patching of an exploit, which can take several months (see also Section 6).

Moncloa

Moncloa hospital maintains modern cloud-based infrastructure, which outsources much of the software and hardware to external suppliers. Concretely, the software and hardware of the hospital uses the Green Cube cloud system developed by TICH Consulting[71] for Moncloa and other hospitals in Spain and around the world. Centralized cloud-based systems have, at least partly, separate security concerns to more traditional IT infrastructures, which we discuss further in Section 5.

Previous threat events:

No previous threat events that impacted the hospital have been reported by Moncloa. However, threats detected by the employed intrusion detection system are common, such as the Venturead adware/malware shown in Figure 3:

Most important potential threat events by risk:

From the second questionnaire we identify the following threat events as the most relevant for Moncloa as defined by risk:

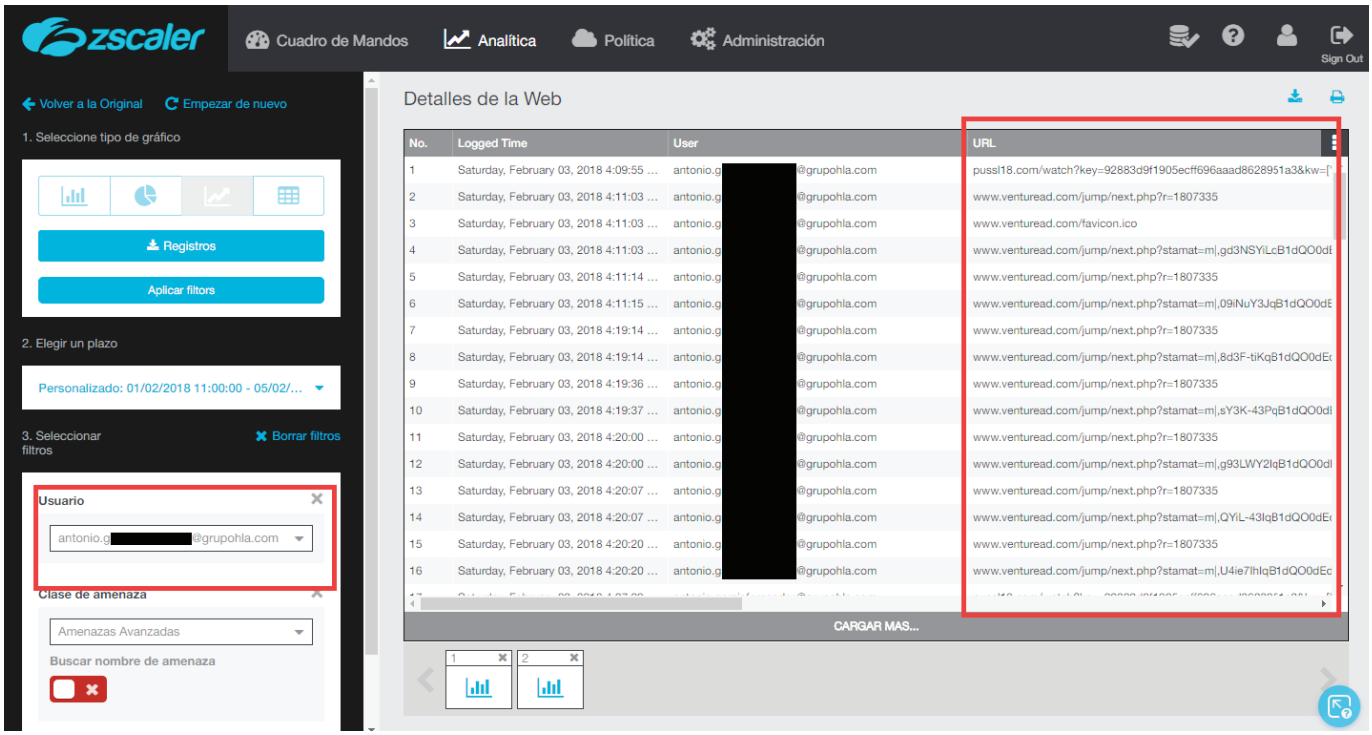
1. **Distributed Denial of Service**
   Malicious denial of service attacks on the cloud provider, their network infrastructure, or the cloud internet connection are a threat that would severely cripple the functioning of the hospital. While the dedicated connection offers high bandwidth and availability, severe distributed denial of service attacks powered by botnets of Internet of Things (IoT) devices have become feasible for many actors and have recently reached the Tbps magnitude, with a strong upwards trajectory.[72]

70 Green Cube is primarily the property of ASISA.

71 https://tichconsulting.com/green-cube/

72 https://www.wired.com/story/github-ddos-memcached/

Figure 3: Screenshot of adware internet connection requests.



2. Malware delivery
The second key threat vector, similar to Fuenlabrada, is the possible delivery of malware using different deployment methods. As there is no restriction on the use of USB devices at Moncloa, this is one likely delivery vector, both by hospital insiders (deliberately or inadvertently) and external attackers. Targeted delivery of custom or zero day exploits may further thwart existing defenses such as corporate email security and antivirus software.

3. Social engineering/phishing on external systems
Despite existing awareness courses and anti-phishing systems protecting the corporate email systems, experience has shown that it is still a very attractive approach for an attacker to deliver (semi-)targeted phishing attempts for example to third-party webmail systems used by hospital workers.

4.2.2 Interview Results

This section provides the insights and results from the semi-structured interviews conducted at Fuenlabrada and Moncloa hospital on 2 February 2018 by Prof. Martinovic and Prof. Kello.

Fuenlabrada

General Risk Assessment

Fuenlabrada is a public hospital, which is part of a regional health service network (central regional authority). Its network infrastructure is managed by the central regional authority, and this also includes the majority of security services. The main part of these network security services is related to network access which is provided over a Virtual Private Network (VPN) and there is a network monitoring system which also serves as an intrusion detection system (IDS) - both VPN and IDS are managed by the central regional authority. The IDS monitors the internet traffic and the analysis of the traffic is done at the regional centre. Once per month there is a report sent from the regional centre to the hospital including the list of network and security events (anomaly detection). In case of a significant security or network incident, which requires communication between regional centre and the hospital, there is a 24/7 on-call contact person.

Staffing Levels regarding Cybersecurity

There is a core IT team of five persons at the hospital. They are managing the overall IT infrastructure and there are additional assistants to help in network management. The core team feels understaffed in the area of IT security. They feel that the team is good for general network and

IT management, but they believe an additional person with the focus on security management would be very valuable to the existing team. There is an in-house training process for the new persons to join the IT team; it usually takes 3 months of training to equip a person with skills to operate and manage the IT systems in the hospital. As a group of 5 they feel they can do their work well, but they would need a full time person for security management; they mostly operate reactively, and they would like to act proactively.[73]

When talking about the security incidents, the team has described the timeline and activities during the Wannacry malware attack. Wannacry has been detected by the installed IDS on Friday and the first response was to take the hospital offline (no Internet connectivity), which was done by Sunday. For a period of the following two weeks, the hospital was offline. During this period, while there was no Internet connectivity, it has been confirmed that the hospital was operational and the majority of services were working (90% of hospital staff could continue with their work).

Patching Processes

We have discussed the process of patching medical equipment, i.e., identifying, reporting, advising, patching, and deploying the patches. In general, the team feels that the relationship with providers is a bit 'obscure' and there is no well-defined patching process in place currently. The provider does send reports about security problems, but there does not seem to be a process and the team is unable to explain a timeline of the patching process (i.e., how long does it take to patch a system). One reason for this might be that there is no clear definition of responsibility for patching specialized equipment (medical devices, such as CT systems). There seems to be another team in the hospital that works directly with the vendor.

Overall, the dependency on the regional centre is high, but it looks like the communication between the two teams works well. There is also a collaboration with the regional health authority on critical infrastructures, and plans to start an 'ethical hacking' programme on a national level.

There were some other patching-related observations mentioned by the interviewees, loosely listed in the following in no particular order:

- The general patching service is not controlled by the hospital but by the regional team; the regional team knows the IT systems and the level of patching.
- Direct patching by Microsoft is not allowed.
- The new patch needs to be evaluated before deployed, this takes around 3 month because the providers test the patch
- There has been a problem with Windows 7; after patching all functionality has been lost.

Moncloa

General Risk Assessment

The security infrastructure at Moncloa is not managed locally, instead, it is managed centrally by the health infrastructure provider ASISA, who runs the whole IT infrastructure and the Green Cube hospital management system. There are two employees assigned to Moncloa working in the local team for ASISA to support incident resolution. The local hospital IT team is only responsible for standard support tasks, not for managing security.

All workstations are thin clients connecting to the Green Cube system and are currently using Windows 7. The hospital is in the process of migrating to Windows 10, this should be finished in the whole of Madrid before summer 2018.

Email clients run on all machines, which also have access to Green Cube, thus, for example, a keylogger sent by email to an employee, who installs it, would be able to get the credentials of the local users.

There are no USB sticks for use on the PCs allowed by policy, but this cannot be guaranteed for all large medical devices such as CTs. For example, there are separate Picture Archiving and Communication Systems (PACS) in use, which are not connected to Green Cube. While all patient data is stored in the cloud used by Green Cube, the medical images stored on PACS are stored locally and thus constitute a separate threat vector.

The interviewees further noted that there is an ongoing program for security awareness and training and that there are lot of standard restrictions on the workstations used by employees. Finally, the interviewees were also asked about recent vulnerabilities in PET/CT scanners in the hospital. This topic is covered further in full detail in Section 6.

Network Management

All health-related groups (e.g., hospitals, insurance) in Spain work inside a Multiprotocol Label Switching (MPLS) network, which comprises more than 250 connected sites and is managed by Vodafone. For Moncloa, all internal systems facing this network are protected by firewalls provided by the ASISA infrastructure.

As ASISA manages the IT infrastructure and the Green Cube system, it controls access and security at the Moncloa network level. Whenever a new workstation is required

73 Note, that for example some hospital providers in the US have dedicated security teams, which also conduct penetration testing on incoming medical devices.

in the hospital, an application to ASISA has to be made. A similar process is required for the installation of new software. Furthermore, it should principally not be possible to install Green Cube on unauthorized machines.

Besides ASISA security services, there are other services are provided by different contractors. Most notably, external access to Green Cube is secured via a Virtual Private Network (VPN) managed by Fortinet.[74]

The network itself is divided into logically separated Virtual LANs (VLANs), which are used for different services in the hospital. For example, there is a separate VLAN for radiology, or one only for Siemens machines, the access to which is provided by ASISA but the machines are managed by Siemens. Overall it is important to note that the hospital is not buying a device but a service, a paradigm difference that is touched upon further in Section 5.

Besides the wired network, there are several wireless networks using the WiFi standard available in Moncloa. One is available to employees (*Moncloa_corp*), another one for visitors (*Moncloa_invitados*). These WiFi networks do not allow access to Green Cube but require the Fortinet VPN to be used, similar to other outside connections made to Green Cube.

Concerning redundancy, there is an emergency plan in a case where many or all of the hospital's workstations are unable to function. As Green Cube can also function on the widely used cloud service AWS provided by Amazon, there is the possibility to switch over the system fully into the cloud.

Intrusion Detection of Cyber Attacks in Moncloa Hospital

There is no internal monitoring of the network traffic, making any data leakage difficult to detect according to the interviewees. The network provider ASISA provides weekly reports on adware/malware events as shown by the threat event example discussed in the previous section.

Whenever an anomaly is detected, ASISA typically sends their team to work with the hospital's local IT team to for in-depth analysis. There is no written policy on these procedures, which is a potential oversight that may need to be fixed in the future.

Green Cube System

Concerning the Green Cube system, the interviewees explained that it logs access to the system and its data, making it possible to verify actions in retrospect. On the network side, Telefonica is again responsible to analyse whether there are any security breaches to the system. For this, Telefonica has specialized security information and event management software (SIEM) deployed.

The main token to authenticate to Green Cube for a user is their user/password combination. There are several policies regarding this key password. It needs to be renewed every 3 months and the guidelines require it to be alphanumeric with at least 8 digits, providing basic security against brute force and dictionary attacks.

Mobile Apps

Moncloa further offers a mobile phone app, which helps in scheduling appointments and advises patients and customers about where to go in the hospital. Crucially, it also allows to access some parts of the patient's health report. There are further apps used within the hospital group, but this was out of the scope of the assessment.

Assessment of Main Exposure

Similar to the questionnaire analysis, the interviewees consider three main exposure areas relating to cybersecurity: First, installation of any malware on workstations. Second, gaining access to Green Cube login information. Third, there are no current measures deployed that would detect any breaches, which cause information leakage, i.e. stealing of hospital or patient data.

5. ADVANTAGES AND DISADVANTAGES OF CLOUD-BASED HOSPITAL IT INFRASTRUCTURE WITH REGARDS TO SECURITY – A COMPARISON

In this section, we discuss the fundamental differences between the underlying IT infrastructure approaches used in Moncloa and Fuenlabrada. On the one hand, we have a more modern cloud-based infrastructure, which outsources much of the software and hardware to external suppliers. In contrast is the more traditional in-house infrastructure, which grows organically and in a much more decentralized fashion with the needs of the separate hospital departments.

We compare these two systems by looking at their characteristics from three different perspectives: **technical, legal and business.**

5.1 Technical Perspective

5.1.1 Single point of failure

From a technical perspective, a centralized cloud system naturally offers a single point of failure. In case of a problem with the system all hospital systems at Moncloa -- and in a worst case scenario all other hospitals served by Green Cube -- are affected at the same time, leading to a potentially severe outage situation. Exemplary problems targeting this single point of failure could be a malicious denial of service attack of the cloud provider, their network infrastructure,

74 https://www.fortinet.com

or the internet connection of a given hospital. It is possible to mitigate these problems using redundant systems, infrastructure and additional security measures (e.g., DDoS protection offered by dedicated service providers).

5.1.2 Homogeneity vs. Heterogeneity

The second main technical difference is the grade of heterogeneity in a traditional enterprise network compared to a cloud-based system. In a large hospital network, such as found in Fuenlabrada, there are hundreds of systems in different departments, with high variation in suppliers, software, hardware, age, and compatibility. High heterogeneity typically has negative consequences for the ease of deployment or replacement of systems, patching processes, and efficient interconnectivity between different entities. This can also negatively affect security, in particular as maintenance can becomes complex and difficult in the long run, compared to unified cloud-based systems. Furthermore, the large number of different systems each offers separate security vulnerabilities, which may be more easily exploitable by an attacker. On the other hand, like in nature and agriculture, a pure soft- and hardware monoculture can potentially aid the quick spread of malicious software as all nodes are vulnerable against the same attacks.

5.1.3 Outsourcing of threat vectors

While in the in-house system many or most attack vectors are physically and logically within the hospital perimeters, this is different for cloud-based IT infrastructures. In a pure cloud environment, were thin client terminals offer only a connection to the cloud middleware, the attack vectors are severely reduced and effectively outsourced to the cloud provider. Controlling access with regards to insiders (e.g., via USB sticks) is less difficult compared to a system with fat clients. In reality, we often see a hybrid model where both thin and fat clients are available in the hospital infrastructure. Furthermore, the handling of many security attacks is naturally also being outsourced to the cloud provider, including the responsibility for availability, redundancy and data backup strategies.

5.2 Legal Perspective

5.2.1 Outsourcing of risk

With regards to the security of the hospital IT infrastructure, a cloud system may constitute an outsourcing of risks from a legal perspective. Whereas a traditional inhouse infrastructure puts the risk squarely on the hospital (subject to negotiated contracts with vendors and suppliers), typical cloud systems outsource the risk of a security breach to the cloud operator(s).

5.2.2 Outsourcing of data / regulatory environment

In a cloud-based hospital infrastructure, the data for patients and employees, which is considered highly sensitive in most jurisdictions is also not held on the hospital premises. Depending on the jurisdictions, customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider and laws on the location where data is being held may restrict the choice of cloud providers.[75] It is imperative to examine all legal and regulatory requirements in the process of moving to cloud-based healthcare systems and to keep up with new regulations such as the General Data Protection Regulation (GDPR), which becomes enforceable in the EU on 25 May, 2018. Lastly, the access to the data by employees of the cloud provider also has to be considered. Encryption can help solve many issues related to the access of sensitive data, but technical necessities may still require non-medical employees to work with patient data in some cases.

5.3 Business Perspective

5.3.1 Efficiency

The use of a single homogenous system can enable synergies and efficiencies in terms of the business expenditure with regards to the security infrastructure. Easier maintenance, employee training and interfacing between systems can reduce both the number of work hours and hard-/software expenditure. Hence, in the long run, there may be potentially significant cost-savings with a unified cloud system. Naturally, this is dependent on many other factors such as the negotiation power of suppliers and customers and the competitiveness of the market.

5.3.2 Outsourcing/contracting of employees

The outsourcing of IT infrastructure, services and employees has been a popular business strategy in many industries since the 1990s. Benefits and drawbacks of this approach have been widely researched and ultimately also apply to a cloud concept such as the one provided by Green Cube for Moncloa hospital. In particular so-called 'total' outsourcing deals with a single supplier are classed as potentially high risk from a business perspective. While these risks could potentially be mitigated with a multi-vendor strategy or co-holdings between vendor and client (or a parent company),[76] these approaches may be in direct conflict with efficiency gains or other goals.

75 Brodkin, Jon. "Gartner: Seven cloud-computing security risks." Infoworld 2008 (2008): 1-3.

76 Willcocks, Leslie P., Mary C. Lacity, and Thomas Kern. "Risk mitigation in IT outsourcing strategy revisited: longitudinal case research at LISA." The Journal of Strategic Information Systems 8, no. 3 (1999): 285-314.

6. CASE STUDY: VULNERABILITIES OF LARGE MEDICAL DEVICES

In this section we study the security process surrounding large medical devices (LMDs) in the participating hospitals, whose operational systems was designed and established by Siemens Healthineers. We seek to contrast these vulnerabilities with the nature and scale of plausible threats. For example, if a cyberattack disrupted the operations of the HIS system, hospital staff would no longer be able to request CT scans or MRI diagnosis tools, nor could they request other laboratory tests during a conventional terrorist event. Attacks could further impair the decision making processes of government and health officials during a public health emergency.

We conducted a study concerning of vulnerabilities in LMDs based on information obtained in pre-assessment interviews (see Section 5) and a separate questionnaire answered by Siemens Healthineers. This questionnaire was further informed by a concrete vulnerability in Siemens Healthineers LMDs discovered during the course of this project in August 2017.[77] This vulnerability affected all Windows 7-based PET/CT and SPECT/CT scanners, which are used in hospitals worldwide.

Successful exploitation of these vulnerabilities allowed the attacker to remotely execute arbitrary code, i.e. potentially control the devices themselves and their access to the hospital networks. Exploits that target these vulnerabilities are known to be publicly available, i.e., they can be used even by unsophisticated threat actors, making this vulnerability one of the highest possible threat level, in particular when considering the importance and power of the involved LMDs.

Our questions focused specifically on the handling of vulnerabilities, i.e., their detection and the subsequent patching process, spanning from development of a patch to the deployment on the hospital's medical devices.

Q1. How does Siemens Healthineers learn about such a vulnerability? Does Siemens Healthineers have in-house penetration testing teams or does it rely on outside information?

Siemens has a dedicated department responsible for reporting vulnerabilities. To take advantage of this, all MI products have all their software components listed in a vulnerability tool and we get notifications of any vulnerability reported against any and all components. Every week, we assess every reported vulnerability and make decisions if the vulnerability is bad "Uncontrolled" or not-so-bad "Controlled."

77 ICS-CERT Advisory (ICSMA-17-215-02) Siemens Molecular Imaging Vulnerabilities, Original release date: August 03, 2017, Last revised: August 09, 2017

Q2. Consider the case, where Siemens Healthineers has been notified of such a vulnerability:

a) How long does it take to produce and publish a patch?

This certainly depends on the vulnerability. We work diligently on Uncontrolled vulnerabilities.

b) How long before Siemens contacts all affected users/ hospitals and lets them know about the problem and any mitigation measures?

For Uncontrolled vulnerabilities, we follow the FDA guidance of communication within 30 days and having a fix available within 60 days. For Controlled vulnerabilities, we usually collect them and either patch as some later date, or include the fixes in future versions.

Q3. How long after a patch for such a critical vulnerability is ready does it typically take to deploy it in a hospital?

For Uncontrolled vulnerabilities, the FDA guidance is 60 days. For e.g. WannaCry, we had patches ready within a week.

Q4. Who is responsible for this deployment (Siemens technicians?) and how long is the device out of use for an update?

(Answered in conjunction with Q5.)

Q5. Siemens Security Advisory SSA-822184 mentions a "Remote Update Handling" capability as opposed to on-site visits. What percentage of devices have this activated on average and is this being used in the Madrid hospitals they are responsible for (in the scope of this project)?

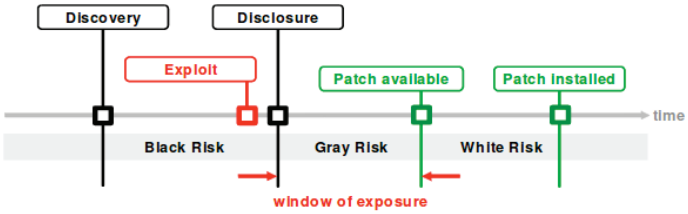
Today, we can either push it via Remote Update Handling (RUH) which is part of Siemens Remote Services (SRS), or we can have a technician on site. If we push via RUH SRS, then it is up to the customer to accept the update which will appear as a dialog box asking them if they want to perform the update. If, after 30 days, the site has not selected to do the update, we will send in a technician.

Lessons Learned

Based on the data obtained in this case study, we conclude that it is crucial to reduce the *Gray Risk* and *White Risk*, which exist between the disclosure of a vulnerability and the installation of a patch, as much as possible (see Figure 3 for an illustration). Whereas this is not sufficient against the most capable attackers with access to zero-day or even undisclosed, tailored exploits (*Black Risk*), quick action in developing and deploying patches (in particular where no mitigation options are available) is effective against the majority of the most common threats. As current guidelines of the US regulatory authority Food and Drug Administration (FDA) allow up to 60 days to develop

and deploy a patch even in critical situations, this leaves a potentially large window of exposure in which threat actors can exploit vulnerabilities in the wild. While vendors such as Siemens Healthineers proactively aim to reduce these risk times and react to critical exploits as quickly as possible, there is potential for improvement in all phases of the lifecycle, from discovery to patch development and patch deployment.

Figure 3. Vulnerability lifecycle and disclosure process.[78]



7. RECOMMENDATIONS

Based on this report, we present our recommendations for how to improve cybersecurity in hospitals. We describe several general measures and further recommend concrete solutions with respect to the two analyzed hospitals, Moncloa and Fuenlabrada.

1. **Future threat vectors:** Based on the review of cybersecurity incidents and the existing literature in Section 2 as well as the vulnerability analysis in Section 4 we name the three most urgent threat vectors that the examined hospitals face in the near- and medium-term future. Common enterprise malware
    - Social engineering and phishing attacks
    - Exploitation of hospital-specific hard- and software systems
2. **Knowledge sharing:** In a recent report on regulatory and non-regulatory approaches to cybersecurity information sharing the European Union Agency For Network And Information Security (ENISA) acknowledges that there is a strong strategic need to share knowledge and information to support the management of incidents, threats, and vulnerabilities.[79] The hospital and healthcare sector in Madrid should strongly consider engaging in regional or national information-sharing organizations to lean more about the cybersecurity risks faced by hospitals and exchange ideas and solutions with other stakeholders.[80]
3. **Cyber insurance:** Considering the potential financial and legal impact of a cybersecurity incident, the insurance industry is beginning to offer products, which cover the responsibilities following a breach. In light of the rapid development of this new field, it is sensible to regularly review the hospital's insurance coverage to determine whether the current coverage is adequate and appropriate given the current cybersecurity threat environment.
4. **Best practices:** While some attack surfaces are highly specific to hospitals and the healthcare sector (e.g., medical devices), much of the network infrastructure follows standard enterprise approaches. Consequently, implementing up to date enterprise security best practices such as regularly provided by the National Institute of Standards and Technology will eliminate a large majority of the existing cybersecurity problems.
5. **Resilience and recovery:** Resilience the ability of a system to "withstand a major disruption within acceptable degradation parameters and to recover within an acceptable time and composite costs and risks".[81] It encompasses the realization that it any complex system such as the ones found in hospitals will always include vulnerabilities. Attack prevention is important but regardless of the investment, a determined and resourceful attacker can find a way into them, as evidenced by breaches of even the most secure military systems. Thus, creating, reviewing, testing and evaluating the plans that mitigate the impact of the eventual breach or incident is crucial.
6. **Cloud solutions:** A unified, cloud-based solutions for hard- and software in hospitals can form one key part of a holistic security concept. By dealing with a single supplier and avoiding the difficulties for setup and maintenance, the overall security of the system may be improved. However, it is important to be aware of the risks of cloud-based solutions, which range from creating a single point of failure to data protection regulations, and also include many non-security-related considerations.

78 Frei, Stefan, Bernhard Tellenbach, and Bernhard Plattner. "0-day patch exposing vendors (in) security performance." *BlackHat Europe* (2008).

79 ENISA. "Cyber Security Information Sharing: An Overview of Regulatory and Non-Regulatory Approaches." 2015.

80 One global example of such an institution is the National Health Information Sharing and Analysis Center (NHISAC). See https://nhisac.org.

81 Haimes, Yacov Y. "On the definition of resilience in systems." *Risk Analysis* 29, no. 4 (2009): 498-501.

7. **Personnel:** Ultimately, people are the key part of a secure system, regardless of the environment. It is imperative to have a dedicated core cybersecurity unit that is tasked with securing hospital systems, in particular when they are complex, in-house administered networked systems such as found in Fuenlabrada. To achieve a security level that is as secure as the current state of the art, a larger budget for dedicated personnel is required, and should include board level involvement as appropriate. Well-trained people, who are first and foremost experts in security, are key to protecting the hospital from future attacks and breaches. Furthermore, they are able to improve the resilience of the system and respond appropriately in case of an attack, significantly minimizing the effects on the core medical functions of the hospital.
8. **Medical Devices:** In the future, it is imperative to work with the suppliers of all medical devices regarding the security of the delivered devices before connecting them to the hospital network. To obtain a base level of security, it is key to investigate the existing medical devices used by the hospital in accordance with the June 2013 FDA guidance to ensure that the devices include intrusion detection and prevention assistance and are not currently infected with malware. This approach may even include the introduction of cybersecurity teams (on a local, regional or national level) that have the contractual right to conduct penetration testing before buying and integrating LMDs into a hospital's network. Finally, where medical devices need to be interconnected, it is crucial to have a prompt patching process within days of a vendor's notification of a new vulnerability.

RESOURCES

[1] Blank, R. M., and P. D. Gallagher. NIST Special Publication 800-30 Revision 1 Guide for Conducting Risk Assessments. Tech. rep., National Institute of 1200 Standards and Technology, 2012.

[2] Strohmeier, Martin, Matthias Schäfer, Matt Smith, Vincent Lenders, and Ivan Martinovic. "Assessing the impact of aviation security on cyber power." In Cyber Conflict (CyCon), 2016 8th International Conference on, pp. 223-241. IEEE, 2016.

[3] Martin, Guy, Paul Martin, Chris Hankin, Ara Darzi, and James Kinross. "Cybersecurity and healthcare: how safe are we?." Bmj 358 (2017): j3179.

[4] Frei, Stefan, Bernhard Tellenbach, and Bernhard Plattner. "0-day patch exposing vendors (in) security performance." *BlackHat Europe* (2008).

[5] Haimes, Yacov Y. "On the definition of resilience in systems." *Risk Analysis* 29, no. 4 (2009): 498-501.

Acknowledgements

The project consultants are grateful for the valuable support that they received during the conduct of their work from CERNER, General Electric, Siemens, Fundación ASISA, Hospital Universitario de Fuenlabrada, Hospital HLA Universitario Moncloa, Dr. Carlos Mur de Víu, Dr. Carlos Zarco Alonso, and Dr. Francisco Ivorra Miralles.