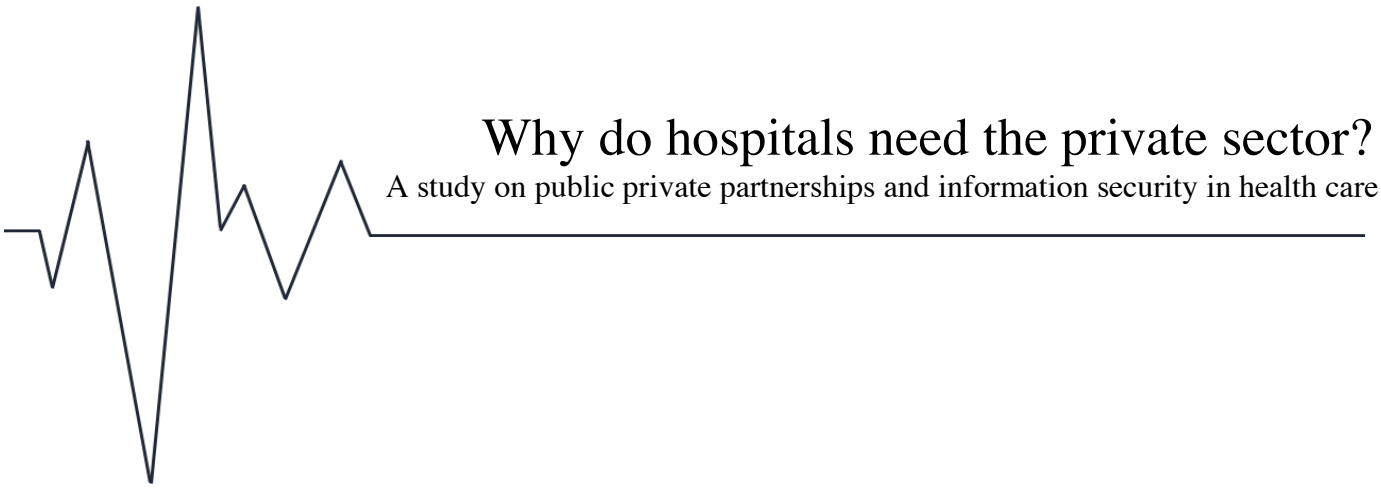
Universiteit Leiden



Why do hospitals need the private sector?

A study on public private partnerships and information security in health care

Master Thesis Crisis and Security Management
Marc van ‘t Hoff (s2304740)
Dr. Tatiana Tropina (Supervisor)
Dr.ir. Vlad Niculescu-Dinca (second reader)
12th of January 2020
20368 words (excluding references)

Table of Contents

List of tables

Chapter 1: Introduction

In the 1990's the concept of electronic healthcare was introduced to the domain of healthcare. All over the internet, people could find online health platforms or health discussion forums. People increasingly desired to know more about their health and track their own personal data (Lupton, 2016). This digitization of healthcare translated seamlessly into the professional sphere of healthcare. Where hospitals started with digitizing their administrative process, sooner rather than later hospitals were collecting various types of data about their patients. By now, almost all hospitals are highly digitized and automated, and have professional information management systems in place (Louwerse, 2004). These information management systems are becoming more and more connected to clinical practices within the hospital, making proper functioning of these systems therefore of great importance. The data hospitals collect on their patients is perhaps the most personal information about a person (Gostin, Turek-Brezina, Kozloff & Faden, 1993). This data includes personal information such as, name, age, sex, race, addresses, family status, sexual relationships and preferences, and Social Security numbers. It may include insurance related information, which can include financial information, employment status and history, and subsidy history. Additionally, it also includes previously established medical information such as, diagnoses, treatments, disease histories, dietary habits, genetic information, and psychological profiles (Gostin et al, 1993, Appari & Johnson, 2010, Khaloufi, Abouelmehdi, Beni-hassane & Saadi, 2018). This is already an extensive enumeration of medical related data collected by healthcare institution, however, the different types of information collected is certainly not limited to this.

The degree of sensitivity of healthcare related data requires the users to handle the information with great care. Users and collectors of this information should pay careful attention to handling or collecting the data without compromising the security or privacy of a patient (Smith & Eloff, 1998). In reality however, both users of patient information as patients themselves fail to see the importance of the security of healthcare related information. Hospital staff tends to enjoy a great degree of trust from their patient and colleagues (Box & Pottas, 2013). Hospital should, in fact, earn a high level of trust, in most cases they are responsible for the well-being of their patients. Still, this may have led to a significant level of negligence with regard to information security. This should concern both hospitals and patients, as healthcare data breaches have significant economic, social, and

legal implications (Gostin et al, 1993). Additionally, patient data can be desired by criminals, as they, for example, might 'exploit social security numbers for financial gain, use health insurance policies to file fraudulent claims, or write counterfeit prescriptions' (Collins, Sainato & Khey, p. 97, 2011).

Considering the above, one should expect healthcare institutions to direct significant attention towards securing their information management systems. However, research shows that this is not the case. In the United States, Security Scorecard ranks the healthcare sector 9th out of all 17 industries in terms of security (Khaloufi et al, 2018). In the Netherlands specifically, data breaches in the healthcare sector have risen significantly, with the sector having the highest total number of data breaches in both 2017 and 2018. Within the Dutch healthcare sector, hospital seem to be the main target, with data breaches nearly doubling from 772 in 2017 to 1450 in 2018 (Autoriteit Persoonsgegevens, 2017, 2018). Achieving a desirable level of information security requires significant financial commitment, however investments in healthcare on IT-related security are around 3-5% of revenue on average, significantly trailing other sectors that deal with sensitive and personal information, such as the financial sector, where investments tend to be around 10% of revenue (Appari & Johnson, 2010).

There is an obvious conclusion to be made regarding information security in the healthcare sector, it is substandard. Potential reasons for this lacking security might include, but are not limited to, the lack of budget, the lack of attention, and the lack of resources and knowledge. As the state is generally considered to be the main actor in providing security for critical infrastructure (Carr, 2016), it seems to be incapable of ensuring security in one of their most important public goods: healthcare. It raises the question if the healthcare and specifically hospitals are capable themselves of providing security for their information management systems. Hospitals are in the business of healing people, and not in that of information security. All patients, and potential patients, should be glad that hospitals devote all of their attention towards the treatment of patients. However, the security of information management systems should not be neglected. In the past, healthcare institutions have reached out to the private sector numerous times for cooperation and support. These partnerships with the private sector include both facility, infrastructural, and service purposes, but mostly with an emphasis on financial support from the private sector (Vecchi & Hellowell, 2018). Healthcare institutions are thus no stranger to public-private partnerships. This research aims

to investigate what the most important factors are that influence the decision of a hospital to engage in private public partnerships to address cyber security threats with regard to their internal digital information management systems.

Using previous theories on public private partnerships, a conceptual framework will be established that will present all the possible factors that affect a decision to engage in public private partnership. To identify which factors affect a hospital's decision the most, three case studies will be conducted. The case studies will be conducted at three Dutch hospitals, and will focus on previous public private partnerships that addressed their information management systems or other IT-systems.

This research will aim to answer the following research question:

"What are the most significant factors affecting the choice of Dutch hospitals to use public-private partnership in addressing pressing cybersecurity threats related to the use of internal digital information management systems?"

In order to answer this research question, several sub-questions will be addressed. These will be the following:

- *What factors affect the choice for Public Private Partnership in general?*
- *What are cybersecurity threats related to information management systems that hospitals need to address?*
- *Is there a relation between the cybersecurity threats and the identified factors?*
- *Why did Dutch hospitals choose for a PPP in the past?*

In addition to the earlier mentioned risks of healthcare data breaches, research has made interesting findings on the perception and result of data breaches. Firstly, Wilkowska and Ziefle (2012) found that patients have, in fact, a high awareness of the use of medical data, and are 'highly motivated to express opinions and fears connected to it' (p. 199). It showed that patients highly value security and 'controlled access' (p. 199) of their medical information. Secondly, Kwon and Johnson (2015) discovered that in the long-run patient visits to hospitals decrease as an effect of a large-scale data breach. Healthcare data breaches

might lead to theft of personal and medical data, a decrease in privacy and security, and fewer hospital visits in the long-run. Healthcare users should therefore be highly concerned with healthcare institution reaching a considerable level of information security. It is in the favor of society if healthcare institutions partner with the private sector to address threats they cannot deal with themselves. This research aims to offer insights to the public in the factors that impact the choice for this potential cooperation.

As mentioned earlier, public-private partnership is not a new phenomenon in the healthcare sector. Within the field of academics there has been a lot of research done on both public-private partnership in general and for the healthcare sector in specific. However, the existing research tends to focus on the private financing and operational side of public-private partnerships in healthcare. The field of academics lacks research on public-private partnership in security related practices within the healthcare sector, and reasons to choose such a partnership. This research aims to fill this gap in the field of academics.

In the next section, the body of knowledge will be presented. This body of knowledge includes the operationalization of key concepts, a literature review on why public organizations engage in PPP, and the theoretical framework. The third section will present the methodology. In this section the research design will be presented, including a clarification of the chosen cases, the topic of data collection will be addressed, and the limitations of this research will be mentioned. The fourth section will focus on the analysis of cybersecurity threats of hospital information management systems. This analysis will use previous research and the main hospital information security regulation to establish a proper understanding of current cybersecurity threats. The fifth section will present the results and the analysis of the case studies, with regard to the theoretical framework and the gained knowledge on current cybersecurity threats. The final section will present the conclusions of this research.

Chapter 2: Body of Knowledge

This section will aim to provide all needed theoretical background to answer the research question. This section will elaborate on the key terms of the research question, and will define them for the purpose of this research. It will over a review of the existing literature on PPP to construct a framework that addresses reasons for public organizations to engage in PPP. Additionally it will aim to identify the cybersecurity threats related to information management systems and how they can be addressed, based on the literature, and address the relationship between those threats and the reasons for choosing PPP.

2.1. Conceptualization of key terms

Cybersecurity

This research will be conducted within the field of security management, with a special emphasis on cybersecurity. Therefore establishing a proper understanding of the concept is critical. Before elaborating on the concept of cybersecurity, it is necessary to first establish an understanding of the domain in which cybersecurity operates: cyberspace. Cyberspace is a concept for which there is little consensus on a mutually agreed definition. To establish a working definition for this research, three definitions of government institutions are used. The joint chiefs of staff of the U.S. Department of Defense (2011) define cyberspace as 'the domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures' (p. 7). The U.S. Department of Defense (2019) itself defined cyberspace in their dictionary of military terms as 'a global domain within the information environment consisting of interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers' (p. 56). The Dutch Centraal Bureau voor de Statistiek (2018) refers to cyberspace as 'the set of links and relationships between objects that are accessible through a generalized telecommunication network, and to the set of objects themselves where they present interfaces allowing their remote control, remote access to data, or the participation in control actions within that cyberspace' (p. 15). This research will adopt the Dutch definition as its leading definition, since the focus of this research will be Dutch hospitals, and the definition avoids complicated detailed aspects of the telecommunication

network, making it a widely understandable definition. According to Von Solms and Niekerk (2013) cybersecurity involves a 'collection of tools, policies, and security concepts' (p. 97) with the general objective of maintaining the availability integrity, and confidentiality of data. This definition is supported by several researches, as there is a clear emphasis on the set of tools and policies implemented with the aim of protecting the availability, integrity, and confidentiality of data within the field of cybersecurity (Khaloufi et al., 2018, Wang & Lu, 2013, NCTV, 2018). This research therefore will define cybersecurity as the set of tools and policies implemented to minimize the probability of damage to the availability, integrity, and confidentiality of data for all users within cyberspace.

Threats to cybersecurity

The primary goal of this research is to identify the most important factors for choosing a PPP to address threats to cybersecurity. In general, threats to cybersecurity are threats that potentially compromise the desired level of confidentiality, integrity and availability (Von Solms & Niekerk, 2013). Within the general definition of threats to cybersecurity, a broad division can be made into two categories: threats with a technical nature and threats with a distinct human factor. For the purpose of this research, threats to the cybersecurity of hospital information management systems will be categorized within these two categories. How this division is established, and what actual threats to the cybersecurity of hospital information management systems are will be discussed in a latter section.

Public Private Partnership

Throughout this research, there will be a continuous focus on trying to identify why organizations choose a PPP to address certain threats. To be able to make this analysis, a clear understanding of the concept of PPP is required. Below, an overview of research that has been done on PPP in general will be presented. This will focus on defining PPP in general, and not on identifying the different arrangements or types within a PPP , since this is not relevant for this study.

Finding a mutual consensus on the definition of PPP in general is hard. As Dunn-Cavelty and Suter (2009) noted, it 'has become an extremely heterogenous concept and it has evolved into a catch-all label for all possible new forms or known forms of collaboration between government and the private sector' (p. 180). They do identify a goal of PPP, being the

'exploitation of synergies' (p. 180) within the cooperative use of resources of both involved parties, in order to achieve previously set goals in the most efficient manner, which would not be possible without the partnership (2009). Brinkerhoff and Brinkerhoff (2011) identify PPP as an agreement between the public and 'any organization outside the public sector' (p. 3), where all parties bring some form of incentives, goals, and resources. Jomo, Chowdhury, Sharma, and Platz (2016) described PPP along six key characteristics. According to their research, PPP's are long term arrangements between a government and a privately owned institution, where they make a key distinction that the private organization allocates its resources towards the improvement of a public service, and not to improve services within the private sector. Private actors receive some form of revenue during the arrangement, but will also have to make some investment contributing to the partnership. The public sector will have to provide all additional resources such as 'access to land, existing assets, or the provision of debt' (p. 5). When the arrangement comes to an end, all assets will be owned by the public entity again, eliminating the possibility of full privatization. Akintoye (2003) also acknowledged that there is no consensus of the definition of PPP, but noted that the existing definitions all have common features. First, PPP is a partnership of at least two parties, from which at least one is a public organization and another is a private institution. Second, all involved actors 'are capable of bargaining on its own behalf, rather than having to refer back to other sources of authority' (p. 6). Thirdly, participants enjoy a good and stable relationship during the partnership. Fourth, all parties are capable of adding relevant capabilities and resources to the partnership. Finally, all parties 'share the responsibility of the outcome of the partnership' (p. 6).

The definition for PPP used for this research will combine elements of the above. Identifying PPP as a mutual agreement between at least two parties, from which one is a public institution and one is a private organization. This partnership is based on a mutual goals, which aims to improve the provision of a public service, where this goal could not be attained without both parties involved. The partnership is no one-way agreement, and all involved parties add relevant resources to the arrangement and share responsibilities.

Hospital information management systems

A key focus of this research will be on internal digital information management systems in hospitals, therefor a proper understanding of the concept needs to be established in order to

analyze the related cybersecurity threats properly. This section will not elaborate on the security threats related to information management systems in hospitals, since an excessive analysis will be done on this topic in section four. This paragraph aims to identify what internal digital information management systems in hospitals are.

The concept internal digital information management systems consists of three separate concepts, internal, digital, and information management systems. The first two concepts are used to specify the research area. This research will look at internal systems, these are systems that are used internally in a hospital, and do not have the function of sharing data with other parties outside the hospital. This eliminates cybersecurity threats that are associated with sharing patient data with other healthcare institutions, and allows for specific focus on the context of the hospital. The concept digital is used to emphasize that this research will analyze computerized and/or automated information management systems. This eliminates potentially existing data collection processes that are being carried out with paperwork.

According to Masrom and Rahimly (2015), 'hospital information systems are integrated information systems designed to manage administrative, financial, and clinical aspects of a hospital. The aim of hospital information management systems is to achieve the best possible support of patient care and administration by electronic data' (p. 52). They identify the key goals of the system as the storage of data in databases, the automation of patient administration and management, and 'support of healthcare activities at the operational, tactical, and strategic levels' (p. 53). Louwerse (2004) identifies hospital information management systems as the IT system in which electronic patient records are being managed, in order to support clinical services, ensure effective communication, provide a reporting system, exchange knowledge and diagnoses between different disciplines within the hospital, and provide interaction between laboratory systems. These systems are typically not one overarching network, but can be implemented to serve a specific purpose within a hospital. These can include, for example, systems to store and internally share medical images, systems to support nursing services that include solely patient data, systems that store large amounts of data analyzed in laboratory environments, or hospital pharmacy systems that include all information used to supervise and distribute medicinal care to patients (Liu, Chung, Chen, & Wang, 2012). Internal digital hospital information management systems can

take on many forms, but these different forms will generally serve the same goal and have the same characteristics. This research will therefore combine elements of the definitions above, and define internal digital hospital information management systems as integrated systems used in multiple departments within a hospital, that store a wide range of hospital related information, which is not limited to patient information, automate administrative processes, and provide internal information sharing between hospital disciplines, in order to support clinical services and improve patient care.

2.2. Literature review: Why do public organizations engage in PPP?

The aim of this research is to address the question why hospitals choose to engage in PPP and what the most significant reasons for this are. In order to be able to analyze this matter, a proper understanding on drivers for PPP is needed. This section will present an overview of drivers for PPP based on existing literature on PPP. These existing theories will be addressed systematically in order to answer the question: why do public organizations engage in PPP? As mentioned earlier, PPP are often seen as a comprehensive term for every possible cooperation between a public and private party. In the previous section, the definition of PPP was addressed, but not the question of what drives a public (or private) organization to engage in PPP.

Carr (2016) addressed the need for PPP in the formation of national cyber-security strategies in her research. She contributes the reason for engaging in PPP towards the observation that both parties of the partnership are unable to achieve the desired results by themselves. Multiple researchers agree with this view. Brinkerhoff and Brinkerhoff (2011) mention “to move from a no-win situation to a potential win-win situation” (p. 5) as one of the reasons for a PPP. Dunn-Cavelty and Suter (2009) mirror the view of Carr by stating that PPP are the go-to solution when parties are unable to achieve goals without each other. Linder (1999) and Li and Akintoye (2003) agree with these views, but have a different approach. As they do not mention that goals are unattainable without the partnership, they both state that the partnership allows public organizations to develop solutions for existing problems with regard to a set goal.

Linder (1999) and Li and Akintoye (2003) share another reason for engaging in PPP in their researches. Both researches address PPP in general and give a systematic overview of what a PPP is, why it is used, and what can be improved. Besides the possibility to create solutions out of PPP, they both see the possibility to achieve a greater extent of innovation as an important driver for PPP. Klijn and Van Twist (2007) who performed a comparable research but focused on the Netherlands in specific agree with this, as they see PPP as the opportunity to establish innovation. In their whitepaper, PWC (2018) addressed the subject of PPP specifically for healthcare. While identifying multiple drivers, they also stated innovation as an important driver, as a PPP allows more access to innovative practices for a public organization.

This increased access to innovation, mentioned by PWC, can also be seen as the case that PPP allows public organizations to get access to resources, capabilities and knowledge of private organizations, as Li and Akintoye mention this as a significant driver for PPP (2003). PWC (2018) mention this as well, by stating that a reason for engaging in PPP could be "the need for additional services, skills, or expanded capacity" (p. 9). Previously mentioned research also acknowledge that this increased access drives the choice for PPP. Dunn-Cavelty and Suter (2009) that the joint-knowledge of both parties in a partnership is a significant added value. Bazzoli (1997) adds to this that public organizations often have a need for more human resources, and private organizations can answer this need through a PPP. Nikolic and Maikisch (2006) also mention that a benefit of a PPP is that public organizations will be able to get access to technical expertise of private organizations, but also add that the management expertise of these organizations is of significant value, as it will lead to "better healthcare management" specifically (p. 5). Other researchers mention this potential benefit of exploiting the management-knowledge of private organizations, as a PPP could improve basic management skills (Linder 1999, PWC 2018), or the decision-making process (Brinkerhoff & Brinkerhoff 2011, Klijn & Van Twist, 2007).

Much related to achieving results that are unattainable without the partnership, is that often, the value of a PPP is that it significantly increases the quality of a project, solution, or outcome (PWC 2018, Klijn & Van Twist 2007, Nikolic & Maikisch 2006). Related to this view, Vecchi and Hellowel (2018) state that healthcare organizations could "achieve greater certainty over the quality of outcomes" (p. 3) by using PPP. Achieving greater certainty over

a certain outcome usually involves decreasing some kind or risk. According to multiple researches, PPP offers an opportunity to transfer risks or to minimize risks. This risk can be risks or uncertainty in general (Li & Akintoye 2003, Nikolic & Maikisch 2006), business risks (Bazzoli 1997), accountability risks (Brinkerhoff & Brinkerhoff 2011) or financial risks (Linder 1999, Vecchi & Hellowel 2018).

Financial risks involve mostly around the outcome of investments related to a project (Vecchi & Hellowel, 2018). According to Vechhi and Hellowel, PPP can decrease risks associated with these investments and result in better investment choices. Additionally, PPP can "reduce the whole-life costs of providing goods of a given quality" (p.2). Lowering costs of a project, service or good is an important feature of PPP, as most researchers mention this as a key driver for PPP. PPP has a key possibility to lower costs (Dunn-Cavelty & Suter 2009, Nikolic & Maikisch 2006, Li & Akintoye 2003, Klijn & Van Twist 2007). Besides the possibility of lowering costs, PPP also offers access to financial resources of the private organizations, therefore public organizations often consider PPP when they are in need of financial resources (Bazzoli, 1997). PWC (2018) add to this that cooperating with a private organizations, and by using its financial expertise, can significantly improve cost efficiency.

Next to decreasing costs, improving efficiency and effectiveness of projects or services is an often mentioned driver for PPP. Public organizations tend to engage in PPP when it aims to increase or improve efficiency (Dunn-Cavelty & Stuer, 2009, Li & Akintoy 2003, Nikolic & Maikisch 2006) and effectiveness (Brinkerhoff & Brinkerhoff 2011, Klijn & Van Twist 2007). Bazzoli (1997) adds to this that PPP is more likely when the joint efforts produce a service that is more efficient than actions without the partnership.

Beside these, often mentioned, main drivers for PPP, there are some miscellaneous and perhaps project dependent drivers for PPP. PWC (2018), which explicitly focusses on drivers for healthcare PPP, adds that a PPP may be considered when healthcare infrastructure is in need of upgrades, or when "there is a need for stronger and more efficient procurement" (p. 9). Linder (1999) offers a whole new reasons why public organizations may consider PPP, as his research considers PPP as a boost for reputation, calling it "a comprehensive tool for remaking governments in the market's image" (p. 44).

2.3. Theoretical framework

In the previous section, an overview of the existing literature on reasons for choosing PPP was presented. Based on this field of literature, a framework will be established with factors driving the choice for choosing PPP. Based on this framework, further analysis will be performed to find which of these factors impacts the choice of Dutch hospitals to engage in PPP to address pressing cybersecurity threats the most.

Costs and other financial reasons:
The first factor that impacts the choice for PPP is 'costs and other financial reasons'. Reasons that will be considered under this factor will be reasons regarding cost reduction, improving cost efficiency, improving quality and outcomes efficiency, and access to financial resources and working capital.

Access to knowledge, resources, and capabilities:
The second factor is the possibility of 'access to knowledge, resources, and capabilities'. This factor addresses PPP's that are based on the need from the side of the public organization for the knowledge, resources, and capabilities of the private partner. These resources and capabilities can be both technical as human. Knowledge can take any form where the private organization can add knowledge, such as, but not limited to, management expertise, innovation, and technical knowledge.

Improving efficiency and effectiveness:
'Improving efficiency and effectiveness' is the third factor of this framework. This will cover all the reasons for a PPP that tries to improve the effectiveness or efficiency of a project, service, or good from the side of the public organization. However, improving cost efficiency will not be considered under this factor, as it is part of the 'cost and other financial resources' factor. Also, when a level of efficiency or effectiveness is desired that is unreachable for both parties in the partnership, the reason will not be considered under this factor, hence it will be part of 'reaching unattainable goals for both parties'.

Reaching unattainable goals for both parties:

'Reaching unattainable goals for both parties', the fourth factor, is considered when both parties of the partnership move from a desired goals that is unreachable for the both of them, towards a reachable goal. Often, in a PPP, the desired goal is unreachable for the public organization, because they are in need of, for example, more techical expertise, and for that reason they engage in a PPP. In some cases both the public organization as the private organization need each other to achieve their desired goals, these are the cases when this factor is considered.

Transfer of risks or reducing risks:

The fifth factor that may impact the choice for PPP is 'transfer of risks or reducing risks'. Among these risks are considered the following cases, the outcome of a project, with the focus on quality, accountability for a project, or business-related risks. Risks associated with financial factors are not considered under this factor, as they are part of the first factor.

Project unique drivers:

The final factor includes project-specific factors that do not fit within one of the previously mentioned factors. Previous research (Linder 1999), and especially those focused on healthcare PPP specifically (PWC 2018, Vecchi & Hellowel 2018), do mention reasons that can vary based on the project. Therefore, this framework will also leave allow for reasons that do not belong to any of the five established factors. It could be the case that Dutch hospitals engage in PPP based on highly specific and project unique reasons, this factor allows for that.

In order to investigate whether the type of threat to the cybersecurity of hospital information management systems has an effect on the factors affecting the choice whether to engage in a PPP, two categories of cybersecurity threats are established: threats with a technical nature and threats with a distinct human factor. These two categories will be used in the analysis of the results to assess whether the type of threat has an impact on the factors affecting the choice of hospitals to engage in PPP. How the division into these categories is made and what actual threats are included in the categories will be discussed in chapter four.

Based on this framework, two hypotheses for the research question of this research are made, which are the following:

H_1 : All factors, both combined or separately, have a positive impact on the choice of Dutch hospitals to engage in PPP to address cybersecurity threats of internal digital information management systems.

H_2 : 'Costs and other financial resources' and 'access to knowledge, resources, and capabilities' have the most significant positive effect on the choice of Dutch hospitals to engage in PPP to address cybersecurity threats of internal digital information management systems.

This research expects all established factors to have a positive effect on the choice of Dutch hospitals, combined or separate, meaning that an increase in significance of one of the factors, several combined, or all combined, will lead to a higher chance of engaging in PPP. The objective of this research is to identify which factors have the most significant impact on the choice of a Dutch hospital to engage in PPP. Based on previous research, that frequently mentions financial reasons and knowledge-based reasons, combined with the lacking IT-budget and IT-knowledge in healthcare, this research expects 'cost and other financial resources' and ' access to knowledge, resources, and capabilities' to have the most significant impact on the choice of Dutch hospitals to engage in PPP.

Chapter 3: Methodology

In this section, the conceptual design of this research will be presented. This aims to clarify questions on why choices were made with regard to the research methodology, how this research will be conducted, and what will be researched.

3.1. Research Design

According to Verschuren and Doorewaard (2010) a research design should focus on what the research aims to achieve. It formulates the steps the research will follow in order to reach the research objective. For the case of this research, this raises the question of what is it this research is going to study, and how will it be doing this.

The purpose of this study is to explore what significantly drives hospitals to engage in PPP to address cybersecurity threats. It aims to identify the most important factors that affect a choice for such a partnership, which specifically addresses cybersecurity threats. Within the field of academics, there has been done much work on PPP and benefits or drivers of PPP. However, this field lacks knowledge on the specific considerations of public organizations to choose a partnership given a certain topic. This study will aim to offer this for Dutch hospitals and corresponding cybersecurity threats. Since there is little research done on this specific topic, this research will be an exploratory research. Exploratory research is best carried out in a field where little to no previous research has been done (Davies 2006, Walliman 2006). Additionally it offers an approach of discovering or generating theory (Davies, 2006) and to research relations between factors or processes (Walliman, 2006).

To achieve its research objective, this research will follow the following steps. During first step of this research the existing literature on PPP was reviewed and analyzed. By reviewing the literature on PPP, this research aims to identify all the potential factors that affect a decision of a public organization to engage in a PPP. On the basis of this review, the second step of this research, a theoretical framework is established, identifying all relevant factors that possibly impact the choice Dutch hospitals to engage in PPP. During the third step of this research the existing literature on cybersecurity threats of hospital information management systems and current regulatory documents of hospital information security, being the

international ISO-standard and the Dutch NEN-standard, is analyzed. This analysis generated a deeper understanding on the cybersecurity threats that need to be addressed through a PPP. This deeper understanding allows for two things. Firstly, a more focused approach to the case studies, as the deeper understanding will lead to a better focus on previous PPP that addressed cybersecurity threats. Secondly, it allows this research to analyze if the specific cybersecurity threats have an impact or relation with the most important factors affecting the choice, this is done based on the two previously mentioned cyber security threat categories. During the fourth step of this research, three independent case studies were performed, these studies will be discussed in more detail in the next section.

3.2. Case Study

The fourth step of this research will be a multiple case study. According to Baxter and Jack (2008) case studies are best suited for research that aims to answer 'why' or 'how' questions. They add that multiple case studies allow the researcher to "explore differences within and between cases" (p. 548). When a researchers expects to find similar results within multiple cases, a multiple case study is best suited (Baxter & Jack 2008, Noor 2008). This research will aim to answer the question of why hospitals choose to engage in a PPP, and expects the factors that affect this choice to be consistent over all hospitals. Therefore a multiple case study will be performed to analyze the established framework within the context of multiple cases to investigate possible similarities and differences.

The subject of these case studies will be Dutch hospitals. As mentioned earlier, the healthcare sector is one of the most vulnerable sectors as it comes to data breaches. Additionally, data collected within the healthcare sector is highly personal, and data breaches could have serious effects. Within the healthcare sector there are multiple organizations that collect data, such as hospitals, insurance companies, home doctors, and pharmacists. This research will focus solely on Dutch hospitals. Hospitals generate the biggest amount and variety of data, but do account for the biggest share of total data breaches within the healthcare sector (Autoriteit Persoonsgegevens, 2017, 2018**).** The focus of this research will be on Dutch hospitals as it allows the case studies to be built around in-depth interviews on location. The case studies will not focus on one particular PPP of a Dutch hospital, but will investigate the general

reasons for engaging in partnerships in the past. Focusing on the general reasons allows to discover trends in the reasoning of hospitals to engage in PPP. A key selection criteria for all hospitals will therefore be that they have been engaged or are currently engaged in multiple partnerships with private organizations. Additionally, the hospitals will be selected in such way that they make a sufficient representation of hospitals in the Netherlands. The focus will not be on one particular type of hospital, large, small, regional or academic, but on the entire field, in order for the result to be representative for all Dutch hospitals instead of just a narrow range of hospitals.

The first hospital that is the subject of one of the case studies is Amsterdam UMC. Amsterdam UMC is an academic hospital that consists of the recently merged VUmc and AMC. Since this merger, Amsterdam UMC is the largest hospital in the Netherlands (De Telegraaf, 2017). Amsterdam UMC is a particular interesting case to study as it generates vast amounts of data, having the highest number of patient-beds in the Netherlands, and because of the complex information management systems as it manages information from two locations. At Amsterdam UMC, two stakeholders were interviewed, being Jasper Luiten, Information Security Officer, and Marcel van der Haagen, Privacy Officer.

The second hospital that will be investigated is Spaarne Gasthuis. In 2015, the Spaarne Gasthuis was founded through the merger of Spaarne Hospital and Kennemer. Spaarne Gasthuis has hospitals spread around six different locations ("Geschiedenis" , n.d.). Additionally, Spaarne Gasthuis started restructuring its entire IT department in 2017, aiming to improve information security (Spaarne Gasthuis, 2018) The combination of the number of locations and the process of restricting the IT department in favor of information security make Spaarne Gasthuis particularly interesting. Besides this, Spaarne Gasthuis was ranked number one in the Netherlands in 2015 (AD, 2015). Analyzing how one of the best hospital in the Netherlands approaches PPP can offer valuable insights. At Spaarne Gasthuis, Marijn Smit, Head of Data Protection, and Ellen Verhoogt, Risk Officer were interviewed.

The third hospital that is investigated is Tergooi hospitals. Tergooi hospitals is a regional hospital based in Hilversum and Blaricum. It was ranked in the top 20 hospitals in the AD Top 100 Hospitals in the Netherlands (AD, 2015). As Amsterdam UMC, Tergooi hospitals also has an information management system across two locations. In addition, Tergooi started

constructing new parts of its hospital in the second half of 2019. This construction project also involves the restructuring of their information management architecture (Tergooi ziekenhuizen, 2019), making Tergooi a particular interesting case. With regard to the type of hospital, Tergooi is a regional, non-academic, mid-sized hospital. Being ranked number 20 in the Netherlands, Tergooi is a good example of an average Dutch hospital. At Tergooi, Jaap Markerink, Information Security Officer, was interviewed.

3.3. Data Collection

The first phase of this research involves desk research. To establish a good basis of theory on PPP and cybersecurity threats, sources will be collected from Leiden University's online library and Google Scholar. Source with a high number of citations are naturally preferred, however, since there is little previous research on this topic, this cannot be guaranteed. These databases offer a wide range of available documents on PPP and cybersecurity threats.

The second phase of this research will be the case studies. During the case studies, data will be collected in various ways. The first step is to perform a desk research to gain deeper understanding on the hospitals itself. This understanding will involve the information management systems they use, the organizational structure of their IT department, their annual budget, and the PPP that are made public. This information can be retrieved from various sources, such as, but not limited to, annual reports of the hospitals, annual reports of private partners, media-sources, and hospital publications. The second step is to perform in depth, semi-structured interviews with the key-stakeholders of the hospitals. This step will use semi-structured interviews as they allow to gain a deep understanding of the topic that is to be covered (RAND, 2009). It allows for a predetermined set of questions, with room for additional questions to ensure that a deep understanding of the reasoning of the hospitals is established. The main questions asked during the interviews will be based on the established framework, these questions can be found in the appendix. Based on the established knowledge on the hospitals, a guide of sub-questions will be established. These questions can vary per hospital in order to achieve the best results.

3.4. Limitations

"The need to spell out limitations of social research arises from the power of research to convince" (Shipman, 1997, p.7). According to Shipman (1997), a researcher is obliged to give its reader answers to claims for validity, reliability, and generalization, in order to address potential limitations of its research.

Validity concerns questions about how the research reflects the reality and add to understanding on how people, or in this case organizations, behave. The results of this research are directly collected from key stakeholders of the subject of the case studies. The results reflect the direct input from these stakeholders. This could have the result that the results are based on personal opinions of the stakeholders, instead of objective reasoning from an organizational perspective. To eliminate this concern, the design of the interview questions is critical. Reliability concerns question about the outcomes of the research if someone else would use the exact same methods. Regarding the results of the case studies, if one would follow the exact same method, there is a high chance that one would retrieve the same results. However the case studies are built on the established framework. This framework is mainly built on theory on PPP and cybersecurity threats, put partially on the, by the researcher established, link between the factors and the cybersecurity. This is the only part were subjectivity can come in, therefore it is necessary to be aware of this concern and to be critical of this link.

The main limitation of this research is its sample size. By looking at three hospitals, the results give a good insight on motivations for engaging in PPP. However, the sample size may not be sufficient to generate conclusive findings for all hospitals in the Netherlands, or the entire health care sector. Furthermore, by looking at small sample of hospitals, it could by the case that identified factors are based on coincidental tendencies within each hospital. While all hospitals are in a similar situation of having several physical locations after mergers and restructuring their IT department in that process, further research will be needed to achieve a higher level of generalization.

Chapter 4: Cybersecurity threats to hospital information management systems

As established in section two, cybersecurity involves all tools and policies that are implemented to minimize the probability of damage to the availability, integrity, and confidentiality of data for all users within cyberspace. This section will explore the threats and issues with regard for this cybersecurity specifically for the hospital environment. It will present an overview of what is most targeted in the hospital setting, and how these subjects are targeted, additionally, this section will present an analysis of the information security standard NEN 7510. The NEN 7510 standard is the most important information security standard for healthcare organizations in the Netherlands and is a direct translation of the international healthcare information security standards NISO 27799 and ISO/IEC 27001 (NEN, 2017a). Hospitals are targeted by criminals or other malicious actors for a variety of reasons. The information management system of hospitals is often targeted for the medical information it contains. This information is valuable for malicious actors as they can use it for identity theft (Murphy, 2015), they can trade the information on the Dark Web for financial gains (Martin, Martin, Hankin, Darzi & Kinross 2017, Luna, Rhine, Myhra, Sullivan & Kruse 2015, Van der Meulen & Lodder 2014), or they can publicly release the information to achieve any type of impact (2017). Another possibility is that criminals may try to shut down the entire system, either to damage the hospital or also for financial gain (Le Bris & El Asri 2016, Ross 2017). For hospitals, it is important to know why malicious parties target them, but it is even more important to understand how they do this and how hospitals can mitigate these threats. The NEN 7510 standards serves as a blueprint for hospitals in the Netherlands to identify these threats and to take appropriate measures. The standard acknowledges that maintaining an adequate level of availability, integrity, and confidentiality is especially important in healthcare organizations, where privacy and security of patients is of great importance but can be damaged easily (NEN, 2017a). The standards offers security measures of which is determined that they are suited to protect the availability, integrity, and confidentiality of information in the healthcare environment. These measures are based on the most critical threats to healthcare information.

4.1. NEN 7510 & Threat Categories

The NEN 7510 is the leading information security standard for healthcare organizations in the Netherlands. Hospitals in the Netherlands are not directly obliged by law or regulation to achieve NEN7510 certification. However, the NEN 7510 does have several relations with important information security law and regulations ("Achtergrondinformatie over NEN 7510", n.d.). For example, the most important regulation with regard to information security, the GDPR, states with regard to information security: "The controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with the Regulation" (Council of the European Union, 2015). Organizations can demonstrate that appropriate measures have been taken by obtaining certification for information security standards that have been approved by the GDPR, which is in the case of the health care sector the NEN 7510 ("Achtergrondinformatie over NEN 7510", n.d.). Hospitals are therefore very keen to obtain a NEN 7510 certification as it proves that their organizations is GDPR compliant. The NEN 7510 consists of two parts 7510-1 and 7510-2. The first part is called 'information security management-systems' and aims to provide guidelines to implement, maintain, and improve a solid management-system for information security ("Achtergrondinformatie over NEN 7510", n.d.). The second part is called 'control measures for information security'. This part is more operational and offers a guideline for health care organizations on how organizations can optimize the protection of confidentiality, integrity, and availability of information ("Achtergrondinformatie over NEN 7510", n.d.). It identifies the most pressing threats and offers suggestions on how to implement measures to counter these threats. There are 25 current threats to information security identified in the second part of NEN 7510. These threats range from simple user errors where hospital employees can accidentally send information to the wrong colleague to acts of extremism aimed to put down critical parts of health care organizations.

A threat to cybersecurity is something that significantly threatens the confidentiality, integrity, and availability of information (Von Solms & Van Niekerk, 2013). However, it is important to note that such a threat does not necessarily require a malicious hacker that tries to steal information using all kinds of hacks and viruses. Threats to cybersecurity resemble anything that can compromise information in any way. For example a hardware failure is a serious threat to the availability of information. However, the origin of the threat can vary

significantly. It can be a simple hardware error causing a hardware failure, but it can also be a hardware failure caused by a denial of service attack of a hacker. The origin of a threat may vary, but the essence of the threat remains the same. Therefore it is important to maintain a wide approach when considering cybersecurity threats in order to include all threats. When looking to the main and most common threats to hospital information security, a clear divide between two broad categories of threats can be made.

Firstly, there are threats with a clear human factor. This category does not regard humans writing a malicious code an infecting a targeted system with it. It covers threats that arise from a concrete human act, which is the direct cause of a data or security breach, either intended or unintended. In a hospital setting this can for example be a nurse that accidentally sends a patient information about another patient. Recently, one of the interviewed hospital had a considerable data breach when around 140 patient e-mail addresses leaked ("Tergooi-ziekenhuis lekt e-mailadressen 140 patiënten, 2019). This was caused by an employee, who accidentally directed the e-mail to all addresses, instead of listing them all under blind carbon copy. This type of threat is one of the most common and most relevant threats to hospital cybersecurity (Wen & Tarn 2001, Narayana Samy, Ahmad & Ismail 2010, Luna, Rhine, Myhra, Sullivan & Kruse 2016, Murphy 2015). A majority of the threats listed in the NEN 7510 standard can be categorized as threats with a human factor. These range from theft or vandalism by either insiders or outsiders of an organization to workarounds using the account of a colleague or user errors as mentioned before (NEN, 2017b). Table 1 presents an overview of the identified threats from NEN 7510 with a human factor.

Threat	Description	Threat	Description
1) Masquerade by insiders	Cases where a system is used by an employee of an organization, using an account that is not their own (ISO, 2008)	2) Masquerade by service providers	Cases where authorized third party personnel use their access to enter systems or view data that they are not authorized to (ISO, 2008)
3) Unauthorized use of applications	Cases where health information applications are used unauthorized. This differs from case 1 in the sense that here someone uses an 'unattended working station' (ISO, p. 45, 2008), instead of deliberately using someone else's account to gain access to data.	4) Misuse of system resources	Cases where employees or other users of resources, use these resources for other goals than the intended goal. For example when employees use their workstation to download personal documents or check their personal e-mail (ISO, 2008)
5) Accidental misrouting	Cases where users accidentally send information to a wrong receiving address when being sent over a network. "Failure in user education". (ISO, p.47, 2008)	6) Operator error	Cases where users make errors operating the system. Can lead to huge amounts of unintended loss of data (NEN, 2017)
7) User error	Cases where users make mistakes handling information. For example information being left wide open on computers or information send to the wrong recipient. (NEN, 2017)	8) Staff shortage	The absence of critical employees or the simple shortage of security workers could lead to information security threats. (NEN, 2017)
9) Theft by in- or outsiders	Theft of either intellectual property by authorized insiders or physical property, such as laptops or briefcases by outsiders (NEN, 2017)	10) Willful damage by in- or outsiders	"Vandalism or other physical damage caused to IT" (ISO, p.49, 2008)

Table 1: Cybersecurity threats with a human factor

Secondly, there are threats with a technical nature. These threats mainly involve network technology, software, and hardware. However, as mentioned before, these threats are not limited to threats such as hackers and viruses, but can also involve power outages or connection failure not caused by malicious third parties. Hospitals often protect themselves against these threats through technical measures, using several layers of network defense such as firewalls and intrusion detection systems. Information security departments within hospitals often direct a lot of attention towards measures that protect hospitals against these types of threats, while threats with a human factor are far more likely . This is because the impact of threats with a technical nature is possibly much greater. Multiplying the impact with the probability of happening leads to the total risk of a threat. With threats with a technical nature, this risk score tend to be much higher than threats with a human factor (M. van der Hagen, personal interview, December 6, 2019)(Murphy, 2015). For example, the likelihood of a complete power outage in a hospital as a result of a cyberattack is very low, however, the impact is very high, as the hospital will shut down completely. Threats in this category include criminal acts such as network penetration by outsiders through for example social engineering or hacking, the introduction of damaging software such as malware, communication infiltration and interception through 'man in the middle' attacks and the embedding of malicious code such as viruses and worms. However, it also includes unintentional threats such as connection failures, repudiation, and network or software failures. An overview of all NEN 7510 threats with a technical nature can be found in table 2.

Thirdly, there are two other threats that fall outside the two identified categories. The first is environmental support failure, according to the NEN 7510 standard this threat includes cases of "power failure arising from natural or man-made disasters" (NEN, p. 159, 2017b). The second threat is terrorism, which includes acts of extremism aimed to disable or harm critical parts of healthcare organizations (NEN, 2017b). Since these threats are highly unlikely to happen and both have an impact of a different proportion then the other threats listed in the NEN standard, these threats are excluded from the two categories.

Threat	Description	Threat	Description
1) Masquerade by outsiders	Cases where information is accessed by unauthorized outsiders of the organization. Often hackers who act as an authorized users through hacks or social engineering (ISO 2017).	2) Introduction of damaging software	Cases where malware is introduced to the system. Malware is malicious software that can damage or disrupt computer systems, malware could be a virus, a worm, or other types of malicious software (ISO 2017, NEN 2017).
3) Communication infiltration or interception	Cases where hackers "tamper with the flow of data across a network" (ISO QUOTE) or intercept the flow of information.	4) Repudiation	Cases where the senders denies sending the messages and receivers denying that they received a message. (ISO 2017, NEN 2017).
5) Connection failure	Cases where connection fails. This could lead to the need to use less secure means to use, access, or send information. (ISO 2017, NEN 2017).	6) Embedding of malicious code	Cases where malicious code is entered into the system of the organization. This code can, for example, enter the system through e-mail viruses. Once entered, hackers can use malicious code to gain access to or control over the system. (ISO 2017, NEN 2017).
7) Technical failure of host	Technical failure of the host of the system. The host can take on several forms, such as hardware, a network facility, or a storage facility. (ISO 2017)	8) System or network software failure	Failure of the system or network, often caused by a denial of service attack (NEN 2017)
9) Application software failure	Failure of applications, often caused by a denial of service attack (ISO 2017)	10) Maintenance error	Cases where either internal maintenance employees or external maintenance employees make maintenance errors. Does often not directly lead to loss of or damage to data, but is a big source of weaknesses that can be exploited by hackers. (NEN 2017)

Table 2: Cybersecurity threats with a technical nature

Chapter 5: Results

In the following sections, the results of each case study will be discussed and analyze. For every hospital the results of the desk research and interviews will be presented. After all results, a brief summary of the overall results will be presented.

5.1. Amsterdam UMC

Amsterdam UMC is an academic hospital that operates from two locations, VUmc and AMC. Since the merger of the two academic hospitals VUmc and AMC into Amsterdam UMC, the hospital is the biggest hospital in the Netherlands, with more than 76000 unique patients in 2018 and a revenue of around 925 million euro. Amsterdam UMC approaches its business through its core values (Amsterdam UMC, 2019a). The hospital desires to deliver a considerable contribution to the quality of healthcare and with that the wellbeing of the people. Patientcare, education, and research are considered to the core business of the hospital, and their information technology and information management is a mean to support this (Amsterdam UMC, 2019a).

The public policy of the hospital states to that both hospitals aim to continuously improve information and communication technology within the hospital, of which information security is a critical part (Amsterdam UMC, 2019a). The organization sets itself targets to always keep their security up to the regulatory standards, and will proactively look for improvements. In 2017, the main focus of both hospitals (still separated as VUmc and AMC) was to be able to get the NEN 7510 certificate (AMC 2018, VUmc 2018). In 2018, after the merger, this remained a main focus, combined with increased efforts to be GDPR-compliant (Amsterdam UMC, 2019a). The hospital fully commits to protect the privacy of their patients and have a strong information security in an environment where changes happen fast and crime continues to increase. In order to establish this strong and stable level of information security, Amsterdam UMC has a specialized information security department. This department consists of a commission information security (location AMC), a commission privacy and information security (location VUmc), several privacy officers, several IT security officers, the director of the IT department and an internal Computer Emergency Response Team (Amsterdam UMC, 2019b).

Amsterdam UMC approaches information security as the matrix of measures that focus on continuously realizing an optimal level of availability, integrity , and confidentiality of information and their information management systems, while minimizing threats from outside and inside. The main goal of all measures is to maintain a stable level of security, while protecting against unintentional mistakes and intentional, malicious threats such as hacking, phishing, malware and fraud (Amsterdam UMC, 2019b). However, even in their information security policy, the hospital stresses that their core business tasks are patientcare, education, and research. Information is a necessary and important complement to this. From this standpoint, the hospital approaches its information security practices from three questions (Amsterdam UMC, 2019b):

- How can we minimize the risk of disruption of our information management systems?
- How can we manage damage in case of a disruption?
- How can we fix and repair the consequences of a disruption as soon as possible?

Based on these questions, the policy offers a set of starting points, from which the information security of Amsterdam UMC is approached. These internal policy goals are summarized in table 3 below (Amsterdam UMC, 2019b).

Category	Policy Goals
Management	• Meet the NEN7510 standard • Meet all laws and regulations • Information security is an integral part of the responsibility of internal management.
Risks	• A risk analysis classifies business units in terms of availability, integrity, and confidentiality • Actively engage in increasing awareness amongst employees • All employees will receive an internal training with regard to information security
Projects & Partnerships	• While designing security measures, Amsterdam UMC actively looks for partnerships with external parties.

Table 3: Amsterdam UMC information security policy goals

From these goals, two things are striking with regard to public private partnerships. First, Amsterdam UMC deliberately states to actively engage in partnerships with external parties. Second, the documents lists possible consequences of the risk analysis. These can be one or any combination of deploying a new information management system, deploying a new technology, or starting new processes or systems, where all of these can be done either internally or by an external partner (Amsterdam UMC, 2019b). Amsterdam UMC commits to engage in partnerships, however, their internal information security policy does not state any specific reasoning for engaging in these partnerships. The hospital's identity & access management policy does mention the processes by which Amsterdam UMC approaches IT-services. With regard to their IT-services, under which the information management systems and information security is situated, the hospital mainly uses three IT management processes: ITIL, BiSL, and ASL (Schriemer, 2019) (M. van der Hagen, personal interview, December 6 2019).

ITIL is a framework that is used to implement an effective IT service management. The ITIL process requires organizations to formulate a clear IT-service strategy, while defining questions like what services are offered and how these will be offered. It moves from a vision on where the organizations stands, to where it wants to go, while establishing how that will be done and what is the 'fundamental', most effective and efficient way of doing that. Parties that use ITIL define what services need to be measured or analyzed, gather and process data, and use this to create 'action plan' and implement new services (Cartlidge, Hanna, Rudd, Macfarlane, Windebank & Rance, 2007).

BiSL is a framework that operates from a business perspective. It assumes that the business is in the lead in determining how IT budget will be spend, that it 'knows and formulates its needs now and tomorrow', it consequently selects it suppliers (internally or externally) and manages all relations (ASL BiSL Foundation, n.d.).

ASL is a process to establish an effective application management. It originates from common problems in IT service, such as quality issues, misunderstandings, complex systems, the increased number of applications, the level of diversification and specialization and the inability to control everything. ALS offers guidance in how to effectively manage your large, complex, and specialized portfolio of applications (ASL BiSL Foundation, 2014).

The combination of the information security strategy outlined in the internal policy and the IT-processes of Amsterdam UMC present an indication on how the hospital approaches security decisions. It states that it actively engages in partnerships with external parties for the design of security measure with regard to information security. How Amsterdam UMC decides to engage in a partnerships rests on the combination of processes and the risk analysis. During their risk analysis, the security officers determine what the desired needs are based on the ITIL and BiSL frameworks. The analysis is done to discover what is needed from the IT-service perspective and from the business perspective. From those identified needs, an action plan is established on how to address these needs or how to establish new security measures. In the philosophy of the ITIL and ALS processes, the choice of measures is based on what the most effective and efficient measure is, the level of diversification and specialization, and the capability of the organization to control all services. This suggest that Amsterdam UMC bases it decision to engage in partnerships with external parties on if they are capable of delivering an effective and efficient measures themselves, if they can handle the level of diversification and specialization of the identified need, or on if they have the capability to handle the load considering their resources.

The following sub-section will present the key findings of the interviews with Amsterdam UMC. This will offer insights into the practical implications of the information security policy.

5.1.1. Interview results

In section four, the most pressing cybersecurity threats with regard to the information management systems in hospitals were established and categorized into two main categories: cybersecurity threats with a human factor and cybersecurity threats with a technical nature. Based on this distinction, Amsterdam UMC was interviewed to investigate based on what reasoning the decisions is made to engage in a partnership.

Cybersecurity threats with a human factor

In the latest risk analysis of Amsterdam UMC, cybersecurity threats related to human factors were ranked as the number two most critical threat. This ranking was based on the exceptionally high level of likelihood. However, the impact of cyber security threats related to this category was relatively low. To mitigate this threat, the hospital has taken several measures. Employees of the hospital are made aware through mandatory e-learning modules, presentations, and educational material. Besides this, all employees are required to sign a data confidentiality agreement at the start of their employment. These measures were both mentioned by the policy documents, and the security officers. Additionally, the hospital has developed clear identity and access management policy, where the hospital states to continuously monitor access granted to its employees. When asked about whether the hospital engages in partnerships to address this category of cybersecurity threats, it was often mentioned that the hospital's policy is to address these threats internally (M. van der Hagen, personal interview, December 6 2019). For example, with regard to the e-learnings used to create awareness, the following was mentioned (M. van der Hagen, personal interview, December 6 2019):

"*To get a grip on the human risks, we like to use e-learnings. We develop these e-learnings ourselves, since we have more knowledge on how data is used within our hospital than external parties would have"*

With regard to the data access management, an significantly important part to mitigate human risks, the hospital's internal data access management policy mentions that the GDPR obliges hospitals to achieve both accountability as auditability with regard to their data access management. This was also echoed by the interviewee, adding that this had led to the desire to keep some of these measures under their own control (M. van der Hagen, personal interview, December 6 2019):

"Since the GDPR, we need to be both accountable and auditable. Therefore, we like to keep some things internally"

Based on both the policy documents as the practical insights of the security offices, it is evident that Amsterdam UMC does not engage in public private partnerships to address cybersecurity threats with a human factor. These results are summarized in table 4.

Factor	Reason?	Specific reason(s)	Level of importance
Costs and other financial reasons	No	• General policy to create awareness internally • More internal knowledge to develop e-learnings • Strong internal access management is sufficient • Desire to keep accountability and auditability internally	---
Access to knowledge, resources, and capabilities			
Improving efficiency and effectiveness			
Transfer of risks or reducing risks			
Reaching unattainable goals for both parties			
Project unique drivers			

Table 4: Amsterdam UMC factors in relation to cybersecurity threats with a human factor

Cybersecurity threats with a technical nature

The first and third place of the three most critical threats, identified by Amsterdam UMC, are occupied by technological and malicious threats, such as ransomware and hacking. These threats are ranked high, not because of the high likelihood that they occur, but because of the potential impact (M. van der Hagen, personal interview, December 6 2019). For example, a complete shutdown of the hospital's information management system as a result of a ransomware attacks would have a disastrous impact on both the hospital and it's patients. To manage these risks, the hospital proactively performs risks assessment. This assessment is based on the identified risks by the NEN7510 standard. To obtain a NEN7510 certificate, a hospital has to have sufficient measures in place according to the identified risks. How these measures are designed is up to the hospital (M. van der Hagen, personal interview, December 6 2019). As described earlier in this section, Amsterdam UMC approaches its IT services from the ITIL, BiSL, and ASL processes, by which they identify what needs to be addressed, how it will be addressed, and how they will do this. Based on these processes within Amsterdam UMC, the decision whether or not to engage in a partnership is based on the desired effectiveness and efficiency, the level of diversification and specialization, and the level of complexity and workload. The interviewees acknowledged that the hospital engaged in partnerships with regard to threats with a technical nature (M. van der Hagen, personal interview, December 6 2019)(J. Luijten, personal interview, December 11 2019). There were multiple reasons for engaging in these partnerships, and mostly in line with the strategy as constructed from the processes. Below the hospital's main reasons for engaging in partnerships will be elaborated in line with the previously established factors for choosing a PPP. A summary of these factors can be found in table 5.

Costs and other financial reasons

From a policy and strategy perspective, Amsterdam UMC does not touch upon budgetary challenges with regard to information security. What is mostly stated is that the focus is to achieve, at all costs, a stable level of security according to all standards and regulations. When asked about financial reasons to engage in a partnerships, the interviewee mirrored this view (J. Luijten, personal interview, December 11 2019):

"*From an organizational perspective, we never engage in a partnership based on budgetary reasons"*

Additionally, it was stressed that while on the long run and in some particular cases a partnership with a private partner often is less costly, it is never a reason to engage in a partnership (J. Luijten, personal interview, December 11 2019). There were two main reasons for this. Firstly, since the GDPR penalties for institutions are clear and significant. For the leaders of Amsterdam UMC these penalties make it clear what they can invest in a sufficient level of security, in order to avoid paying this amount as a penalty. Secondly, reputational damage is something Amsterdam UMC wants to avoid at all costs (M. van der Hagen, personal interview, December 6 2019). Therefore, the hospital tends to take no risks when it comes to budgetary questions (M. van der Hagen, personal interview, December 6 2019):

"We never select partners based on costs. From an organizational perspective, there is zero risk taken on that part."

Access to knowledge, resources, and capabilities

Based on the relation between Amsterdam UMC's policy and the IT processes the hospital has incorporated. The factor access to knowledge, resources, and capabilities should be a significant reasons for engaging in partnerships if the hospital does not have sufficient in-house capabilities or resources.

The information management architecture within Amsterdam UMC is very complex, in total there are around 150 different information management systems, connected to over 24000 devices that send information into these systems (M. van der Hagen, personal interview, December 6 2019). This makes the control and maintenance of all these systems very complex. This has led to the point that the hospital simply isn't able to maintain all these systems by themselves anymore. Private parties are significantly better suited to design systems or perform maintenance on systems that require a high level of specialized knowledge or skills. Amsterdam UMC does not have the ability anymore to maintain the same level of specialized knowledge that private parties can offer, therefore the hospital often engages in partnerships because a private party does have this knowledge (J. Luijten, personal interview, December 11 2019):

"The architecture is extremely specialized, as an organization you have to be really dedicated to maintain that level".

In addition, private parties are often capable of offering Amsterdam UMC services that they could never offer themselves. Such as a 99.99% level of availability of private data centers, 24-hour firewall and intrusion detection services, or large user-data databases where they collect large amounts of data on security incidents of other customers and use this to improve their services (M. van der Hagen, personal interview, December 6 2019). These capabilities are an important factor in the decision to engage in a partnership for Amsterdam UMC.

Improving efficiency and effectiveness

Similar to the previous factor, the factor improving efficiency and effectiveness runs parallel with the IT processes of Amsterdam UMC. The level of complexity of the information management systems of Amsterdam UMC does not only require a high specialized set of knowledge, it also makes it difficult to effectively and efficiently manage all the information systems. When partnering with a private party, the high priority the private party assigns to the hospital is a significant advantage (M. van der Hagen, personal interview, December 6 2019):

"*We often partner with a private party for maintenance purposes, they do not have priority-challenges. This keeps everything continuously maximal secured, never: could this wait a week longer?"*.

Additionally, private parties can simply make security measures more effective. As Amsterdam UMC acknowledges that private parties can make security measures more effective in some cases, and that they use private parties to perform checks or Pen tests to assess the effectiveness of current security measures (J. Luijten, personal interview, December 11 2019).

Transfer of risks or reducing risks

As mentioned earlier, the GDPR requires both accountability and auditability, and Amsterdam UMC expresses a preference to take as little risk as possible and not to outsource risks. However, this does not mean that they can engage in partnerships to reduce the risk. In case of a large incident, the hospital often partners with private parties to perform what the hospital calls 'health checks' to identify what the cause of the incident was, eliminate the risk of the incident happening again, and reduce the risks of getting penalized (M. van der Hagen, personal interview, December 6 2019).

Reaching unattainable goals for both parties

Most private parties the hospital partners with have a business model of delivering information security products. It is in their best interest to deliver the best possible services, but this comes rarely from a distinct and intrinsic motivation to improve security in healthcare. There is, however, one partnership Amsterdam UMC engages in that does find its basis in a mutual goal of improving security. Amsterdam UMC partners with Z-CERT, a non-profit, non-public computer emergency response team. Z-CERT main purpose is to battle cybersecurity threats in partnership with hospitals and other healthcare organizations (J. Luijten, personal interview, December 11 2019). To state that the goals of information security is unattainable for Amsterdam UMC without this partnership is an overstatement, but both parties definitely need each other to reach their goals.

Project unique drivers

In the information policy of Amsterdam UMC, the hospital states that with every unique project, information security should always receive a high level of consideration (Amsterdam UMC, 2019b). This does not necessarily means the hospital engages in partnership for unique projects specifically aimed for security purposes. However, the hospital does take this into consideration. For example, after the merger, the Amsterdam UMC switched its digital patient information system to EPIC, a system developed by Chipsoft. After this decision the hospital chose to host this system in an external data center. They did this because they saw the possibility of an inter-hospital shared patient information system, and an external data center was best suited to achieve for example the required level of security and availability (J. Luijten, personal interview, December 11 2019).

Factor	Reason?	Specific reason(s)	Importance
Costs and other financial reasons	No	• We never choose a partnership solely based on financial reasons • From an organizational perspective, there is zero risk taken on security measures	--
Access to knowledge, resources, and capabilities	Yes	• We do not have the specific knowledge or capacity internally. The systems have become too complex (4x) • Private parties can deliver a level of service we can never match (2x) • Private parties have a higher level of specialized knowledge (3x) • Private parties have a very large amount of user information. This is a large advantage. (3x)	High
Improving efficiency and effectiveness	Yes	• We actively partner with private parties to perform audits, health checks or pen tests to assess the effectiveness of security measures • Private parties often do not have priority challenges • Private parties make our information security more effective	High
Transfer of risks or reducing risks	Yes	• In case of large incidents, private parties come in to control, check, and fix the problem. This reduces risks on our side.	Low
Reaching unattainable goals for both parties	Yes	• Our partnership with Z-CERT is based on the mutual goal of improving information security in healthcare	Low
Project unique drivers	Yes	• We hosted our mutual patient information system at a private party. To make it possible for other hospitals to join in the future.	Low

Table 5: Amsterdam UMC factors in relation with cybersecurity threats with a technical nature

5.2. Spaarne Gasthuis

The Spaarne Gasthuis is a hospital that operates from four locations, two in Haarlem, one in Hoofddorp and one in Heemstede. The hospital is a merger between the Kennemer Gasthuis and the Spaarne Ziekenhuis (Spaarne Gasthuis, 2019) Across all locations Spaarne Gasthuis has 611 available hospital beds and had a total of around 34000 hospilizations in 2018 and around 220000 clinic visits. It has around 4000 employees and generated a total revenue of 459 million euros in 2018 (Spaarne Gasthuis, 2019). The Spaarne Gasthuis was the first Dutch hospital to use EPIC as their information management systems, which made them clear frontrunners in that field (M. Smit, personal interview, December 20 2019).

In the past decade the hospital has continuously stated to actively protect information security within the hospitals. Measures that the hospital mentions in their public policy include firewall protection, active access management, and strong password management. The main risk that is identified is the potential of large scale patient data leaks, as that may damage patients (from a security and privacy perspective), and the hospital, both reputational and financial (Spaarne Gasthuis, 2019, 2018, 2017). To proactively maintain a clear overview of what are the most pressing cybersecurity threats the hospital performs risks assessments. In 2016, the hospital even performed a zero measurement to identify clear security gaps that needed to be addressed (Spaarne Gasthuis, 2017). In its policy, the hospital states that it has a clear view on their state of information security and where this could be improved. It actively puts efforts into raising awareness among their employees through campaigns which include phishing and pen tests, awareness training, and the 10 golden privacy rules with regard to patient information. The hospital also adopted an EPIC feature called ‘Break the Glass’, through which end users receive a notification when they surpass their personal authentication limits (Spaarne Gasthuis, 2018). Additionally, the hospital states that it does identify room for improvement with regard to their information security and recognizes that a potential data leak as the biggest risk. To mitigate this, the hospital vows to implement strong information security policy, use internal and external audits to keep their security standards up to date, use pen testing and ethical hacks to assess the level of their security, and promises to increase investments in IT (Spaarne Gasthuis, 2018).

Currently, the IT department of Spaarne Gasthuis is completing the restructuring caused by the merger of Kennemer and Spaarne (Spaarne Gasthuis, 2018). In 2016, 15 percent of all investments were directed towards IT related services, and the board stated the desire to increase this number further (Spaarne Gasthuis, 2017). In order to effectively support the merger of the IT departments, the hospital engaged in a partnership with BPSolutions. The goal of this partnership was to effectively transition two IT architectures and programs into one integrated IT environment. The partnership with BPSolutions was based on the level of expertise BPSolutions has with regard with the supervision of mergers and the desire for an effective transition ("BPSolutions ondersteunt Spaarne Gasthuis met IT Programma & Integratie management", 2015). One of the key desires was to keep things simple and design a structure that aims to identify critical weak spots in IT cooperation and addresses these. The Spaarne Gasthuis is currently working according to the ITIL standard. However, this still needs to be formalized. As mentioned earlier, the ITIL process approaches IT services from a strategic perspective. The organizations identifies the needs, makes an assessment on how this can be achieved, what the most effective way is to achieve this and what a fundamental way of continuing to achieve it is (Cartlidge, Hanna, Rudd, Macfarlane, Windebank & Rance, 2007). Next to working according the ITIL process, Spaarne Gasthuis approaches it's IT services from a SaaS approach. SaaS, or Software as a Service, is a methodology where associated software is hosted on a central server. This software can be remotely accessed by the end user, often through a web browser (Dibbie & Hang, n.d.). Using SaaS presents organizations with an easy way to get quick access to software without large scale investments on hardware, software licenses or maintenance.

From the hospital's policy and IT approach, it is clear that Spaarne Gasthuis actively engages in partnerships. It's partnership with BPSolutions is a good example of how Spaarne can use private parties to improve their own business. There are several other examples of partnerships between Spaarne Gasthuis and private parties.

In 2017, Spaarne Gasthuis was engaged in a big partnership with the private party SecureLink to replace their entire (W)LAN network. The hospital identified that the users of their network required a better performing network than they currently had in place. This wasn't the most technical task, but during the transition, it had to be guaranteed that the network was constantly active, since critical hospital tasks operate on that network. Therefore it was chosen to engage in a partnership with SecureLink. SecureLink approaches its

businesses mainly from the security perspective, and its products are subordinate to it. This was exactly how Spaarne wanted to approach this project. Additionally, SecureLink currently offers 24 hour customer service in case of emergencies (SecureLink Nederland B.V., 2017).

The employees of Spaarne Gasthuis use a lot of different devices to access the information management systems, ranging from desktops, to laptops, to their own mobile phones. A problem with this was that when an employee left one computer, and logged onto another computer, the initial session was deleted and the employee had to start again. This not only is inefficient, it also led to security risks, since employees often left their computer running and unlocked in order to later continue the session ("Spaarne Gasthuis – zorginstelling kiest voor snel wisselen van werkplek", n.d.). Spaarne wanted to address this issue and partnered with LogIn Consultants to address the challenge. LogIn Consultants subsequently developed a virtual desktop environment, which solved the issue. Spaarne Gasthuis used the partnership to reach an innovative and technical solution.

Currently, Spaarne Gasthuis has a partnership with Zivver, an encryption organization, to ensure that it is able to send e-mails containing sensitive information securely to its patients or other healthcare organizations ("Veelgestelde vragen Zivver", n.d.). Their partnership with Zivver is a good example of how Spaarne partners with private organizations to improve their information security.

It is evident from the policy of Spaarne Gasthuis, the use of ITIL and SaaS, and recent examples of information security partnerships that Spaarne does engage in partnerships. The following subsection will further elaborate on factors that impact the choice to engage in these particular partnerships.

5.2.1. Interview results

Cybersecurity threats with a human factor

Threats with a human factor are common threats to the Spaarne Ziekenhuis. Accidental data leaks or misuses of authorizations are prone to happen with around 4000 employees (E. Verhoogt, personal interview, December 20 2019). To mitigate these threats, the hospital engages in awareness training and campaigns. These trainings and campaigns aim to make employees aware of what they should know about information security in a hospital setting and how they should handle data. The interviewees emphasize that the hospital prefers to keep these measures internally (M. Smit, personal interview, December 20 2019):

"The soft side, that is really an internal affair. We know our people the best and know how they work. Besides, a familiar face often helps when employees have questions".

Their access management is also done completely internally. The hospital actively monitors and logs data access, and periodically checks if certain departments have misused their authorization. The hospital is still able to do this with their own knowledge and workforce. This does not mean, however, that they completely reject partnerships with regard to this type of security threats. For several awareness campaign the hospital has incorporated real-life scenarios such as phishing attempts or hackers. These technical aspects are done by external parties, as the hospital itself does not have the capability to perform them (E. Verhoogt, personal interview, December 20 2019).

"*We think of the scenario we want to implement, and for the technical side, we partner with a private company. We are not able to perform those technical elements ourselves."*

Spaarne Gasthuis deliberately chooses to add these technical elements through partnerships, as these real-life scenarios often make the message much more powerful and effective. Table 6 summarizes the results for this category.

Factor	Reason?	Specific Reason(s)	Level of importance
Improving efficiency and effectiveness	Yes	• In some cases, private parties perform the technical part of the campaign. • No in-house capabilities to perform the technical part • The technical part often makes the campaign more effective	Medium
Access to knowledge, resources, and capabilities			
Costs and other financial reasons	No	• Soft side of these measures kept internally • Internal knowledge of own people is the best, additionally, a familiar face behind the campaign helps • Private parties take too long to fully understand the internal way of working	---
Transfer of risk or reducing risks			
Project unique drivers			
Reaching unattainable goal for both parties			

Table 6: Spaarne Gasthuis factors in relation to cybersecurity threats with a human factor

Cybersecurity threats with a technical factor

Spaarne Gasthuis has identified the possibility of a patient data leak caused by a hack as the most critical risk with regard to their information security (Spaarne Gasthuis, 2018, 2019) This is because such an incident not only could lead to financial penalties and reputational damage for the hospital, it could also do serious harm to patients, as their privacy is harmed, but also their security within the hospital is compromised. To mitigate this threat and other information security risks, the hospital has implemented several measures, such as pen tests, ethical hacks, gap analysis, and risk assessment. As discussed earlier the hospital actively engages in partnerships to achieve a higher level of security and address threats. Below the hospital's main reasons for engaging in these partnership are presented, and finally summarized in table 7.

Costs and other financial resources

With regard to costs, Spaarne Gasthuis has a clear approach: security measures are never led by financial incentives. Security is always the number one priority and financial reasons will never determine the outcome of a security decision (E. Verhoogt, personal interview, December 20 2019):

"*We always make choices with regard to partnership in security based on security, what is the most secure and responsible. We handle highly sensitive information, therefore security is always number one. Security and reputation are number one, money is not."*

However, when looking to other measures, costs seems to be having a negative impact on the choice to engage in partnerships. For example, the hospitals would like to improve their data access management by implementing a tool from a private party that would automate the process. However, since the primary task of the hospital is patient care, it is important that most of the hospital's budget is directed towards patient care. Improving security measures that are already sufficient and will require significant investment will therefore not be done (M. Smit, personal interview, December 20 2019).

Access to knowledge, resources, and capabilities

Spaarne Gasthuis has a clear approach to their IT services. They identify their needs, according to the ITIL framework, see if they could deliver this themselves, and if not, engage in a partnership. The fact that Spaarne Gasthuis prefers to engage in Software as a Service points towards sense that the hospital tends to engage in partnerships when it comes to specialized knowledge and resource (M. Smit, personal interview, December 20 2019):

"We do not have the capacity to develop software, that is one of the main reasons we engage in partnerships"

The hospital follows a clear process in their decision making with regard to partnerships (M. Smit, personal interview, December 20 2019):

"We identify what the needs are, we check whether we already have it in-house. If not, we check whether we could develop it ourselves. If not, we engage in a partnership."

Their partnership with Zivver, for example, is completely based following this principle. There was a clear need to send secure e-mails, but the hospital was unable to develop this themselves, hence they partnered with Zivver. On the other hand, Spaarne Gasthuis also acknowledges that the amount of information private parties have is a significant advantage. For example, the biggest advantage of their partnership with Z-CERT is the continuous flow of information they receive from Z-CERT (M. Smit, personal interview, December 20 2019):

"*The combination of specialized knowledge and amount of information private parties possess are two of the most important reasons [we engage in partnerships]."*

Improving efficiency and effectiveness

Spaarne Gasthuis regularly performs gap analysis to address the effectiveness of their security measures and try to identify weak spots in their information security. To maximize the effectiveness of these analyses and their security measures, Spaarne Gasthuis acknowledges that they could be blind to their own weak spots, and that their own analysis could miss those. Especially in the current situation at Spaarne, where they are integrating two IT departments and all their associated systems, networks and processes, the hospital regularly questions itself whether or not they have been accurate enough in their security

measures. Therefore, the hospital regularly uses third parties to perform voluntary audits, risk analyses, or pen tests to optimize the effectiveness of their security measures (E. Verhoogt, personal interview, December 20 2019):

"At some point, you become blind for all the blind spots you have in your security measures. You know they are there, but will you be able to spot them? An analysis with the help of third parties helps to keep our measures sharp and effective"

Transfer of risks or reducing risks

With regard to risks involving patient information, the hospital will never be able to transfer these to other parties. The hospital will always be responsible for the information. However, other information management system risks are transferable. For example, Spaarne Gasthuis hosts its HR information system at an external party, this transfers a certain amount off risks. However, in the end the hospital remains responsible for that information, but will be able to hold the other party accountable in case of incidents (M. Smit, personal interview, December 20 2019).

Reaching unattainable goals for both parties

From the perspective of Spaarne Gasthuis, the hospital's partnership with Z-CERT is more significantly based on knowledge sharing than on intrinsic motivation from both parties. The hospital does acknowledge that Z-CERT most likely operates from an intrinsic motivation, however Spaarne Gasthuis feels that this is also the case with other security partners (M. Smit, personal interview, December 20 2019). The reasons that the hospital chose for SecureLink to update their network was based partially on the technical side, and partially of the culture of putting security first at SecureLink (SecureLink Nederland B.V., 2017). However, intrinsic motivation is not a leading reasons, as the hospital feels that most parties have this motivation.

Project unique drivers

Within the Spaarne Gasthuis there was no recall of cases where the hospital engaged in a partnership based on project unique drivers

Factor	Reason?	Specific reason(s)	Level of importance
Costs and other financial reasons	Yes	• It is important that most parts of the budget are invested in actual care. This has led to low budget capabilities within the IT department • Due to the low budget the way of working is adapted, not everything can be done as desired • Costs are never the primary reason to engage in a security partnership	Low (negative)
Access to knowledge, resources, and capabilities	Yes	• Hospitals are no software development organization, no in-house capacity or knowledge to develop software (3x) • Services like Zivver offers are very hard to do ourselves. Focus tends to be on patient care. • Not enough people • If a capability is not present in-house, we engage in a partnership • Specialized maintenance is performed by private parties	High
Improving efficiency and effectiveness	Yes	• Private parties make gap and risk analyses much more effective. • Pen tests and ethical hacks identify weaknesses in security measures and make them more effective	High
Transfer of risks or reducing risks	Yes	• It is not possible to transfer risks based on patient information. The hospital will always be responsible for that • HR-system is outsourced. The external party then carries the risk, but the hospital always remains responsible for the information	Low
Reaching unattainable goals for both parties	No	• It could be said that Z-CERT has more or less an intrinsic motivation. But not necessarily more than other private parties. • The partnership with Z-CERT is more based on knowledge sharing	---
Project unique drivers	No	• No project specific partnerships	---

Table 7: Spaarne Gasthuis factors in relation to cybersecurity threats with a technical nature

5.3. Tergooi Ziekenhuizen

Tergooi is a hospital organization that operates from two locations, Hilversum and Blaricum. At the beginning of the 2000, Tergooi was founded by the merger of Gooi-Noord Blaricum and Hospital Hilversum. As of 2018, both hospitals combined have 370 hospital beds, over 2600 employees, around 20000 clinical take-ins, and 125000 unique clinic visitors per year (Tergooi, 2019). Over the past years, Tergooi's approach to information security has changed slightly. In 2016, the hospital adopted a new centralized information system, HIX from Chipsoft, with this the hospital took an important step towards their main goal:

"*Our patients need to be able to trust that all the information on their health and the care we provide to them will remain confidential. Therefore, it is crucial that the confidentiality of all the information within the hospital is guaranteed" (Tergooi, p.45, 2017).*

In 2017, the applicability of the GDPR was approaching, and therefore the hospital was taking all the measures needed. At the end of 2017 it stated to constantly work on improving the hospital's information security and to be fully compliant with regard to all requirements of the GDPR. In order to maintain this level, the hospital appointed a privacy officer and started preparation for the complete replacement of their network to "better protect the network against intruders" (Tergooi, p. 50, 2018). Once the GDPR was applicable, Tergooi was working towards making their compliancy demonstrable. In order to do so, the Privacy and Information Security officers performed a risk assessment based on the Privacy Control Framework (PCF), developed an internal information security policy and covered all relevant aspects of the NEN7510 standard. This PCF is a different approach to performing the risk assessment then the other interviewed hospitals. The PCF serves as a guide for organizations to assess whether the control mechanisms in place regarding privacy and data protection are sufficient (NOREA, 2018). Using PCF as a framework for a risk assessment is very similar to using the NEN 7510 standard, as the PCF covers most of the standard, while adding a privacy dimension to the risk assessment (J. Markerink, personal interview, January 9, 2020). Another area where Tergooi differs from the other interviewed hospitals is the processes it uses within its IT department. Tergooi has changed the way of working within their IT department. They moved from the classic division in focus areas such as system, network, and application management to a department split into two divisions: operational and change. Employees can work in both areas and are divided based on the need for resources in both

areas. Once the hospital moved to the new way of working, it ceased working according the ITIL processes as well (J. Markerink, personal interview, January 9, 2020). The new way of working required a new method, hence, Tergooi adopted the Lean IT method. Lean IT is based on the elimination of waste, where waste is equal to non-value added (Plenert, 2011). It focusses on achieving the highest quality in the most efficient way. Organizations using lean will need to determine what creates value, "identify all the steps necessary to design, order and produce the desired products" (Arlbjøn & Vagn Freytag, p. 177, 2013) and "take those actions that create a value flow" (Arlbjøn & Vagn Freytag, p. 177, 2013), and those actions will have to optimize efficiency in order to add the most value. According to lean IT, partnerships are not fully in line with the lean strategy, but when designed properly can certainty add value to an organization. With regard to partnerships, Tergooi makes a general statement that the hospital "aims to strategically choose partners to achieve our goals" (Tergooi, p. 64, 2018). This is in line with lean, when partnerships are based on solid relationships and strategic goals, they have the potential to add value to both organizations.

In the past years, Tergooi has engaged in multiple partnerships with regard to information technology and security. In 2012, the hospital replaced most parts of their internal computer network, this replacement was performed by TenICT and Huawei. The decision of Tergooi to engage in a partnership with these two parties was based on quality, innovation, scalability, performance, and price (Hulsman, 2012). In 2015, Tergooi partnered with M&I partners to select a new information management system for the laboratories of the hospital. The expertise of M&I partners was an important factor in this partnership (Van Luxemburg, n.d.). In 2016, Tergooi adopted the information management system of Chipsoft, HIX. To support the transitioning to the new system, Tergooi partnered with PinkRoccade. The expertise and capabilities of PinkRoccade were decisive in choosing this partnership (Skipr Redactie, 2016). These partnerships offer a preview in how Tergooi approaches their partnerships, and shows that the hospital strategically determines the reasons for engaging in a partnership. The following subsection will offer more insights in the factors affecting the decision of Tergooi to engage in PPP's.

5.3.1. Interview results

Cybersecurity threats with a human factor

"Most of all data breaches, in general, are caused by human error. Exactly the same goes for our organization, data breaches caused by a human error happen with regularity".

This was stated by the information security officer of Tergooi (J. Markerink, personal interview, January 9, 2020) when asked whether the hospital experiences a lot of threats with a human factor. The biggest recent data breach of Tergooi was caused by a simple e-mail mistake of an employee, leaking 140 e-mail addresses of patients ("Tergooi-ziekenhuis lekt e-mailadressen 140 patiënten, 2019). Two thirds of all reported data breaches within Tergooi in 2018 was caused by human error, and mostly involved patient information send to the wrong recipient (Tergooi, 2019). To combat those threats Tergooi wants to accomplish two things, increase awareness and establish a willingness to report data breaches (J. Markerink, personal interview, January 9 2020). While zero data breaches is the ultimate goal, Tergooi acknowledges that human errors may occur and realize that one of the most important things in those cases is that breaches are reported to the security and privacy officers. Once reported, the officers can report and investigate the breaches, and, if necessary, implement the needed additional measures. In order to create an environment were reporting breaches is as easy as possible, the hospital has designed an easily accessible reporting tool on their internal network, where employees can report data breaches within a few minutes. This report is then categorized to be able to involve all relevant stakeholders. When it becomes clear that a particular department is constantly involved in a high number of incidents, the security and privacy officers will take additional security measures for that particular department. In order to prevent these types of incidents, Tergooi directs it's efforts into raising awareness among their employees (J. Markerink, personal interview, January 9, 2020). The hospital issues a code of conduct to new employees, it is developing an e-learning module focused specifically on information security, and it occasionally does a phishing test. All of these measures, including the reporting tool, are designed, developed, and implemented internally, without the aid of any third party. Tergooi has deliberately made the decision to do this internally, because, internally, they know their people, the issues and the available time the best (J. Markerink, personal interview, January 9 2020):

"We chose to develop the e-learning internally, based on a few relevant and pressing threats. It is a short, quick and dirty module. This is the most effective"

Externally developed e-learning modules often are to generic and take too long to complete. Tergooi develops short and specific modules, that can be done in under 20 minutes. In this way, everybody will be able to complete the modules. This approach fits the lean method Tergooi uses in its IT department, it designs short and problem specific modules, maximizing other employee's available time. Additionally, Tergooi likes to solely address these type of threats internally, since it allows for short lines of communication and a trusted environment to report issues. For example, each department has an information security contact person, who is able to quickly respond to colleagues with pressing issues (J. Markerink, personal interview, January 9 2020). Technical campaigns that Tergooi occasionally performs, such as phishing awareness campaigns, are carried out internally as well. The hospital does have the technical knowledge in-house, and performs these types of campaigns combined with larger soft- or hardware updates. In this way, the campaigns require the least effort, making them more efficient (J. Markerink, personal interview, January 9 2020). Below, table 8 summarizes the factors with regard to cybersecurity threats with a human factor.

Factor	Reason?	Specific Reason(s)	Importance
Improving efficiency and effectiveness	No	• E-learnings are developed internally. The hospital itself is better equipped to tailor specific e-learning modules • E-learning modules from external parties often are generic and take too long to complete • Internally able to talk to people fast, address issues and make sure solutions are found.	---
Access to knowledge, resources, and capabilities			
Costs and other financial reasons			
Transfer of risk or reducing risks			
Project unique drivers			
Reaching unattainable goal for both parties			

Table 8: Tergooi factors in relation to cybersecurity threats with a human factor

Cybersecurity threats with a technical nature

"Either we have failed to notice it, but I'm not under the impression that we are currently exposed to a lot of targeted attacks" (J. Markerink, personal interview, January 9 2020)

Tergooi is currently not experiencing a lot of pressure from threats with a technical nature. The only major threat the interviewee could recall was an attempted CFO fraud, where multiple employees were targeted by cybercriminals who managed to pretend to be the CFO of Tergooi (J. Markerink, personal interview, January 9 2020). While the hospital is currently not experiencing technical threats, this does not mean that they are not protecting their information management systems against it. The hospital assesses the risks it is exposed to through, as mentioned earlier, a PCF (Tergooi, 2019). This framework is a combination of privacy and information security risks, and covers most parts of the NEN 7510 standard. As opposed to the other two interviewed hospitals, Tergooi does not use the NEN 7510 standard to make their risk assessment, but focusses solely on the PCF. This is, however, sufficient, as the hospital has obtained an assurance statement from an external auditor (J. Markerink, personal interview, January 9 2020). Based on the PCF and the lean IT method, through which the hospital maximizes effectiveness and efficiency, the hospital determines how their information systems are designed, what security measures are adopted, and whether or not they develop or implement these in-house or collaborate with an external party to accomplish their goals. Over the years Tergooi has continuously adapted their information security strategy, moving from separated information systems to one integrated system, designing a multilayer firewall defense, and developing an innovative digital workplace. (Tergooi, 2019, 2018, 2017). A lot of the technical security measures are developed while partnering with an external organization, while some are deliberately kept in-house. Below the hospital's main reasons for engaging in partnerships will be elaborated in line with the established factors for choosing a PPP. A summary of these factors can be found in table 9.

Costs and other financial reasons

As mentioned earlier, the IT department of Tergooi has been one of the primary goals of the investment budget of Tergooi for the past years (Tergooi, 2019, 2018). Over the past years the hospital has committed to invest in developing its IT. Looking at the previously mentioned partnership between Tergooi en TenICT, TenICT states that they won the partnership based on quality, innovation, scalability, performance, and lastly on price

(Hulsman, 2012). This was echoed by the interviewee when discussing budgetary reasons for engaging in a partnership. The information security team of Tergooi does not seem to struggle with budgetary restriction when considering security measures, as higher management acknowledges the importance of security and provides the necessary resources. Additionally, whether an external party is able to deliver a service or product less costly then the hospital itself is also never a factor. As with the partnership with TenICT, other factors such as quality, and most importantly security, are considered before looking at costs (J. Markerink, personal interview, January 9 2020):

"Yes, security will always come first. We always look into the quality of the third party, often based on their compliancy to NEN 7510, and if they have obtained any certificates to prove quality."

Costs and other financial resources are therefore no factor in the choice of Tergooi to engage in a PPP.

Access to knowledge, resources, and capabilities

Based on the lean IT approach of Tergooi, the hospital identifies its needs and addresses those in the most efficient way, maximizing value. Developing information systems, or security software for those systems is not something that Tergooi does internally (J. Markerink, personal interview, January 9 2020):

"We basically do not develop software ourselves, every system we (the IT department) uses is developed in the cloud or by third parties"

Tergooi experiences that the scale of the information systems needed today, and all security requirements require simply too much knowledge and time to develop internally. Therefore, the decision was made to engage in partnerships to develop information management systems and the security measures for those systems. These partnerships allow the hospital to find simple solution in an increasingly complex environment. For example, since a few years, Tergooi uses an innovative concept called 'The New Working Place' (Tergooi, 2017), which is a digital environment where employees can log in from any desktop within the Tergooi hospitals. The innovative approach of this concept is that the digital environment combines numerous software packages ranging from Adobe, Microsoft Office and the latest Windows

version to VMware and SQL. The developer of this concepts makes sure that these software packages are constantly running on the latest version. This eliminates any transitioning issues for Tergooi when upgrading to new versions, and maximizes security as there are no old, weaker, versions of software running on the environment. According to Tergooi, this is something that the hospital would never be able to develop, and, most importantly, maintain on their own (J. Markerink, personal interview, January 9 2020):

"We would need a lot more people, and a way, way bigger department to develop something like that and keep it up to date to all technical developments".

Besides looking to questions on whether the hospital has the resources to develop products or services, Tergooi also addresses whether they will be able to meet the demands of the end-users. Currently, the hospital is evaluating where to host their databases in order to maintain the desired level of availability. For the database of their main electronic patient records, the hospital is able to host them internally and guarantee the availability. However, for their radiology database, called PACS, which is a database that processes huge amounts of data, the decision was made to host the database externally (J. Markerink, personal interview, January 9 2020). The combination of the importance of a constant availability and the amounts of processed data led to this decision.

Where it is able to perform tasks by themselves, the hospital tries to keep as much as possible internally. However, due to the increasing scale and requirements, rapidly changing technology and high demands the hospital often needs the capabilities and resources of external parties.

Improving efficiency and effectiveness

Working according the lean IT method has the ultimate goal of maximizing value through optimizing efficiency (Arlbjøn & Vagn Freytag, 2013). This is mirrored by Tergooi's strategy to engage in partnerships based on efficiency and effectiveness (Tergooi, 2018). Take for example the maintenance of software. Small scale maintenance is done by the hospital itself, as they can perform and tests this easily within their own environment, without needing a third party, making it quicker and more efficient. Large scale maintenance is done by the third parties who developed the software, since they possess over a greater knowledge of the system in order to perform the maintenance more effective (J. Markerink, personal

interview, January 9 2020). These arguments are purely based on performing the workload the most effective. Looking towards the effectiveness of the security measures themselves, Tergooi also tends to partner with external parties to optimize this (J. Markerink, personal interview, January 9 2020):

"Through partnering with multiple external parties we try to optimize our level of detection"

Additionally, Tergooi voluntarily engages in audits and pen-tests to assess whether their security measures are still sufficient and effective (J. Markerink, personal interview, January 9 2020). Partnerships not only are for Tergooi a way to efficiently perform the workload, they establish effective security measures and keep them effective.

Transfer of risks or reducing risks

"*That will always be your own responsibility, we need to make sure that our partners meet all security requirements" (J. Markerink, personal interview, January 9 2020)*

With regard to information security and privacy measures, it is impossible for Tergooi to transfer risk to potential partners. They will always carry the final responsibility over the information of their employees or patients, and will have to oblige their partners to meet all requirements. The method Tergooi uses for their risk assessment, PCF, also obliges organizations to require third parties to meet requirements:

"*If the entity procures third parties in these activities, it will require these third parties to deploy the same risk management activities" (NOREA, p.31, 2018).*

The ability to transfer risks to a third party through a partnership is therefore never a factor for Tergooi when choosing to engage in a partnership.

Reaching unattainable goals for both parties

Tergooi highly values its partnership with Z-CERT. Z-CERT adds a lot of value to the information security practices of Tergooi, in form of additional information, "to-the-point information" (J. Markerink, personal interview, January 9 2020) on current weaknesses in the healthcare sector, and actual measures such as emergency controls or blocking IP addresses.

However, whether the partnership is based solely on the mutual goal of improving healthcare information security was difficult to assess by the hospital. Since the hospital does not have any of their security services completely outsourced, there was little comparative material (J. Markerink, personal interview, January 9 2020):

"That is hard to compare, since none of our security services are outsourced. However, I really appreciate the partnership, they (Z-CERT) act quickly and deliver valuable information".

The partnership between Tergooi and Z-CERT is not fully based on reaching their mutual goal, but more on the capabilities and resources of Z-CERT. However, there is evidence of a low level of importance based on the mutual goal.

Project unique drivers

Tergooi does not engage in any partnerships that are project specific.

Factor	Reason for choosing?	Specific reason(s)	Level of importance
Costs and other financial reasons	No	• Costs are never a reason to take a security measure or not • Costs are never a driver to engage in a partnership	---
Access to knowledge, resources, and capabilities	Yes	• The scale of developing software internally has become too large to do this as a hospital. External parties are needed for this (3x). • Internal resources are not sufficient to supply all demands and needs of end-users • External parties support the hospital to find solutions in an environment of increasing complexity • Some databases are hosted externally, internally not able to guarantee the required level of availability. • Technology is developing fast, this makes it almost impossible to keep internally.	High
Improving efficiency and effectiveness	Yes	• Audits and Pen-tests performed by external parties keep security measures effective • Through patterning with external parties, the level of detection becomes optimal and the most effective • External software is always up to date, this makes it highly efficient (2x)	High
Transfer of risks or reducing risks	No	• It is impossible to transfer risks through partnerships. The hospital will always stay responsible	---
Reaching unattainable goals for both parties	Yes	• Partnership with Z-CERT is based on a mutual goals of improving hospital information security, this makes it a very pleasant partnership. • Hard to compare and see if this is truly because of intrinsic motivation, due to lack of similar partnership with other external parties	Low
Project unique drivers	No	• No project unique partnerships	---

Table 9: Tergooi factors in relation to cybersecurity threats with a technical nature

5.4. Summary of results

The previous subsections have offered multiple insights in the factors that affect the decisions of three different Dutch hospitals to engage in PPP. In the analysis of the results of the three case studies, a division was made between cybersecurity threats with a technical nature and with a distinct human factor. The results of this distinction shows that the nature of the cybersecurity threats does have a significant effect on the activity of the hospitals with regard to PPP. The hospitals tend not to engage in partnerships when addressing cybersecurity threats with a human factor. Both Amsterdam UMC and Tergooi indicated to address the threats with a human factor completely internally, where Spaarne Gasthuis indicated to engage in partnerships for more technical oriented awareness campaigns, or to increase the effectiveness of a campaign. The overall results with regard to cybersecurity threats with a human factor can be found in table 10 below. This table represents the general reasons for all three hospitals to engage in PPP to address threats with a human factor. The results show that the factors established in the framework of this research have very little to no effect on the decisions of Dutch hospitals to engage in PPP to address threats with a human factor.

	Amsterdam UMC	**Spaarne Gasthuis**	**Tergooi**
Costs & other financial resources	No	No	No
Access to knowledge, resources and capabilities	No	Yes (Medium)	No
Improving efficiency and effectiveness	No	Yes (Medium)	No
Transfer of risk or reducing risks	No	No	No
Reaching unattainable goals for both parties	No	No	No
Project unique drivers	No	No	No

Table 10: Overall results cybersecurity threats with a human factor.

The hospital were significantly more active in partnerships to address cybersecurity threats with a technical nature. All three hospitals engaged in partnerships to improve their security against technical cybersecurity threats. Where reasons for engaging in these partnerships varied for some hospitals, the results show a strong overall similarity. The overall results with regard to cybersecurity threats with a technical nature can be found in table 11. This table represents the general reasoning of all three hospitals with regard to engaging in PPP to address cybersecurity threats with a technical nature. The results show that the factors established in the theoretical framework significantly affect the choice of Dutch hospitals to engage in PPP to address this type of cybersecurity threats.

	Amsterdam UMC	**Spaarne Gasthuis**	**Tergooi**
Costs & other financial resources	No	Yes (Low negative)	No
Access to knowledge, resources and capabilities	Yes (High)	Yes (High)	Yes (High)
Improving efficiency and effectiveness	Yes (High)	Yes (High)	Yes (High)
Transfer of risk or reducing risks	Yes (Low)	Yes (Low)	No
Reaching unattainable goals for both parties	Yes (Low)	No	Yes (Low)
Project unique drivers	Yes (Low)	No	No

Table 11: Overall results cybersecurity threats with a technical nature

Chapter 6: Conclusion

In the introduction of this research, the argument was made that the healthcare sector, and in particular hospitals were no stranger to public private partnerships. However, available literature tended to focus around partnerships designed to finance health care equipment, or construction projects. Little information was available on whether hospitals partnered in favor of the security of their information management systems. This study has found that hospitals do frequently engage in partnerships with the private sector in order to establish, maintain, or improve the level of security of their information management systems. Efforts from external organizations seem to be critical to the functioning of Dutch hospitals. That being said, Dutch hospitals will remain in control over their products, projects, services, and other business related efforts. IT departments of Dutch hospitals work through a various of processes and methods, all carrying the same essence. Hospitals systematically approach projects or issues, identifying what the desire is, what is needed to achieve this, and how this can be achieved, all in a way that, in the end, will maximize output. This study has shown that hospitals tend to approach this in a rational manner, if a private party is better suited to perform this task, for whatever reason, the hospital will look for options to engage in a partnership.

The goals of this study has been to identify the specific factors that drive Dutch hospitals to engage in these partnerships. Hospitals handle large amounts of highly sensitive data, but are not necessarily optimally equipped to establish a sufficient level of information security. Therefore, one could expect hospitals to be active in engaging in partnership to address this information security. However, there is no clear cut answer to the question of why hospital specifically engage in these partnerships. This study aimed to add more insights to this gap. Based on previous literature on public private partnerships in general, a framework was established addressing possible reasons for public organizations to engage in public private partnership in general. This framework was used to analyze the reasoning of three different Dutch hospitals. Additionally, based on the relevant threats to the cybersecurity of hospital information management systems, a categorization of cybersecurity threats was made in order to analyze for two things. First, it allowed the analysis to be more focused around the relevant cybersecurity threats. Second, the analysis was able to investigate whether the origin of the threats had an effect on the factors affecting the choice to engage in public private partnerships.

The division of cybersecurity threats into threats with a human factor and threats with a technical nature offered valuable insights. This study has shown that the type of cybersecurity threat has a significant effect on the reasoning of hospitals to engage in public private partnerships. Dutch hospital actively engage in partnerships to address threats with a technical nature, with all three investigated hospitals being engaged in multiple partnerships These partnerships are even critical to the functioning of the information technology within the hospital. However, Dutch hospitals rarely engage in partnerships to address threats with a human factor. The reasoning for this? Dutch hospitals prefer to keep the human characterized threats close. They know their own people the best, they know the way-of-working within the hospital, and a familiar face will be the most approachable for their colleagues. This outweighs the potential benefits of the knowledge, capabilities, (cost)-efficiency, and expertise of private parties. The overall results show that the factors, as established in the theoretical framework, do not affect the choice of Dutch hospitals whether to engage in public private partnership. Therefore, when identifying the most significant factors that affect this choice, these results can be neglected.

With regard to the most frequently engaged partnerships of Dutch hospitals, the partnerships that address cybersecurity threats with a technical nature, this study has shown that not all established factors affect the choice of Dutch hospitals to engage in public private partnerships. Costs and other financial resources are never a factor for engaging in a partnership, this was mostly caused by the level of sensitivity of information security. Higher management of hospitals tend not to take risks when it comes to security measures, and often provide all needed resources. Reaching unattainable goals for both parties neither had a significant effect on the choice of the hospitals. Only the partnership with Z-CERT had a sense of a mutual goal that couldn't be obtained without each other, however most of the hospital mostly preferred the valuable information and capabilities provided by Z-CERT. Additionally, there were no project unique drivers for partnerships at the investigated hospitals. The transfer of risks or reducing associated risks had a little, but positive, effect on the decision of the hospitals to engage in partnerships. Two of the three hospitals were engaged in partnerships in order to lower risks or shift risks to the private party. However, it needs to be noted that this was never with regard to threats to the electronic patient records, but always to a business-oriented information management system, such as the HR-system. All hospitals acknowledge that they would never be able to shift risks regarding their electronic patient records to a private party.

Improving efficiency and effectiveness had a significant positive effect on the decision to engage in partnerships. All three hospitals had multiple partnerships that were based on improving efficiency and effectiveness and all hospitals valued the partnerships based on efficiency and effectiveness with a high level of importance. The final, and perhaps most important factor, was the access to knowledge, resources and capabilities. All three hospitals acknowledged the same thing: hospitals simply do not have the workforce, resources, and expertise to develop security software themselves. The benefits that a private party brings, such as its use user database, continuous updates, technical expertise and additional information on relevant threats, are impossible for hospitals to develop in-house. Therefore, often the main reason for Dutch hospitals to engage in partnerships is the access to knowledge, resources and capabilities.

Certainly not all established factors affected the choice of Dutch hospitals to engage in public private partnership. However, several factors proved to have an significant effect on the choice to engage in partnerships. When determining whether or not to engage in a public private partnership, Dutch hospitals are affected the most by the access to knowledge, resource and capabilities, and the potential to improve efficiency and effectiveness.

The results of this study showed great similarity. However, it difficult to confidently address the outcomes of this research to “all Dutch hospitals”. The sample size of investigated hospitals is simply too little to be able to make such a statement. Future research could build on this research by investigating more Dutch hospitals, to investigate whether the Dutch landscape of hospitals approaches public private partnerships to address cybersecurity threats in the same way as the three investigated hospitals in this research. Another avenue for future research opened up by this research is the reasoning of Dutch hospital to not engage in partnerships to address cybersecurity threats with a human factor. One of the hospitals stated in both the interview as their annual report, that two thirds of all data breaches in the hospital are caused by human acts, either intentional or unintentional. However, this hospital chose to develop all measures to counter this threat themselves. Investigating why hospitals choose to do so, and where they could potentially benefit from the private sector is a very relevant and interesting field for future research.

7. References

Achtergrondinformatie over NEN 7510. (n.d.). Retreived from https://www.nen.nl/Alles-over-NEN-7510/Achtergrondinformatie-over-NEN-7510.htm

Akintoye, A. (2003). Public-Private Partnerships: Managing Risks and Opportunities/Akintoye A., Beck M., Hardcastle C.

AMC. (2018). Maatschappelijk Jaarverslag 2017. Retreived from https://www.amc.nl/web/over-de-locatie-amc/organisatie/jaarverslagen.htm

Amsterdam UMC. (2019a). Bestuursverslag 2018. Retreived from https://www.vumc.nl/over-vumc/jaardocumenten.htm

Amsterdam UMC. (2019b). Informatiebeveiligingsbeleid VUmc-AMC

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: current state of research. *International journal of Internet and enterprise management*, *6*(4), 279-314.

Stentoft Arlbjørn, J., & Vagn Freytag, P. (2013). Evidence of lean: a review of international peer-reviewed journal articles. *European Business Review*, *25*(2), 174-205.

ASL BiSL Foundation (2014), ASL 2 Introduction [PowerPoint slides]. Retrieved from https://aslbislfoundation.org

ASL BiSL Foundation (n.d.), Business information management supported by BiSL [PowerPoint slides]. Retrieved from https://aslbislfoundation.org

Autoriteit Persoonsgegevens. (2018). *Meldplicht datalekken: facts & figures.* Retrieved from https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/jaarrapportage_meldplicht_datalekken_2018.pdf

Autoriteit Persoonsgegevens. (2017). *Meldplicht datalekken 2017: sector gezondheid en welzijn.* Retrieved from https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/01_2018-02-27_2017_jaarrapportage_gezondheid_en_welzijn.pdf

Baxter, P., & Jack, S. (2008). Qualitative case study methodology: Study design and implementation for novice researchers. *The qualitative report*, *13*(4), 544-559.

Bazzoli, G. J., Stein, R., Alexander, J. A., Conrad, D. A., Sofaer, S., & Shortell, S. M. (1997). Public–private collaboration in health and human service delivery: Evidence from community partnerships. *The Milbank Quarterly*, *75*(4), 533-561.

BPSolutions ondersteunt Spaarne Gasathuis met IT Programma & Integratie management. (2015 April 16). Retrieved from https://executive-people.nl/527354/bpsolutions-ondersteunt-spaarne-gasthuis-met-it-programma-en-integratie-management.html

Box, D., & Pottas, D. (2013). Improving information security behaviour in the healthcare context. *Procedia Technology*, *9*, 1093-1103.

Brinkerhoff, D. W., & Brinkerhoff, J. M. (2011). Public–private partnerships: Perspectives on purposes, publicness, and good governance. *Public administration and development*, *31*(1), 2-14.

Carr, M. (2016). Public–private partnerships in national cyber-security strategies. *International Affairs*, *92*(1), 43-62.

Cartlidge, A., Hanna, A., Rudd, C., Macfarlane, I., Windebank, J. & Rance, S. (2007). An introductory overview of ITIL V3. *The UK Chapter of the itSMF*

Centraal Bureau voor de Statistiek. (2018). *Cybersecuritymonitor 2018*. Retrieved from https://www.cbs.nl/nl-nl/publicatie/2018/38/cybersecuritymonitor-2018

Collins, J. D., Sainato, V. A., & Khey, D. N. (2011). Organizational Data Breaches 2005-2010: Applying SCP to the Healthcare and Education Sectors. *International Journal of Cyber Criminology*, *5*(1).

Council of the European Union. (2015). *Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data an on the free movement of such data (General Data Protection Regulation).* Brussels

Davies, P. (2006). Exploratory research. *The Sage dictionary of social research methods*, 110-111.

Dibbie, O. & Hang, H. (n.d.). Software as a Service [PowerPoint slides. Retrieved from: https://www.cs.colorado.edu/~kena/classes/5828/s12/presentation-materials/dibieogheneovohanghaojie.pdf

Dunn-Cavelty, M., & Suter, M. (2009). Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection*, *2*(4), 179-187.

Geschiedenis. (n.d.). Retrieved from https://spaarnegasthuis.nl/over-spaarne-gasthuis/geschiedenis

Gostin, L. O., Turek-Brezina, J., Powers, M., Kozloff, R., Faden, R., & Steinauer, D. D. (1993). Privacy and security of personal information in a new health care system. *JAMA*, *270*(20), 2487-2493.

Hulsman, S. (2012, August 20). TenICT helpt Tergooiziekenhuizen naar Huawei. Retrieved from: https://www.channelweb.nl/artikel/nieuws/infrastructuur/4552582/5226433/tenict-helpt-tergooiziekenhuizen-naar-huawei.html

'ICT Projectleider bouwen aan Tergooi' (2019). *Tergooi ziekenhuizen*. Retrieved from: https://www.werkenbijtergooi.nl/vacatures/details/ict-projectleider-bouwen-aan-tergooi-20881/

ISO. (2008). *ISO 27799:2008.* Retrieved from https://slidex.tips/download/health-informatics-information-security-management-in-health-using-iso-iec-iso-2

Jomo, K. S., Chowdhury, A., Sharma, K., & Platz, D. (2016). Public-Private Partnerships and the 2030 Agenda for Sustainable Development.

Khaloufi, H., Abouelmehdi, K., Beni-hssane, A., & Saadi, M. (2018). Security model for Big Healthcare Data Lifecycle. *Procedia Computer Science*, *141*, 294-301.

Klijn, E. H., & Van Twist, M. J. W. (2007). Publiek-private samenwerking in Nederland, Overzicht van theorie en praktijk.

Kwon, J., & Johnson, M. E. (2015, June). The Market Effect of Healthcare Security: Do Patients Care about Data Breaches?. In *WEIS*.

Le Bris, A., & El Asri, W. (2016). State of Cybersecurity & Cyber Threats in Healthcare Organizations. *ESSEC Business School*.

Linder, S. H. (1999). Coming to terms with the public-private partnership: A grammar of multiple meanings. *American behavioral scientist*, *43*(1), 35-51.

Liu, C. H., Chung, Y. F., Chen, T. S., & Wang, S. D. (2012). The enhancement of security in healthcare information systems. *Journal of medical systems*, *36*(3), 1673-1688.

Louwerse, C. P. (2004). Elektronisch Patiëntendossier. *Nederlands Tijdschrift voor Klinische Chemie en Laboratoriumgeneeskunde*, *29*, 217-218

Luna, R., Rhine, E., Myhra, M., Sullivan, R., & Kruse, C. S. (2016). Cyber threats to health information systems: A systematic review. *Technology and Health Care*, *24*(1), 1-9.

Lupton, D. (2016). Digitised health, medicine and risk.

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: how safe are we?. *Bmj*, *358*, j3179.

Masrom, M., & Rahimly, A. (2015). Overview of data security issues in hospital information systems. *Pacific Asia Journal of the Association for Information Systems*, *7*(4).

Murphy, S. (2015). Is cybersecurity possible in healthcare. *National Cybersecurity Institute Journal*, *1*(3), 49-63.

Narayana Samy, G., Ahmad, R., & Ismail, Z. (2010). Security threats categories in healthcare information systems. *Health informatics journal*, *16*(3), 201-209.

Nationaal Coordinator Terrorisme en Veiligheid. (2018) *Nederlandse Cybersecurity Agenda: Nederland Digitaal Veilig.* Retrieved from https://www.rijksoverheid.nl/documenten/rapporten/2018/04/21/nederlandse-cybersecurity-agenda-nederland-digitaal-veilig

NEN. (2017a) *NEN 7510-1.* Retrieved from https://www.werkenmetnen7510.nl/normen

NEN. (2017b) *NEN 7510-2.* Retrieved from https://www.werkenmetnen7510.nl/normen

Nikolic, I. A., & Maikisch, H. (2006). Public-private partnerships and collaboration in the health sector: an overview with case studies from recent European experience.

Noor, K. B. M. (2008). Case study: A strategic research methodology. *American journal of applied sciences*, *5*(11), 1602-1604.

NOREA. (2018). *NOREA Guide Privacy Control Framework.* Retrieved from https://www.norea.nl/download/?id=4160

Plenert, G. J. (2011). *Lean management principles for information technology*. CRC Press.

PwC (2018). *PPPs in healthcare: models, lessons and trends for the future.* Retrieved from https://www.pwc.com/gx/en/industries/healthcare/publications/trends-for-the-future.html

RAND Corporation (2009). Data Collection Methods. Semi-Structured Intervies and Focus Groups.

Rösken, T. (2017, September 05). 'Grootste hospital door fusieteostemming AMC en VUmc'. *De Telegraaf*. Retrieved from: https://www.telegraaf.nl/financieel/332177/grootste-hospitaal-door-fusietoestemming-amc-en-v-umc

Ross, J. (2017). Cybersecurity: A Real Threat to Patient Safety. *Journal of PeriAnesthesia Nursing*, *32*(4), 370-372.

Schriemer, H. (2019). *Identity & Access Management Beleid Amsterdam UMC*

SecureLink Nederland B.V. (2017, July 13). Spaarne Gasthuis vervangt (W)LAN access network. Retrieved from: https://www.computable.nl/artikel/techwire/infrastructuur/6062986/2499347/spaarne-gasthuis-vervangt-w-lan-access-netwerk.html

Shipman, M. D. (2014). *The limitations of social research*. Routledge.

Skipr Redactie. (2016, March 23). PinkRoccade helpt Tergooi bij migratie van EPD. Retrieved from: https://www.skipr.nl/nieuws/pinkroccade-helpt-tergooi-bij-migratie-van-epd/

Smith, E., & Eloff, J. H. (1999). Security in health-care information systems—current trends. *International journal of medical informatics*, *54*(1), 39-54.

Spaarne Gasthuis (2017). Jaarplan 2016. Retrieved from https://spaarnegasthuis.nl/publicaties

Spaarne Gasthuis (2018). Jaarplan 2017. Retrieved from https://spaarnegasthuis.nl/publicaties

Spaarne Gasthuis (2019). Jaarplan 2018. Retrieved from https://spaarnegasthuis.nl/publicaties

Spaarne Gasthuis – Zorginstelling kiest voor snel wisselen van werkplek. (n.d.). Retrieved from: https://www.loginconsultants.com/nl/referenties/spaarne-gasthuis

Tergooi. (2017). Jaarverslag 2016. Retrieved from https://www.tergooi.nl/over-ons/wie-zijn-wij/publicaties/

Tergooi. (2018). Jaarverslag 2017. Retrieved from https://www.tergooi.nl/over-ons/wie-zijn-wij/publicaties/

Tergooi. (2019). Jaarverslag 2018. Retrieved from https://www.tergooi.nl/over-ons/wie-zijn-wij/publicaties/

Tergooi-ziekenhuis lekt e-mailadressen 140 patiënten. (2019, May 27). Retrieved from https://www.nu.nl/internet/5910435/tergooi-ziekenhuis-lekt-e-mailadressen-140-patienten.html

Top 100 Ziekenhuizen (2015). *Algemeen Dagblad.* Retrieved from: http://ziekenhuis.i-serve.nl

United States Department of Defense (2019). *DOD Dictionary of Military and Associated Terms.* Retrieved from https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf

United State Department of Defense Joint Chiefs of Staff (2011). *Joint Terminology for Cyberspace Operations.* Retrieved from http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf

Van der Meulen, N. S., & Lodder, A. R. (2014). Cybersecurity (ch. 13).

Van Luxemburg, A. (n.d.) Maasstad en Tergooi Ziekenhuis begeleiding LIMS. Retrieved from: https://mxi.nl/klanten/74/maasstad-en-tergooi-ziekenhuis-begeleiding-lims

Vecchi, V., & Hellowell, M. (Eds.). (2018). *Public-Private Partnerships in Health: Improving Infrastructure and Technology*. Springer.

Veelgestelde vragen Zivver. (n.d.). Retrieved from: https://spaarnegasthuis.nl/kwaliteit-en-veiligheid/veelgestelde-vragen-zivver

Verschuren, P., Doorewaard, H., & Mellion, M. (2010). *Designing a research project* (Vol. 2). The Hague: Eleven International Publishing.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102.

VUmc. (2018). Jaarverslag VUmc 2017. Retreived from https://www.vumc.nl/over-vumc/jaardocumenten.htm

Walliman, N. (2006). Research strategies and design. *Social Research Methods. London*, 37-50.

Wang, W., & Lu, Z. (2013). Cyber security in the smart grid: Survey and challenges. *Computer networks*, *57*(5), 1344-1371.

Wen, H. J., & Tarn, J. M. (2001). Privacy and security in e-healthcare information management. *Information systems security*, *10*(4), 1-16.

Wilkowska, W., & Ziefle, M. (2012). Privacy and data security in E-health: Requirements from the user's perspective. *Health informatics journal*, *18*(3), 191-201.

8. Appendix

A. Interview questions

1. Could you tell me something about the information management systems your hospital uses. (Possibly ask about: different types of systems, data bases, online access portals).

2. How is the IT department of your hospital designed? (Ask about: organizational structure, how many people employed, IT processes)

3. What is the approach of your hospital with regard to information security (Ask about: risk assessments, risk matrices, NEN 7510)

4. In my research, I make a division between cybersecurity threats with a human factor and threats with a technical nature. Do you experience many threats with a human factor?

If yes:
5. What kind of measures do you take to protect the hospital against these threats?
6. Do you partner with private parties in order to achieve these measures?

    If yes:
    7. Why?
    If no:
    8. Why not?

If no:
5. Why do you think your hospital does not experience these threats?
6. Have you ever partnered with a private party in order to avoid these threats?

    If yes:
    7. Why?
    If no:
    8. Why not?

9. Do you experience many threats with a technical nature?

If yes:

5. What kind of measures do you take to protect the hospital against these threats?
6. Do you partner with private parties in order to achieve these measures?

    If yes:

    7. Why?

    If no:

    8. Why not?

If no:

5. Why do you think your hospital does not experience these threats?
6. Have you ever partnered with a private party in order to avoid these threats?

    If yes:

    7. Why?

    If no:

    8. Why not?