The role of cybersecurity in hospital procurement processes

Rutger van Baren

TU Delft

The role of cybersecurity in hospital procurement processes

by

Rutger van Baren

to obtain the degree of Master of Science
at the Delft University of Technology
to be defended publicly on Tuesday February 02, 2021 at 2:00 PM.

Student number:	4208714	
Project duration:	April 17, 2020 – February 02, 2021	
Graduation committee:	Prof. dr. M. Van Eeten,	TU Delft, first supervisor
	Prof. dr. Ir. I. Van de Poel,	TU Delft, second supervisor
	Dr. K. Labunets,	TU Delft, external supervisor

An electronic version of this thesis is available at `http://repository.tudelft.nl/`.

TU Delft

Executive summary

Introduction

Cybersecurity is a growing problem in healthcare. Many healthcare institutions are targeted by cybercrime and the confidentiality, integrity and availability of patient data and critical systems for patient care are under threat. Trying to address these threats, hospitals have encountered various issues in the technological, human and organisational domains. These various factors interact, making cybersecurity a complex problem.

Efforts to improve cybersecurity focus on development and deployment of systems and equipment. However, in between lies an opportunity to address cybersecurity during procurement. Procurement dictates which systems enter a hospital's digital ecosystem and therefore considers cybersecurity as part of the purchase process.

Previous research highlighted the importance of procurement for cybersecurity and showed the importance of decision power in this process. However, it did not account for the complex interactions that occur within. The purpose of this research is to examine how complex interactions during procurement shape the role of cybersecurity.

Various techniques were used to this end, including an interview transcript coding technique that combined grounded theory and an analysis framework. Based on a combination of a complex-decision-making framework and a cyclical purchase process model, interviews were held with hospital Chief Information Security Officers to examine how cybersecurity formed a part of the procurement process. Based on the findings, a survey was developed to scale this research to the sector. The interviews were analysed using semi-grounded theory techniques to provide an answer to the main research question:

What is the role of cybersecurity in hospital procurement processes and how can that role be analysed across the sector?

Theoretical framework

Purchase processes are dominantly modelled as a series of discrete events such as process steps and decisions or as strategic activities. Existing models that view the purchase process from a decision-making perspective do not capture complex interactions. To successfully do so, a combination of a purchase process model and complex decision-making framework were needed. Using a cyclical process model from the European Union Agency for Cybersecurity and a framework designed to capture complex decision-making processes in politics, a combined complex decision-making framework for procurement was synthesised. This provided a novel perspective of cybersecurity in procurement.

Results

Five key factors were found that influence the role of cybersecurity in procurement:

- The *supplier-hospital relationship* is characterised by decision power being distributed in favour of suppliers. Important themes are hospitals not being able to switch to other suppliers, the distinctions between suppliers based on willingness and ability to cooperate, as well as cybersecurity maturity, and the preference of hospitals for known suppliers.
- *Knowledge exchange and retention* involves recording and sharing knowledge between hospitals to benefit their position in negotiations and improve their processes. Exchanged knowledge is used to obtain supplier cooperation, improve processes or address threats. Retained knowledge primarily focuses on process improvement.
- *Alternative purchase processes* are deviations from the regular purchase process that do not allow for proper consideration of cybersecurity needs. Actors choose to engage in these processes because of their simplicity or because they resist involvement of other actors.

- The *cloud transition* provides a unique set of considerations in procurement, due to the trade-off that hospitals have to make concerning cost-effectiveness and convenience. Cloud solutions can be a way to achieve more security, at the cost of less control and customisability.
- *Conflicting priorities* occur when actors pursue one goal and encounter opposition from another actor in doing so. Externally, such conflict arises between hospitals and suppliers over deployment of cybersecurity measures or patching schedules. Internally, departments may differ in prioritising confidentiality, availability and integrity.

Conclusion
The role of cybersecurity in procurement is growing, but this change is slow as suppliers resist efforts to improve, enabled by an imbalance in decision power. Knowledge exchange can provide an avenue for improvement, allowing cybersecurity a bigger role in procurement, as hospitals are at disadvantage with suppliers during negotiations. This results in further conflict after signing and in future purchase processes.

Recommendations
Based on the results, the following recommendations are made to improve the role of cybersecurity in procurement:

- **Regulators should protect hospitals from supplier lock-in**
  The effect of supplier lock-in should me minimised by fostering competition. This may not be feasible in the case of highly specialised systems. Regulation should provide hospitals with a better position in negotiations by putting more responsibility for cybersecurity at suppliers, and by implementing mechanisms that restore the distribution of decision power back to a healthy balance between suppliers and hospitals.
- **Hospitals should perform regular critical evaluation of known suppliers**
  Hospitals rarely evaluate their suppliers for repeated purchases, allowing changes in supplier performance to go unnoticed. This can be prevented by scheduling a regular, critical evaluation of the suppliers involved in repeated purchases. Additionally, for every purchase, hospitals should consider if continuing a relationship with a known supplier increases their risk of supplier lock-in emerging.
- **Hospitals should actively request supplier information from other hospitals during procurement**
  Hospitals can improve their position in negotiations relative to suppliers by learning from other hospitals how cooperation was achieved, and by checking if suppliers' arguments against cooperation hold true. Group purchasing alliances likely have members who can provide the required supplier information and make a good starting point to request this information from.
- **Hospitals should actively engage in process information exchange with other hospitals to improve dissemination of best practices**
  Hospitals are still adapting their processes to account for cybersecurity. To avoid reinventing the wheel, hospitals should look to each other to identify best practices and implement those. The added benefit of this approach over redesigning processes by yourself is that these best practices are already tailored to the uniquely complex and resource-constrained environment of hospitals.
- **Hospitals should improve inclusion of cybersecurity in alternative purchase processes**
  Alternative purchase processes introduce cybersecurity threats into the hospital IT ecosystem, but on the other side, increased connectivity of modern systems is improving the visibility of these purchases to IT departments. The inclusion of cybersecurity in these processes should therefore rest with them, as they indirectly gain more decision power from this development.
- **Clearly state priorities of all actors involved in procurement processes**
  Priorities can vary between hospitals and suppliers and between internal actors within hospitals. Hospitals should dedicate time in procurement processes to identifying these priorities and any potential resulting conflicts. Through early identification of potential priority conflicts, any resulting issues during negotiations and contract supervision can be preempted. Resolving these conflicts can streamline the procurement process, benefiting all involved actors.

Preface

A long time ago, someone told me there are two kinds of thesis projects: the kind that leverages the things you already know, that plays to your strengths and drives those skills to new heights, and the leap of faith, jumping in the deep end, out of your comfort zone, and provides a huge opportunity to acquire new skills. While I set out in search of the former, I quickly found myself writing a thesis that sorted itself in the second category. On several occasions I lost sight of the right research direction. But that's just the thing: if you do not know where you are going, each new step can be a step in the right direction. The new knowledge and skills I picked up along the way will most certainly prove their added value further down the line. This thesis has been a long process of learning and I believe this valuable experience will be a useful lesson in the years to come. I hope that the results within are also of value for other students and healthcare experts.

Over the course of this research project, I received help from a lot of people. I would first like to thank Kate Labunets for her patience and guidance throughout this research. When I started working on this project, we came up with a very different research design. She has provided immense support while the research design had to be revised several times and as I struggled to acquaint myself with new research methods that challenged me to step out of my comfort zone. I would also like to thank my other supervisors, Michel van Eeten and Ibo van de Poel, for their support and feedback. All interviewees have my thanks as well. Your contribution of time and knowledge made this thesis possible, and your contributions all proved valuable. I hope that this research has succeeded in giving you something valuable in return. I would also like to express my gratitude to my roommates Wouter and Daan. You were there all along the way, and the value of your patience and presence at home is both unquantifiable and invaluable. Finally, I also want to mention my old roommate Gijs, as his provision of an out-of-home workspace during the CoViD-19 pandemic enabled me to make the progress I needed and bring this research to a close.

Rutger van Baren
Delft, February 2021

Contents

List of Figures

List of Tables

1

Introduction

Cybersecurity is a growing problem in healthcare. In 2014, a study found that 94% of healthcare institutions had been targeted by cybercrime (Filkins, 2014) and since then, the number of healthcare data breaches has been increasing at a high rate (McLeod & Dolezel, 2018). This is likely connected with the tendency for data inside hospital IT systems to be more complete compared to what can be obtained elsewhere (Dockery et al., 2015) and the value of this data to hackers (Connolly, 2018). The consequences of data breaches for hospitals include fines, litigation and reputation damage (Jalali & Kaiser, 2018), costing hospitals millions each year (Davis, 2019). Patients are also affected, as data breaches allow malicious actors to buy medical equipment and drugs using fake identities based on the obtained data. As Information Technology (IT) adoption in healthcare grows, the connections between devices and systems scale with it. This increased connectivity comes at a cost, introducing numerous vulnerabilities in a hospital's threat landscape (Argaw et al., 2020). Adoption of IT security and privacy practices has not scaled in a similar fashion (Uwizeyemungu et al., 2019). As medical systems are becoming increasingly connected, the level of exposure and security risk increases, resulting in an organisation exposed to data breaches (McLeod & Dolezel, 2018).

Data breaches are not the only threats to cybersecurity in hospitals. The WannaCry ransomware attack from 2017 infected over 300.000 computers (Coventry & Branley, 2018), demanding a bitcoin ransom from users who wanted to regain access to their systems which had been encrypted by the ransomware. This can be seen as a form of cyber-extortion. At least 16 organisations of the United Kingdom National Health Service were severely affected (Mohurle & Patil, 2017), causing system-wide lockouts and function loss in devices connected to the organisation's networks, severely impacting their ability to provide patient care.

A newer threat is targeted compromise of functionality. An example of this is the remote hack of a pacemaker published at the Breakpoint security conference (Kirk, 2012). It should be noted that at the time of writing there have been no documented instances of hacks targeted at individual device functionality. However, the possibility of remotely harming a person with the press of a button is worrying. As an audience member at the aforementioned Breakpoint conference put it: "There's no muzzle flash with a laptop".

The potential misuse of data and the dangers of disruption of healthcare services warrant a high level of attention to cybersecurity in the healthcare sector. Unfortunately, this is not the case, as this sector is lagging behind others in protecting its main stakeholder, patients, in cyberspace (Jalali & Kaiser, 2018). In the meantime, the confidentiality, availability and integrity of healthcare data and systems are under threat. Further improvement of cybersecurity levels in healthcare is therefore needed. However, this is not a trivial task, as cybersecurity is the result of many different interacting elements.

1.1. Cybersecurity: a complex problem

The term cybersecurity is used to refer to *protecting confidentiality, integrity and availability of data* (Martin et al., 2017), *the protection of patients in cyberspace* (Coventry & Branley, 2018) or "*the organisation and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights*"

(Craigen et al., 2014). While data breaches are the dominant threat to healthcare IT (Connolly, 2018), compromised system performance is of increasing concern (Schwartz et al., 2018). Cybersecurity therefore involves more than protecting against data breaches, motivating a broader definition. Combining the definitions above, the author defines cybersecurity in this research as *the organisation and collection of resources, processes and structures to protect confidentiality, integrity and availability of assets in cyberspace*. Note that, while cybersecurity protects assets in cyberspace, the tools and processes employed to achieve that protection are not limited to cyberspace. Similarly, the obstacles are encountered in the pursuit of cybersecurity objectives are not limited to cyberspace either. Below, an overview is provided of the technological, human and organisational factors that negatively impact cybersecurity.

1.1.1. Technological limitations

On the technical side, systems with long lifecycles result in a legacy of outdated operating systems and software. Incompatibility between such systems leaves vulnerabilities such as misconfiguration and security holes (Williams & Woodward, 2015). The issue of legacy IT is also encountered in other sectors, such the energy sector (Langer et al., 2016) and manufacturing industry (Ani et al., 2016). It can sometimes be remedied by patching those older systems, but patching itself is often difficult due to disruption of the organisational workflow (Williams & Woodward, 2015) and the extremely high number of systems that need to be patched and the variety of these systems, which is also known as endpoint complexity (Jalali & Kaiser, 2018). Medical devices often contain proprietary software, meaning healthcare IT teams are unable to access the internal software at all (Coventry & Branley, 2018) and even if they could, many of them cannot support onboard cybersecurity measures due to a lack of processing capacity (Williams & Woodward, 2015).

1.1.2. Human elements

Human behaviour or error account for the majority of cyberattacks (Malatji et al., 2020). Medical staff especially sees cybersecurity measures as a barrier, as they see less positive impact of cybersecurity measures on their ability to perform their duties (Jalali & Kaiser, 2018). In healthcare context, availability is frequently prioritised over confidentiality (Coventry & Branley, 2018). According to the European Commission ”awareness raising of staff working in healthcare settings on security and data privacy is important to reduce cybersecurity vulnerabilities and exposure” (European Commission, 2018). Increasing the cybersecurity awareness of hospital staff is therefore an important part of an organisation’s cybersecurity efforts.

A lack of awareness is detrimental to staff compliance to cybersecurity policy. Another factor that increases staff noncompliance is deployment of too many controls at once, which is known as ”controls creep” (Dedeke, 2017). Security measures can compromise the real-time performance of a system, by slowing down the system itself or by making interaction with it tedious, for example by requiring users to log in every time they use a regularly accessed device (Ani et al., 2016). Since employees prefer a security portfolio that maximises utility (Meeuwisse, 2016), security portfolios that negatively impact this utility suffer more noncompliance. Security-aware employees may use a workaround that is not as secure as the ’official’ policy, but is a better fit for their their workflow. This is known as ”shadow security” (Kirlappos et al., 2014).

1.1.3. Organisational limits

Institutional factors create the conditions under which cybersecurity policy can be effective (Angst et al., 2017), which points to the role the organisation plays in such policy. According to Jalali and Kaiser (2018) ”hospital management support is essential for user compliance with information security policies”. Laybats and Tredinnick (2016) found that organisations focus on intentional consequences of intentional actions, as opposed to unintentional consequences of intentional or unintentional actions. This means they pay more attention to events such as hacking, malware and deliberate data theft, than to unintentional leaks and accidental data deletion or destruction. The intentional consequences are the easiest to predict and protect against and draw the most attention in media. These risks are easier to define and easier to mitigate through technology. When mitigating a risk, organisations must believe the benefits of their investment will exceed the costs, but the returns on cybersecurity investments are subject to high uncertainty (Fischer, 2016), as estimating the benefits of an investment (e.g. unobservable prevented losses and avoided liabilities) is difficult (Gordon, 2007). Moore (2010) recognised this

difficulty with assigning value to solutions, pointing to a cybersecurity market failure where actors were unable to properly compare products, causing the market to flood with inadequate solutions.

Healthcare institutions have several characteristics that further complicate the pursuit of cybersecurity objectives. They are often constrained in budget and expertise (Uwizeyemungu et al., 2019), and suffer from a fragmented organisational structure (Martin et al., 2017) which complicates decision-making.

Moore (2010) highlights a misalignment of incentives between patients and hospitals. He states that hospitals do not suffer direct consequences from a data breach, but patients do. This means the stakeholder in the best position to take action to improve cybersecurity levels does not have the proper incentive to do so, even if not doing so will harm the overall outcome. Hospitals are concerned with the suitability and costs of new systems, which reduce the role of cybersecurity in the procurement process (Ghafur et al., 2019). However, the financial burden on a hospital (fines) as well as the negative perceptions of breached organisations represent a direct consequence of data breaches to hospitals (McLeod & Dolezel, 2018). This directly contradicts Moore's perspective, as hospitals do experience direct consequences and can therefore be said to have incentives for improving cybersecurity levels that align with those of their patients. The consequence is that Moore's argument of misaligned incentives as an explanation for low cybersecurity levels in hospitals might not hold.

1.1.4. Improving cybersecurity

Different approaches have been used to research improvement of cybersecurity in healthcare. The Health Care Industry Cybersecurity Task Force (2017) took a sector-wide view and suggested six avenues for improvement: streamlining leadership and governance, increasing security through technical measures, developing the cybersecurity workforce capacity in healthcare, increasing cybersecurity awareness and education, protecting R&D efforts and intellectual property from attacks and improving threat, risk and mitigation information sharing. Other research concluded that:

- A holistic approach was needed with changes to human behaviour, technology and processes (Coventry & Branley, 2018)
- A more preventative and proactive approach to cybersecurity is required (Argaw et al., 2020)
- Cybersecurity considerations must be integrated into healthcare processes (Martin et al., 2017)

Supporting a similar process integration viewpoint, Goff et al. (2014) stated that "including cybersecurity in the procurement process can ensure that these activities are considered starting from the design phase."

Achieving cybersecurity objectives through technological measures is the focus of cybersecurity, both for researchers (McLeod & Dolezel, 2018) and organisations (Kumar et al., 2020). Generally, recommendations for improvement of cybersecurity levels are focused on securing existing IT systems or on securing new systems by arguing for security-by-design and regulation. However, an opportunity exists for improving cybersecurity in between these moments in the procurement process.

1.2. Procurement and cybersecurity

Procurement is "*the process of finding and agreeing to terms, and acquiring goods, services, or works from an external source, often via a tendering or competitive bidding process*" (Laffont & Tirole, 1993). In the context of this research, procured goods, services and works are any device or system a hospital needs and which affect the cybersecurity landscape of that hospital. It is important for cybersecurity because it determines what systems enter an organisation's IT ecosystem.

Dominant procurement models view purchase processes as a series of discrete events and focus on either business actions, decisions or strategic activities (Bäckstrand et al., 2019). In an effort to improve cybersecurity by design for energy delivery systems, Goff et al. (2014) developed common cybersecurity procurement language specific to the sector. This aids in addressing "some of the evolving challenges faced by asset owners, operators, and suppliers by providing a starting point for these stakeholders to communicate expectations and requirements in a clear and repeatable manner." This can be seen as an effort to improve information flow within the procurement process by enabling better communication. When looking at procurement from a market perspective, an analysis of public

procurement in Europe for medical devices revealed barriers to switching suppliers, such as staff requiring product-specific training, making switching suppliers less attractive (Decarolis & Giorgiantonio, 2015). Focusing on more practical experience, the ENISA Procurement Guidelines for Cybersecurity in Hospitals are an aggregation of best practices, each mapped to one or more steps in their cyclical procurement process model (Drougkas et al., 2020). While the focus of these guidelines is on procurement, they include cybersecurity best practices throughout the lifecycle of systems. These practices range from practical (”Conduct data protection impact assessments for new products or services”) to high-level recommendations (”Take into account interoperability issues”).

Taking a decision-making view, Kushniruk et al. (2010) found that the system-organisation fit can improve by making more evidence of that fit available to decision-makers, further highlighting the importance of knowledge and information in the procurement process. Ransford et al. (2017) advocated for the development of cybersecurity standards and their integration into the procurement process as requirements, which would benefit alignment between organisations.

1.2.1. Decision power

In an ideal situation, cybersecurity considerations are integrated into every asset’s lifeycle (Schwartz et al., 2018). However, this is often not the case. Viewing a purchase process as a decision-making process where the decision in question is the conclusion after consideration of options, which in this case is the final purchasing decision, or the solution selected to address the business need. Decision power can impact not only the final purchasing decision, but also the decision-making process leading up to it. This may cause a purchasing decision to be made without proper consideration of the associated cybersecurity implications.

Power is understood as the ”*capability of one social actor to overcome resistance in achieving a desired objective*” (Pfeffer et al., 1981). Decision power, or decision-making power, is the ability to do so in a decision-making process, in this case procurement in hospitals. Decision power is therefore defined in this research as *the capability of an actor to overcome resistance in fulfilling their own objective in procurement*.

On the buyer side, decision power often resides with a hospital department’s leadership. The inclusion of cybersecurity considerations during procurement happens at their discretion. People may make a purchasing decision without properly considering cybersecurity implications, due to overconfidence in their own decision-making ability (Fast et al., 2012) or because they lack the relevant skill set to evaluate trade-offs (Gibson et al., 2005). Such a situation may result in disregarding cybersecurity as a source of criteria or in blind purchases of cybersecurity solutions without much discernible vision (Abraham et al., 2019). After potentially insecure devices or unsuitable cybersecurity solutions have been purchased, IT personnel is then faced with integrating these insecure assets into a hospital’s existing IT infrastructure. Instead of having IT personnel help improve a hospital’s level of cybersecurity, they are made to degrade it instead. This role reversal illustrates an adverse impact on a hospital’s ability to pursue cybersecurity goals, as a result of improperly allocated decision power. A situation where IT personnel can equally influence the decision-making process alongside other interests would be preferable. Related to this imbalance in decision power is the notion of cybersecurity importance. If department leadership considers cybersecurity unimportant relative to other criteria, then their purchasing decisions may reflect this by ignoring warnings from cybersecurity personnel. Thus, department leadership potentially plays a large role in determining an organisation’s cybersecurity level as they may make irrational decisions, although the nature of this role remains unknown.

On the supplier side, the market for medical devices does not favour hospitals. Taking the pacemaker market as an example, the world market consists of about thirty suppliers, with three of them representing an 85% market share (Persistence Market Research, 2016). The low amount of suppliers makes it hard to foster competition, which is the main goal of the procurement system (Decarolis & Giorgiantonio, 2015). This gives them significant bargaining power over buyers. Their position is strengthened by the preference of hospitals for suppliers with established track records. In response, European healthcare organisations increasingly engage in group purchasing (Nollet & Beaulieu, 2003). While this is one example for medical devices, similar situations are found with suppliers of other systems, such as Electronic Health Records (EHR) or laboratory information management systems (LIMS). Regulators like the United Stated Federal Drug Authority (FDA) recently began requiring cybersecurity protection in medical devices, illustrating an initial shift in responsibility towards suppliers (FDA, 2020). While this shift does provide some incentive for suppliers to improve their products’ cybersecurity lev-

els, there is little incentive to do so from a competitive perspective, as the limited number of suppliers offers few alternatives for hospitals to switch to. Other factors can further strengthen a supplier's position. For example, the limited availability of resources in hospitals can increase reliance on a supplier for cybersecurity expertise (Uwizeyemungu et al., 2019).

Pressure from local interests can drive deviations from procurement procedures (Hansson & Holmgren, 2011). For example, suppliers tend to approach department leadership directly, getting a head start on any formal purchase processes (HIMSS Analytics, 2013). This leads to a number of important considerations. To what extent do department leadership and suppliers determine the purchasing decision? Is there even room at all to improve cybersecurity levels in hospitals by taking it into account during procurement, or is the purchase process structured to avoid it? Where does decision power lie? How do these interactions affect cybersecurity in procurement? Or, in short, how is cybersecurity affected in the procurement process?

1.2.2. Cloud services and responsibility

Cloud services warrant additional considerations in procurement, as cloud solutions are inherently connected to multiple nodes over a network. The healthcare sector is experiencing significant outsourcing growth (Guimarâes & de Carvalho, 2011) and transcription (rendering reports from a doctor's audio recordings) and data storage (e.g. cloud services) are the most outsourced IT services. The main reasons for this are improving patient care and saving money in the long term (Lorence & Spink, 2004). However, using cloud services results in a new risk profile by combining the hospital's and the service provider's risks (Benaroch, 2020). Perceptions of the effect of IT outsourcing on cybersecurity levels differ. Some claim insourcing IT allows for finer control over resource allocation to close cybersecurity gaps. Others view outsourcing as a way to do more with fewer resources and consider it a reason to pay less attention to cybersecurity themselves (Jalali & Kaiser, 2018). The latter perspective is important, as it may indicate that hospitals that rely strongly on IT outsourcing consider their own cybersecurity responsibilities lesser than hospitals that do not rely on IT outsourcing as much. This inspires more questions in the context of cybersecurity in procurement. How is cybersecurity addressed in negotiating service contracts? How do hospitals view cybersecurity responsibilities of themselves and their IT providers? And do they consider cloud services as an increase to their risk profile? How does the purchase of a cloud solution change the decisions made in the purchase process? And how do these decisions affect the role of cybersecurity?

1.3. Research gaps

The previous sections revealed a research gap in several themes:

- Cybersecurity is affected by technology, organisation and actors. This combination of factors makes it a complex problem that can be studied from various angles. One of these is procurement. There are currently no studies that cover cybersecurity and healthcare procurement.
- Procurement "should be at the forefront when it comes to meeting cybersecurity objectives" (Drougkas et al., 2020) but the majority of cybersecurity research focused on integrating cybersecurity at suppliers (before purchase processes start) and improving cybersecurity of existing systems within organisations (after purchase processes have concluded). The intermediate step of procurement is therefore underrepresented in cybersecurity research.
- Dominant procurement models view the purchase process as a series of discrete events (e.g. business activities or choices). Such models do not capture the complex nature of cybersecurity. A procurement process framework is needed that can capture complex interactions.
- Healthcare institutions have specific attributes (e.g. extreme resource constraints, highly complex organisation) and there are open questions about cybersecurity in the context of decision power and cloud services that are currently not accounted for in recommendations for improving cybersecurity.
- The majority of cybersecurity research in healthcare is based on literature review or small-N case studies. To generalise findings across a sector, more empirical data is needed.

1.4. Research questions

Cybersecurity is a complex phenomenon and can benefit from a complex research perspective, especially in the context of healthcare. An important finding from literature review is that decision power is a result of internal (department leadership) and external actors (suppliers) as well non-human factors. This makes procurement a complex decision-making process. Existing procurement models do not capture complexity, meaning a new approach is needed. Recognising the above, this research will examine procurement processes from a complex decision-making perspective to establish the role cybersecurity plays in the procurement process. This leads to the main research question:

What is the role of cybersecurity in hospital procurement processes and how can that role be analysed across the sector?

This main research question is itself divided into three sub-questions:

1. *How can the role of cybersecurity in procurement processes be studied?*
   Given the need for a complex view of cybersecurity in procurement, a framework must be developed that captures both the procurement process and the complexities of cybersecurity in hospitals. Different models are presented and evaluated, and a new framework is synthesised. The purpose of this research question is to provide a novel framework for examining cybersecurity in procurement.
2. *What are key factors that influence cybersecurity in procurement?*
   By examining cybersecurity in procurement from a novel perspective, the key factors that influence it can be discerned. This improved understanding can help in understanding how cybersecurity is a part of procurement processes.
3. *How can a research instrument be made to scale this research in the healthcare sector?*
   Recognising the need to analyse the role of cybersecurity in procurement across hospitals, the research results will lead to the design of a survey, preparing the way for future research to assume a quantitative approach to examining cybersecurity in healthcare procurement processes. This will allow for collection of results across the sector, scaling this research.

1.5. Approach

The main research question will be answered using a qualitative approach, which is a better fit than a quantitative approach for questions of ”what?” and ”how?”. First, a literature review will be conducted to examine how cybersecurity and procurement can be studied from a complex decision-making perspective. A theoretical framework will be constructed based on a combination of these perspectives, providing an answer the first sub-question. The theoretical framework provides the basis for an interview protocol, which will be used to conduct a small number of interviews with hospital personnel in the Netherlands. These interviews are then analysed using semi-grounded theory techniques to identify key factors, providing the necessary information to answer the second sub-question. In grounded theory, the research questions should rely on minimal assumptions. The choice for semi-grounded theory is a consequence of the interview design: since the interview questions are based on the theoretical framework, those questions are subject to the assumption of a specific mental model. Since the analysis techniques of grounded theory are used even though the data in question was gathered based on an assumed mental model, this approach is referred to as semi-grounded theory.

The qualitative approach allows for rich data collection, but is time-intensive for the interviewer and interviewee. This makes scaling the research difficult. Recognising this limitation, the interview results will be used to construct a survey with which a sector-wide image can be obtained, scaling this research by examining the prevalence of the key factors across hospitals. The survey is a key deliverable of this research, and provides the answer to the third sub-question.

1.6. Scope and limitations

Because healthcare facility complexity increases the odds of a healthcare data breach and hospitals are highly complex organisations (McLeod & Dolezel, 2018), this research specifically examines cybersecurity in hospitals. The Netherlands was chosen as a geographic boundary in this research, because

it was easier for the author to approach Dutch hospitals than those in other countries. Interviewing hospitals across borders might have introduced additional cultural and regulatory variables into this research. Since applicable regulations are primarily EU-based due to the single market structure, the results of this thesis may still prove valuable to hospitals across Europe.

As this is a master thesis, there is a limitation of time and research experience. The initial research setup focused on obtaining survey results, but was changed to focus on obtaining an overview of cybersecurity in procurement in hospitals through interviews, with the survey as a final deliverable. Due to the time constraint, the survey will not be sent out for response in this research. Not all potential interviewees can be interviewed, which means this research may overlook important themes. A more experienced researcher might have asked different follow-up questions in the interviews, resulting in richer data. Due to the ongoing CoViD-19 pandemic, all interviews must be conducted digitally. This reduces the interviewer's ability to pick up nonverbal communication, further reducing the information the interviews yielded.

This research has been approved by the Human Research Ethics Commission of Delft University of Technology (reference number: 1247). All interviewees consented with their interviews being processed in this research. For privacy reasons, the interview recordings were destroyed after transcription.

1.7. Relevance and contribution

Cybersecurity in healthcare is a growing problem that is difficult to solve due to healthcare-specific conditions such as extreme resource constraints and fragmented organisational structure. This thesis provides scientific value by taking a novel, complexity-based view of cybersecurity to better understand how the involved actors and surrounding conditions interact to shape its role in procurement. While cybersecurity in healthcare is an active research topic, it is not clear to what extent actors are able to account for cybersecurity in purchase decisions. Existing purchase process models failed to capture this, which is a limitation this thesis aims to remedy. By applying a semi-grounded theory approach for analysis, the findings of this research can be used to further refine the used framework, benefiting of future research efforts. Additionally, this research contributes empirical data in the field of cybersecurity in healthcare. This research also contributes to our understanding of procurement processes, deviating from dominant event-based process models by developing a framework to accommodate for complex interactions within the process. The findings of this research can also be used to improve this framework to tailor it specifically to the healthcare sector. The development of a survey enables further research using quantitative methods, complementing the approach used in this research.

The societal benefit of this research resides in enabling healthcare services to become more resilient against digital threats. By increasing this resilience, the risks of direct harm to patients from disrupted healthcare systems and indirect harm through data breaches are reduced. By enabling hospitals to better utilise procurement as an avenue for cybersecurity improvement, they become less 'soft' as a target, hindering cybercrime efforts and therefore profitability. New insights into the role of cybersecurity in procurement enable hospitals to improve their own processes in pursuit of higher cybersecurity levels, benefiting the entire sector. The research results also provide a current snapshot overview of the state of cybersecurity in hospitals, which is valuable as a historic record in an actively changing landscape.

The Complex Systems Engineering and Management Information and Communication (CoSEM I&C) track focuses on information technology and the design and governance of information systems with complex stakeholder landscapes, which aligns with the notion that cybersecurity in healthcare requires a socio-technical perspective (Williams & Woodward, 2015; de Bruijn & Janssen, 2017). The healthcare sector is a complex stakeholder landscape with patients, doctors, hospitals, suppliers and insurance companies representing different priorities and values. The objective of this research is provide hospitals with new insights into the role of cybersecurity in procurement. Such insights directly feed into the design and governance of healthcare IT.

1.8. Overview

The methodology for this research is discussed in Chapter 2, which provides a description of the literature review process, argumentation for the use and structure of the interviews and an overview of the analysis process. In Chapter 3, a procurement process model and a complex decision-making framework will be introduced and integrated into a combined framework. In Chapter 4, this framework is then

used to derive questions for an interview protocol and the data collection and analysis processes for these interviews are described. In Chapter 5, the obtained results are discussed by going over each element of the combined framework. Interviewee quotes will be used to illustrate interesting viewpoints. Five key factors were discerned from the interviews and are explained, and the findings are compared with existing literature. The findings are then used as the basis for the survey in Chapter 6, to scale this research. Chapter 7 concludes this thesis by answering the main research questions.

2

Method

This chapter outlines the various research activities that are used in this research. First, Section 2.1 explains how a literature review was conducted to provide background information and support for the theoretical framework. The framework was then used to construct an interview protocol for semi-structured interviews, which are discussed in Section 2.2. The interviews were subsequently analysed using semi-grounded theory techniques. Finally, the steps to construct the survey are explained in Section 2.3. The findings are summarised in a conclusions chapter, and the research project concludes with a presentation and submission of the full thesis and accompanying research article. An overview of these research activities is provided in Figure 2.1.

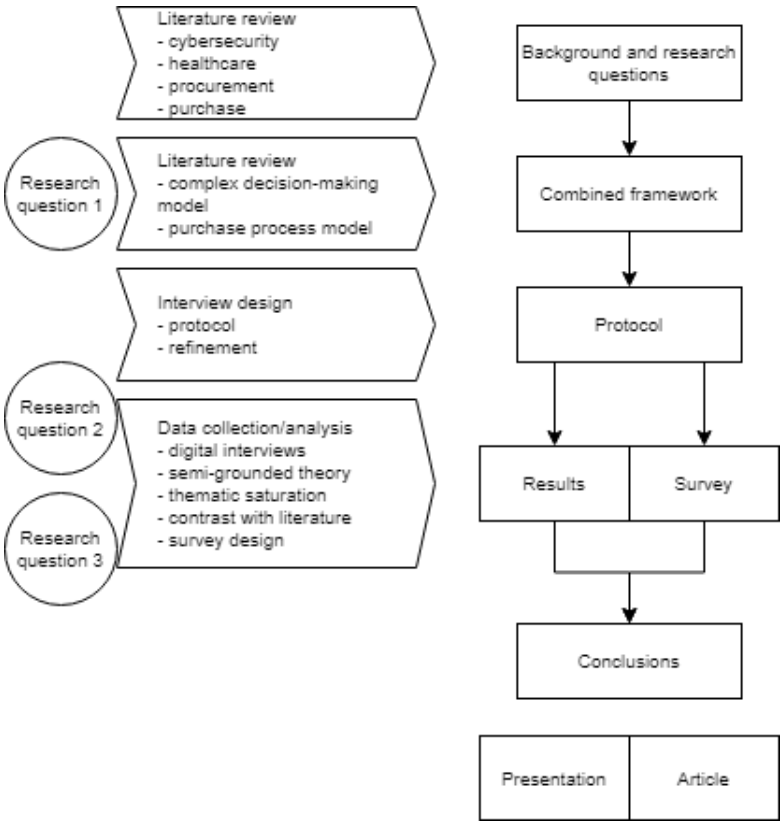

Figure 2.1: Research flow diagram

2.1. Literature review

The introduction revealed a need for a complex decision-making view of cybersecurity in procurement. Existing models and frameworks did not take this view, so a new framework had to be developed from a combination of a procurement process model and a complex decision-making model. Both were found through a literature review of decision-making frameworks and procurement process models. An initial analysis of cybersecurity in procurement was made by applying the new framework to the information found whilst writing the introduction and performing the literature review.

The articles selected for the literature review were found by searching Google Scholar, Scopus and Science Web using search strings that were combinations of the following search terms: cybersecurity, healthcare, procurement and purchase. Additional journal articles were found using backwards snowballing. The supervising committee also provided several papers. Other information from non-academic sources such as market reports and regulatory information was retrieved through desk research.

Literature filtering was based on the title and abstract. If the paper was relevant to the topic, the introduction and conclusion were also read, followed by a complete read. The selected articles were limited to those published in English. A large number of research articles on cybersecurity and procurement focused on securing the procurement process itself, instead of securing an organisation through procurement. As this subject is out of scope, these articles were excluded from the literature search.

2.2. Semi-structured interviews

Based on the outcome of the literature review and the resulting theoretical framework explaining how procurement works, interviews will be designed to collect data to answer the second sub-question. The interviews are semi-structured. The question list is based on the theoretical framework to ensure all the parts are covered, but depending on the raised topics, additional in-depth questions may be asked as well.

The interviewees were CISOs in hospitals or staff with similar responsibilities for maintaining and improving cybersecurity in their organisation, similar to the approach used by Jalali and Kaiser (Jalali & Kaiser, 2018). They were ideal candidates for the interviews, as they are responsible for cybersecurity in hospitals and are sometimes involved in purchases.

This research has been approved by the Human Research Ethics Commission of Delft University of Technology (reference number: 1247). In accordance with TU Delft policy, all interviewees were asked to provide informed consent through a consent form that was provided up front by e-mail. Consent could be given either by returning the signed form, providing written consent over e-mail or by giving verbal consent at the start of the interview. The interview recordings were started only after obtaining consent. In accordance with the consent form, the interview recordings were deleted as soon as the transcripts were finished.

All interviews were recorded and transcribed. All transcripts were anonymised so they could not be traced back to specific individuals or organisations.

Interviewees were sourced by approaching Dutch hospital CISOs over LinkedIn, through the author's and supervisory committee's personal networks and by reference from previous interviewees. As an incentive for participation, interviewees were offered a summary of the results of this thesis.

Sourcing interviewees via LinkedIn means only hospitals that have one appeared in the search results. This was not considered a problem, as hospitals without a CISO are expected to have less relevant insights into their cybersecurity.

2.2.1. Data analysis

Since the interviews were based on the theoretical framework, the coding process was already partially based on existing theory. For analysis, the coding techniques from a grounded theory approach were used, resulting in a semi-grounded theory approach used to analyse the transcripts.

First, each transcript was given a thorough read, and a memo with the key points of each transcript was made. Coding then started with labelling relevant words, phrases and sections. The codes themselves were developed by marking each quotation with a descriptive code, starting with transcript one. Transcript two was then coded the same way. The newly developed codes from transcript two were then compared to the codes in transcript one. New codes from transcript two were then applied to transcript one, merging strongly overlapping codes in the process. This retroactive process was applied

iteratively until all transcripts were coded.

Having established an initial codebook, the number of codes was further reduced by merging codes with low grounding (codes that did not occur much) where possible. During this process, initial groups were also developed by sorting codes together based on overarching themes. While the aim of a researcher is to remain objective, the coding process is the result of experience and knowledge of the researcher (Saldaña, 2016). Coding is therefore always subjective to a degree.

The information retrieved from the literature review was compared with the results of this research, to establish which of the findings aligned with previous research and which did not.

2.3. Survey design

Based on the results from the second sub-question, a survey was designed to make this research scalable to the sector and establish to which extent these results hold for all hospitals in the Netherlands. The core objective of the survey is to verify whether the findings from the results hold for a larger population.

2.3.1. Survey format

At the time of writing, the COVID-19 pandemic is impacting the ability of people to meet worldwide. A method for administrating surveys that avoids researchers and participants having to travel or meet is therefore preferable. For this reason, the survey is designed with digital distribution in mind. Additionally, digital surveys result in faster response time and decreased costs, as well as increased response rates, although this last benefit can ”differ based on variables beyond administration mode alone” (Jansen & Corley, 2007). They list three formats of digital surveys: point-of-contact, e-mail and web-based surveys. Below follows a summary of the benefits and drawbacks of these options, as listed by Jansen and Corley (2007). Point-of-contact surveys have the researcher provide a computing device (e.g. tablet) to the respondent to fill in the survey. This is both time-intensive and can limit the researcher’s ability to reach a large sample. With the current need to minimise travel and interpersonal contact add on top of that, point-of-contact surveys are not a viable candidate. E-mail based surveys are the digital equivalent of pen-and-paper surveys. They can contain questions inside the e-mail or as an attached file. These surveys may be subject to concerns over the target population having restricted internet access, but in the context of cybersecurity and healthcare, it is safe to assume the target population has internet access. E-mail based surveys do raise issues of confidentiality and anonymity, since replies over e-mail are generally identifiable through the sender’s email address. The third option for digital surveys is the web-based survey. This kind of survey resides physically on a web server and is accessible only through a browser. Web-based surveys allow for customisation and are adaptive, meaning they can change their content dynamically based on the received response. Additionally, they do not require manual data entry, compared to e-mail based surveys, making them less labour-intensive. This is a tradeoff, as development of these surveys tends to take more time. A final drawback of web-based surveys is the risk of technological problems impacting the response rate. For example, a respondent might not be able to view the interview due to an outdated browser version or office internet restrictions. Given the need for a survey method without personal contact and the downside of manual data entry in the case of e-mail based surveys, the survey will be designed with a web-based format in mind.

2.3.2. Steps in survey design

Survey design should start with a careful review of literature and conversing with experts on the subject matter, followed by a review of previous survey work to determine which approach works best. The preparation stage of survey research also includes designing plans for data gathering, entry and reporting (Iarossi, 2006). In contrast, Groves et al. (2009) argued that a step-by-step approach to survey design does not guarantee quality and viewed surveys as “requiring the implementation of principles in unique ways to fit a particular substantive purpose for a particular target population”. According to Umbach (2005), the survey design process starts with the survey objective, then constructs are identified and subsequently operationalised using literature. Regardless of researchers’ views of the survey design process, there appears to be consensus on the general process of survey design. The process starts with a core objective, continues to identification of constructs and moves on to operationalisation of these constructs into measurements, or survey items. After addressing concerns regarding pop-

ulation and distribution, survey research transitions into data collection and analysis. Due to a time constraint, this research will stop short of distributing the survey. For that reason, the focus of the survey design is in the preparatory activities, and not on the distribution plan.

Supporting the view that identification of constructs starts with thorough literature review and expert opinion, the literature review and interview results provide all the necessary background to identify constructs. Once these have been identified, they will be operationalised into survey items. This is done using a combination of the findings from the results and existing literature. The intended target population and the consequences for survey distribution will also be discussed.

3

Theoretical framework

In this chapter, a purchase process model and a complex decision-making framework are combined to derive a theoretical framework. This framework is the answer to the first sub-question: *How can the role of cybersecurity in procurement be studied?* This conceptual model is then used to derive an interview protocol, later in this research. In Section 3.1, the choice for a cyclical purchase process model is explained. In Section 3.2, the complex decision-making framework is explained and applied in the context of cybersecurity in healthcare. Finally, Section 3.3 discusses the combination of both into a combined framework.

Earlier, this research found evidence that the procurement process in hospitals is not so much a rigid, structured procedure but more likely the result of interactions between factors like organisational structure and relations with other actors. Previous research suggests that the process is a complex non-linear interaction of actors (Hansson & Holmgren, 2011; HIMSS Analytics, 2013; Jalali & Kaiser, 2018). Since hospitals must ensure some degree of accountability for their purchases, it is likely that the real nature of hospital purchasing lies somewhere in the middle between complex interaction and rigid process. To establish how the purchasing decision is shaped, a framework is used that accounts for both perspectives. This is done by combining a tactical/operational process model and a complex decision-making framework. First, the circular ENISA procurement process model is chosen for its relevance to cybersecurity, procurement and hospitals. Second, given the questions raised in the introduction about the influence of decision power and the need for a complex view of cybersecurity, a complex decision-making framework is selected.

3.1. Purchase process model

3.1.1. Models

Procurement is generally modelled as a series of discrete events, decisions or choices (decision-making), business activities (tactical/operational) or strategic activities (strategic) (Bäckstrand et al., 2019). Here, a short overview is given of the different types of purchase process models.

Decision-making perspective Decision-making purchase process models view the purchase process as a series of questions, choices, information flows or decision trees(Bäckstrand et al., 2019). From the buyer's point of view, a model of a customer's decisions leading up to a purchase is called buyer decision process (Halvorsrud et al., 2016). The benefit of the decision-making perspective is that it can model separate decisions, aiding in identifying the need for additional information during the purchase process.

Tactical/operational perspective Tactical/operational purchase process models represent the separate activities contained within the purchase process. Each step can represent its own process, containing multiple sub-steps of its own. Depending on the purpose of the model, the level of detail can vary. This type of purchase process model is useful for analysing business processes and alignment. There are three variations of the tactical/operational form to consider. These are the linear, cyclical and hybrid linear-cyclical variations (Bäckstrand et al., 2019).

Linear variations represent purchase processes a series of steps, which generally cover specification, selection, contracting, ordering, monitoring and evaluation. The steps are categorised by a buying

moment in the middle, where the sourcing phase ends and the supply phase begins (Van Weele, 2009). Åge (2011) studied business-to-business selling processes, and concluded that linear process models failed to capture their dynamic nature, as the process depends on solving sellers' and buyer's problems in the context of human interactions. While this study is about selling processes, this finding also applies when looking at the process from the buyer perspective since the interactions between sellers and buyers have not changed.

The presence of an evaluation step near the end of linear models implies that lessons are being learned for future use. This property is further emphasised in cyclical process models, which recognise that few purchases start from a blank slate.Instead, purchases start with knowledge from previous purchases in mind. This knowledge may impact the requirements that are set, the solutions that are chosen to overcome any problems and which supplier is selected.

The third variation is an amalgamation of the first two, and separates new suppliers and existing suppliers. The entrance of new suppliers is modelled as a linear process because they have to go through a one-off selection phase, and the interaction with existing suppliers is modelled as a cyclical, continuous process.

Strategic perspective The third type of purchasing process model is the strategic model, which is less detailed than the tactical/operational types. These models discuss how purchasing can become an integrated part of the rest of an organisation. They are focused on developing policy, and not on individual purchase processes.

3.1.2. ENISA procurement model

ENISA published a set of best practices for hospitals to adopt in procurement processes to improve cybersecurity (Drougkas et al., 2020). These practices are each relevant to one or more steps in the procurement process, delineated by their own procurement process model. The ENISA model has been adopted in this research because of the relevance to both hospitals, cybersecurity and procurement.

The ENISA guidelines consider the procurement process as a continuous cycle (Figure 3.1). The ENISA process model is therefore a cyclical purchase process model. The process starts with identify-

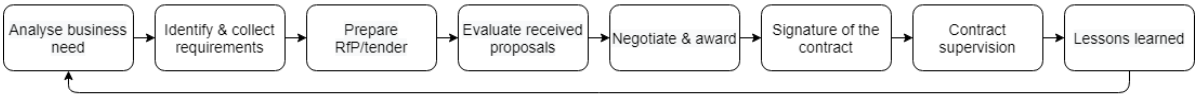

Figure 3.1: ENISA procurement process model for hospitals, adapted from Drougkas et al. (2020)

ing the business need. This is where the hospital realises new equipment or systems are needed, and the purchase process commences. Reasons for purchase could be replacement of older equipment, or a desire to modernise with completely new systems. After the business need has been established, the need is further developed into requirements. Different departments are involved to add to the requirements. These may be functional requirements from clinical staff, or non-functional requirements such as reliability or cybersecurity features. Once the need and desired functionality of the new asset have been identified, the purchase process moves on to the next step.

In the next step, a Request for Proposal (RfP) or tender are prepared. This starts with translating the requirements from the plan phase into technical specifications. Once all of the functional and non-functional requirements have been specified, the RfP or tender are published. Potential suppliers then develop and submit their proposals, marking the transition into the proposal evaluation step. The hospital checks the received proposals and compares them with each other to select the most appropriate one. Negotiations are entered with a selected contractor to iron out final details, preparing a process phase transition.

This phase commences with awarding and signing the final contract. This is the buying moment that separates sourcing and supply in Van Weele's process model, and represents a transition from preparation to execution. The supplier now delivers as agreed, and any after sale support such as servicing is conducted over the duration of the contract agreement. A business owner within the hospital is responsible for managing and monitoring the contract. During this time, feedback from users or other staff are collected to take into consideration in any future purchase processes. This final step closes the cycle.

3.2. Complex decision-making framework

Bäckstrand et al. (2019) showed that purchase processes can be represented as decision-making processes. However, this perspective frames the decision-making process as a simplified flow diagram, thereby excluding any complex macro-micro interactions between internal actors and the hospital itself, and between hospitals and the market around them. The framework by Nyhlén and Lidén (2013) was developed to analyse such complex interactions in decision-making processes (Table 3.1). In this research, it will be used to to analyse complex interactions in the hospital procurement process between structural conditions and the involved actors, providing a richer picture of macro-micro interactions. The framework operates on two dimensions. The first dimension distinguishes the structural conditions and actor-oriented explanations, which are potential influences on individual's behaviour and actors and their corresponding actions, respectively. The other dimension distinguishes which of the above are endogenous or exogenous to the analysed system, separating actors and conditions from inside the decision-making system boundary and outside it.

Table 3.1: Complex decision-making analysis framework

	Structural conditions	**Actor-oriented explanations**
Exogenous	Macro variables Characteristics of sector	Outside actors exerting influence
Endogenous	Cultures Norms and values Internal economical conditions Organisational culture	Beliefs, convictions of internal actors

Exogenous structural conditions are properties of society. They include macro variables and sector characteristics, or any aspect of society that may influence the final decision. On the other hand, endogenous structural conditions are unique to the analysed system and reflect traits like internal culture, norms and values but also organisational economical conditions. Exogenous actor-oriented explanations are actors from the surrounding environment and their influence over the final decision. Important actors are often found in this part of the framework (Nyhlén & Lidén, 2013). Finally, the endogenous actor-oriented explanations are beliefs and convictions of the actors inside the system boundary.

Complex decision-making framework applied to hospitals

The framework by Nyhlén and Lidén was originally developed with political decision-making processes in mind, hence the focus on interplay between structure and agency. To illustrate how the framework works and how it applies to hospitals, the findings of the literature review are positioned in terms of this framework. This gives a first impression of decision-making in hospital procurement processes. The boundary for endogenous framework elements is set at the level of the hospital organisation. Any elements outside the individual hospital organisation are considered exogenous. Based on the literature review, the decision-making framework can help create a partial image of the complexities of procurement in hospitals (Table 3.2).

Table 3.2: Preliminary decision-making analysis in hospital procurement

	Structural conditions	**Actor-oriented explanations**
Exogenous	Seller's market Increasing cybersecurity regulation	Suppliers using their network
Endogenous	Patient care first Budget constraints Preference for known suppliers	Dept. leadership deviating from regular process May neglect cybersecurity

Structural conditions Exogenous structural conditions are those conditions, not related to specific actors and their actions, outside of the hospital boundary. From the literature review we know these include the concentration of market power on the supplier side, and the influence of regulation on cybersecurity responsibility of suppliers. Within the hospital boundary, the purchase decision may be

affected by the prioritisation of patient care over other considerations (Jalali & Kaiser, 2018), the overall presence of tight budgets (Low & Chen, 2012) and the preference for suppliers with an established track record (Decarolis & Giorgiantonio, 2015).

Actor-oriented explanations While suppliers are able to affect the final decision, they do not have the authority to make it. For this reason, they are considered exogenous actors in the hospital purchase process. Their network and relations with department leadership may cause a deviation from the regular purchase process, impacting the ability of other departments to include their requirements early on. This may result in neglecting cybersecurity, resulting in an insecure system being added to the hospital ecosystem.

3.3. Combining the cyclical process model with the complex decision-making framework

The preliminary analysis of the decision-making process in Table 3.2 shows a clear influence of structural conditions, and highlights a lack of information about the actors involved in the process. For this reason, the focus in this research will be obtaining more information on the actors and their actions during the procurement process.

By applying the complex decision-making framework to the ENISA model, an improved procurement process analysis framework is obtained that integrates the tactical/operational process perspective and the notion of complex decision-making, which is otherwise not found in decision-making purchase process models based on flow diagrams. A representation of this combined framework is included in Figure 3.2.

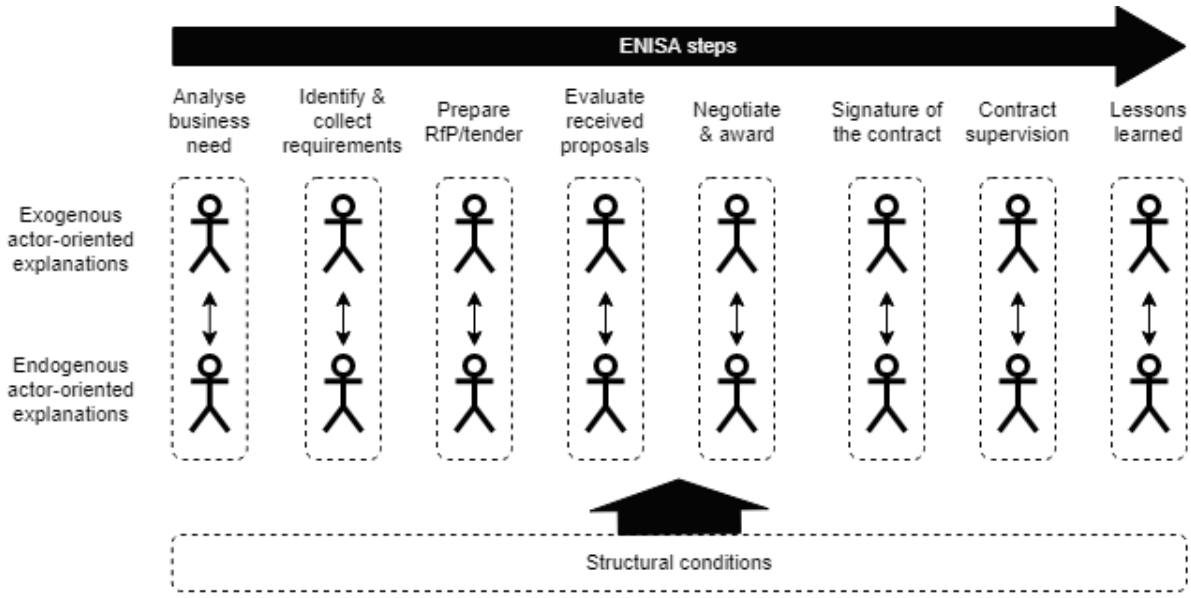

Figure 3.2: Combined analysis framework

4

Interview process

This chapter explains how the semi-structured interviews with hospital CISOs were setup and executed. Section 4.1 explains the process of developing the initial interview protocol from the theoretical framework, and how this protocol was refined over the course of the data collection period. Then, Section 4.2 explains how data was collected and provides an overview of the interviewees. Finally, Section 4.3 explains how the interviews were analysed and discusses if thematic saturation has been reached.

4.1. Developing the interview protocol

The interview protocol was developed based on the theoretical framework. Over the course of several interviews, changes were made to the protocol to elicit more information form interviewees. This section details the development of the protocol over the course of this research.

4.1.1. General questions

The interviews started with an introduction and verification of interviewee consent for recording and processing their data and a short overview of the objective of the research of the interview. Next, the interviewee's role, responsibilities and experience with cybersecurity and procurement in hospitals were asked to establish a background for the interviewee (see Table 4.4).

The introduction highlighted a potential relevance of cloud solutions to cybersecurity in procurement, where the perceived responsibility for cybersecurity might depends on whether or not the purchased system is cloud-based. In an effort to answer the cloud solution-related questions raised in the introduction, the following questions were added:

- What drives the decision to transition a service to the cloud?
- How does the procurement process for a cloud service differ from other purchases?
- Who is responsible for cybersecurity of such a cloud-based system?

The main body of questions was somewhat generic and was not likely to elicit the desired information by itself. Interviewees were asked to provide specific examples associated with each question to compensate. The interview questions themselves were not asked verbatim, allowing for a normal conversation flow. After concluding the main body of the interview, interviewees were asked if they had any of their own topics to add to the discussion.

The initial interview protocol is included in Appendix A.

4.1.2. Deriving questions from the combined framework

The interviews must determine which actors are involved in the process and what their role is. To identify actor-oriented explanations for the role of cybersecurity in procurement, the interview protocol was structured from the perspective of an actor analysis. The main information of interest when analysing actors in a complex decision-making process consists of five elements (Bruijn, 2008): actor's views, their motivations, ability to affect the process, relations with other actions and interactions outside the

specific decision-making arena. In this research, this information need was summarised into three questions:

- Who are involved in this process step?
- What is their desire and motivation to engage with the process?
- What does this process step involve and how can actors affect it?

By applying these questions to each step of the combined framework, a set of interview questions is obtained that can elicit the required information about actors and their actions during procurement in hospitals. The resulting questions are shown in Table 4.1. This table contains several empty cells. These cells are empty because the questions that might have belonged in these cells overlapped with other questions. In choosing which questions to keep and which to discard, the question that was expected to elicit the most information was kept. Consider for example the first process step, 'analyse business needs', and the third information need, 'process step and actor influence'. Asking what the process step 'analyse business needs' involves, might result in a question such as "How is a new business need observed?", which closely overlaps with the earlier question "What are the reasons for starting a purchase?", leading to one of these questions being dropped. It is also important to know that these questions were developed with the option for follow-up questions in mind, which stemmed from the choice for semi-structured interviews.

Table 4.1: Interview questions to elicit actor-oriented explanations

	Who are involved	**Desire/motivation to engage**	**Process step and actor influence**
Analyse business needs	Who decide to start a new purchase?	What are the reasons for starting a new purchase? Are purchases sometimes motivated by external forces, and if yes, how?	-
Identify and collect requirements	Who are involved in setting the requirements for new purchases?	Which organisational roles are involved in setting procurement requirements? How do they affect the set of requirements?	How are requirements gathered for a purchase? What kind of requirements are these?
Prepare RfP/tender	-	-	How many offers do you typically get for a purchase?
Evaluate proposals	Who evaluate these proposals?	What are their interests in selecting a proposal?	How are different proposals evaluated?
Negotiate and award	Who can block or promote a final decision? Who has the final say on selecting a supplier?	-	-
Signature of the contract	Who is responsible for the contract?	-	-
Contract supervision	Who is responsible for evaluating contract performance?	-	Is there an evaluation process for contracts? If yes, could you explain this process?
Lessons learned	-	-	How do previous experiences inform supplier selection in future contracts? How do previous experiences inform setting requirements in the future?

4.1.3. Refined interview protocol

The first two interviews were conducted by adhering to closely to the interview protocol. After the first two interviews, it became apparent that the most valuable information came from deviating from the protocol. Some questions (e.g. about contract signing authority) proved less valuable for eliciting useful information. These questions were dropped in later interviews, which focused more on expanding newly mentioned topics from previous interviews. An overview of the original questions and and what happened to them in later interviews is provided in Table 4.2.

From interview three and onward, the interviews were conducted based a revised set of questions instead. The new interview questions provided more avenues for follow-up questions, providing depth to the information that the original protocol could not elicit. Changes to the interview protocol were mainly motivated by:

- Directly asking participants about the role of cybersecurity in procurement, which elicited good responses and made several interview questions focused about the early procurement process obsolete.

Table 4.2: Overview of original interview questions in the interview protocol

Framework component	Original questions	Refinement (questions labeled N.x refer to Table 4.3)
Analyse business need	O.1. Who decide to start a new purchase? O.2. What are the reasons for starting a new purchase? O.3. Are purchases sometimes motivated by external forces and if yes, how?	Replaced O.1, O.2 and O.3 with N.1.
Identify and collect requirements	O.4. Who are involved in setting the requirements for new purchases? O.5. Which organisational roles are involved in setting procurement requirements? O.6. How do they affect the set of requirements? O.7 How are requirements gathered for a purchase? O.8 What kind of requirements are these?	Partially replaced with N.1. O.4, O.6 and O.8 kept as follow-up questions. Dropped O.5 and O.7.
Prepare RfP/Tender	O.8. How many offers do you typically get for a purchase?	Dropped O.8, as discussing relations with suppliers shed more light on the number of offers and ability to switch.
Evaluate proposals	O.9. Who evaluate these proposals? O.10. What are their interests in selecting a proposal? O.11. How are different proposals evaluated?	All questions retained. New questions led with O.11, as this frequently elicited the rest of the desired information.
Negotiate and award	O.11. Who can block or promote a final decision? O.12. Who has the final say on selecting a supplier?	After mentions of supplier pushback and cooperation during negotiation, replaced O.11 and O.12 with N.4 and N.4.1.
Signature of the contract	O.13. Who is responsible for the contract?	Dropped O.13 after third interview, did not elicit valuable information or avenues for follow-up questions.
Contract supervision	O.14. Is there an evaluation process for contracts? O.15. Who is responsible evaluating contract performance? O.16. If yes, could you explain this process?	O.14 frequently answered with ”No”, negating the need to ask O.15 and O.16.
Lessons learned	O.17. How do previous experiences inform supplier selection in future contracts? O.18. How do previous experiences inform setting requirements in the future?	Dropped O.17 and O.18, as any means of learning lessons would be mentioned when discussing requirement collection.

- Repeated mentions of alternative purchase processes, which motivated a closer look at how those process steps differed from regular purchases.
- Repeated mentions of the increasing importance of cybersecurity, the connection of that trend with regulation and how that affected negotiations hospitals and suppliers.
- Repeated mentions of supplier resistance and cooperation during negotiations.

Table 4.3 provides an overview of the new questions and their relevance to the elements of the framework.

4.2. Interview execution

At the end of each interview, interviewees were offered a summary of the final research results. The interviews concluded with a short recap of the remaining research activities. After the interviews, interviewees were sent their interview transcripts for review and approval. In total, nine interviews were conducted and analysed. The transcripts of each interview are provided in Appendix B.

During interviews four and six, the recording failed. In these cases the researcher’s notes were used as a substitute for the full transcript. The author conducted the interviews over digital media. A variety of digital media were used to record the interviews. Reasons for this variation were interviewee preference for a specific medium and technical difficulties. All interviews were conducted in Dutch.

Each interview lasted approximately 30 minutes. The interviews started with obtaining consent, and a short recap of the purpose of the interview. Then, the first questions of the protocol were asked and based on the response, the next questions from the protocol were selected. If interviewees happened to answer questions before they were asked, they were skipped later on, as the answer to those questions had already been given.

4.2.1. Participant demographics

Nine interviews were conducted with hospital CISOs and healthcare cybersecurity experts across eight different hospitals. These hospitals were located throughout the Netherlands, limiting sampling bias based on location. They varied in size between 500 and 1300 beds, capturing all but the smallest hospital sizes. Searching for hospital CISOs on LinkedIn results in the exclusion of hospitals that do not have a CISO from this research. Assuming that hospitals without a CISO are less occupied with improving their cybersecurity levels and therefore have less relevant cybersecurity insights, this is not considered a problem. One interviewee was not directly affiliated to a hospital. An overview of the interviews and

Table 4.3: Refined interview questions and mapping to the procurement steps

New questions	Rationale	Analyse business need	Identify and collect requirements	Prepare RfP/ Tender	Evaluate proposals	Negotiate and award	Signing the contract	Contract supervision	Lessons learned
N.1 What kind of role does cybersecurity play in new purchases?	This question proved more effective at eliciting the same information than O.1 through O.6 and serves as their replacement	X	X	X					
N.1.1 Who are involved in setting the requirements for new purchases?	Kept from original protocol; same as O.4.		X		X				
N.1.2 How do they affect the set of requirements?	Kept from original protocol, same as O.6.		X		X				
N.1.3 What kind of requirements are these?	Kept from original protocol, same as O.8.		X		X				
N.2 Do purchases sometimes deviate from the proper process?	Added after interviewees mentioned alternative purchase processes.	X	X	X	X	X	X	X	X
N.2.1 What is the effect of that?	Added to elicit additional background information is interviewees did not volunteer it.	X	X	X	X	X	X	X	X
N.3 How are different proposals evaluated?	Kept from original protocol, same as O.11. Made this the leading question as it frequently elicited the follow-up information automatically.		X		X	X		X	
N.3.1 Who evaluate received proposals?	Kept from original protocol, same as O.9.				X				
N.3.2 What are their interests in selecting a proposal?	Kept from original protocol, same as O.10.				X				
N.3.3 How important is cybersecurity compared to other criteria?	Added after interviewees made comments about cybersecurity importance in general and in alternative purchase processes.				X	X			
N.3.4 What drives the increasing importance of cybersecurity?	Added after repeated mention of an increase in cybersecurity importance.				X				
N.3.5 How does regulation factor into this process?	Added after repeated mentions of GDPR and FDA .				X				
N.4 How do suppliers react to your requirements?	Added after mentions of differing supplier responses (cooperation or resistance).		X	X	X	X			
N.4.1 Are they willing to cooperate?	Added as a follow-up question if N.4 was unclear to the interviewee.				X	X			

(anonymised) interviewee background is provided in Table 4.4. The interview designations (I1, I2 etc.) will be used in the next chapter to show which interview yielded each statement.

Table 4.4: Participants' background and demographics

Interview	Function	Cybersecurity/procurement experience	Organisation type
I1	Manager CIO Office	Final responsibility for IT and processes surrounding purchase	Hospital
I2	Clinical Informatics specialist	Responsible for IT-side of medical equipment	Hospital
I3	ISO, security specialist	Incident management, provides cybersecurity information on multiple subjects, including purchase process	Hospital cybersecurity umbrella organisation
I4	Senior in purchase dept.	3 years IT purchasing experience	Hospital
I5	CISO, IT manager	Regularly encounters security/privacy matters in purchasing process	Hospital
I6	CISO	Responsible for information security, working on obtaining certification for hospital	Hospital
I7	CISO	Previous security experience in other sectors	Hospital
I8	CISO	Previously responsible for medical technology and IT in hospital	Hospital
I9	Information Advisor Technical Security Officer	Involved in IT projects and policy Focus on information security and privacy	Hospital

4.3. Data analysis

The recorded interviews were transcribed using ExpressScribe Pro. During the transcription process, the transcript was anonymised by replacing any information specific to the individual or organisation with generic substitute words or phrases. The transcripts (or notes in the case of failed recordings) were sent to interviewees before further analysis, to allow for changes or removal of passages. The approved transcripts are included in Appendix B. After obtaining approval of the final transcript from interviewees, the transcripts were coded using Atlas.ti.

The initial codebook primarily focused on the actors involved, the actions they took and their role in the procurement process. Several overarching factors emerged: supplier-hospital relationship, knowledge exchange and retention, alternative purchase processes, cloud transition, value conflict and structural conditions. The codebook is included in Appendix C. The results are provided in Chapter 5.

4.3.1. Thematic saturation

The results described in this chapter are limited due to the small number of interviews conducted. To determine if the number of interviews was sufficient for identifying the underlying themes, the thematic saturation assessment method by Guest, Namey, and Chen (2020) was used. This method uses the amount of new information gained from new interviews compared information gained from the base set of interviews to calculate a ratio of new information gained. When this ratio drops below a chosen threshold value, the subsequent interviews have not added enough new information and thematic saturation has been reached. Note that reaching thematic saturation with this method does not imply that all possible information was gleaned from the assessed data, as determining the point of saturation is typically a matter of judgement and experience of the researcher. The formula to calculate thematic saturation is: $new\ information = themes\ in\ run / themes\ in\ base$. Three parameters are needed to assess thematic saturation:

- **Base size**, which refers to ”the body of information already obtained” (Guest et al., 2020).
- **Run length**, which in this case is the number of consecutive interviews in which to calculate new information.
- **New information threshold**, which is the proportion of new information that is accepted to indicate that saturation has been reached.

Taking the parameter values used in the example approach in the paper Guest et al. (2020), the base size is set as 4, the run length is 2 and the new information threshold is set at <5%.

The exact interpretation of the ’themes’ referred to in thematic saturation is intentionally left ambiguous by Guest et al. (2020). Using the identified codes as themes, the total number of themes is 86. The first four interviews (in the base set) yielded 73 new themes, giving the base themes for the denominator. Using a run length of 2, the first run is comprised of interviews 5 and 6. These respectively yielded 7 and 1 new theme, making the total new themes in the run 8. The new information gained in this run then becomes $5/73 \approx 0.11\%$. This process was repeated for each run (the next run consists of interviews 6 and 7, then 7 and 8 etc.). The results are displayed in Table 4.5. As the underlined result in the bottom right shows, the new information yield in run 4 dropped below the new information threshold of 5% , indicating thematic saturation has been reached and that additional interviews would not yield substantial new information on top of that what had already been collected.

Table 4.5: Thematic saturation results

									Run 4
							Run 3		
						Run 2			
	Base				**Run 1**				
Interviews	**I1**	**I2**	**I3**	**I4**	**I5**	**I6**	**I7**	**I8**	**I9**
New themes	41	12	17	3	7	1	3	2	0
Themes in base / run				73		8	4	5	2
New information						0.11%	0.05%	0.07%	<u>0.03%</u>

A critical note should be made of this saturation analysis, as different parameters will change the outcome considerably. For example, with the same data, using the same base size of 4 but changing the run size to 3, the final run yields 7% new information compared to the base information, indicating saturation has not been reached. In a similar fashion, picking a more stringent information threshold like 0% would also point to saturation not being reached. However, given the limited time and resources available for this research, a more lenient approach to saturation is warranted. The low saturation score does indicate that this research did almost reach complete thematic saturation. Given the time and resource constraints, this is considered good enough to continue this research.

5

Results

This chapter presents the results obtained from the interviews. The structure of the chapter is based on the process steps of the framework presented in Chapter 3 and focuses on the actors involved, their actions within each step of the procurement process and their motivation to do so. While the initial interview design was not aimed at eliciting structural conditions, the findings presented multiple links with them. Quotes from interviewees are used throughout this chapter, and are marked with the interviewee number (I1, I2 etc.) which corresponds to their number in the interviewee overview (Table 4.4).

Since the actor-oriented explanations were the focal topic of the interviews, these are presented in Section 5.1. Some results belonging to the structural conditions were inadvertently obtained, and are included in Section 5.2. The key factors that influence the role of cybersecurity in procurement are described in Section 5.3. Finally, the results are compared with literature in Section 5.4.

5.1. Actor-oriented explanations: interactions in the procurement process

In this section, the findings for each process step from the combined framework are discussed. An overview of each process step is provided first and then the relevant findings per factor are discussed. Five key factors that influence the role of cybersecurity in procurement were inductively identified: supplier-hospital relationship, knowledge exchange and retention, alternative purchase processes, cloud transition and conflicting priorities.

5.1.1. Analyse business needs

Process

A procurement process is usually initialised by an actor inside the hospital, who represents the role of purchase **requester**. A requester can be one of many actors, such as the head of a clinical department, an IT department, a security team or a Purchasing department. After establishing a purchase need, the purchase is guided through the purchase process by a **process controller**. Depending on a hospital's internal organisation, the requester may assume the role of process controller, or may only be involved in part of the purchase process, in which case the role of process controller is delegated to one or more other internal actors. In that case, the process controller is usually the same actor throughout the purchase process. If this is not the case, different actors may assume the role, such as clinical physicians, IT-managers or -architects or members of a Medical Technology department.

Purchase motivation A requester has a need for a new system or equipment, which can have various motivations. Different departments have different motivations for their purchases. In the context of cybersecurity, three important purchase motivations were mentioned by interviewees.

The first purchase motivator is repeated or replacement purchase. If the purchase is actually a replacement purchase due to existing equipment reaching end-of-life, then the purchase process tends to be much simpler since information from the previous purchase can be reused and a preferred supplier

often comes into play. A second motivation can be a ”technology push”. I2 explained his department (Medical Technology) would observe new technology being used at other departments or hospitals and then actively promote (’push’) this new technology in departments that might benefit from adoption. One interviewee highlighted a third and newer motivation for purchases, namely cybersecurity itself:

> ”[When] we say to our supplier: ’We’re seeing this, can you fix that?’ and the supplier isn’t receptive, then we do sometimes ask ourselves the question if there might be a replacement product that does live in 2020.” **(I3)**

However, I8 limited cybersecurity as a purchase motivator to operating system discontinuity. If an operating system is no longer supported, then new vulnerabilities will add up over time without further support, making it harder to secure. In that case, it is preferable to move to a new system with ongoing operating system support. An operating system upgrade generally implies a full replacement purchase.

Knowledge exchange and retention
I9 shared that knowledge exchange with other hospitals is very rare, and stated that cooperation between hospitals is not common for purchases that concerned only one hospital. If hospitals were on a purchase track together, then cooperation is more common.

Alternative purchase processes
A fragmented approach with different process controllers is not ideal. I1, I5, I7 and I8 indicated a lack of grip on internal purchase processes:

> ”One of the biggest problems you have in a hospital, and I think you’ll have heard this from other colleagues, is that it’s incredibly difficult to get a grip on purchase processes. We see a substantial number of contracts being closed with external parties, where we (the IT department) are involved too late or not at all.” **(I7)**

Purchases do not always pass through the proper channels, resulting in systems entering the hospital ecosystem without the requisite assessment. These systems may cause vulnerabilities by creating security gaps in the network, or by a lack of patching as they are not registered in a hospital’s information processing registry.
Requesters have been known to show resistance to involvement of internal actors in the procurement process. This sometimes stems from the requester having a specific product in mind, and wishing to avoid running through all the requisite steps of the procurement process if the end result is already clear to them:

> ”[Departments] sometimes feel slowed by Medical Technology or another department within the hospital when doing their own purchases. There is a number of people who find it annoying that we involve ourselves in that process. [...] Generally they say ’We know what we want and we’re going to purchase that specific thing’. **(I2)**

Relevant to note here is that a purchase controller is able to bypass some steps and its associated actors in the procurement process. These purchase processes are therefore not visible to actors that would usually be involved, limiting their ability to address their own concerns, such as cybersecurity. This impacts many of the following steps in the procurement process.

Alternative purchase processes are partially caused by ignorance:

> ”When you have a buyer who didn’t understand that [IT had to be involved], then you can run into those kinds of issues. Or when a medical specialist pays for things from their own pocket.” **(I5)**

When medical specialists pay for software by themselves, they automatically become purchase controller. The actual intended purchase controller is therefore kept out of the process and this results in exclusion of internal actors who should be involved, like the IT department. I5 also indicated that alternative purchase processes are usually about software, as for medical equipment there are rules that must be adhered to regarding safe application of medical technology. These rules make the purchase process lengthy and cumbersome to control. The resulting organisational burden may incentivise going through the proper channels, to split the load across the relevant internal actors.

Cloud transition

Hospitals show reluctance to transition to cloud-based solutions. I2 indicated a preference to keep sensitive data within the hospital boundary. I3 spoke of a stigma around cloud, but did stress that the choice no longer defaulted to on-premise solutions anymore, signalling a change in hospital attitude compared to the past.

I7 noted a supplier exerting a lot of pressure to transition to their cloud solution. Their hospital prefers on-premise solutions, which puts it at odds with the supplier's goal to transition. While in this case the choice defaults to on-premise, I7 did expect this to change in the future, citing a "hybrid solution", where core IT is kept on-premise but support services are more frequently transitioned into the cloud.

Suppliers often motivate the transition to a cloud-based solution, rather than hospitals. I9 saw this as a desire of suppliers to "deal with their hosting problems", providing some insight to the motivation for suppliers to move towards the cloud. Suppliers enact this push towards cloud solutions in different ways:

> "I see suppliers who say: 'Listen, in five years we will be in the cloud, so you need to start phasing out your on-premise solutions. We will help you transition to the cloud'. I also see suppliers who offer both and give you that choice." **(I8)**

Both I3 and I6 echoed this distinction between forcing a transition by completely discontinuing the on-premise solution support and offering both types of solutions.

5.1.2. Identifying & collecting requirements

Process

In this step, all relevant requirements for the desired asset are gathered and translated into technical specifications. The purchase controller should involve various actors at this stage to utilise their knowledge and assemble a list of requirements. These actors range from end users to finance and IT departments.

I1 noted that newer medical devices all need some kind of network connection, while I5 noted a frequent coupling between networks and security. When connecting new equipment to a hospital network, cybersecurity automatically comes into play. If a new asset requires a connection, then either the IT department or CISO should be involved. By including these actors, process controllers who are less knowledgeable about the procurement process are made aware of the need to include cybersecurity as a criterion.

Requesters tend to specify requirements in specific terms, pointing to a product or functionality that they know from prior experience. This illustrates a preference for known products and the purchase intent for one specific product. When replacing a system, functional specification is often overlooked. It is seen as an unnecessary step (because the desired end result is already known) and end users also tend to have difficulties with providing functional specification by themselves.

Knowledge exchange and retention

I1 and I2 indicated the use of a kind of "purchase dossier", which is used to store any information about an asset and its purchase:

> "So they do have a kind of purchase dossier for each previously purchased component. Factually, that dossier is a kind of blueprint they use during procurement." **(I1)**

For repeat purchases, a purchase dossier can serve as a kind of purchase blueprint, speeding up the process by removing the need to collect information. I1, I2, I5, I6 and I9 have started using standardised requirement lists, which include a cybersecurity component. A variation of this is the development of standardised means of gathering requirements. These take the form of a kind of process flow diagram to be used by the purchase controller, indicating which internal actors to involve in which step in the process, given the properties of the asset to be purchased. Such properties include connectivity, medical device classification and sensitivity of the processed data.

By providing guidance throughout the purchase process, process controllers can be made more aware of the need to include cybersecurity as part of the requirements.

Alternative purchase processes
When an alternative purchase process occurs, important actors may be excluded from this process step, preventing them from imposing their requirements on the purchase. Five out of nine interviews (I1, I2, I5, I7, I9) contained mentions of such purchase processes, showing they are a common occurrence and have a noticeable impact on cybersecurity.

This deviation from the regular purchase process might simplify the purchase process considerably but potentially introduces unmitigated cybersecurity risks into the hospital ecosystem. A note should be made of the relation between increased connectivity of systems and visibility of purchase processes. The increased need to connect to other systems requires involvement of the IT department to perform the integration, regardless of whether the purchase process went through the proper channels or not. Indirectly, increased connectivity of hospital systems therefore increases the ability of the IT department to address cybersecurity concerns by making alternative purchase processes more visible to them. The presence of standardised requirements or tools to gather them was indicated by several interviewees (I1, I3, I5, I8), where I8 indicated that they were still developing these. These are attempts to increase guidance in the purchase process, simplifying the role of the purchase controller. This makes following the proper steps less cumbersome than guiding a purchase on your own.

Cloud transition
In a transition to a cloud-based solution, many requirements for that transition stem from the cloud service provider. They serve multiple customers and, therefore, are generally less flexible. On that topic, three interviewees commented:

> ”It’s often hard to couple those pieces of software to a modality, because that piece of software is extremely integrated, sometimes with direct cables, or it runs on a whole separate environment, et cetera.” **(I1)**

> ”The problem with cloud solutions is that you can’t customize much about them. I think that will result in a functional bottleneck eventually.” **(I7)**

> ”In reality it often comes down to us having to change so much that, if you’re not careful, result in huge costs for all those changes and mutations.” **(I8)**

These quotes show that the lack of customizability of cloud-based solutions stems from endpoint complexity and cloud vendor inflexibility. Together, these can result in a cloud transition’s cost effectiveness dropping below the point where the transition is viable at all.

Another important aspect of cloud-based solutions is the notion of control. Cloud-based solutions come in various forms, ranging from provisioning infrastructure and virtualization to the entire application being run in the cloud. Hospitals tend to desire a certain degree of control over their applications; I5, I7 and I8 specifically mentioned control as a criterion in the cloud transition.

5.1.3. Preparing Request for Proposal / tender

Process
In preparing the RfP, the set of requirements is made available to potential suppliers, who may start developing their proposals. The hospital may be approached to provide additional clarification of requirements. Ideally, this step results in multiple competitive proposals being submitted.

Public procurement According to EU law (European Commission, n.d.), certain hospital purchases with a monetary value over €214.000 and which might be of cross-border interest must be awarded by public tender. Purchases below this value may still be subject to mandatory tendering, depending on national regulation.

Supplier-hospital relationship
Existing relationships of suppliers with a hospital can influence the selection of a proposal. Two different mechanisms were described in the interviews.

Preferred suppliers Suppliers can attain a status of ’preferred’ or ’standard’. Once vetted during a previous purchase process, subsequent purchases are subjected to less scrutiny. This applies primarily to replacement purchases, where hospitals don’t look further than the same supplier. When a purchase involves a new asset, then it is more common to look at the wider market (I1).

Supplier lock-in The public procurement process is intended to be fair, equitable, transparent and non-discriminatory (European Commission, n.d.) and is designed to achieve a competitive and open market. However, various factors may limit a hospital's ability to switch to another supplier. This phenomenon is referred to as supplier lock-in. Even in public procurement, supplier lock-in can have a significant impact on the final outcome of the purchase process. It can prevent effective competition by limiting the viability of competing offers. High switching costs can make the current supplier's offer the only viable one, as illustrated by one interviewee:

> "If you want to [replace some components] and you have to go through European procurement, and if you have to choose another supplier, you have to replace everything. If your installed base comes from one supplier and you want another, then to replace one million in components, you have to spend six." **(I2)**

This refusal of suppliers to allow partial upgrades may come from a desire to limit the variation in products they have to maintain. This is especially true for requests to replace an operating system:

> "Many suppliers simply say: 'If you want to replace Windows XP, that's fine, but you'll have to buy a whole new MRI, because those are connected. We don't sell or upgrade those separately'. So that makes things quite difficult." **(I8)**

If maintaining cybersecurity requires an operating system upgrade, suppliers may in turn require the hospital to purchase a full replacement. This escalates a security upgrade into a complete replacement purchase process, where the associated costs may prove too great to justify the resulting cybersecurity risk mitigation.

Related to the difficulty in upgrading systems, is the limited ability of hospitals to customise products. Suppliers generally offer closed-box systems, meaning the hospital can't access or modify equipment under threat of losing product support (I8). The inability to customise systems lessens the ability of hospitals to secure such systems. Customisation of systems is also an important theme in the choice for cloud-based solutions (see Section 5.1.2).

Another side of lock-in is technology. With highly interconnected systems, or systems critical to the hospital's operations (e.g. EHR), changing suppliers can incur prohibitively high switching costs, both financial and organisational. If switching suppliers is too expensive, a hospital is stuck with their current supplier. The inability of the hospital to switch to a competitor confers an advantage to the supplier in negotiations.

Another side of supplier lock-in is monopolised services. I6 provided an example of an Electronic Data Interchange (EDI) service between their hospital and general practitioners. In this example, there used to be only one such provider, who held a monopoly over the service. As there was no other provider to switch to, the hospital found itself at a disadvantage in negotiations. This imbalance in negotiations can take on extreme forms. For example, another monopoly-holding supplier was bought out by an investment firm, resulting in them doubling their prices, capitalising on their powerful position. Important to mention is the response of the hospital in the EDI case. As the terms of the agreement with the current provider became less agreeable over time, the hospital approached another party, asking them to start providing a similar service. Eventually, they were joined by several other hospitals at this new EDI provider, successfully breaking up this specific EDI service monopoly. This shows that even though a monopoly confers a strong advantage to suppliers, there is a limit to how far this advantage can be pushed.

5.1.4. Evaluating proposals

Process

Once a RfP has been sent out, suppliers send back proposals, which are subsequently assessed. Different departments in the hospital set their own requirements for purchases and are responsible for evaluating to which extent a proposal satisfies those requirements. This requires coordination between multiple internal actors, which is the an important task of the process controller. Proposal evaluation not only examines the extent to which requirements were satisfied, but includes additional aspects of the purchase. Examples given by interviewees are vulnerability history of a supplier's products, implementation plans for the asset to be purchased, creditworthiness of the supplier and legal and financial context. I1, I3 and I7 indicated that the size of the purchased asset matters, as larger purchases are given more attention than smaller ones.

In practice, evaluation of proposals often involves negotiation. Because of this, many of the findings in this step and the next can apply to both.

Flexible requirements In the context of cybersecurity, the goal is to mitigate risk. This is reflected in the recurring mentions of risk analyses in this process step (I2, I5, I6, I8). While insuring against risks or accepting them based on organisational impact does occur, the default approach is to attempt to secure systems before they enter the hospital ecosystem. While some of the requirements may be lock-out criteria (where failure to satisfy a requirement results in proposal rejection), cybersecurity requirements are often flexible. Two quotes explain why:

> ”It is very hard to make a solid statement about [specific cybersecurity demands], because you’re really only trying to reduce risks. Often, those risks can be mitigated in more than one way.” **(I5)**

> ”The first choice is a supplier that meets the requirements, but if all the suppliers can’t meet those requirements, then we have to negotiate about what is possible and then you see that additional measures are taken, or are already put in place.” **(I5)**

What the quotes above explain, is that setting specific cybersecurity demands is difficult as they represent one specific way of dealing with a risk. While one specific measure might be preferred and therefore specified in the RfP, the options for mitigating a risk vary and are up for negotiation. Examples of additional measures from the interviews are hardening (stripping functionalities in operating system, reducing attack surface), network segregation and intrusion protection systems. A preference for proposals that don’t require additional measures can also be discerned.

If it completely impossible to mitigate a risk, a proposal is rejected. I6 made mention of alternative ways to handle risk: insuring against it or simply accepting it, depending on the potential impact of the risk on the organisation. What the quotes above also showed is a tendency to enter negotiations during evaluation, while multiple offers are still being considered. Evaluation and negotiation are frequently mentioned together.

Cloud transition

Transferring responsibility Part of the choice to put a system in the cloud is the responsibility for the digital assets within. The GDPR made hospitals responsible for the personal data they store and requires data processing agreements with any organisation they share that data with. Three observations provide an image of responsibility for personal data in hospitals:

> ”A hospital always has too little funding and too few people. Which creates a shortage of knowledge and experience in IT, which in turn, for cybersecurity, that you sometimes have trouble getting thigs done because you lack the knowledge. It’s easier to contractually get that from a [supplier].” **(I7)**

> ”Pretty much all parties I know, that have an EHR in the cloud, were very careful in doing so. [...] The feeling of ’chucking it over the fence’ is something I didn’t have.” **(I3)**

> ”We set requirements for that supplier and we test those requirements at regular intervals. That doesn’t go very deep, but we prefer to ask for certification that suppliers have been audited. At set times, we also test, quite simply, how the basic systems are doing: are they patched or not, that is pretty easy to see from the outside.” **(I5)**

Together, these statements first present cloud solutions as a way to enforce cybersecurity where a hospital could not when trying on their own. Once a cloud solution is chosen, these systems are adopted with consideration for cybersecurity. However, the attention to cybersecurity appears to reduce once a system is in place, with only superficial evaluation of cloud vendors afterward.

Vendor specialisation Hospitals focus on patient care, and IT supports this. However, cloud vendors are able to specialise in the provision of their service. This can provide significant advantages:

> ”Many cloud vendors and datacenters that are used, they have that as their core business. Because of that, they can focus much more on securing those systems and certifying their infrastructure against all kinds of security and availability requirements”**(I3)**

> ”[One] reason is making equipment or software available outside the contours of the hospital. If you think of home dialysis equipment, then it’s a lot easier to link that to a cloud application, than to shoot a hole in your firewall to ensure you can connect to your datacenter.” **(I5)**

Additionally, I6 engaged cloud vendors when specialised knowledge was required that the hospital itself did not have. Cloud vendors are able to focus on their systems as a core product, whereas hospitals cannot develop this specialised knowledge. One aspect of this specialisation is that cloud solutions allow for easier external access compared to localised on-premises solutions.

Conflicting priorities
In evaluation, criteria are weighted relative to each other. These weights are sometimes made explicit in a multi-criteria decision analysis, but are always an implicit part of the evaluation process due to priorities and convictions of the decision makers. The following responses were gathered on the importance of cybersecurity relative to other criteria.

> ”[Cybersecurity] is viewed as important, fortunately. More so now than when I started, before that wasn’t the case. The CISO role wasn’t there back then. ” **(I7)**

> ”I think you could say [the importance of cybersecurity] is growing. I see that with users, but with the Board of Directors as well. That does not mean that we can do everything, that we get a ’yes’ to everything. But there is a dialogue, and that, I believe, is much more than a few years ago.” **(I8)**

Additionally, I2 confirmed that the importance of IT requirements and by extension cybersecurity requirements was increasing. I4 noted that the hospital’s priorities were patient care first, then privacy and security, then other concerns.

The common observation here is an increase in cybersecurity importance across hospitals. While patient care still is the top priority, cybersecurity is now part of evaluation, instead of something to be handled after a purchase is concluded.

Position of the CISO within the organisation A side note should be made of an observation made by I3, who related cybersecurity importance in a hospital to the organisational position of its CISO. In some hospitals, the CISO reports to an IT manager and is missing ”clout”, which may be interpreted as a lack of decision power. Instead, cybersecurity might be treated as an afterthought in procurement, resulting in cybersecurity being addressed after the purchase process has transitioned into the supply phase. In these cases, the CISO is sporadically informed of purchases and has to actively involve himself in them to fulfil his role. When he is not involved, cybersecurity can only be addressed after the purchase process has concluded. In other hospitals where a CISO reports to a CIO or directly to a Board of Directors, he has a lot more authority. I3 saw a parallel with the overall importance of cybersecurity in those hospitals: hospitals who did not prioritise cybersecurity would grant a CISO less influence than hospitals that did. On the other hand, hospitals whose CISOs reported directly to the CIO or to board members were perceived as generally more developed in cybersecurity.

5.1.5. Negotiations and awarding

Process
A proposal received by a supplier may require adjustments or further clarification, in order for a hospital to properly evaluate it. During negotiations, any uncertainties in a proposal are addressed and the final details of the contract are worked out. If suppliers can’t satisfy cybersecurity requirements, the negotiations provide an opportunity to identify alternatives, taking into account the limitations of the asset to be purchased.

Proof-of-Concept The availability of a testing environment or a Proof-of-Concept (PoC) sometimes constitutes an additional step before final implementation. By performing a trial run of a new system, cybersecurity or implementation issues can be signalled early. Such issues may result in additional costs by requiring additional cybersecurity measures. For equipment, a PoC is generally only used for new equipment with a large deployed base. The example given by I5 was that a PoC is useful in the procurement process of monitoring equipment, but not for an MRI. Running a PoC can also happen after signing off on a purchase, making it part of the implementation process.

Supplier-hospital relationship
At the negotiation stage in procurement, supplier lock-in can have a strong impact on the final outcome. When a supplier is aware that a hospital cannot easily switch to a competitor, they may use this to their advantage and impose their own requirements on the purchase, even if these are unfavourable to the hospital. One hospital may not be able to influence a supplier, but may be able create a better negotiation position by combining forces with other hospitals:

> ”When you’re in that procurement process, and you’re doing that on your own, then you can’t stand up to a supplier who isn’t cooperating. The moment you know that twenty out of a hundred and fifteen hospitals use the same supplier, then you can make a stand and tell them: ’If you don’t get your affairs in order, then the deal is off for all of us.’” **(I9)**

In the case of I9, this cooperation with other hospitals was formalised in a purchasing alliance, which negotiated deals with suppliers on behalf of its participating hospitals.

Supplier distinctions During negotiations, hospitals may request additional information about proposals and their cybersecurity implications. On this topic, interviewees provided several pieces of information:

- I2 indicated smaller suppliers sometimes have difficulties providing cybersecurity information.
- I3 encountered small suppliers who had paid no attention to cybersecurity at all.
- I4 indicated supplier’s willingness to cooperate is growing, as cybersecurity differences between suppliers start to affect their competitive position.
- I6 stated that smaller suppliers tend to focus primarily on functionality over non-functional features like cybersecurity.
- I5 described non-cooperation for large suppliers as a matter of willingness, where for small suppliers it is a matter of ability.
- I7 used the term ’maturity’ to differentiate between suppliers who barely have cybersecurity features and suppliers who have fully fledged cybersecurity policies and guidelines.
- I9 indicated that larger suppliers either cooperate and ask what they can do to present an ideal situation, or that they present their product as a ’one size fits all’-solution without any flexibility. Additionally, smaller suppliers sometimes lacked flexibility or margins to accommodate any additional demands.

These results point towards a distinction in size or maturity of suppliers. Larger suppliers have an established product, which may allow for customisation to fit the hospital’s needs. This depends on the exact offering of the supplier. Smaller suppliers are often still in the process of developing functionalities for their product. Developing functionalities takes priority over developing non-functional properties. They are sometimes unable to accommodate customisation requests and are generally less secure (I7).

”You’re the only ones asking for this” When asking for cybersecurity features or measures from suppliers, an argument that hospitals initially encountered was ”You’re the only ones asking for this”. Suppliers would claim that other clients had never requested anything similar, trying to convince the hospital in question that there was no reason for them to cooperate on it. Fortunately, this attitude has changed:

> ”That last argument I haven’t heard in years, ’You’re the only ones asking for this’. That’s really out. That argument isn’t used anymore. I do have the idea that that’s because of the market, because colleagues ask suppliers for that with me.” **(I5)**

Here, I5 indicated that a change in demand from hospitals was eventually recognised and acknowledged by suppliers, albeit after some initial resistance. Another way to overcome this argument was through knowledge exchange, which is discussed below.

Knowledge exchange and retention
In the evaluation and negotiation stages of procurement, hospitals exchange information about specific products and suppliers. For all intents and purposes, a product and its supplier are inseparable, as the product and supplier associated with a proposal are simultaneously evaluated. Product requirements are as much part of that process as supplier properties (I2). During this step in the process, hospitals exchange knowledge to get a supplier to cooperate (I5) or to obtain clarification on a specific supplier's cybersecurity measures (I3). Furthermore, in order for hospitals to cooperate and combine forces in negotiations, they need to be aware of the suppliers each of them is working with. This kind of knowledge exchange is facilitated by purchasing alliances or branch organisations (I9). According to I9, the knowledge that hospitals exchange at this stage in the process is mostly focused on functionalities and implementation. Details about the exact contract that another hospital has entered into, are not shared. The knowledge exchange between hospitals is therefore more about how to handle a problem than about the precise contractual outcome.

Another kind of exchanged knowledge are testing results. If one hospital has tested certain security aspects of a supplier, it is both cheaper and easier for another hospital to request those results instead of repeating the test itself. The exchange of supplier security test results between hospitals suggests they trust each other enough to execute a test thoroughly. I5 indicated testing results obtained from other hospitals are valued as if they were their own.

I9 primarily exchanged knowledge with other hospitals to figure out if other hospitals encountered the same problems they encountered and how they dealt with that. This prompted the question if conflict with suppliers was a reason for them to start looking at how other hospitals had gotten something done, which I9 confirmed.

"You're the only ones asking for this" As discussed earlier, this argument is being heard less over time. This may in part be because of hospitals verifying such statements amongst each other:

> "Sometimes a supplier tells a healthcare institution: 'You're the only one worrying about this. 99% of our other customers don't make a point out of this.' And then in practice, that might not be true at all. They pose the question and three other hospitals tell us: 'We experienced the same thing'." **(I3)**

This might be considered a variation of knowledge exchange in order to obtain cooperation from a supplier.

Cloud transition
For Proof-of-Concept or testing situations, cloud services offer a useful quality:

> "If you're running a certain project in the short term, then it's best to do that with a Microsoft or Amazon, because that allows you to quit just as easily. Otherwise an investment runs for three to five years."**(I9)**

This quote demonstrates the convenience of cloud solutions in testing situations. If a test is successful, a hospital may reconsider an on-premises solution for the longer term. For the duration of a test, cloud solutions are more cost-effective than on-premises solutions.

5.1.6. Signing the contract

Process
Final decision authority usually lies with a hospital's Board of Directors, a clinical department head or the Purchasing department head. However, they operate based on advice from internal actors, so purchases must first pass an internal signature process before moving on to the final signing. That internal signature process involves reporting on and checking off requirements from the RfP. These are covered in the previous procurement steps. Once all involved internal actors have signed off on a purchase, is it submitted for final approval. Signing the final contract agreement marks the procurement process transition from the sourcing to the supply phase.

Alternative purchase processes
In the case of an alternative purchase process, where a medical specialist is paying out of his own pocket, the purchase may not be visible to the signing authority at all. The requisite internal signature

processes will have been bypassed at this point and involvement of IT is likely to only happen after the purchase has been made.

5.1.7. Contract supervision

Process

After signing of on an agreement, a supplier delivers the requested good or service, entering the supply phase of the procurement process. During contract supervision, contract performance is monitored and feedback is gathered from end users. This step also includes any after sale support and maintenance.

Evaluating after signing When asked about post-purchase evaluation, interviewee responses varied. I1 stated that evaluation of medical equipment is not standard procedure. Some larger systems like EHR may be tested independently by a supplier, who provides this as a separate service. This is a form of contract supervision by the supplier itself. I2 indicated that the purchase process includes drafting an evaluation plan. I5 performs a regular evaluation of their security portfolio to check if all their cybersecurity measures are still relevant and up to date. In the context of cybersecurity, contract supervision is not done on the level of individual equipment. This is related to the way cybersecurity is generally tested. Cybersecurity tests in hospitals like penetration testing and vulnerability scanning are performed at the department or organisation levels, encompassing a range of systems and equipment in one test.

Supplier-hospital relationship

Contract supervision can be a source of conflict between hospitals and suppliers. Hospitals and suppliers are both trying to set their own patching agendas. Some hospitals set up a regular patching regime, with scheduled testing activities and deployment windows. On the other side, some mature suppliers have their own patching schedule, choosing when to visit and install patches themselves. In such cases, the hospital is often not allowed to perform these installations, making them dependent on the supplier to keep their equipment up to date. While a supplier doesn't perform an update, a device remains insecure. In other cases, suppliers indicate that systems are not to be updated at all, under threat of losing customer support. Often this means that additional measures must be taken to address unmitigated risks, such as network segregation or installing intrusion protection systems.

I6 spoke of security options as additional packages on top of products. These might be additional security features or additional costs to enable patching.

Knowledge exchange and retention

Cybersecurity after signing off on a purchase involves monitoring any new threats, risks and vulnerabilities. This information becomes more important as systems age, especially for medical systems that are no longer updated which require additional cybersecurity measures to remain secure.

The relationship between hospitals may be competitive on the healthcare side, but on the IT side hospitals enjoy "warm relations" (I8). An example of this is the Emotet trojan malware, which prompted I8 to contact others in his personal network to handle it together. However, post-signature cybersecurity knowledge exchange is changing:

> "In IT, we have exchanged knowledge for a long time, but I think that, because of the developments of the last five years, because of Z-CERT[1], that it is improving, that it is increasing. Z-CERT is not that old, and before that you just had to know the right people." **(I8)**

Personal networks are important, but in recent years, efforts to support cybersecurity knowledge exchange such as Z-CERT have had a positive effect. However, I7 did note that only a third of the hospitals involved in one of their knowledge exchange channels actively engaged in exchanging knowledge and information.

I8 encountered another hospital that was working on improving their cybersecurity processes. This motivated I8 to start doing the same, basing their own improvements on those of the other hospital. To improve accountability and reporting, they are implementing a plan-and-control cycle, developing a cybersecurity roadmap and developing a common set of cybersecurity acceptance criteria. The development of these criteria is another example of standardisation of requirements. This is a form of process knowledge exchange between hospitals, which was not observed in earlier steps.

[1] Z-CERT is a cybersecurity expertise centre for healthcare. For more information, visit www.z-cert.nl/en

Alternative purchase processes
In this process step, the consequences of alternative purchase processes become evident. A major consequence of goods purchased this way is the additional costs that may be associated with securing the system after purchase:

> ”If you purchased something improperly, then it has to be installed and you get hit with the facts. You then received budget for one amount, only to get feedback to double that amount to buy the appropriate security measures.” **(I5)**

Additional measures can be expensive and should be factored into the total purchase costs. When this is not the case, the resulting additional costs disincentivise future alternative purchase processes. When a medical specialist needs to contact the Board of Directors to obtain additional budget for cybersecurity measures as a result of not going through the proper purchase channels, that reflects poorly on the specialist. If a hospital incurs considerable costs from such purchases, this stand to profit from minimising such processes.

Conflicting priorities
Part of contract supervision is systems management and maintenance. Even after an asset in purchased and installed, there are still choices to be made about its functioning within the organisation. The preferred resolution of a problem may differ depending on people’s viewpoints. In the interviews, patchmanagement was revealed to be one such issue. I6 illustrated this with an example of conflict between two internal actors: the IT department and Medical Technology department. In this example, IT represents the cybersecurity side of things, where their objective is to maintain the confidentiality, integrity and availability of the hospital’s systems. When faced with new vulnerabilities, they want to mitigate these as soon as possible, which often means deploying a patch. On the other side of the story is the Medical Technology department, whose focus on providing continuity of patient care means they focus on availability. They focus on keeping equipment operational, to ensure clinical staff is able to provide optimal care.

Installing a patch comes with some risk, as the updated system may stop functioning in the way the hospital needs it to. Therefore, while the IT department is focused on patching as soon as possible, the Medical Technology department can resist patching as it might impact the availability of a system, jeopardising the ability of the hospital to deliver patient care. This highlights two conflicting goals. I4 called patching equipment a risk tradeoff, where the risk of compromise is weighed against the risk of inoperability. The outcome of this tradeoff then determines whether a system is patched, or left as-is.

Whichever is the case, the urgency of a problem may dictate bypassing the regular patch processes. If a critical issue is detected and if no solution exists at that time, a hospital may even decide to take a system offline until an open risk can be mitigated. An example of such an event was the Citrix hack early 2020 (Adriano, 2020).

5.1.8. Lessons learned

Process
In the final step of the procurement process, the experiences gained from previous purchases are used to inform new purchases. As hospitals are now being faced with the consequences of their installed base of legacy systems and devices, they need to rethink the way these assets enter their digital ecosystem to prevent the problems they are faced with now from recurring in the future. This takes the form of ongoing process improvement efforts, both of the procurement process itself and of other business processes.

Supplier-hospital relationship
I6 indicated that they did not perform any post-purchase evaluation of suppliers, stating a desire to do so. Examples of experiences taken into new purchases might include a preference (positive or negative) associated with a product or supplier, which may affect the decision to do host services on-premise or in the cloud. Another example was the desire to reduce reliance on a single supplier, diversifying the installed base.

Knowledge exchange and retention
To some extent, the purchase dossiers mentioned in Section 5.1.2 are used to simplify replacement purchases and constitute a form of structured knowledge retention. For example, supplier certification is already provided, relevant requirements are known and any required cybersecurity measures for a system are already inventoried and available from the previous system.

5.2. Structural conditions: market structure and regulation

While the structural conditions were not emphasised in the original interview protocol, the interviews did reveal several links structural conditions. Because these conditions shape the context in which the procurement process is situated, the findings are provided below.

Old players, new demands
A new technological paradigm of interconnected systems is emerging in hospitals. This increase in connectivity resulted in increased demand from hospitals for cybersecurity features in new systems and equipment. This is the first important change for cybersecurity in the procurement process.

This shift partially originated from regulation by the FDA in 2017, calling for increased attention to postmarket management of medical devices. This guidance resulted in an increase in patching of medical devices, as well as connectivity features. Suppliers only recently realised the need to embrace security as part of their product offering. They are still catching up in terms of patching, certification and testing (I8).

Many suppliers are older players, who are used to offering closed-box solutions focusing on healthcare only. On the origin of suppliers, two interviewees revealed a clear picture:

> ”Suppliers come from the era of old machines. Just a small screen in monochrome, with a few buttons so you can press reset, on/off and that was it.” **(I8)**

> ”[Cybersecurity] negotiations usually started with ’What do you mean by that?’.” **(I5)**

Initially, hospitals attempting to address cybersecurity in negotiations with suppliers were met with surprised reactions. As they were not originally IT-focused organisations, suppliers didn’t understand the security implications of increased connectivity.

Influence of regulation
While the increased need for cybersecurity features has forced suppliers to grow their cybersecurity capacities, another important influence is that of regulation. The interviewees made repeated mention of three specific regulations.

Already mentioned is the influence of FDA regulation in 2017, which called for increased attention to postmarket management of medical devices. FDA regulation only applies to products inside the US, but its effect is being felt overseas in Europe, because the majority of the medical device market is located in North America so compliance with US regulation is more likely to affect the overall product line.

Another important influence of local regulation is the General Data Protection Regulation (GDPR). The GDPR instated new security and privacy requirements for organisations processing data from within the EU. This has prompted hospitals to seek certification, with NEN 7510 and ISO 27001 most frequently cited examples. NEN 7510 is an information security norm for Dutch healthcare. Certification for NEN 7510 is required for Dutch healthcare institutions. ISO 27001 specifies requirements for an information security management system and is essentially another information security norm. NEN 7510 primarily focuses on patient data, while ISO 27001 focuses on any information the organisation deems valuable and is not specifically targeted towards healthcare. In practice, NEN 7510 amounts to an extended, healthcare-specified version of ISO 27001 (van Heeswijk, n.d.). These norms in turn forced hospitals to consider cybersecurity in new purchases, prompting them to more frequently ask for cybersecurity features, under threat of fines of the Dutch authority for personal data (AP). As all hospitals throughout the EU are subject to the GDPR and therefore experience have the same incentive to secure sensitive data, the argument *”You’re the only ones asking for this”* has effectively been nullified.

A third relevant regulatory influence is the requirement for CE-certification. Medical equipment must be CE-certified before it can be used inside Europe. CE-certification can take several years, resulting

in certified systems being outdated before they enter the market. One of the interviewees did say that has occurred less over time. Additionally, I6 specifically mentioned that CE-certification has created high entry barriers to the market, observing that smaller players cannot attain CE-certification while still developing their core products.

5.3. Key factors

In this section, the key factors that influence the role of cybersecurity in procurement are described. The implications for hospitals are explained and the relations between these factors are discussed. Five key factors were discerned: supplier-hospital relationship, knowledge exchange and retention, alternative purchase processes, cloud transition and conflicting priorities.

5.3.1. Supplier-hospital relationship

The first factor observed in the results is that of the relationship between suppliers and hospitals. The division of decision power between these two actors dictates who can direct negotiations to their advantage.

Supplier lock-in

The first important sub-theme in the relationship between hospitals and suppliers is supplier lock-in, which refers to a situation where switching to another supplier is not an economically viable option. In this situation, a hospital cannot play two suppliers against each other and cannot threaten to leave a supplier. This significantly reduces their ability to direct negotiations to their advantage. In other words, supplier lock-in confers decision power to the supplier. The cause of supplier lock-in varies and is often a combination of multiple things. Here, the causes are summarised into two categories: high switching costs and a lack of suppliers.

Prohibitively high switching costs When a hospital will purchase a product repeatedly and finds it costly to switch to another supplier, that product is said to have classic switching costs (Farrell & Klemperer, 2007). Hospitals are complex organisations, with matching IT complexity. They have systems that have been in place for a long time which, when coupled with the tendency of IT systems to become more complex over time, results in complex IT ecosystems. This is further exacerbated by high endpoint complexity. The result is that these older, ingrained systems are very expensive to replace, because their replacement results in cascading changes throughout other connected systems. Replacing such a system with a supplier's alternative, the switching costs can become prohibitively high. The only feasible option left is to stay with the old supplier, who may now benefit from supplier lock-in. While the initial cost of staying with the same supplier may be lower, a hospital may eventually need to 'bite the bullet' when maintenance becomes too expensive or when the version in use in that hospital is no longer supported by the supplier.

Lack of suppliers The other side of supplier lock-in is the lack of suppliers to switch to. The interviews revealed the presence of monopolised services, where a hospital was completely dependant on one supplier to provide one specific service. This lack of competition also renders hospitals unable to reap the benefits of supplier competition. However, this may not be a common problem, as it was not encountered in the literature review and was cited by only one interviewee (I6). That interviewee also explained how they, in collaboration with other hospitals, successfully broke up the monopoly by engaging another party to start providing the same service.

Hospital responses Supplier lock-in gives suppliers the upper hand during negotiations. This research revealed two strategies hospitals use to increase their ability to influence the final purchase decision: bloc formation and knowledge exchange. Since knowledge exchange is a separate factor itself, it will be discussed in the respective section (see Section 5.3.2). Bloc formation is the bundling of hospital influence to collectively counteract the decision power of suppliers. This refers to group purchasing behaviour (Nollet & Beaulieu, 2003), which takes the shape of purchasing alliances. Another variant of bloc formation is exerting combined pressure in a user group, where hospitals meet with suppliers to discuss their experiences with purchased systems and voice their concerns.

Supplier distinctions

The second sub-theme in the supplier-hospital relationship is the distinctions between suppliers. Results indicated a distinction based on size and maturity.

Large vs. small suppliers While both vary in terms of customer-mindedness, the reason for (not) cooperating is different for large and small suppliers. For larger ones, cooperation is a matter of willingness. Some large parties are customer-minded and open to cooperation, while others maintain a noncooperative attitude. The results did not contain comments about the underlying motivations, but it is possible suppliers become noncooperative in an attempt to limit their own systems' complexity, at the expense of their clients'. Enforcing such demands may be aided by the supplier lock-in mentioned above.

On the other side are the small suppliers, whose noncooperation stems from inability. The results showed they focus on functionality and are often less secure. Another important influence on smaller suppliers is regulation, which can be restrictive and may be causing smaller suppliers to disappear. Larger incumbent market players stand to profit.

Combined with descriptions such as lack of flexibility and small margins, small suppliers appear to be defined by their constrained resources compared to larger ones. They focus on their core product and do not have the 'luxury' of attending to non-functional qualities just yet.

Cybersecurity maturity The second supplier distinction is cybersecurity maturity, which is the degree to which cybersecurity is a part of a supplier's offerings. This maturity ranges from suppliers having a poor understanding of cybersecurity to having fully fledged policies, guidelines and security features. In general, larger suppliers who are able to address cybersecurity have more developed product offerings, which involve additional cybersecurity features or patching support. However, large suppliers without such understanding of cybersecurity also exist. If a supplier's product offering does not have sufficiently developed cybersecurity features, this may be indicative of lower cybersecurity maturity of the organisation overall. A noncooperative attitude in negotiations could be an attempt to avoid having to implement cybersecurity measures.

Existing relationships

A hospital may prefer a supplier out of convenience. If a supplier has had previous dealings with a hospital, information from previous interactions can be used in newer purchase processes. For example, a known supplier need not be tested for every purchase, and if a product is already known to the hospital, the experience from previous implementations can help implementation of new assets. This is convenient for both the hospital and the supplier, especially since suppliers are generally subjected to less scrutiny once they have an active relationship with a hospital.

Sticking with a preferred supplier out of convenience is not the same as supplier lock-in, because the former includes other viable offers in the procurement process, while the latter does not. However, prolonged cooperation with a supplier may cause other choices to be made under the assumption that the supplier will remain the same, which could eventually lead to a lock-in situation.

Suppliers are generally not periodically evaluated, which suggest that the initial entry of a new supplier is different from a known one in any given purchase process. The implications of this are discussed in Section 7.6.1.

Impact on cybersecurity in procurement

When purchasing assets, hospitals gravitate towards known or preferred suppliers. This can start to influence the procurement process during requirement collection (see Figure 5.1), as the requirements may be formulated to fit the supplier or may not be formulated at all, shortening the process. This can be motivated by convenience or costs. When switching to another supplier becomes too difficult, supplier preference can turn into supplier lock-in, where a supplier may not be preferred per se, but alternatives are either too expensive or not available at all. This lock-in prevents hospitals from satisfying cybersecurity demands by reducing their decision power during negotiations, as they cannot threaten to leave the current supplier. However, this does not necessarily influence the relationship between hospitals and suppliers negatively, as suppliers can still choose a cooperative attitude and work with the hospital in overcoming their problems. The approach suppliers take differs, with supplier size and cybersecurity maturity as main distinguishing characteristics.

Dominant firms with a large installed base or with a proven track record tend to seek incompatibility with competitors, hindering a hospital's ability to respond to changes in efficiency (Farrell & Klemperer,

2007). In hospitals, this means that preferred suppliers will not seek compatibility with other suppliers' systems, maintaining their lock-in. This aligns with the supplier resistance hospitals encounter.

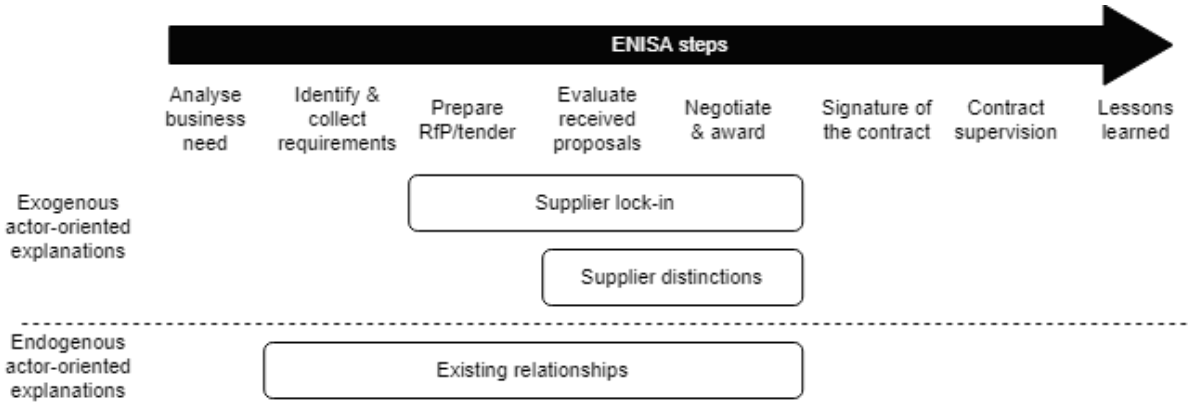

Figure 5.1: Impact of supplier-hospital relationship on cybersecurity in procurement

5.3.2. Knowledge exchange and retention

The second factor identified in the results was the exchange en retention of knowledge. The word knowledge is used, as the term health information is frequently used in the field to indicate information exchanged between digital systems (e.g. EHR). Hospitals exchange knowledge with each other, with suppliers and with other parties and are increasing their efforts to retain knowledge critical to improving cybersecurity. First, the two sub-themes are explained, followed by their impact on cybersecurity.

Knowledge exchange

Hospitals are increasingly gathering and sharing cybersecurity knowledge. Whether this trend started because hospitals are being targeted more or because of regulation is unclear, although the results show that regulation did have some role by increasing the need for a digitally secure environment. This is an ongoing trend that started roughly five years ago, which may signify that hospital cybersecurity is still in its infancy. A large role in this is reserved for Z-CERT, according to I8. Other arenas where knowledge exchange currently takes place are NVZ (Dutch branch organisation of hospitals) and user groups managed by suppliers (I7).

There is room for improving knowledge exchange, according to I7. Hospitals tend to exchange more information when they enter a purchase process together. It is not common for hospitals to involve other hospitals when they engage in a purchase alone (I9).

The different kinds of knowledge being exchanged are summarised here into three categories:

- Supplier information, such as how to get a supplier to cooperate, security testing results or information about cybersecurity measures specific to a supplier. Supplier information is mostly used before signing a contract, in evaluating proposals and in negotiations. Hospitals ask other hospitals for their experience in dealing with a supplier's demands in an attempt to increase improve their position in negotiations.
- Threat information, which encompasses threats, risks, vulnerabilities, indicators of compromise and mitigation strategies. This information is mostly used after signing, although the vulnerability track record of a supplier may also be checked before entering into an agreement.
- Process information, which is information about how hospitals organise their processes to maintain and improve cybersecurity across their organisation. Process information is useful for disseminating best practices and operational experience.

IT, and by extension cybersecurity, are not a competitive arena for hospitals. This creates an environment conducive to mutual knowledge exchange. This may explain why hospitals source this knowledge primarily from each other. Other sources of knowledge are experience of new staff, third party cybersecurity experts, branch organisations, purchasing alliances, personal networks or suppliers themselves.

"You're the only ones asking for this" Suppliers have made false statements to avoid having to accommodate client requests. By exchanging experiences with suppliers they have in common, hospitals can verify is statements made by suppliers are true. In doing so, they reduce the ability of suppliers to deny their requests. This can prove beneficial to a hospital's efforts to secure their systems.

Knowledge retention

Alongside gathering and distributing knowledge, hospitals are improving their ability to retain knowledge as well. This involves recording experiences and learning lessons from previous mistakes, and mainly serves to improve the purchase process itself. Knowledge retention in hospitals can be improved. For example, previous experiences with known suppliers are not recorded explicitly and hospitals do not perform post-purchase evaluations of suppliers.

Hospitals are improving their knowledge retention by changing their processes. Process controllers are provided with process guidance tools to navigate the purchase process and to ensure they involve the right actors at the right time. Examples of these tools are standardised requirement lists and process flow diagrams. Lessons learned while using these tools can then be used to improve them, creating a feedback loop of continuous process improvement.

Standardised requirement lists help in addressing cybersecurity requirements in purchases. Not every requirement applies to every purchase, but such lists do promote thinking about cybersecurity at the least. The usefulness of these lists does depend on their successful dissemination and integration into the rest of the purchase process.

The integration of these lists can be aided by providing further purchase process guidance, such as process flow diagrams or centralised purchase management systems. These assist process controllers in guiding a purchase through the proper channels, ensuring the inclusion of cybersecurity in the process.

Hospitals are confronted with issues while securing legacy systems. Process improvements may be inspired by a desire to avoid these issues in the future.

Impact on cybersecurity in procurement

Knowledge exchange and retention are affecting the role of cybersecurity in procurement in several ways. First, knowledge exchange between hospitals can improve their position in negotiations relative to suppliers. Second, hospitals can improve their ability to handle threats by exchanging information on their different approaches. Third, knowledge exchange improves the dissemination of best practices, allowing hospitals to improve their processes to better account for cybersecurity throughout their organisations. These process improvements can also come from within as a result of learning from past mistakes, by adjusting requirements of future purchases. An overview is provided in Figure 5.2.

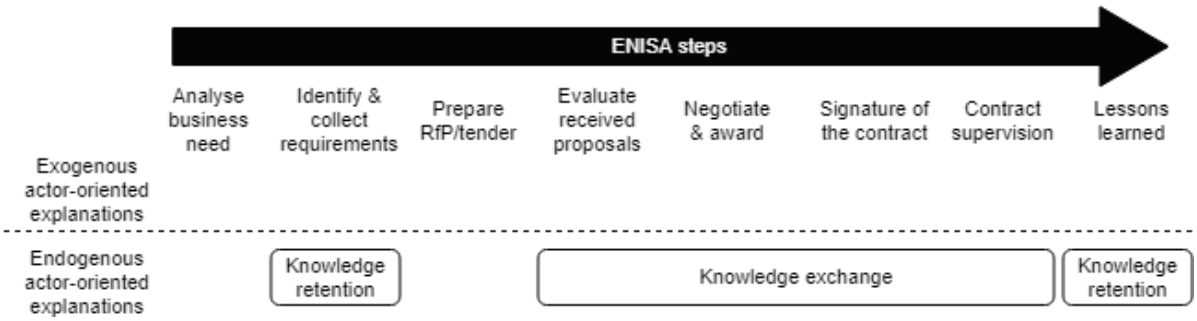

Figure 5.2: Impact of knowledge exchange and retention on cybersecurity in procurement

5.3.3. Alternative purchase processes

Hospitals have channels and procedures for procurement that ensure the relevant actors are involved, the right requirements are set and met and that the whole process in general comes to a satisfying conclusion. Alternative purchase processes are deviations from this structure and occur frequently in hospitals. In such processes, cybersecurity may be addressed after contract signing, or not at all.

Alternative purchase processes are mostly limited to specialised software. When specialists need to acquire this kind of product, they may pay for this out of their own pocket, bypassing the standard purchase process.

Going through the formal purchase process may be a futile effort in the case of highly specialised products. If there is no suitable alternative to a product then there is no need to entertain multiple offers. This simplifies the process. Even if there are suitable alternatives available, the requester may have a strong preference for a specific product. They may not be willing to consider other options, which results in those options always losing out in a comparison. Another reason to go through an alternative purchase process is that they tend to be more simple compared to the formal procedure. Such purchases still start with a business need but skip straight to signing and implementation. This can be much faster than the regular process. A process controller may choose to avoid involving other actors, in an effort to avoid complicating the process. In this case, simplifying the process can reduce the frequency with which alternative purchases occur. Finally, alternative purchase processes may occur as a result of ignorance. If an actor does not understand cybersecurity needs to be a part of the process, it will not be addressed either.

Over time, systems and equipment have become more connected. To function properly, alternative purchases therefore increasingly require network connections and to establish those, a process controller needs to involve their IT department. Even if a process controller showed resistance to involvement of internal actors before, connectivity makes it impossible to keep IT out. IT is therefore better able to influence alternative purchase processes than before, as their increased involvement offers them more decision power.

After an alternative purchase process is completed, additional costs can arise from securing the system after deployment. These additional costs need to be justified to the Board of Directors by the purchase controller. Through this mechanism, the consequences of an alternative purchase process can be attributed to a specific actor.

Impact on cybersecurity in procurement

It is difficult to address cybersecurity in alternative purchase processes because these purchases are poorly visible to IT departments and CISOs. These purchases diverge from the regular process from requirement collection to contract supervision (see Figure 5.3. Alternative purchase processes can introduce unknown risks into a hospital's IT ecosystem, affecting the hospital far into the lifecycle of the purchased asset. Securing systems after they have been implemented is costly, increasing the negative impact of these purchases on hospitals.

The increase in connectivity of systems and equipment is increasing the visibility of these purchases, allowing for better inclusion of cybersecurity in the process before signing. To address the root of the problem, hospitals need to increase their grip on these processes by reducing the resistance to involvement of internal actors and simplifying the process.

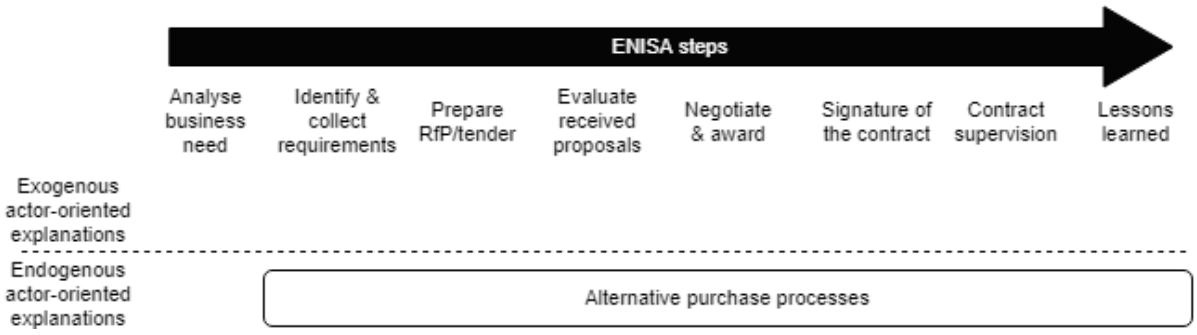

Figure 5.3: Impact of alternative purchase processes on cybersecurity in procurement

5.3.4. Cloud transition

The general attitude of hospitals towards cloud services varies. Some hospitals had a strict policy against cloud services, with one phrasing it as "unknown is unloved" (I2) and another mentioning a "stigma around cloud" (I3). These statements reflect the older, more controlling attitude of hospitals

that their data should be on their systems. However, the attitude of hospitals towards cloud services is improving and adoption is increasing. While cloud services have their own set of advantages and disadvantages, an overarching preference for cloud services could not be discerned. In a departure from strict policies against them, the choice in the evaluation step no longer defaults to on-premise solutions. The topic of cloud transition revealed multiple closely interlinked sub-themes: control, customisability, transferring cybersecurity responsibility, vendor specialisation, cost-effectiveness and convenience.

Control
The first theme in cloud adoption is control, or the extent to which a hospital can manage or interact with the cloud service. I7 envisioned a hybrid solution, stating that they would not move their core IT onto a cloud service, but they would do so for peripheral services, as the advantages far outweighed the reduced ability to control those systems. For peripheral systems, the degree to which control is required over a system may be less and therefore the downsides of cloud services are less severe.

Customisability
Digital infrastructure in hospitals is highly complex, and varies considerably between one hospital and the next. Cloud services tend to have a standardised interface, as they need to connect to different organisations. This complex digital infrastructure and standardised interface are at odds. A lack of customisability, which is needed in order to successfully connect a cloud service with a hospital's complex infrastructure, can make the entire project too expensive, as the integration may require many costly changes on the hospital side. This is a problem for hospitals, which are already experiencing trouble sourcing the right IT knowledge and skills to maintain their systems. This was described as a potential "functional bottleneck" in the future (I7). Endpoint integration with cloud services as particularly difficult due to different modalities having their own software highly integrated with their hardware, creating a scenario where both cloud service and modality need to interface but neither is very customisable. The decision to transition to a cloud service centers around the financial and organisational costs, and the convenience this might provide. The convenience of cloud services stems from two sources: the ability to transfer cybersecurity responsibility to the cloud vendor, and the ability of cloud service providers to specialise where hospitals cannot.

Transferring cybersecurity responsibility
Transferring responsibility increases the convenience of cloud services by contractually moving responsibility for the processed data to the cloud service provider. The GDPR makes hospitals responsible for the personal data of their patients. It requires a juridical basis (a data processing agreement) which a cloud service provider must adhere to in order to continue providing their service. However, as cloud services do involve sending sensitive data to third parties, some hospitals subject a transition to the cloud to careful consideration. One interviewee stated:

> "[When transitioning to a cloud service] there is extensive discussion about the availability demands, how is data secured, backup processes, failover systems, are they certified? The feeling of 'throwing it over the fence' is not something I've felt." **(I3)**

This statement shows much attention is paid to the cybersecurity aspect of cloud services and contradicts the view of Jalali and Kaiser (2018). However, a decrease in attention to cybersecurity will probably not be mentioned by interviewees as such. It is possible that some of the arguments surrounding the cloud theme 'convenience' are actually disguised admissions of reduced attention to cybersecurity. On the other side, some hospitals harbour a more passive attitude towards cybersecurity which might best be described as "It's their problem". I5 indicated that they do test their cloud service providers but that this is not very thorough, citing certification and patching status as regularly tested requirements.

Vendor specialisation
Another element of convenience is the ability of a vendor to specialise. Cloud service providers are responsible for their systems only, which means their core business is to manage and maintain their cloud service. Cloud services are designed for remote access, while on-premise solutions might involve "shooting a hole in your firewall" (I5). With remote care as a growing trend, this may become an increasingly important motivation for cloud adoption. With their own cloud service as their core business, cloud service providers have the expertise required to secure those systems, whereas a hospital

might not be able to do so in the case of an on-premise solution. Additionally, they have cybersecurity knowledge and skills that the hospital does not. Making use of these skills reduces hospital's need to source this themselves. This allows hospitals to achieve more with the same investment, increasing the cost effectiveness of the cloud service. I7 stated that hospitals always lacked funding and people, resulting in a shortage of cybersecurity knowledge and skills. In that case, he claimed it was easier to contractually demand that a cloud service provider provide that security than to source it yourself. This might be interpreted as a statement of the convenience of cloud services, but might also be construed as a desire to not have to worry about cybersecurity yourself. Unfortunately, this research did not examine the distinction.

Cost-effectiveness and convenience trade-off
The overarching themes within cloud are cost-effectiveness and convenience, where the potential costs of a cloud transition must be weighed against the potential benefit it can bring to the organisation (similar to the findings of Jalali and Kaiser (2018)). This leads to the core question surrounding cloud adoption: do the downsides of cloud solutions (reduced control and customisability) weigh up against the convenience (vendor expertise and reduced organisational burden)?

Forced transition
In any case, that question sometimes does not matter. Some suppliers are transitioning to the cloud, forcing their clients to move with them, potentially through supplier lock-in. If the transition to cloud services is forced by providers, hospitals are forced to adopt either way. Not all of these providers force cloud service adoption, as some provide a choice between cloud or on-premise solutions. The attitudes on cloud services vary between hospitals, as cloud adoption is still new within the sector. As the trend continues and adoption increases, the stigma will likely lift somewhat and the general attitude of hospitals towards cloud services is likely to improve further as such cloud services become more established within the healthcare sector.

Impact on cybersecurity in procurement
The transition to cloud-based solutions originates from a push by suppliers. Another motivation for transitioning comes from a desire to achieve better security with less resources which is where vendor specialisation comes in (see Figure 5.4). The main drawback of cloud solutions is the decreased control over and customisability of those systems, compared to on-premises solutions. Control is important during contract supervision, as it covers system management. Customisability is a concern during evaluation and negotiations, as a lack of customisability can result in additional costs for the hospital. For a software vendor, reduced variation in their deployed systems might benefit their ability to specialise, further aiding them in securing their systems. By transferring some of the cybersecurity responsibility to a supplier, hospitals further reduce their own cybersecurity burden during contract supervision.

When evaluating proposals for cloud-based solutions, hospitals make a tradeoff between cost-effectiveness and convenience. The costs and benefits of this tradeoff are difficult to quantify, but there exists a possibility that the cloud transition may be a blessing in disguise for hospitals. The cloud transition presents unique cybersecurity challenges in procurement and its impact on cybersecurity is still unclear, as both a positive and negative impact are possible.

5.3.5. Conflicting priorities
The final factor discerned in this research is conflicting priorities. Conflicting priorities occur when actors try to pursue one goal and in doing so, encounter opposition from other actors who are trying to do the same. Two types of conflicting priorities were observed in this research: conflicting priorities with suppliers and conflicting priorities between internal actors.

With suppliers
Negotiations highlighted a conflict between hospitals and suppliers. Hospitals aim to secure their systems various technical and non-technical measures, but such measures can complicate a system in the eyes of a supplier. This research did not examine procurement from the supplier's point of view, but one explanation for supplier resistance in this situation might be a desire to avoid variation in their product. If a supplier adheres to a strict policy where only they themselves are allowed to update and maintain systems, a high degree of variation in their installed base would complicate maintenance

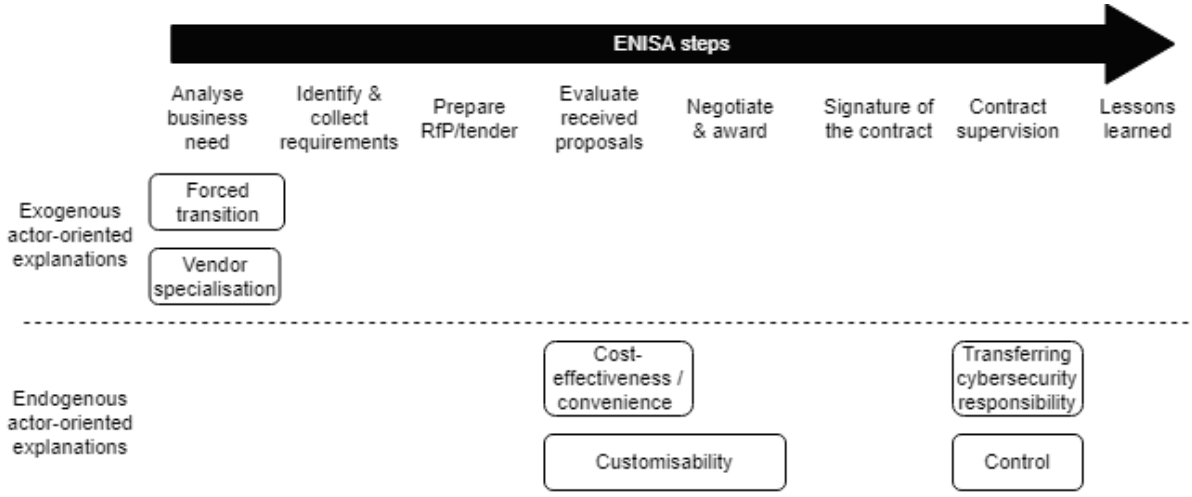

Figure 5.4: Impact of cloud transition on cybersecurity in procurement

considerably, as maintenance becomes more complicated when there are more variables to account for. Furthermore, it is likely that the associated burden on maintenance varies from hospital to hospital, depending on the local IT infrastructure and deployed cybersecurity measures. This would make the resulting maintenance costs hard to quantify. Thus, suppliers would have incentive to minimise variation in their deployed systems to minimise and reduce uncertainty in their maintenance costs.

Another area where priorities differ is during contract supervision, on the topic of patchmanagement. Hospitals desire to patch their systems and keep them operational, while suppliers are profit-oriented and have their own schedules they aim to keep. Given the power imbalance between hospitals and their (digital) suppliers, the latter are in a good position to enforce their will and put their commercial priorities over the hospital's. In short, this might be termed as ”profits over security”.

What these conflicts illustrate is a dissonance between a customer and their supplier. A customer (hospital) does not share the interests of the supplier. From this viewpoint, a supplier is not incentivised to further a customer's interests, unless they align with their own.

Between internal actors

Aside from conflict between suppliers, actors within the hospital may also differ in priorities from each other. The results highlighted an example of conflict between an IT department and Medical Technology department, where the former was concerned with security and the latter with availability. This conflict can be reduced to the conflict between patient care and security. Patient care is the primary focus of hospitals and any systems that enable them to provide this care should therefore be kept operational. Keeping them operational may imply delaying an update, posing a risk. In the presented scenario, the IT department was concerned with confidentiality, integrity and availability, whereas the Medical Technology department was not. This points to a nuance in the importance of cybersecurity in hospitals. The distinction between the cybersecurity triad of confidentiality, integrity and availability appears to be of importance to explain the actions of internal actors. The ethical discussion about where priorities should lie within a hospital is an interesting one, but is not discussed in detail in this research.

An exception to this conflict occurs when the threat becomes big enough to require bypassing the regular update schedule. In that case, the threat to compromising the operational status of a system warrants an immediate update, causing the priorities of these actors to align temporarily.

Security of patient data is a growing concern in hospitals. The GDPR plays a role in this, by formalising repercussions for improperly handled data. Cybersecurity plays a part in reducing the threat of fines, and any fine not incurred is budget that can be allocated elsewhere, to the benefit of patient care. From this perspective, hospitals may opt to improve cybersecurity out of risk mitigation instead of patient benefit. Either way, both hospitals and patients stand to benefit. Note that the GDPR only covers data. It does not cover other cybersecurity breaches (e.g. ransomware attacks). Such breaches affect the availability of hospital systems, directly impacting their ability to provide patient care. This need for availability is not changed by the GDPR.

A note should be made of the connection to alternative purchase processes. If a requester engages in an alternative purchase process knowing the potential negative impact on cybersecurity it might have, then that requester is putting their own interests (whether they stem from a desire to provide patient care or not) over security interests. This would only be the case if the requester sidelines cybersecurity in the purchase process intentionally.

Impact on cybersecurity in procurement
Suppliers do not have the same incentives for cybersecurity as hospitals. The resulting misalignment of priorities caused conflict between these actors during negotiation and contract supervision (see Figure 5.5). Since suppliers have the upper hand in the supplier-hospital relationship, this reduces a hospital's ability to dictate the conditions of their own cybersecurity.

Conflict between internal actors boils down to a trade-off between patient care and security. The example conflict found within the results highlighted conflict during contract supervision, regarding patching schedules. Interests can align between internal actors if the threat is big enough. Framing the avoidance of fines and negative consequences for patients as part of the provision and continuity of patient care might help resolve conflict between internal actors by aligning their interests much like a large threat does.

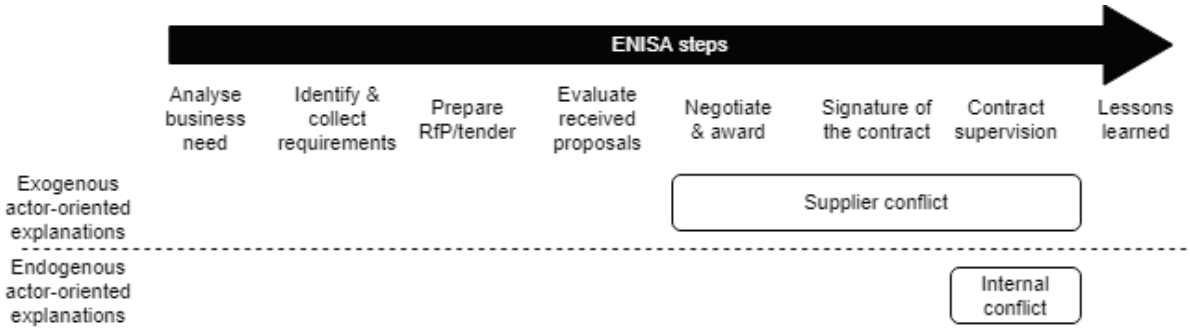

Figure 5.5: Impact of conflicting priorities on cybersecurity in procurement

5.3.6. Interrelations between factors

Having established the key factors that influence the role of cybersecurity in procurement, the next step is describing the interrelations between these factors. Note that these relationships are likely more complex in reality, and that the those described here are merely the relationships that could be identified from the results from the interviews. The interrelations are shown in Figure 5.6.

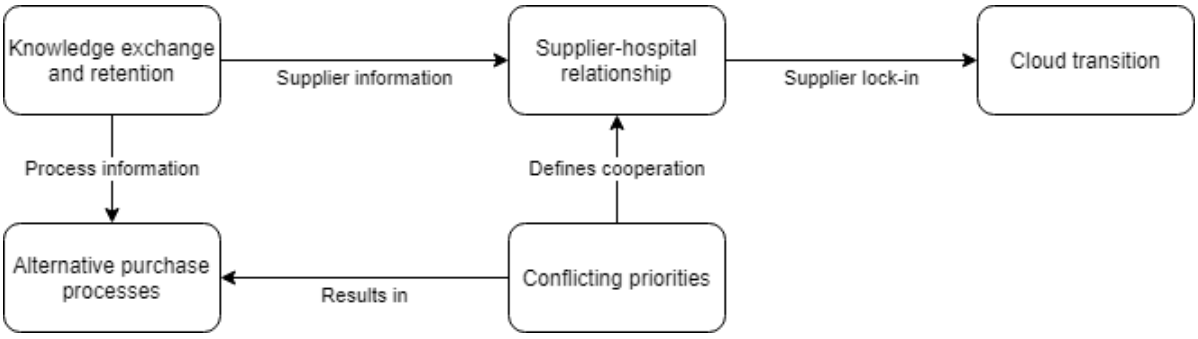

Figure 5.6: Identified interrelations between key factors

Knowledge exchange and alternative purchase processes
The occurrence of alternative purchase processes can be reduced through process information exchange. By sharing process improvements and best practices and increasing their grip on purchase processes, hospitals can gain more control over purchases that bypass the regular process.

Conflicting priorities and alternative purchase processes
An internal conflict over priorities can result in actors within a hospital engaging in an alternative purchase process. By prioritising patient care over security, some steps in the procurement process (such as identification and collection of requirements and evaluation of proposals) can appear an unnecessary burden to the requester. To simplify the process, a requester can choose to skip these steps, thereby deviating from regular procedure and engaging in an alternative purchase process.

Conflicting priorities and the supplier-hospital relationship
Differing priorities between hospitals and suppliers results in differing goals for these actors in the purchase process. However, differing priorities do not necessarily define the relationship in one way, as suppliers may choose cooperation as a suitable approach over resistance during negotiations. A priority conflict is therefore one small influence of the supplier-hospital relationship.

Knowledge exchange and the supplier-hospital relationship
The supplier-hospital relationship is defined by skewed decision power, in favour of the supplier. In an effort to even the playing field, hospitals exchange information about suppliers. This enables them to learn from each other and position themselves better in negotiations with suppliers.

The supplier-hospital relationship and the cloud transition
The cloud transition is the result of a cloud solution push by suppliers. To enact this product push, suppliers who have clients subjected to supplier lock-in can choose leverage this power and force a transition.

5.3.7. Summary of the results
In this chapter, five factors were identified and described: supplier-hospital relationship, knowledge exchange and retention, alternative purchase processes, cloud transition and conflicting priorities. The supplier-hospital relationship is defined by a decision power imbalance favouring suppliers, impacting hospital's ability to satisfy cybersecurity requirements. Knowledge exchange and retention contributes to cybersecurity by evening out the decision power imbalance and enabling continuous process improvement. Alternative purchase processes negatively affect cybersecurity by reducing visibility of purchases and making inclusion of cybersecurity in those processes difficult. The direction of the effect of the cloud transition on cybersecurity remains unclear, as there are arguments that support improvement and deterioration of cybersecurity as a result of this transition. Conflicting priorities negatively affect cybersecurity, by fostering conflict between hospitals and suppliers and between internal actors.

5.4. Relation with literature
This section reviews the key factors to establish if the findings support or contradict existing literature. This separates findings that align with previous research from novel findings.

5.4.1. Supplier-hospital relationship
The three sub-themes of the supplier-hospital relationship were supplier lock-in, supplier distinctions and existing relationships with suppliers.

Supplier lock-in
Previous research highlighted the importance of endpoint complexity (Jalali & Kaiser, 2018) and legacy IT (Williams & Woodward, 2015), but stressed them as standalone factors. The results showed another avenue how they complicate cybersecurity: by complicating the set of requirements, hospitals are forced to require more of suppliers, who in turn push back on this demand.

Lack of suppliers A lack of suppliers is implied in the results with mentions of a lack of alternatives and highly specialised products. Both point to the same notion that there is a small number of options available to hospitals. The literature review found evidence that the market favoured the supply side, with low supply and high demand. The findings therefore align with existing literature, supporting that suppliers have much bargaining power due to the current market structure.

Hospital responses One of the attempts to gain more decision power is group purchasing, as pointed out by Nollet and Beaulieu (2003). In the results, this was reflected in the mentions of purchasing alliances. However, a new finding was the use of knowledge exchange to obtain decision power or

cooperation of a supplier in negotiations. The use of knowledge exchange in negotiations is therefore a valuable new finding from this research.

Supplier distinctions
The distinctions between suppliers were not encountered in the earlier literature review. The notion that there is a difference between small and large suppliers in the development of their products is supported by Walker and Petty (1978), who found that the financial management of small businesses may be dictated by the restricted choices available to that business, like limited access to the financial market, limiting the ability of smaller firms to source capital. The two reasons for noncooperation (willingness and ability to cooperate) were not encountered in previous literature.

Existing relationships
The tendency of hospitals to build relationships with suppliers was encountered by Decarolis and Giorgiantonio (2015)who noted a hospital preference for known suppliers.

5.4.2. Knowledge exchange and retention

Knowledge exchange
Threat information is the current focus of cybersecurity knowledge exchange in hospitals. Research has advocated for this (see Health Care Industry Cybersecurity Task Force, 2017) and in the results mentioned a significant improvement in this area in the last five years, aided in no small part by the arrival of Z-CERT. The other two kinds of information are being shared less. The exchange of process information can help in spreading best practices. Efforts to this end have been made in previous work (see Drougkas et al., 2020). The third kind of knowledge exchanged is supplier information. This kind of information is actively sought by hospitals as it can improve their position in negotiations. For this reason it is an important finding in this research.

Knowledge retention
Prior to the interviews, this research did not find evidence of the importance of knowledge retention within hospitals. Few attempts were mentioned in the results, perhaps indicating procurement process knowledge retention in hospitals is in its infancy. Hospitals stand to benefit from this by streamlining purchases, which can be achieved by structural evaluation of processes and suppliers and using that information in future purchases.

5.4.3. Alternative purchase process

Previous literature did not offer much on alternative purchase processes in hospitals, except that suppliers sometimes approach department leadership directly to engage in a purchase (HIMSS Analytics, 2013). This research did not find further evidence to support this, likely because the purchase controllers of alternative purchase processes were not part of the group of interviewees. Results regarding the motivation to engage in alternative purchase processes are less reliable for the same reason. Regardless, new information on alternative purchase processes was found, such as the nature of these purchases(specialised software and specialists paying out of their own pocket) and the effect of connectivity on the visibility of these purchases. The results did indicate that requesters sometimes do not understand that cybersecurity had to be involved in a purchase, pointing to an inability to evaluate the tradeoff as pointed out by Gibson et al. (2005).

5.4.4. Cloud transition

Literature supports the connection between control over systems and the preference for on-premises solutions. Similarly, the ability to achieve more with less resources (leveraging vendor specialisation) is also supported (see Jalali and Kaiser (2018)). The introduction left an open question whether hospitals considered their own cybersecurity responsibilities smaller in the context of cloud solutions. The results showed differing views, as some hospitals were very thorough in reviewing cloud vendors and products, and others only subject them to limited review. How widespread these views are within the sector, remains unknown. A new finding is that the attitude towards cloud solutions in hospitals is improving. The increased adoption is lifting the stigma on cloud solutions, and this trend can be expected to continue, fuelled by the push for cloud solutions by suppliers. There is evidence of a change in attitude towards cloud solutions, but how far this new attitude is spread is not known.

5.4.5. Conflicting priorities

Literature revealed the conflict in priorities between hospitals and suppliers through two technical issues with cybersecurity, which were limited access to equipment for patching and the limited ability of equipment to support cybersecurity features (e.g. lacking processing power to support encryption). Since suppliers were not interviewed, their motivations can only be inferred through observations from interviewees. While the finding itself is not strictly new, framing these technical issues as symptoms of misaligned priorities is.

Regarding conflicting priorities within hospitals, literature supports that cybersecurity importance is reflected in purchasing decisions. The importance of management support for compliance to security policies was recognised (Jalali & Kaiser, 2018), but a second avenue discerned in this research was not. If management support for cybersecurity is low, this is reflected in the organisational position of the CISO, who may not receive the authority required to sufficiently influence purchases to include cybersecurity. Examining if this finding holds for the sector is valuable, as hospitals who are in this situation may benefit from allocating more decision power to their CISO.

A new finding is conflict between internal departments. This was not recognised in previous literature directly. However, the priorities in the conflict between the IT and Medical departments did represent a previously identified tradeoff between smooth operation and high cybersecurity levels (de Carvalho & Saleem, 2019). A probable explanation for the differing priorities of internal departments is the day-to-day activities they are concerned with. For example, IT staff is likely to think about cybersecurity more often than other employees. whether such conflict is common within hospitals is unknown. This kind of conflict might be an important barrier to improving cybersecurity, highlighting the value of internal alignment within an organisation. In this, there is likely a role for staff awareness of cybersecurity.

6

Scaling the research

The interviews revealed five factors that affect the role of cybersecurity in procurement. However, the number of interviews is limited and represents a very small sample of the population of hospitals in the Netherlands. This means that more information is needed to measure the *prevalence* of these factors in the sector. To this end, the findings from this research are used to develop a survey, enabling a quantitative approach to examine the role of cybersecurity in procurement. This extends the research by adding a magnitude to each of the factors' effects, and can provide an answer to the third sub-question: *How can a research instrument be made to scale this research the healthcare sector?* The additional benefit of a quantitative approach is the possibility of examining correlations between the factors. A mock-up of the survey is included in Appendix D.

6.1. Target population overview

6.1.1. Population size

As the survey represents an extension of this research, the target population remains the same: hospital CISOs or staff with similar responsibilities for maintaining and improving cybersecurity. As the interviews were conducted amongst Dutch hospitals only, an evaluation of the probable response can be made. The Netherlands contains 549 hospitals (Stewart, 2019), spread across 69 organisations in 116 locations (RIVM, n.d.). The definition of a hospital is therefore ambiguous. The following estimate is made based on the estimates of Stewart (2019) and assumes one CISO per hospital. Previous surveys of cybersecurity in organisations showed response rates ranging from roughly 40% (Kumar et al., 2020) to 50% (Lorence & Spink, 2004). Assuming the entire population can be reached and using a conservative estimate of 35% response yields $549 \times 0.35 \approx 192$ responses. The actual response will likely be lower because not all hospitals have a CISO (or similar staff member) and because it is unlikely all hospitals can be reached.

6.1.2. Important variables

Aside from the main body of survey items, there are several aspects of hospital organisations that should be controlled for. The influence of hospital size on cybersecurity in hospitals remains unclear. Larger hospitals are generally slow to enact change, while smaller hospitals are more flexible (Jalali & Kaiser, 2018). This leads to the expectation that smaller hospitals adopt cybersecurity practices faster than larger ones. However, resource allocation for cybersecurity appears to be lacking regardless of hospital size (Uwizeyemungu et al., 2019). Increased investment must be made in the healthcare IT environment to embed security culture (Ghafur et al., 2019). This implies that increased cybersecurity investment will enable improved adoption of cybersecurity practices in hospitals. A note should be made of the relation between hospital size and resource allocation. Larger hospitals will have a larger budget, but are also likely to require more resources to improve cybersecurity, as the scope of such improvements will probably change with the size of the organisation. The amount of allocated resources therefore likely depends on hospital size. However, it is still unclear if the amount of allocated resources affects cybersecurity when controlled for hospital size.

6.2. Survey items

This section details the construction of survey items from the five factors identified earlier. The survey consists of 35 survey items: three items for contextual variables (CV), thirteen for supplier-hospital relationship (SHR), seven for knowledge exchange and retention (KER), two for alternative purchase processes (APP), seven for cloud transition (CT) and three for conflicting priorities (CP). A mock-up of the survey is provided in Appendix D.

6.2.1. Constructs and measurements

The objective of this survey is to assess the extent to which the key factors found in the results influence the role in procurement in a larger population of hospitals. This objective calls for a slightly different approach to survey design. The literature review and interview results provided various ways in which the role of cybersecurity in procurement in hospitals is influenced. These were grouped during the coding process into the five factors discussed in Section 5.3. These five factors will serve as constructs under study in the survey.

Measurements are the ways to gather information about constructs (Groves et al., 2009). They are also called survey items, or question items (Iarossi, 2006). The sub-themes from the results represent the different ways in which each factor affects the ability of actors to address cybersecurity requirements in procurement.

Validity is the extent to which measures reflect the underlying construct (Groves et al., 2009). Since the five factors were themselves a product of grouping during the transcript coding process, the sub-themes inherently define the overarching factor, lending validity to this survey setup.

Using the five factors and their sub-themes for constructs and measurements, the next step is to operationalise them into survey items. Given the objective, information of interest is whether hospitals in general experience the impact of these factors on cybersecurity similar to what was observed in the interviews. This will be done by posing a set of statements and asking how frequently they are encountered by respondents. A dichotomous True/False answer set would suit the survey objective, but another option may prove more useful. By asking the *frequency* with which these items influence a respondent's ability to address cybersecurity in the procurement process, more information is solicited compared to the dichotomous True/False answer set.

Consider an example survey examining employee workloads that contains the statement: ”I do not have enough time to complete my work”. A True/False response would provide some information as to whether a respondent needs more time to do his work. A frequency response using a rating scale ranging from ”Never” to ”Always” reveals how often this is the case, which is likely more useful to a researcher as it sheds light on the severity of the problem.

For this reason, the survey items are formulated as statements, where respondents can answer on a five-point rating scale. This frequency scale consists of ”Never”, ”Rarely”, ”Sometimes”, ”Often” and ”Always” (Vagias, 2006).

6.2.2. Feedback

Feedback revealed that the survey design required a lot of cognitive effort of the respondent, meaning they had to read and understand a lot of information to be able to answer the questions properly. To reduce the required effort, the statements were simplified. This involved changing the statements to ask how often respondents recognised the sub-themes in their day-to-day work activities. This shortened the survey items and made them easier to answer. Items SHR6 to SHR13 and the items for cloud transition were left unchanged. A few lines of explanatory text were added per section of the survey, to explain why those sections were included and provide a coherent 'storyline' that respondents could follow, further reducing the effort required from respondents.

6.2.3. Contextual variables

The two proposed contextual variables are hospital size and allocated resources. These can be accurately measured through the number of beds and IT budget, respectively (Uwizeyemungu et al., 2019). The resulting survey items are included in Table 6.1, using the same scales for these metrics as Uwizeyemungu et al. (2019). A third question will ask about the organisational role of the respondent in their respective hospital, as this can affect how they perceive the role of cybersecurity in procurement.

Table 6.1: Survey items for contextual variables (CV)

Variable	Survey items	Answer categories
Hospital size	CV1: How many beds does your hospital have?	<101, 101 to 250, 251 to 750, >750
Allocated resources	CV2: How large is the IT budget in your organisation? (% of total hospital budget)	<1%, 1% to 3%, 3.1% to 5%, >5%
Role	CV3: What is your your function title within your organisation?	[open question]

6.2.4. Supplier-hospital relationship

The concept of supplier lock-in comes about through a lack of suppliers or through high costs associated with switching to a new supplier. Hospital responses are bloc formation (group purchasing) and exchanging supplier information. The second sub-theme of this relationship was the existing relationships with suppliers, noted through a preference for known suppliers with an established track record. The final sub-theme was the types of distinctions to be made between suppliers, where a cooperation willingness and ability were linked to the size of the supplier. Additionally, a distinction was made based on cybersecurity maturity, defined as the extent to which suppliers understand what is required from them and if they have the desired information. The resulting survey items are included in Table 6.2.

Table 6.2: Survey items for supplier-hospital relationship (SHR)

Sub-themes	Survey items
Supplier lock-in	**Please indicate how often you encounter the following notions in purchase processes:**
Lack of suppliers	SHR1: A lack of alternative suppliers to consider
High switching costs	SHR2: High costs associated with switching to another supplier
Bloc formation	SHR3: Membership of a purchasing alliance or similar organisation
Knowledge exchange about suppliers	SHR4: Exchanging information with other hospitals about suppliers
Existing relationships	**Please indicate how often you encounter the following notions in purchase processes:**
Preference for known suppliers	SHR5: A preference in my hospital for known suppliers over unknown ones
Supplier distinctions	**When discussing cybersecurity features during negotiations …**
Willingness versus ability	SHR6: Large suppliers are willing to cooperate
	SHR7: Large suppliers are able to cooperate
	SHR8: Small suppliers are willing to cooperate
	SHR9: Small suppliers are able to cooperate
Cybersecurity maturity	SHR10: Large suppliers understand what we want from them
	SHR11: Large suppliers have the desired information ready
	SHR12: Small suppliers understand what we want from them
	SHR13: Small suppliers have the desired information ready

6.2.5. Knowledge exchange and retention

Three types of knowledge exchange between hospitals were identified: supplier information, threat information and process information. Identified forms of knowledge retention were purchase dossiers, standardised requirement lists, process guidance tools and supplier evaluation. In the corresponding statement, purchase dossiers are called ”records of previous purchases”, to make the statement easier to understand. Purchase process tools like flowcharts or purchase management systems serve the same purpose, namely to improve the grip hospitals have on purchase processes. In the corresponding statement, they are called ”purchase process management tools” to emphasise their function. The last element is about supplier evaluation. Even though the results indicated this occurred rarely or never, it is still included in survey in the interest of completeness. The resulting survey items are shown in Table 6.3.

6.2.6. Alternative purchase processes

Alternative purchase processes occur when hospital staff bypasses the regular procurement process. Since the impact of such processes is a reduced ability to address cybersecurity in procurement, one statement asking for the frequency with which these processes occur will suffice. The results also revealed a link between increased connectivity of equipment and systems and an increased ability to address cybersecurity. This motivated the second statement. The resulting statements are shown in Table 6.4.

Table 6.3: Survey items for knowledge exchange and retention (KER)

Sub-themes	Survey items
Knowledge exchange	**Please indicate how often you encounter the following notions in purchase processes:**
Supplier information	KER1: Supplier information from other hospitals (how to get a supplier to cooperate, security test results, information about cybersecurity measures specific to a supplier)
Threat information	KER2: Threat information from other hospitals (threats, risks, vulnerabilities, indicators of compromise, mitigation strategies)
Process information	KER3: Process information from other hospitals (best practices for processes)
Knowledge retention	**Please indicate how often you encounter the following notions in purchase processes:**
Purchase dossiers	KER4: Records of previous purchases
Standardised requirement lists	KER5: Standardised requirement lists
Process flow diagrams	KER6: Purchase process management tools (e.g. process flow diagrams, purchase management systems)
Supplier evaluation	KER7: Previous evaluations of suppliers

Table 6.4: Survey items for alternative purchase processes (APP)

Sub-themes	Survey items
	Please indicate how often you encounter the following notions in purchase processes:
Occurrence in general	APP1: Hospital staff bypassing regular purchase procedures
Connectivity and visibility	APP2: Purchased assets requiring a network connection to function

6.2.7. Cloud transition

Most of the sub-themes identified in the results are concerned with motivations underlying the cloud transition, and do not directly impact cybersecurity in procurement. The sub-themes identified in the interviews did not lend themselves for operationalisation in the context of cybersecurity in procurement. However, the choice was made to still include this factor in the survey as measuring hospital attitudes towards cloud solutions and keeping control over their digital ecosystems can prove valuable.

The attitude of hospitals towards cloud solutions affects their adoption, but does not affect cybersecurity directly. Control over and customisability of cloud solutions is part of the reasoning behind its adoption. The trend of suppliers forcing the transition to cloud solutions is similarly related to adoption. The same goes for cost-effectiveness and convenience. The sub-themes that did directly influence cybersecurity in procurement were transference of cybersecurity responsibility to cloud vendors and vendor specialisation, where vendors can allocate more resources towards securing their systems.

By transferring the responsibility for cybersecurity, some hospitals consider their own responsibilities reduced. A significant issue arose in phrasing a statement for responsibility transference, as ”transferring responsibility” might make the respondent feel like the he was being asked if he was hiding from responsibility. This makes denial a morally preferable answer. This can skew the response and should be avoided (Iarossi, 2006). No survey item that accurately reflected the sub-theme without mentioned ”responsibility” or ”transference” was found, resulting in the exclusion of this sub-theme in the survey.

An overview of the survey items for the cloud transition is included in Table 6.5. Two types of answer categories are used. The five-point agreement scale contains the answers ”Strongly disagree”, ”Disagree”, ”Neither agree or disagree”, ”Agree” and ”Strongly agree” and the five-point importance scale contains the answers ”Unimportant”, ”Slightly important”, ”Moderately important”, ”Important” and ”Very important”.

Table 6.5: Survey items for cloud transition (CT)

Sub-themes	Survey items	Answer categories
Hospital attitude	CT1: My hospital prefers on-premises solutions over cloud-based solutions	5-point agreement scale
	CT2: My hospital is more willing to adopt cloud solutions than five years ago	5-point agreement scale
Vendor specialisation	CT3: Cloud solutions help us achieve higher security levels with fewer resources	5-point agreement scale
Forced transition	CT4: Transitions to cloud solutions are forced by suppliers	5-point agreement scale
Adoption	**In a transition to a cloud-based solution, how important is [...]?**	5-point importance scale
Control	CT5: Control (patching access)	
Customisability	CT6: Customisability (ability to adjust the solution to your needs)	
Cost-effectiveness	CT7: Cost-effectiveness	

6.2.8. Conflicting priorities

Conflicting priorities occurred between hospitals and suppliers, and internally at hospitals. These two sub-themes resulted in two additional survey items, included in Table 6.6. An additional item was included about involvement of IT after a purchase had been made, to assess how often they are forced to integrate insecure assets into their systems.

Table 6.6: Survey items for conflicting priorities (CP)

Sub-themes	Survey items
With suppliers	**Please indicate how often you encounter the following notions in purchase processes:**
Occurrence in general	CP1: Conflicting priorities between the hospital and a supplier
Between internal actors	**Please indicate how often you encounter the following notions in purchase processes:**
Occurrence in general	CP2: Conflicting priorities between hospital departments
IT involvement after purchase	CP3: IT personnel being engaged after the purchase process has concluded

7

Conclusions and recommendations

This chapter will discuss the final research outcome. First, the research questions are answered in Section 7.1. In Section 7.2, recommendations are provided to improve the inclusion cybersecurity in procurement in hospitals. The scientific and societal contribution of this research is discussed in Section 7.3, which is followed by a short discussion of implications for cybersecurity policy in hospitals in Section 7.4. The chapter then continues with a discussion of limitations and future research avenues in Section 7.5 and ends with a reflection in Section 7.6.

7.1. Conclusion

7.1.1. Answers to sub-questions

This research aimed to study the role of cybersecurity in hospital procurement processes. In this process, three sub-questions were answered.

SQ1: How can the role of cybersecurity in procurement processes be studied?

To analyse procurement processes, a framework was needed. Because the level of cybersecurity in organisations is the result of complex interactions and because existing decision-making purchase process models did not capture complex interactions in decision-making, a new framework was developed by combining a tactical/operational purchase process model and a complex decision-making framework. The combined framework was able to analyse complex decision-making across procurement processes, providing a novel answer to this sub-question.

SQ2: What are key factors that influence cybersecurity in procurement?

Based on qualitative analysis of interviews with hospital CISOs and healthcare cybersecurity experts using the combined framework, five factors were identified that influence the role of cybersecurity in procurement: supplier-hospital relationship, knowledge exchange and retention, alternative purchase processes, cloud transition and conflicting priorities.

Supplier-hospital relationship

The supplier-hospital relationship is important for the role of cybersecurity in procurement because it defines how these parties can work together to fulfil a hospital's cybersecurity objectives. It defines to what extent hospitals can propose and satisfy cybersecurity requirements during procurement. An imbalance in decision power favouring suppliers makes it difficult for hospitals to pursue their own cybersecurity objectives in negotiations. This imbalance in decision power mainly comes from hospitals being locked in to a supplier, which can be the result of a lack of suppliers or because switching to another supplier has become too costly. In such situations, the risk of losing a customer to competitor is small, reducing the need for competition between them, rendering hospitals unable to leverage competition between suppliers as a tool in selection and negotiations. During negotiations, another important theme is supplier cooperation. This depends on their willingness or ability to cooperate, and on their cybersecurity maturity. Larger suppliers tend to have a choice in cooperation, whereas smaller suppliers are resource-constrained and have to prioritise which aspects of their product they develop first. Hospitals should consider this in negotiations with smaller suppliers to keep their expectations

realistic. A preference for suppliers with an existing relationship with the hospital gives them an advantages over those who do not. Preferred suppliers are subjected to less evaluation than new suppliers, although this primarily goes for smaller purchases, as larger purchases are subjected to more scrutiny. Repeated purchases from one supplier can appear convenient, but can introduce a risk of supplier lock-in over time.

Knowledge exchange and retention
In an effort to even the playing field with regards to decision power during negotiations, hospitals have started exchanging information about suppliers with each other. This information is used to strengthen their position in negotiations, providing them with much-needed decision power and therefore helping them in satisfying their cybersecurity requirements. While this practice has proved useful, it is not common to engage other hospitals in purchases, providing an area for improvement. Aside from supplier information, they also discuss threat information and exchange process information, improving their purchase processes to better integrate cybersecurity requirements. This is complemented with improved knowledge retention, to better learn from past experiences. This can yield benefits in the long term by increasing the grasp hospitals have on purchases and on the inclusion of cybersecurity within those processes.

Alternative purchase processes
Alternative purchase processes are purchases that deviate from the regular procedure. They are motivated by a desire for a simpler purchase process, as the buyer often has a specific product in mind before the process starts. Such purchases tend to skip one or more steps in the procurement process, which can result in the purchase of assets without accounting for cybersecurity requirements. These processes occur mainly for specialised software, as equipment is subject to more stringent regulation. The increased connectivity of hospital systems is making such purchases more visible to IT staff by requiring their involvement to realise a connection with other systems. While this does not directly improve cybersecurity levels, the increased visibility of alternative purchase processes likely improves the ability of actors to include cybersecurity requirements in those purchases.

Cloud transition
The transition to cloud-based solutions forms a separate factor in the procurement process because it is often forced by suppliers and because it is strongly characterised by cost-effectiveness and convenience. These properties make such purchase processes unique. The transition to cloud-based solutions comes from suppliers pushing those products. In the context of cybersecurity, transition to cloud-based solutions involves weighing the control over and customisability of those systems, the extent to which the cybersecurity responsibilities are reduced for the hospital and the ability of the cloud vendor to attain a higher level of cybersecurity than the hospital could otherwise. This boils down to the cost-effectiveness and convenience of such solutions. The downsides of cloud solutions (reduced control and customisability) must be weighed against their convenience (vendor expertise and reduced organisational burden). This consideration may be part of any purchase decision, but in procurement of cloud solutions it characterises the process to a large degree. The effect of the transition to cloud-based solutions on cybersecurity levels in hospitals can be either positive or negative, depending on how the up- and downsides of such a transition play out in practice.

Conflicting priorities
In procurement processes, suppliers have different priorities than hospitals which can create conflict. Conflict is not guaranteed and depends on the view a supplier takes towards its clients and their willingness to cooperate. Internal actors can also have different priorities, which may incentivise exclusion of actors during procurement, hindering their ability to address cybersecurity requirements in the process. Different actors are bound to have conflicting priorities at any given point in time, making this issue unavoidable. Both the pursuit of cybersecurity objectives and patient care continuity are reasonable and likely interests for actors within a hospital, just like the pursuit of business objectives is for a supplier. For urgent security threats, cybersecurity and patient care continuity can even align, as a cybersecurity threat may present a bigger risk to patient care continuity than the potential negative effects of mitigation (for example, system downtime).

Accepting that conflict is likely to happen and perhaps inevitable, the focus should shift towards productive handling of such conflict. Taking the cybersecurity and patient care conflict as an example,

a blind focus on either can have negative outcomes for both. Prioritising cybersecurity objectives can lead to frequent or long downtime due to unexpected incompatibility issues with new patches or through other interactions between digital systems. Such downtime then affects a hospital's ability to provide patient care, posing risk to patients. Prioritising patient care over cybersecurity can leave threats unaddressed, which then pose a risk to patient care (for example, by allowing ransomware to enter a hospital's systems). Conflict can also occur within one actor role. In the example of negotiations between a hospital and a supplier, the hospital may experience internal conflict about their approach to negotiations and the requirements they should set for their suppliers. This highlights another complexity in negotiations, with possibilities for conflict on multiple levels.

Instead of focusing on one priority or the other, a more productive solution considers the optimal outcome for a hospital, which is a combination of the two. This requires mutual understanding and cooperation of the actors involved, and could involve drafting a plan to achieve this outcome over a longer time span.

SQ3: How can a research instrument be made to scale this research in the healthcare sector?
Having identified the key factors that influence the role of cybersecurity in procurement using a small number of interviews, a survey was developed to examine the correlations between and prevalence of these factors within the sector. It addresses the shortcomings associated with the original design of this research, primarily in response numbers. This survey addresses as many of the key factors and their sub-themes as possible and provides a starting point to scale this research in future efforts, adding value on top of the findings in this research.

7.1.2. Answer to the main research question

What is the role of cybersecurity in hospital procurement processes and how can that role be analysed across the sector?

This research started with an examination of the state of cybersecurity in healthcare and how to improve it. In this, a role is reserved for the procurement process, as it represents the introduction of new assets into hospitals' IT ecosystems. The role of cybersecurity in hospital procurement is the result of complex decision-making processes, both within the hospital and between a hospital and its suppliers. It plays a smaller role in alternative purchase processes. Conflicting priorities inside and outside the hospital affect to which extent cybersecurity is included while setting initial requirements, and during evaluation and negotiation. Depending on the cooperation in the supplier-hospital relationship and the extent to which hospitals engage in knowledge exchange and retention, the role of cybersecurity in procurement is improved. In the case of procurement of cloud-based solutions, the outcome for cybersecurity levels is unsure. They can result in degradation or improvement of a hospital's level of cybersecurity, dependent on the final outcome regarding cost-effectiveness and convenience. The convenience of outsourcing cybersecurity policies to a third party may outweigh the costs incurred by moving towards that party's cloud solution. However, moving to a cloud solution reduces the control a hospital can exert over those systems and may require significant integration efforts and result in long-lasting consequences for the hospital IT ecosystem. This research used a small number of interviews to examine how cybersecurity played a part in procurement processes. To analyse this across the sector, a survey was constructed based on the interview result, enabling future research efforts to extend this research and address the shortcomings of the research design.

7.2. Recommendations

Based on the conclusion, the following recommendations are made to improve the role of cybersecurity in procurement:

- **Regulators should protect hospitals from supplier lock-in**
  The effect of supplier lock-in should me minimised by fostering competition. This may not be feasible in the case of highly specialised systems. Regulation should provide hospitals with a better position in negotiations by putting more responsibility for cybersecurity of products at suppliers, and by implementing mechanisms that balance decision power between suppliers and hospitals.
- **Hospitals should perform regular critical evaluation of known suppliers**
  Hospitals rarely evaluate their suppliers for repeated purchases, allowing changes in supplier

performance to go unnoticed. This can be prevented by performing a regular, critical evaluation of the suppliers involved in repeated purchases. Additionally, for every purchase, hospitals should consider if continuing a relationship with a known supplier increases their risk of supplier lock-in emerging.

- **Hospitals should actively request supplier information from other hospitals during procurement**
  Hospitals can improve their position in negotiations relative to suppliers by learning from other hospitals how they achieved cooperation, and by checking if suppliers arguments against cooperation hold true. Group purchasing alliances likely have members who can provide the required supplier information and make a good starting point to request this information from.

- **Hospitals should actively engage in process information exchange with other hospitals to improve dissemination of best practices**
  Hospitals are still adapting their processes to better integrate cybersecurity requirements. To avoid reinventing the wheel, hospitals should look to each other to identify best practices and implement those. The added benefit of this approach over redesigning processes by yourself is that these best practices are already tailored to the unique complex and resource-constrained environment of hospitals. A separate role is also reserved for academia to objectively identify best practices.

- **Hospitals should improve inclusion of cybersecurity requirements in alternative purchase processes**
  Alternative purchase processes introduce cybersecurity threats into the hospital IT ecosystem, but increased connectivity of modern systems is improving the visibility of these purchases to IT departments. The inclusion of cybersecurity requirements in these processes should therefore rest with them, as they indirectly gain more decision power from this development. Additionally, hospitals may choose to acknowledge and support the existence of alternative purchase processes and leverage their efficiency over regular purchase processes. By using the proverbial carrot instead of a stick, requesting parties may become more open to inclusion of a small number of cybersecurity requirements, which is an improvement over the default alternative purchase process where none are included.

- **Clearly state priorities of all actors involved in procurement processes**
  Priorities can vary between hospitals and suppliers and between internal actors within hospitals. Hospitals should dedicate time in procurement processes to identifying these priorities and any potential resulting conflicts. Through early identification of potential priority conflicts, any resulting issues during negotiations and contract supervision can be preempted. Resolving these conflicts can streamline the procurement process, benefiting all involved actors.

7.3. Scientific and societal contribution

The scientific relevance of this research stems from the novel view of decision-making in procurement. This view is new because it captures complex interactions instead of discrete choices. This approach allows for a new take of decision-making in procurement and emphasises that such a process perhaps should not be modelled in discrete choices within hospitals. Additionally, the ENISA purchase process model was tuned to hospital procurement. The most noticeable change was the merging of evaluation and negotiations, which turned out to be practically inseparable. Another important change was returning the signature moment as a transition in the process, downgrading it from a process step. While signing serves as an important transition from the pre-purchase to post-purchase process, the step itself is insignificant in terms of interactions that belong to it. The last important scientific addition is current snapshot of the state of cybersecurity in hospital procurement. Key factors and sub-themes were identified, but the extent of these effects remains unknown. The scientific value of this research will grow as the survey is used to supplement the results to establish the magnitude of these effects.

The societal relevance of this research stems from a better understanding of decision-making in procurement and how that affects cybersecurity levels. Acknowledging that cybersecurity levels in organisations are the result of interactions instead of 'simple' decisions can help hospitals understand why their cybersecurity landscapes look the way they do. The importance of relationships with suppliers

was demonstrated both through a factor dedicated to it, and tangentially in the related factors knowledge exchange and retention, conflicting priorities and cloud transition.

7.4. Implications for hospitals

Regulation and market demand have resulted in suppliers developing their cybersecurity capabilities. As these capabilities grow, understanding of cybersecurity issues between suppliers and hospitals is likely to grow with it and hospitals may find it easier to secure their systems. However, the downside of suppliers improving their product's cybersecurity features is that each supplier can end up with their own solution, resulting in the reduced customisability of their systems. Systems that are less customisable than others are harder to integrate into a hospital's digital ecosystem. In this development, a role is reserved for knowledge exchange about supplier cooperation, which can help hospitals assess how flexible a supplier can be in tailoring a product to their organisation.

Another important implication for hospitals from this research is the transition from supplier preference to supplier lock-in. Supplier preference can make for easier purchases in the short term, but blind reliance on a single supplier for certain systems can eventually result in dependence. Evidence of such preferences was found in this and other research. The root causes for supplier lock-in (lack of suppliers and high switching costs) remain present. This means new cases of supplier lock-in are likely to emerge in the future and hospitals should prepare to deal with them. One means of doing so is periodical evaluation of known or preferred suppliers, which should include an assessment of the risk of supplier lock-in occurring.

This research also has implications for the current efforts for improving cybersecurity levels that suppliers and hospitals have. Current efforts focus on designing secure products (suppliers) or securing systems after deployment (hospitals). While there is not always room for cybersecurity considerations in procurement, this research did show room for improvement and underlines the value of procurement in ongoing cybersecurity improvement efforts. If hospitals become more selective, products with poor cybersecurity performance may automatically lose out to competitors.

The increasing need for more secure systems creates new challenges for hospitals and suppliers and both are struggling to cope with these. The aspiration for higher levels of cybersecurity has led to various forms of resistance and conflict. Significant barriers exist in the technological, organisational and human domains but signs of cooperation and coping can be observed, showing promise for cybersecurity of patients and hospitals going forward.

7.5. Limitations and future research

Several limitations to this research were covered in Section 1.6. As this research is a master thesis, the author was inexperienced in the research field and with the research methods. Coupled with the time constraint, it is likely that the quality of the results was negatively affected to some degree.

During the interview analysis, the process model used in the theoretical framework showed inconsistencies with the mental model provided by interviewees. While the framework served its purpose in this research, several improvements should be made, were it used in future research. A reflection on this is provided in Section 7.6.

The use of interviews with hospital personnel makes it possible to gather tacit knowledge about the research subject. However, this approach introduced additional limitations in this research. While a researcher aims for an objective truth, qualitative research is always subjective to a degree, as it relies on the experience of the researcher and their personal observations. The changed interview protocol demonstrates this influence. Additionally, the results provide a snapshot of the current state cybersecurity in hospitals. This state is in flux and therefore the results of this research depend on when they are are gathered. A similar study in the future may reach different conclusions. The geographic limitation to Dutch hospitals may have further impact on the results, as cultural and regulatory differences may affect both cybersecurity levels and procurement processes.

It was not possible to interview every CISO in Dutch hospitals. Since only a small number of interviews was conducted, this study could have benefited from more data. Additionally, the interviewee group consisted of hospital CISOs or similar roles and healthcare cybersecurity experts.

7.5.1. Future research

The survey developed in Chapter 6 is the first avenue for future research and can be used to scale this research to more hospitals. Additionally, future research could extend the geographical scope beyond the Netherlands, but would have to account for cultural and regulatory differences. Another avenue to pursue lies in the cloud transition, as this research uncovered several considerations unique to cloud solution procurement (e.g. vendor specialisation and customisation). Future research should scope specifically on procurement of cloud solutions, as this presents unique challenges to improving cybersecurity. Other avenues for future research include the determination of the optimal frequency for critical supplier evaluation, continued identification of best practices in the purchase process of hospitals, and improving our understanding of the motivations behind alternative purchase processes and how to stop these from occurring.

7.6. Reflection

7.6.1. Reflection on the theoretical framework

ENISA process model

The ENISA process model was selected for its relevance to both hospitals, cybersecurity and procurement. However, throughout this research, several suggestions for improvement of the process model were revealed.

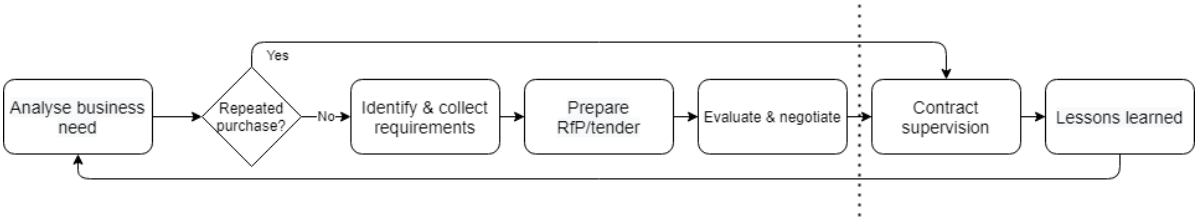

Figure 7.1: Revised ENISA procurement process model

One improvement to the ENISA process model can be made in the evaluation and negotiation steps. Because cybersecurity requirements are targeted at risk mitigation and risk mitigation can often be achieved in multiple ways, these requirements are flexible and therefore subject to negotiation. Depending on the outcome of these negotiations, a proposal may become more or less attractive. The negotiations are thus part of evaluation, and in the context of cybersecurity should not be regarded as separate procurement steps.

A second, smaller improvement would be the removal of contract signing as a separate step. Even though in practice it is an important transition from the sourcing to supply phases, for the purposes of this research the step contains no meaningful cybersecurity-related actions.

There is a strong connection between the kind of purchase and the execution of the first four process steps (analysing business need, identifying and collecting requirements, preparing the RfP and evaluating proposals). If the business need is replacement of an existing system, then the requirements for that system are not collected as the new system's requirements are simply to match the functionality of the old one. For replacement with an identical system, this will pose no additional cybersecurity risk. For replacement with a newer system, the cybersecurity properties of that new system may differ from the old one, which would warrant a closer look at the otherwise expedited replacement purchase process. The evaluation step is also simplified by the expedited selection of a known or preferred supplier, most likely the supplier of the previous system. This makes this part of the process less elaborate, speeding it up considerably at the cost of potential cybersecurity risk increase.

A final note should be made of the cyclical nature of the ENISA process model. Ongoing efforts for knowledge retention in the procurement process point towards an increasingly cyclical nature. However, as product-supplier proposals only pass the stringent purchase process once, to then make use of the expedited replacement purchase process. This points to a hybrid purchase process model, which is linear for new entrants but is cyclical with the simplified repeat purchase steps included.

Based on these findings, an improved procurement process model is provided in Figure 7.1.

Complex decision-making framework

The complex decision-making framework was selected because traditional decision-making process models did not allow for complex interaction between actors and and their surroundings. While the traditional models do clarify the choices an actor makes during the procurement process, the story captured in the interviews turned out to be more complex than a set of dichotomous decisions. The complex decision-making perspective highlighted changes in motivation and attitude, and has turned out a good fit for the analysis of hospital procurement processes.

In Chapter 3, the focus in this framework was put on the actor-oriented explanations, which is why the structural conditions were deliberately underrepresented in the original interview protocol. Regardless, the interviews yielded a richer picture of the structural conditions than the literature review provided, even without the original intent to elicit that information. It is evident that the initial focus on actor-oriented explanations was therefore incorrect.

Combined framework
The combined framework posed the structural conditions as constant during a procurement process. The structural conditions of market and regulation have changed over time and this influence is important to consider, but for the time span of a procurement process, they do not change. It is therefore not necessary to separate these conditions per process step.

7.6.2. Personal reflection

My original choice for the CoSEM I&C program came from a longstanding interest in technology and digital systems. Regardless of this interest, I had little prior knowledge in the cybersecurity field. Studying this topic proved a big challenge, as it is a large and active research field with many different avenues to explore.

Regarding the research design itself, I understood there were two kinds of theses: the ones where you do something you're good at and leverage that, and the ones where you learn entirely new skills. The original plan was to do the former, but as the research plan pivoted over time, I found myself doing a thesis that belonged to the latter category. This was an important learning opportunity, as I had almost no experience with interviewing and coding processes. Those skills have improved over the course of this thesis and are not perfect, but having concluded this research, I am better prepared for future interviews and analysing them, which will prove a useful experience for future research efforts.

References

Abraham, C., Chatterjee, D., & Sims, R. R. (2019, jul). Muddling through cybersecurity: Insights from the u.s. healthcare industry. *Business Horizons*, *62*(4), 539–548. doi: 10.1016/j.bushor.2019.03.010

Adriano, L. (2020, February). *Citrix says hackers were inside its networks for nearly five months.* Retrieved 2020-20-30, from https://www.insurancebusinessmag.com/us/news/cyber/citrix-says-hackers-were-inside-its-networks-for-nearly-five-months-214333.aspx

Åge, L.-J. (2011). Business manoeuvring: a model of b2b selling processes. *Management Decision*, *49*(9), 1574–1591. doi: 10.1108/00251741111173998

Angst, C. M., , Block, E. S., D'Arcy, J., Kelley, K., , & and. (2017). When do IT security investments matter? accounting for the influence of institutional factors in the context of healthcare data breaches. *MIS Quarterly*, *41*(3), 893–916. doi: 10.25300/misq/2017/41.3.10

Ani, U. P. D., He, H. M., & Tiwari, A. (2016). Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. *Journal of Cyber Security Technology*, *1*(1), 32–74. doi: 10.1080/23742917.2016.1252211

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., … Flahault, A. (2020). Cybersecurity of hospitals: discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making*, *20*(1). doi: 10.1186/s12911-020-01161-7

Benaroch, M. (2020). Cybersecurity risk in it outsourcing—challenges and emerging realities. In *Information systems outsourcing* (pp. 313–334). Springer.

Bruijn. (2008). *Management in networks : on multi-actor decision making*. London New York: Routledge.

Bäckstrand, J., Suurmond, R., van Raaij, E., & Chen, C. (2019). Purchasing process models: Inspiration for teaching purchasing and supply management. *Journal of Purchasing and Supply Management*, *25*(5), 100577. doi: 10.1016/j.pursup.2019.100577

Connolly, B. (2018, July). *Medical data more valuable to hackers than credit information.* Retrieved from https://www.cio.com/article/3499405/medical-data-more-valuable-to-hackers-than-credit-information.html

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, *113*, 48–52. doi: 10.1016/j.maturitas.2018.04.008

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10), 17.

Davis, J. (2019, July). *Data Breaches Cost Healthcare $6.5M, or $429 Per Patient Record.* Retrieved 2021-01-25, from https://healthitsecurity.com/news/data-breaches-cost-healthcare-6.5m-or-429-per-patient-record

de Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1–7. doi: 10.1016/j.giq.2017.02.007

Decarolis, F., & Giorgiantonio, C. (2015). Public procurement of healthcare in europe: The case of medical devices. *Rivista di Politica Economica*, *104*, 4.

de Carvalho, R. S., & Saleem, D. (2019). Recommended functionalities for improving cybersecurity of distributed energy resources. In (Vol. 1, pp. 226–231). IEEE. doi: 10.1109/RWS47064.2019.8972000

Dedeke, A. (2017). Cybersecurity framework adoption: using capability levels for implementation tiers and profiles. *IEEE Security & Privacy*, *15*(5), 47–54. doi: 10.1109/MSP.2017.3681063

Dockery, M., Beal, C., & Howell, P. (2015, June). *Defending against cyberattacks.* Published via: https://nchica.org/wp-content/uploads/2015/06/Dockery-Beal-Howell.pdf. (Presentation of the 2015 Privacy and Security Conference)

Drougkas, A., Liveri, D., Zisi, A., & Kyranoudi, P. (2020, February). *Procurement guidelines for cybersecurity in hospitals* (Tech. Rep.). European Union Agency for Cybersecurity (ENISA). doi: 10.2824/943961

European Commission. (n.d.). *Public procurement.* Retrieved 2020-11-09, from https://ec.europa.eu/growth/single-market/public-procurement_en

European Commission. (2018). *Topic: Raising awareness and developing training schemes on cybersecurity in hospitals.* Retrieved 2020-11-02, from https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/su-tds-03-2018

Farrell, J., & Klemperer, P. (2007). Coordination and Lock-In: Competition with Switching Costs and Network Effects. In *Handbook of industrial organization* (Vol. 3, p. 1967-2072). doi: 10.1016/s1573-448x(06)03031-7

Fast, N. J., Sivanathan, N., Mayer, N. D., & Galinsky, A. D. (2012). Power and overconfident decision-making. *Organizational Behavior and Human Decision Processes*, *117*(2), 249–260. doi: 10.1016/j.obhdp.2011.11.009

FDA. (2020, March). *Cybersecurity.* Retrieved 2021-01-25, from https://www.fda.gov/medical-devices/digital-health/cybersecurity#guidance

Filkins, B. (2014, February). *SANS health care cyberthreat report: widespread compromises detected, compliance nightmare on horizon.* Available at https://www.redwoodmednet.org/projects/events/20150731/docs/Norse-SANS-Healthcare-Cyberthreat-Report2014.pdf.

Fischer, E. A. (2016, August). *Cybersecurity issues and challenges: In brief.* Congressional Research Service.

Ghafur, S., Grass, E., Jennings, N. A., & Darzi, A. (2019). The challenges of cybersecurity in health care: the uk national health service as a case study. *The Lancet Digital Health*, *1*(1), e10–e12. doi: https://doi.org/10.1016/S2589-7500(19)30005-6

Gibson, J. L., Martin, D. K., & Singer, P. A. (2005). Priority setting in hospitals: Fairness, inclusiveness, and the problem of institutional power differences. *Social Science & Medicine*, *61*(11), 2355–2362. doi: 10.1016/j.socscimed.2005.04.037

Goff, E., Glantz, C., & Massello, R. (2014). Cybersecurity procurement language for energy delivery systems. In *Proceedings of the 9th annual cyber and information security research conference on - CISR '14.* ACM Press. doi: 10.1145/2602087.2602097

Gordon, L. (2007). *Incentives for improving cybersecurity in the private sector: A cost-benefit perspective.* (Testimony for the House Committee on Homeland Security's Subcommittee onEmerging Threats, Cybersecurity, and Science and Technology)

Groves, R. M., Fowler Jr, F. J., Couper, M. P., Lepkowski, J. M., Singer, E., & Tourangeau, R. (2009). *Survey Methodology* (Vol. 561). John Wiley & Sons.

Guest, G., Namey, E., & Chen, M. (2020). A simple method to assess and report thematic saturation in qualitative research. *PLOS ONE*, *15*(5), e0232076. doi: 10.1371/journal.pone.0232076

Guimarâes, C. M., & de Carvalho, J. C. (2011). Outsourcing in the healthcare sector-a state-of-the-art review. *Supply Chain Forum: An International Journal*, *12*(2), 140–148. doi: 10.1080/16258312.2011.11517267

Halvorsrud, R., Kvale, K., & Følstad, A. (2016). Improving service quality through customer journey analysis. *Journal of Service Theory and Practice*, *26*(6), 840–867. doi: 10.1108/jstp-05-2015-0111

Hansson, L., & Holmgren, J. (2011). Bypassing public procurement regulation: A study of rationality in local decisionmaking. *Regulation & Governance*, *5*(3), 368–385. doi: 10.1111/j.1748-5991.2011.01110.x

Health Care Industry Cybersecurity Task Force. (2017). *Report on improving cybersecurity in the health care industry* (Tech. Rep.). Retrieved from https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf

HIMSS Analytics. (2013, May). *Hospital decision makers study.* Retrieved from https://www.thinkwithgoogle.com/_qs/documents/1450/how-hospital-administrators-make-purchase-decisions_research-studies.pdf

Iarossi, G. (2006). *The power of survey design : a user's guide for managing surveys, interpreting results, and influencing respondents*. Washington, D.C: World Bank.

Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in hospitals: A systematic, organizational perspective. *Journal of Medical Internet Research*, *20*(5), e10059. doi: 10.2196/10059

Jansen, J., & Corley, K. (2007). E-survey methodology. In *Handbook of research on electronic surveys and measurements* (pp. 1–8). IGI Global. doi: 10.4018/978-1-59140-792-8.ch001

Kirk, J. (2012, October). *Pacemaker hack can deliver deadly 830-volt jolt.* Retrieved from https://www.computerworld.com/article/2492453/pacemaker-hack-can-deliver-deadly-830-volt-jolt.html

Kirlappos, I., Parkin, S., & Sasse, M. A. (2014). Learning from "shadow security:" why understanding non-compliant behaviors provides the basis for effective security. In *Proceedings of the 10th symposium on usable privacy and security (soups 2014).* Internet Society. doi: 10.14722/usec.2014.23007

Kumar, S., Biswas, B., Bhatia, M. S., & Dora, M. (2020). Antecedents for enhanced level of cybersecurity in organisations. *Journal of Enterprise Information Management*, *ahead-of-print*(ahead-of-print). doi: 10.1108/jeim-06-2020-0240

Kushniruk, A., Beuscart-Zéphir, M.-C., Watbled, Ludivine, A. G. E. B., & Kannry, J. (2010). Increasing the safety of healthcare information systems through improved procurement: toward a framework for selection of safe healthcare systems. *Healthcare Quarterly*, *13*, 53–58.

Laffont, J.-J., & Tirole, J. (1993). *A theory of incentives in procurement and regulation*. MIT press.

Langer, L., Skopik, F., Smith, P., & Kammerstetter, M. (2016). From old to new: Assessing cybersecurity risks for an evolving smart grid. *Computers & Security*, *62*, 165–176. doi: 10.1016/j.cose.2016.07.008

Laybats, C., & Tredinnick, L. (2016). Information security. *Business Information Review*, *33*(2), 76–80. doi: 10.1177/0266382116653061

Lorence, D. P., & Spink, A. (2004). Healthcare information systems outsourcing. *International Journal of Information Management*, *24*(2), 131–145. doi: 10.1016/j.ijinfomgt.2003.12.011

Low, C., & Chen, Y. H. (2012). Criteria for the evaluation of a cloud-based hospital information system outsourcing provider. *Journal of Medical Systems*, *36*(6), 3543–3553. doi: 10.1007/s10916-012-9829-z

Malatji, M., Marnewick, A., & von Solms, S. (2020). Validation of a socio-technical management process for optimising cybersecurity practices. *Computers & Security*, *95*, 101846. doi: 10.1016/j.cose.2020.101846

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: how safe are we? *British Medical Journal*, j3179. doi: 10.1136/bmj.j3179

McLeod, A., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems*, *108*, 57–68. doi: 10.1016/j.dss.2018.02.007

Meeuwisse, K. (2016). *The usability-security tradeoff* (Tech. Rep.). Delft University of Technology. (Available at https://repository.tudelft.nl/islandora/object/uuid%3A6eafeb06-cb6e-4d0e-898c-4af3ca1045ce)

Mohurle, S., & Patil, M. (2017). A brief study of wannacry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science*, *8*(5). doi: 10.26483/IJARCS.V8I5.4021

Moore, T. (2010). The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection*, *3*(3-4), 103–117. doi: 10.1016/j.ijcip.2010.10.002

Nollet, J., & Beaulieu, M. (2003). The development of group purchasing: an empirical study in the healthcare sector. *Journal of Purchasing and Supply Management*, *9*(1), 3–10. doi: 10.1016/s0969-7012(02)00034-5

Nyhlén, J., & Lidén, G. (2013). Methods for analyzing decision-making: a framework approach. *Quality & Quantity*, *48*(5), 2523–2535. doi: 10.1007/s11135-013-9905-6

Persistence Market Research. (2016, November). *Global Market Study on Cardiac Pacemakers.* Retrieved from https://www.persistencemarketresearch.com/market-research/cardiac-pacemaker-market.asp

Pfeffer, J., Aamurusko, A., Szász, M., & Duque, R. (1981). *Understanding the role of power in decision-making.* Retrieved from https://www.researchgate.net/profile/Jeffrey_Pfeffer/publication/265142760_Understanding_the_role_of_Power_in_Decision_Making/links/56cbb52b08ae96cdd06fd535/Understanding-the-role-of-Power-in-Decision-Making.pdf

Ransford, B., Kramer, D. B., Kune, D. F., de Medeiros, J. A., Yan, C., Xu, W., … Fu, K. (2017). Cybersecurity and medical devices: A practical guide for cardiac electrophysiologists. *Pacing and Clinical Electrophysiology*, *40*(8), 913–917. doi: 10.1111/pace.13102

RIVM. (n.d.). *Ziekenhuislocaties en buitenpoliklinieken.* Retrieved 2020-12-17, from https://www.volksgezondheidenzorg.info/onderwerp/ziekenhuiszorg/regionaal-internationaal/locaties#methoden

Saldaña, J. (2016). *The coding manual for qualitative researchers*. Los Angeles, California London: SAGE.

Schwartz, S., Ross, A., Carmody, S., Chase, P., Coley, S. C., Connolly, J., … Zuk, M. (2018). The evolving state of medical device cybersecurity. *Biomedical Instrumentation & Technology*, *52*(2), 103–111. doi: 10.2345/0899-8205-52.2.103

Stewart, C. (2019, August). *Hospitals in the netherlands 2005-2017.* Retrieved from https://www.statista.com/statistics/949593/hospitals-in-the-netherlands/

Umbach, P. D. (2005). Getting back to the basics of survey research. *New Directions for Institutional Research*, *2005*(127), 91–100. doi: 10.1002/ir.157

Uwizeyemungu, S., Poba-Nzaou, P., & Cantinotti, M. (2019). European hospitals' transition toward fully electronic-based systems: Do information technology security and privacy practices follow? *Journal of Medical Internet Research*, *7*(1), e11211. doi: 10.2196/11211

Vagias, W. M. (2006). *Likert-type scale response anchors.* Clemson International Institute for Tourism Research Development, Department of Parks, Recreation and Tourism Management. Clemson University.

van Heeswijk, J. (n.d.). *Wat is het verschil tussen de NEN 7510 en de ISO 27001?* Retrieved from https://www.certificering-keuring.nl/wat-is-het-verschil-tussen-de-nen7510-en-de-iso27001

Van Weele, A. J. (2009). *Purchasing and supply chain management: Analysis, strategy, planning and practice*. Cengage Learning EMEA.

Walker, E. W., & Petty, I., J William. (1978). Financial differences between large and small firms. *Financial Management (pre-1986)*, *7*(4), 61.

Williams, P., & Woodward, A. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *Medical Devices: Evidence and Research*, 305. doi: 10.2147/mder.s50048

A

Interview protocol

Before the interview
Interview subject receives the Informed Consent Form up front per e-mail and is asked to return it signed, or agree to its contents per e-mail or verbally at the start of the interview.

Introduction

- Thank you for your time today
- I will now start the recording of this interview. Please let me know if at any point you wish for me to turn off the recorder or keep something you said off the record.
- If consent form not yet signed: Before I can start with the rest of the interview, I need to obtain your consent to process the information I'm gathering today. Have you read the consent form?
- (If no)
  - Do you understand the information provided on the consent form I sent you?
  - Do you have any questions resulting from that form?
  - Do you consent to participate in this study, under the knowledge that you may refuse to answer a question at any time, without providing a reason?
  - Do you understand that the information you provide will be used in research that is to be made public?
  - Do you understand that your personal information will not be shared beyond me and my supervisor?
  - Do you agree that your information may be anonymously quoted in my research?
  - Do you give permission to have the anonymised interview transcript archived in 4TU.ResearchData so it can be used for future research and learning?
- (If yes)
  - Do you consent with me processing this interview as described in the consent form?
- If consent form signed: thank you for signing the consent form. For the record, consent was obtained [by e-mail / verbally / by signing the consent form provided].
- This interview will take about 30 minutes.

Background
I'd like to start with some questions to establish your background on the subject, and then continue on to the main body of the interview.

- What is your function or position at your organisation?

- Could you elaborate on your daily responsibilities?
- What is your experience with procurement in hospitals?
- What is your experience with cybersecurity in hospitals?

Main body

I'd like you to describe a typical procurement process, or otherwise describe a recent one you were involved in.

- Analyse business needs
  - Who decide to start a new purchase?
  - What are the reasons for starting a new purchase?
  - Are purchases sometimes motivated by external forces, and if yes, how?
- Identify and collect requirements
  - Who are involved in setting the requirements for new purchases?
  - Which organisational roles are involved in setting procurement requirements?
  - How do they affect the set of requirements?
  - How are requirements gathered for a purchase?
  - What kind of requirements are these?
- Prepare RfP/Tender
  - How many offers do you typically get for a purchase?
- Evaluate proposals
  - Who evaluate these proposals?
  - What are their interests in selecting a proposal?
  - How are different proposals evaluated?
- Negotiate and award
  - Who can block or promote a final decision?
  - Who has the final say on selecting a supplier?
- Signature of the contract
  - Who is responsible for the contract?
- Contract supervision
  - Who is responsible for evaluating contract performance?
  - Is there an evaluation process for contracts?
  - If yes, could you explain this process?
- Lessons learned
  - How do previous experiences inform supplier selection in future contracts?
  - How do previous experiences inform setting requirements in the future?

Cloud services

- Services like EMR, drug databases, laboratory information systems are sometimes outsourced to a cloud-based provider. Can you name such a cloud-based system in your organisation?
- What drives the decision to outsource to a cloud-based provider instead of running it in-house?

- How does the procurement process for a cloud service differ from other purchases?
- Who is responsible for cybersecurity of such a cloud-based system?

Closing

- Before we conclude this part of the interview, is there something else that you think influences the hospital procurement process that we have not yet had a chance to discuss?

That concludes the main body of questions. I'll be conducting multiple interviews about the adoption of cybersecurity practices in hospital procurement processes. Once this interview has been processed, I will send you a summary of my findings so you can verify the accuracy of the information. If you're interested, I can send you a summary of all my findings which could prove useful to your organisation.

- Would you like me so send you a summary of my findings? [Y/N]

Recap

- I will send you a summary of findings from this interview once all interviews have been processed.
- I will send you a summary of all my findings as well.
- I would like to thank you for your time and contribution today.

[Send thank-you e-mail to interview subject for participation]

B

Interview transcripts

This appendix contains all the interview transcripts and notes. Before each transcript, the designations for interviewer and interviewee are explained. The interviews were anonymised during the transcription process and interviewees were given the opportunity to make changes to the transcripts. The contents of square brackets in the transcripts represent three things:

- A substitution for information that could be used to identify the interviewee or the interviewee's organisation.
- A clarification of what adjectives referred to (for example, "they" might have been replaced by "suppliers").
- Other content that interviewees wanted to leave out.

B.1. Transcript 1

Researcher designated "R", interviewee designated "I".
R: Vooraf even wat formaliteiten, u heeft het [consent] formulier toegezonden gekregen, en bent het eens dat ik het interview verwerk zoals beschreven in het formulier?
I: Ik ben akkoord met wat er op het formulier staat.
R: Ja, okee. Tot zover toestemming. Dan, orde van de dag: dit interview zal dus, ik heb gemikt dat het max 45 minuten duurt. Ik denk dat het wat korter is, aangezien we één onderdeel niet behandelen. Dus we gaan het vooral hebben over inkoopprocessen bij ziekenhuizen. Voordat ik daarmee echter begin, zou ik graag wat achtergrond informatie van u willen hebben. Kunt u wat vertellen over uw functie en uw ervaring met inkoopprocessen in ziekenhuizen?
I: Ja, dat kan. Mijn huidige functieomschrijving is Manager CIO Office & PMO. CIO Office richt zich op architectuurvraagstukken, lange termijn en de projectkant heeft vooral te maken met change portfolio binnen die organisatie. Dat is mijn huidige rol, hiervoor heb ik diverse andere functies gehad, niet alleen bij dit ziekenhuis maar ook bij andere ziekenhuizen, als eindverantwoordelijke voor ICT. Een belangrijk onderdeel van die verantwoordelijkheid is ook de aanschaf van diverse activiteiten en uiteindelijk daarmee ook de processen rondom inkoop. Is dit voldoende?
R: Ja dat is prima, dat voldoet. Tot zover dan de korte achtergrond. Ik wilde het dus gaan hebben over inkoop in ziekenhuizen. Ik probeer eigenlijk een beeld te vormen van hoe dat proces verloopt. Wie zijn er wanneer mee gemoeid en hoe beïnvloeden zij dan dat proces? Mijn onderzoek gaat vooral over cybersecurity dus heeft u toevallig een voorbeeld van een inkoopproces waar u zelf mee te maken had, waarbij cybersecurity ook een rol speelde? Zo niet, heeft u dan een ander voorbeeld?
I: In principe is het zo dat investeringen die gedaan moeten worden van ICT langs mij lopen. Dus ik zie al die investeringen langskomen en vervolgens ben ik bezig geweest sinds ik binnen ben bij [mijn organisatie] met het verbeteren van dat proces rondom inkoop en control. Een voorbeeld specifiek? We hebben heel veel gedaan, We hebben een aanschaf van een netwerk gedaan. Ik ben nu bezig, misschien wat praktischer, met de aanschaf van een portfoliomanagementtooling. En een van de belangrijkste stappen daarin is de rol van Inkoop die we daarin meenemen omdat zij ook niet alleen de

onderhandelingen doen, maar ook regie hebben of nemen over alle activiteiten die samenhangen met het contractueel aangaan van zaken die horen bij het ziekenhuis.
R: Okee. U gaf een voorbeeld net, de aanschaf van een netwerk noemde u iets. Kunt u daar wat meer over vertellen?
I: Ja nou kijk, als je kijkt naar het netwerk, dat is een vrij grote component. Dat gaat om enorm veel geld en ook een lange duur. En daarin speelt Inkoop natuurlijk ook een rol, omdat het met name gaat over strategisch partnerschap aan de ene kant, waarbij je soms af wil wijken omdat een leverancier sterker of beter is dan de strategische partner. Dit kan ook te maken hebben met onderhandelingen rondom kosten. Dat zijn allemaal aspecten die via Inkoop verlopen. Daarnaast hebben wij nog gemeend om, helemaal zelfzinnig, ook nog een externe partij te vragen om een review te doen van de aanschaf van dat netwerk vanuit het perspectief van kwaliteitscontrole, en om die adviezen ook mee te wegen.
R: Dat is dan nadat het al aangeschaft is, bedoelt u?
I: Uhm, nee, een stap daarvoor. Het was onderdeel van het hele aanschafproces.
R: Okee, dus in die zin is dat een stukje evaluatie het voorstel.
I: Ja, dus eigenlijk voordat je daar naar Inkoop gaat, zorg je eerst voor het.. Goed zorgen dat de informatie die je gaat aanleveren al concreet is.
R: Dat is dus een externe partij?
I: Dat is een externe partij ja.
R: Is dat iets wat vaker gebeurt, of is dat alleen voor grotere aanschaffen?
I: Alleen voor grotere.
R: Alleen voor grote, begrepen.
I: Ja, dit ging om een aanschaf van [een groot bedrag]. Bij dat soort bedragen vinden we het wel goed om toch nog eventjes te laten kijken door een andere partij, of dat wat we doen wel goed is.
R: En dat is iets wat formeel ook vereist wordt, zo'n partij erbij roepen, of is dat meer voor de eigen verantwoording?
I: Ja dat is nieuw bedacht. De CIO die binnen is, is nieuw. Die is nog geen jaar hier, en dit soort ontwikkelingen komen wel van buitenaf want binnen de zorg is niet vanzelfsprekend, in mijn beeld.
R: En wat voor terugkoppeling ontvangt u dan van zo'n organisatie?
I: Eigenlijk een adviesdocument op basis van het plan wat we zelf gemaakt hebben, met daarin een advies van hoe zij er tegenaan kijken. Wat ze goed vinden, en wat beter zou moeten. Dat neem je dan mee in je plan om het beter te krijgen. Dekt dat de lading voor jou?
R: Jawel. Ik zit persoonlijk met mijn onderzoek nog wat dichter bij het ziekenhuis, maar ik ben even aan het kijken. Er zit wel nuttige informatie hier. Als je dus zo'n aankoop voorbereidt, dan ga je van een reeks eisen uit.
I: Ja.
R: Wie zijn er allemaal betrokken bij het opstellen van die eisen, en kunt u mij vertellen hoe dat proces gaat?
I: Dat verloopt eigenlijk wel via Inkoop. Inkoop heeft van diverse afdelingen die relatie hebben met dat wat aangeschaft wordt, een soort vragenlijst. Inkoop zit ook echt in de regie als het gaat over dat al die lijsten, al die informatie die nodig is, ook wordt afgevinkt. Dat is ook goed, die regiefunctie. Zij kunnen ook goed beoordelen of er genoeg naar alternatieven is gekeken, of partijen kredietwaardig zijn, de ervaringen die bij andere ziekenhuizen worden opgehaald. Er zijn diverse aspecten die zij meenemen in de beoordeling.
R: Dat is wel een onderdeel waar ik naar wil kijken, wat komt er dan bij die evaluatie kijken. U noemde kredietwaardigheid ook wel. Wat zijn nog andere criteria die belangrijk zijn in dat proces?
I: Bijvoorbeeld IT-requirements, dus wat, als je iets nodig hebt aan de IT-kant, voldoet dat dan aan dat wat ze hebben vastgelegd? Betreft het een medisch component, een medisch apparaat, dan doen ze feitelijk hetzelfde alleen dan heet het niet alleen IT maar dan is het ook alle aspecten die nodig zijn voor het medische apparaat op die afdeling. Financieel kader wordt getoetst. "Is er ruimte voor investering" is een belangrijke daarin. Er wordt ook gekeken of zo'n contract ook goed dichtzit. Als het gaat over een samenwerkingsovereenkomst, als het een SaaS-partij betreft, of.. Ze betrekken ook de SLM, service-level management erbij als het gaat over een SLA [service level agreement]. Dus ze hebben daar echt een regierol in, voor het goed zorgen dat alle partijen goed aangehaakt zijn, om dit te realiseren.
R: U zei dat die evaluatie werd gedaan door een externe partij. Dan neem ik aan dat het gaat om meerdere voorstellen die geëvalueerd worden.

I: Uhm, ja... Maar dat met die externe partij, dat is niet een doel op zich. De externe partij was in huis om te kijken of het proces om te komen tot een keuze voor de werkleverancier en netwerkcomponenten, of dat de goede weg is geweest. Dus dat is vooraf geweest voordat we bij Inkoop zijn terechtgekomen.
R: Nog daarvoor?
I: Ja.
R: Dan wil ik graag nog wel even het voorbeeld nemen van de aankoop van een medisch apparaat. Als we het hebben over, laten we een MRI-machine pakken. Zo een aankoopproces, worden dan echt verschillende partijen overwogen, of is dat meer één partij waarmee een dialoog wordt aangegaan? Hoe werkt dat?
I: Dat is niet per definitie meer dan één partij. Vaak is een leverancier al een soort huisleverancier, waarbij een apparaat gewoon vervangen wordt omdat de levensduur ten einde is. Als het gaat om vervanging, dan wordt er meestal niet veel verder gekeken en wordt dezelfde leverancier benaderd. Betreft het echt een uitbreiding of een vernieuwing, dan wordt nog wel eens naar de hele markt gekeken. Dat zijn op dit moment de meest gangbare types. En, zo, die worden aangeschreven. En het gaat ook eigenlijk via een Request for Proposal, waarin eigenlijk al die elementen die belangrijk zijn voor die afdeling worden meegewogen.
R: Dus vanuit de afdeling zelf is daar ook veel input in?
I: Ja, maar Inkoop begeleidt wel dat traject. Dus die heeft al wel van tevoren bij elke component wat ze al een keer eerder hebben aangeschaft een soort van aanschafdossier. Feitelijk is dat dossier een soort blauwdruk wat zij toepassen bij de aanschaf.
R: Op dat dossier wil ik straks nog even terugkomen. U zei dus dat er veelal dat er veelal met de ”huisleverancier” wordt gewerkt. Is het ook wel eens die leverancier die aankomt met een nieuw.... dat die leverancier zelf doorheeft dat er iets nieuws moet komen en dat zij dan actief dat proces starten, of is het eigenlijk altijd het ziekenhuis zelf met die aanschaf start?
I: Dat weet ik eigenlijk niet. Ik kan me, als ik kijk naar I&I, dan is het meestal ICT zelf die daarmee komt. Ik kan me ook voorstellen dat afdelingen dat zelf doen. Maar als je kijkt naar medische apparatuur is er misschien wel een kans dat, door middel van accounting vanuit zo’n leverancier, dat er daarbinnen contacten zijn ter vervanging. Ik weet het niet zeker.
R: En stel, we kopen een medisch apparaat. We hebben een proposal uitgestuurd en daar komt een reactie op, wat zijn.. Oh volgens mij heeft u dit net al verteld, wat de belangrijke criteria zijn voor een proposal.
I: Ja dat zijn eigenlijk de [Requests for Proposals] die helpen voor de verschillende afdelingen die betrokken zijn bij de aankoop. Daar is bij medische apparaten I&I een klein deeltje daarin, namelijk de huidige apparaten hebben allemaal een koppeling met het netwerk nodig. Is het echt een IT-component, dan hebben we uitgebreide requirement lists waar zo’n apparaat aan moet voldoen. En verschillende apparaten vragen dus om andere elementen.
R: Als we nog even blijven plakken bij het idee van een MRI-scanner, wie zijn er allemaal betrokken bij het maken van die uiteindelijke beslissing? Wie hebben er zeggenschap om de knoop door te hakken?
I: Formeel is alleen het bestuur tekenbevoegd. Daar zit nog wel wat voorwerk in. We hebben zogenaamde ITC, dat is de Interne Toetsings Commissie, en die beoordeelt eigenlijk alle investeringen die iedereen aangaat door het hele huis, inclusief de IT-zaken. Ik zit daar binnenkort ook in. Dat was nog niet zo, wel een collega van mij. Zij gaan eigenlijk kijken, ”is deze investering relevant?”, ”zijn er kosten?”. Dat nemen zij mee. Daar zit Inkoop ook in. Vervolgens gaat dat verhaal via Inkoop naar het bestuur voor een finaal akkoord.
R: Okee, dus het overleg gebeurt elders, maar het is het bestuur wat dan soort van het laatste akkoord moet geven.
I: Het bestuur doet op basis van advies, gaan zij akkoord. Zij zijn ook eigenlijk de enigen die tekenbevoegd zijn, maar er zijn natuurlijk wel interne handtekeningtrajecten voor dit soort aanvragen.
R: En als het dan alle fases passeert, dan gaat het naar het bestuur voor de final...
I: Ja.
R: Het is ook het bestuur wat dus uiteindelijk de handtekening zet?
I: Ja.
R: Okee. Dan hebben we een medisch apparaat gekocht.. Kunt u wat vertellen over wat er gebeurt nadat dat gekocht is? Is er een vorm van evaluatie daarna? Wordt er gekeken of iets naar behoren werkt?

I: Dat is een goede vraag. Ja, misschien wel, maar niet altijd denk ik. Ik denk dat dit met name gewoon bij het aanschafdossier zal staan. Het is denk ik ook weer niet standaard dat het gebeurt.
R: Okee, en daaraan gerelateerd, en dit is waar we terugkomen op dat document waar u het eerder over had - u noemde iets van een soort inkoopblauwdruk. Hoe worden er lessen getrokken uit inkopen uit het verleden? Worden daar lessen uit getrokken, of ervaringen opgedaan?
I: Wat bedoel je daarmee?
R: Wel bijvoorbeeld, als er dan sprake is van een verlenging of vernieuwing van een contract, wordt er actief bijgehouden wat voor aanpassingen er gewenst zijn aan bijvoorbeeld een SLA?
I: Ja, maar niet consequent. Ik denk wel dat het deels gebeurt, maar niet als standaard onderdeel van het proces. Geeft dan antwoord op je vraag?
R: Ja hoor, dat voldoet. Dan heb ik nog een vraag ook over.. iets meer op outsourcing, op cloud-based services gericht. Je ziet dat veel ziekenhuizen, met sommige systemen, dat ze ervoor kiezen om dat te outsourcen en dus, dat kan zijn dat een labinformatiesysteem via de cloud gaat, of andere zaken zoals een EPD. Heeft u een concreet voorbeeld zelf in uw hoofd waar ergens actief de keuze is gemaakt om het via de cloud te laten verlopen?
I: Ja, bijvoorbeeld mijn portfoliomanagementtooling is een volledig samengesteld product. Dat draait in [het buitenland] en dat is voor ons. Je hebt een browser nodig om de, om je portfolio bij te houden. Ik kan wel voorstellen als het gaat om om een LIMS [lab informatie managementsysteem], van een laboratorium, ik weet dat ons EPD bezig is met een soort van inrichting om dat aan te bieden vanuit een SaaS-omgeving [Software as a Service]. Dus daar zijn we wel degelijk richting in... Zij het nog niet zo standaard.
R: En kunt u mij iets vertellen wat de beslissing om in de cloud te gaan, drijft?
I: Dat is een goede vraag. Het is in mijn beleving veel gelegenheid. Als een partij of leverancier zijn software levert via de cloud, dan is het relatief makkelijk. Als die beide mogelijkheden heeft, dan kan gekozen worden voor een lokale oplossing. Dan wordt er voor het laatst gekozen vanuit commons-oogpunt. Als je kijkt naar hoe ik er tegenaan kijk, denk ik dat je zo veel mogelijk moet proberen in de cloud te brengen, zolang dat je primaire proces niet hindert. Grootste problemen die ontstaan zitten bij de koppeling software en modaliteit. Ben je bekend met modaliteit?
R: Bedoelt u het loskoppelen van onderdelen?
I: Modaliteit is de hardwarematige component. Neem een irisscanner ofzo, daar zit software aan. Die irisscanner zelf heet dan de modaliteit, en het stukje software draait vaak op een PC die in de buurt staat. Het is vaak lastig om die stukjes software te koppelen aan zo'n modaliteit, omdat dat stukje software heel erg verweven is met de modaliteit, soms met rechtstreekse kabels, of het draait nog op een hele omgeving et cetera.
R: De grote variatie in die eindpunten is dus een probleem?
I: Ja.
R: En wanneer wordt er besloten tot het overgaan naar een cloud-based service? Is dat helemaal aan het begin, van "we gaan dit in de cloud doen"? Of is het later als er al een pakket met eisen is en dan wordt er een cloudoptie overwogen?
I: Ik denk dat de gebruiksorganisatie [ziekenhuisstaf] niet eens heel veel bezig is of weet dat het cloud-based is, ja of nee. Op het moment dat ICT betrokken is, dan kan ik me voorstellen dat wij daar wel naar kijken, maar nog niet echt een hele sterke mening hebben op dat moment of dat ook voorkeur geniet ten opzichte van [een lokale oplossing].
R: Dan heb ik nog een korte vraag betreffende cybersecurity. Als er dan met een cloud-based systeem wordt gewerkt, zit er ergens in de overeenkomst met de provider een overeenkomst betreffende cybersecurity? Zijn daar afspraken over gemaakt? Hoe wordt dat gezien binnen het ziekenhuis?
I: Security is onderdeel van het toetsingsmechanisme. Zodra er iets nieuws wordt aangeschaft, dan gaat dat langs een aantal [stappen]. Ook daarin heeft Inkoop de regie. En vervolgens wordt gekeken op architectuur, er wordt gekeken bij de security, is het veilig, zijn er ISO-certificaten, hoe is dat geregeld et cetera. Op die manier zijn ze aangekaart.
R: Okee, u noemde certificaten als eis.
I: Bijvoorbeeld, ja.
R: Okee.
I: Het gemakkelijke bij een SaaS-leverancier is dat je zegt, "die gebruikt een ISO-gecertificeerd datacenter", dat helpt toch een beetje mee om te denken dat het veiliger is. **R**: Is er ook kennis aanwezig binnen ziekenhuizen om ook voldoende oordeel te kunnen vellen over certificering van leveranciers?

I: Nou, deels. Als ik heel eerlijk ben denk ik dat cybersecurity een te specifiek vakgebied is, waarbij je hulp van buiten zou moeten halen. En dat doen wij ook. Maar we hebben wel bijvoorbeeld iets, voor iets als ISO, daarvoor hebben we wel iemand die aanspreekpunt is voor alles wat te maken heeft met cybersecurity. Dat is wel handig.

R: En is dat dan iemand die ook over andere certificeringen gaat, of specifiek cybersecurity?

I: Die is voornamelijk gericht op cybersecurity.

R: Okee, dat is eigenlijk het einde van het hoofd... Oh wacht, ik heb nog één vraag voor u. Voordat ik ga afsluiten wilde ik graag nog weten of er verder nog belangrijke invloeden op inkoopprocessen zijn in ziekenhuizen die ik nog niet heb kunnen aankaarten vandaag? Zijn er nog grote elementen die ik nog niet gedekt heb?

I: Nou, wat ik nog zou willen toevoegen is dat , dat het niet altijd zo vanzelfsprekend is om Inkoop in de loop te houden. Ik denk dat er op diverse plekken, omdat het natuurlijk ook een complexe omgeving is, Inkoop niet altijd betrokken is als het wel moet. Of betrokken is als het eigenlijk niet nodig is.

R: Wat voor scenario's gaat het dan om?

I: Ik kan mij voorstellen dat een afdeling zelfstandig in staat is om een contract aan te gaan met een derde partij, zonder dat ze daar Inkoop bij gevraagd hebben. Dat zou natuurlijk kunnen gebeuren. Het is in die zin niet echt verankerd. Inkoop weet natuurlijk alleen wat ze weten, waar ze bij betrokken zijn.

R: Maar het kan dus voorkomen dat er volledig aparte processen plaatsvinden [buiten Inkoop om]?

I: Ik denk dat dat voor kan komen dat Inkoop niet wordt geraadpleegd terwijl dat wel zou moeten.

R: Dat is bijzonder waardevol om te weten. Daarmee is het procesgedeelte van het interview af.

B.2. Transcript 2

Researcher designated "R", interviewee designated "I".

R: Eerst vooraf even wat korte formaliteiten. Ten eerste dat het consent-formulier is ontvangen en getekend. We zullen zo'n dertig minuten bezig zijn. Het doel is dat ik een iets beter beeld krijg van hoe het inkoopproces binnen ziekenhuizen loopt. Laten we maar gewoon beginnen, eerst met wat achtergrondvraagjes. Kunt u mij vertellen wat uw functie is binnen uw organisatie en uw ervaring met inkoop?

I: Ik ben klinisch informaticus. Ik werk bij de medische techniek in [organisatie]. Dat betekent dat ik mij met medische apparatuur bezighoud, en de ICT daarvan. Ik houd me niet zozeer met het inkoopproces an sich bezig, want daar hebben wij een hele grote Inkoopafdeling voor. Maar, wij doen heel veel projecten binnen [organisatie], waarbij aanschaf wel degelijk heel belangrijk is. Voor grote projecten zijn dat vaak Europese aanbestedingen. We zijn Europees aanbestedingsplichtig. Voor de rest zijn er wel kleinere aanschaffen, dat aanschaftraject dat loopt altijd langs die medische techniek heen. We hebben binnen [organisatie] daar een procedure voor opgesteld, daar ga ik je straks het een en ander van laten zien. Ik denk dat het het handigste is dat.. Ik begrijp dat ik mijn scherm kan delen met jou? Ik kan ook wat documenten opsturen, die zijn verder relatief generiek, daar zit verder volgens mij geen geheim in.

R: Dat zou nuttige informatie zijn, graag.

I: Het is wel zo dat wij de afgelopen tijd, laten we kijken naar, pak hem beet een jaar geleden, of twee jaar geleden... Toen hebben we dat hele proces nog eens goed tegen het licht gehouden. Afdelingen die zijn zelf financieel verantwoordelijk voor de apparatuur die zij aanschaffen. Dan vinden zij zich nog wel een geremd door Medische Techniek of een andere afdeling binnen het ziekenhuis, als het gaat om die aanschaffen. Er zijn best wel een aantal mensen die het vervelend vinden dat we ons met die aanschaf bemoeien.

R: Hoe reageren zij dan?

I: Over het algemeen zeggen zij "Wij weten wel wat we willen en dat gaan we dan aanschaffen". Soms werkt dat zo, soms werkt dat ook niet zo. Als Medische Techniek hebben we natuurlijk een overzicht in alle apparatuur die we in het ziekenhuis gebruiken. Stel jij wil een echografiemachine aanschaffen, dan hebben we daar een soort standaard voor. Als jij iets leuks ziet op de markt, als arts, en je wil dat leuke graag aankopen, dan word je dus als het ware op het matje geroepen en zeggen we "Nee, je moet je aan de standaard houden". We hebben hier een systeem voor. Dat komt ook omdat steeds meer medische apparatuur gekoppeld wordt aan het netwerk en data uitspuugt. Daar wil je natuurlijk ook in standaardiseren.

R: Dus, als ik het goed begrijp, worden in toenemende mate eigenlijk die randeisen die buiten, de eisen die de arts zelf niet stelt maar vanuit IT worden gezet, die worden in toenemende mate belangrijker?
I: Ja. En dan komen we ook op cybersecurity-regels terecht.
R: Die cybersecurity, hoe belangrijk is dat in dat hele aanschafproces? Wat voor vorm neemt dat aan? Is dat een aparte review, of worden certificaten vereist...?

[participant deelt scherm]

I: Wij hebben op ons intranet dit staan: "Aanschaf/gebruik/verwijdering van medische hulpmiddelen en apparatuur". Iedere afdeling kan deze informatie raadplegen. Bij aanschaf van een medisch hulpmiddel, of dat nou Europees aanbesteed is of niet, wordt er een aanschafdossier gemaakt. In dat aanschafdossier zitten een hele hoop zaken. Daar zitten ook handleidingen in, er zit van alles in. Als je als afdeling een apparaat wil aanschaffen wat al in gebruik is, dan heb je een soort verkorte procedure, omdat het al bekend is binnen de organisatie, en omdat het al eerder aangekocht is. Is het compleet nieuw, dan heb je wel wat te doen als afdeling. De Medische Techniek heet hier Instrumentele Zaken, dat is misschien wat verwarrend. Instrumentele Zaken en Inkoop werken hierin samen. Het wordt ook allemaal in een productdossier opgeslagen. Dus we kunnen achteraf bekijken hoe het allemaal verlopen is, wat voor documenten er zijn.
R: Dat wordt ook achteraf gedaan? Een stuk evaluatie erna?
I: Evaluatie erna? Niet heel... Ja ik denk dat die wel gedaan wordt. Ik heb hem eerlijk gezegd nooit zelf zo meegemaakt. Maar voor dat moment moeten een heleboel zaken in orde zijn. Ik zal de beslisboom erbij pakken. Dit is heel simpel neergezet. De afdeling wordt gevraagd: "Ik wil een medisch hulpmiddel aanschaffen. Staat dit artikel al in het systeem?". Als hij er al in staat, dan kan je gaan bestellen en dan kan je collega's bekwaam maken met het hele verhaal en dan kan je aan het werk. Dus dan ga je op bestellen drukken. Staat het nog niet in die catalogus, dan ga je een aantal vragen in. Ga je het artikel gebruiken in de patiëntenzorg, voor behandeling of therapie of diagnose, dan moet je dus het plan van aanschaf gaan volgen. Dit is eigenlijk een simpel begin om die afdeling op gang te helpen. Dan hebben ze een stroomschema gemaakt. De behoefte eerst, is het een middel, als er geen middel in zit dan hoef je deze procedure niet in te gaan. En middel op zicht, dat gebeurt ook wel eens. Dat ze een product op zicht krijgen van een leverancier, dan is daar een speciale aanvraag voor, dat is een andere procedure. Als het niet op zicht is, is het medisch, is het een medisch hulpmiddel? Als het geen medisch hulpmiddel is, dan ga je er ook uit, dan ga je deze lijn ook niet volgen. Is het een nieuw merk of een nieuw model? Als dat niet zo is, dan kunnen ze het gewoon bestellen. Dan kunnen ze een deskundige inventarisatie doorlopen en dan is het proces van bestellen al daar.
R: Dat is dan een voorafbepaalde partij die iets gaat vervangen?
I: Ja. Stel ik heb een Philips bewakingsmonitor op de afdeling en ik wil er nog eentje bij hebben. Dan hoef je niet helemaal die procedure door want die hebben we dus al gedaan de eerste keer. Daar zit die cybersecurity en inkoopvoorwaarden al in. Is het wel een nieuw merk of model, dan moet je eigenlijk wel iets meer doen. Dan gaan we kijken naar "Is het een CE-klasse IIa of hoger?" Dat zegt wat over hoe kritisch het apparaat is. Als dat niet zo het geval is, dan moet je een voorblad productdossier invullen. En dan kan je ook doorgaan met bestellen. Is het wel klasse IIa of hoger, dan moet je een risicoscan doen en een Prospectieve Risico Inventarisatie, of PRI. Die PRI is een vrij uitgebreid document. Dan moet je dus alle aspecten die met het apparaat in verband staan, moet je inventariseren en kijken waar je als afdeling risico's loopt. Als je die risico's ziet, wat voor tegenmaatregelen ga je dan nemen om die risico's te dekken.
R: Dit zijn risico's met betrekking tot patiëntenzorg vooral, of ook met andere aspecten?
I: Ja, ook cybersecurity. Dat PRI is vrij breed. Dat gaat over gebruik, dat gaat over onderhoud, dat gaat over beveiligingen, van alles en nog wat. Het maken van zo'n PRI wordt overigens door mijn afdeling ook ondersteund. De afdeling moet hem zelf maken, maar wij ondersteunen in dat proces omdat wij ervaring met dit soort dingen hebben. Afdelingen doen dit mogelijk voor het eerst. Als je zo'n PRI gedaan hebt en is de risicoscan-uitkomst laag, dan kan je gewoon door naar aanschaf. Is het risico hoog, dan moet je een noodzaak tot verwerving en een pakket van eisen opstellen. Dus waar moet het product aan voldoen. Goed, ook dat pakket van eisen gaan wij vanuit de Medische Techniek ondersteunen. Ook daar hebben wij meer ervaring in. Ondertussen wordt ook de CE-documentatie opgevraagd en de handleiding. Dit wordt allemaal in het aankoopdossier gestopt. Die CE-documentatie die is belangrijk, want als een medisch hulpmiddel niet CE-gecertificeerd is, mogen we het eigenlijk officieel niet gebruiken. Daar houden we ons ook aan. We kunnen dan bij controles op onze vingers getikt worden en dat willen we niet. Wat de afdeling dan ook moet doen is een scholingsplan opstellen: wie gaat ermee

aan het werk en wat moet die persoon voor kennisniveau hebben? Wie moeten er geschoold worden? En het evaluatieplan, je noemde het net al, het staat hier toch in. Er wordt dan een evaluatieplan opgestuurd en dan, bij apparatuur moet je ook onderhoud regelen. Dat is een verplicht nummer. Je kan geen apparatuur kopen en dan het onderhoud niet regelen.
R: Als je dan in dit traject terechtkomt en het gaat om een nieuw product, worden er dan verschillende proposals geëvalueerd, van verschillende partijen?
I: Het hangt van de hoogte van de aanschaf af. Boven de 210.000 ga je het aanbestedingstraject in. Dan gaan ze het in de markt zetten, dat is een heel verhaal. Dat doet onze inkoopafdeling meer en die publiceert dat. Die gaat leveranciers uitnodigen om in te schrijven. Dan gaan we diverse leveranciers inschrijven en worden wegingen toegekend. Gaan we wegen op kwaliteit, of op prijs? Dat soort zaken. Dan heb je vaak meerdere aanbieders. Bij sommige systemen is het ook lastig. Ik ben nu bezig met een Europese aanbesteding voor patiëntmonitoren. We hebben dat nu bij een leverancier in huis, we hebben er twee in huis die dat leveren op het ogenblik. En daar zie je toch, als je bepaalde componenten wil vervangen, maar niet alles, en je moet dat Europees gaan aanbesteden... Als je dan moet kiezen voor een andere leverancier dan moet je dus eigenlijk wel alles vervangen. Dus je moet als organisatie er wel goed over nadenken hoe je dat gaat doen. Want stel je wil voor een miljoen monitoren vervangen, maar je hele installed base is van één leverancier en je wil een ander, dan moet je dus om één miljoen te vervangen, dan moet je zes miljoen uitgeven.
R: Dus dat factort ook mee, en dan kom je sneller op dezelfde leverancier uit?
I: Ja, maar dan heb je het wel eigenlijk over een vendor lock-in. Maar goed, dat staat ook los van de cybersecurity.
R: Maar dat is wel iets wat je keuze beperkt. Wordt onderhandelen over cybersecurity dan ook weer moeilijker?
I: Ja absoluut. En als je dan deze stappen hebt doorlopen, kunnen we door met de aanschaf. Ze moeten wel een checklist doorlopen. In het Aanschafdossier Medisch Hulpmiddel is een checklist, daar vullen ze naam aanvrager in. Soort product, fabrikant, type leverancier, noem het maar op. En dan gaan ze allemaal dingen aan je vragen. Is het middel disposable? Ja of nee, en wat moet je dan doen? Neem dan contact op met dit telefoonnummer. Dient dit middel of onderdeel gesteriliseerd te worden? Dan moet je naar de sterilisatieafdeling. Al dat soort vragen. Hier wordt eigenlijk degene die de aanschaf doet begeleid in de stappen die hij moet nemen en de afdelingen of organisaties waar hij contact mee moet opnemen.
R: En deze partijen kunnen dan additionele eisen gaan stellen?
I: Ja. Neem iets als een flexibele scoop, daar wil onze expertgroep Scopen bij betrokken worden. En zo hebben we ook voor radiologische apparatuur of klinische chemie, voor allerlei dingen, expertgroepen. ICT heeft ook zo zijn aansluitvoorwaarden voor het netwerk. Daar kom ik straks op terug. Er is ook nog een deel 2 [in het formulier], dat is voor Team Aanschaf. Dat zit bij Inkoop. Zij gaan nog een aantal dingetjes na: ligt de noodzaak vast? Is het programma van eisen opgesteld? Is er een PRI gedaan? Hier worden eigenlijk al die dingen gecontroleerd. Zodoende houden we als organisatie dat hele dossier in de gaten. Als het eenmaal is aangeschaft, dan krijg je dus ergens een controle van Inspectie Gezondheid en Jeugd, dan moeten we alles over die aanschaf kunnen overleggen. En dan denk je van, waar zit die cybersecurity nou?
R: Ja, waar zit die hier?
I: In dat hele verhaal met CE-documentatie, in de gebruiksaanwijzing, in offerte. In die hele toestand vragen we tegenwoordig een MDS2-formulier. Dat is dus een generiek formulier wat iedereen kan gebruiken. Dat gebruiken wij als organisatie ook bij een inkoop. Daar staan nou heel veel vragen over data en cybersecurity in. Dit moeten leveranciers invullen. Dan kan je als organisatie, dan krijg je een goed beeld van hoe zo'n medisch apparaat, aangesloten op jouw netwerk, omgaat met security. Dus hier ligt dan voor jou het zwaartepunt van jouw vraag.
R: Ik heb wel een vervolgvraag hierop. Dit is niet altijd even makkelijk in te vullen door iemand. Wie vult dit in?
I: De leverancier moet dit invullen.
R: Die doet zelf dus de beschrijving van de cybersecurity-implicaties.
I: En wij gaan dat als organisatie evalueren.
R: Wie zijn daarbij betrokken? Is dat alleen Inkoop of ook met artsen?
I: De arts ligt hier buiten. Die laten we weten wat er uit het formulier komt. Wij kunnen hier mensen van ICT bij betrekken, maar ook van de Medische Techniek. In mijn geval, als Klinisch Informaticus, houd

ik mij hiermee bezig, met dit formulier. Ik kijk naar wat is ingevuld en als ik vervolgvragen heb, dan bel ik de leverancier en dan vraag ik wat ik moet weten. Voor een leverancier kan het soms lastig zijn om deze vragen in te vullen. De interpretatie van de vragen is wel eens anders.
R: Dus de leverancier zelf is niet altijd in staat om dit in te vullen?
I: Hangt van de leverancier af. De grote leveranciers hebben hier niet zoveel moeite mee, die hebben daar over het algemeen ook best wel specialisten op zitten. Maar kleinere leveranciers hebben hier nog wel eens moeite mee. En dan vragen we gewoon uit: ”wat bedoel je met dit antwoord?”. Als ze het goed kunnen verwoorden, dan zetten wij die antwoorden gewoon op okee of groen. Maar dit formulier gaat vrij ver. Er zitten best wel veel dingen in. Ook het automatisch uitloggen en audit controls.
R: Dan zijn er nog een paar andere vragen die ik ook graag wil dekken. Ik was nog even nieuwsgierig naar het begin van het proces, als zo'n aanschaf wordt gestart. U noemde dat dat vooral vanuit de arts gaat, of dat een apparaat vernieuwd moet worden. Is het ook wel eens een externe motivatie zoals een supplier zelf die aankomt met iets nieuws?
I: Nou, dat is op het ogenblik, dat gebeurt niet zo heel erg veel. Het gebeurt wel, en over het algemeen komt het initiatief dan bij die Medische Techniek vandaan, bij onszelf. Dan doen we dat in de vorm van een technology push, als het ware. Waar ik zelf nu mee bezig ben is, bijvoorbeeld, ik ben veel met patiëntbewaking bezig. Ik zie nu dat, en zeker in de huidige situatie met CoViD-19 patiënten, dat er draadloze monitoring gebruikt wordt binnen diverse organisaties. Dat gebruiken wij als LUMC op dit moment nog niet. Ik ben ook lid van de expertgroep die daarover gaat. Vanuit die expertgroep hebben we nu bij diverse afdelingen de vraag neergelegd. We zien een nieuwe techniek, we zien ook andere organisaties deze techniek gebruiken, hebben jullie daar interesse in? We zijn nu met afdelingen in gesprek over die techniek. Dan zie je dus inderdaad dat de vraag niet van de afdeling komt, maar dat de afdeling als het ware geïnteresseerd gemaakt wordt voor een nieuwe techniek, dus ook nieuwe apparatuur. Dan moet je nog steeds deze hele inkoopprocedure volgen, die blijft hetzelfde.
R: De volgende vraag gaat over de uiteindelijke krabbel eronder. Wie zijn daartoe bevoegd? Wie hebben dat laatste zeggenschap?
I: Dat is in principe het afdelingshoofd, samen met de divisiedirecteur.
R: Ik begon eerder al even over evaluatie nadat er getekend is. Is er een proces waarbij er echt lessen worden geleerd uit het verleden? Of gebeurt dat impliciet?
I: Nou, er is dus wel een evaluatieformulier maar ik moet zeggen dat ik daar in de praktijk niet zo heel erg veel van heb gezien. Wat wij wel als Medische Techniek doen, en we lopen nu ook tegen dingen aan op cybersecurity, op ICT-gebied, lopen we ook tegen dingen aan waarvan we zeggen dat we dit in de toekomst anders aan moeten gaan pakken. Er is ook een soort expertgroep die gaat over medische technieken in netwerken. Die is daarmee bezig. Dan doen we dus aanpassingen in de techniek samen met ICT om apparaten veilig in netwerken te plaatsen. En waar we ook tegenaan liepen is dat medische apparatuur vaak met accounts en wachtwoorden worden uitgerust. Het grappige is datje dus op het internet heel erg makkelijk achter die gegevens kan komen. Stel, je bent een hacker en je kan inbreken op netwerken, dan zou je dus op echoapparatuur met het standaardwachtwoord en het standaardaccount in kunnen breken. Dat standaardaccount zou best wel eens heel veel rechten kunnen hebben op het apparaat. Dan kan je het hele proces in het honderd laten lopen, bij wijze van spreken.
R: Daar worden dus wel lessen uit geleerd om dan de volgende keer te zorgen dat, voordat je iets aansluit, er maatregelen zijn getroffen?
I: Ja. Als medisch technische dienst hebben wij gezegd dat het moment dat een apparaat binnengebracht wordt, dan moet dat standaardwachtwoord gewijzigd worden. Als medisch technici kunnen we dat netjes in een passwordkluis opslaan en kunnen we dat allemaal gebruiken, dat is prima. Mocht er dan reparatie of onderhoud gedaan worden, door de leverancier over het algemeen, dan kan die leverancier dat account niet meer gebruiken. Dan zijn er twee mogelijkheden. Of er wordt een nieuw account aangemaakt voor die maatschappij, voor die leverancier, dan moeten ze daar hun eigen wachtwoord ingeven en zelf bijhouden, dat mogen wij dan niet weten. Dan hebben ze een tweede account waar ze mee werken en daar zijn ze dan verantwoordelijk voor. Of we wijzigen het password en maken het bekend bij de leverancier en zodra die de deur uit is, wordt het password weer gewijzigd, ook in ons passwordsysteem. Er is één uitzondering op deze regel. Dat is apparatuur die niet aan het netwerk aangesloten is, en die standalone is, daar laten we de wachtwoorden wel standaard staan omdat we er dan vanuit gaan dat iemand toch fysiek aanwezig moet zijn. Dan is eigenlijk de extra control niet nodig. Dat geeft verder geen problemen. Dat heeft geen impact op andere ICT-systemen.

R: Dan heb je op dat moment bovendien allerlei andere problemen om eerst op te lossen.
I: Precies. Dus we hebben daar wel een passwordbeleid op los gelaten. Dat functioneert goed.
R: Ook in de praktijk, met verschillende wachtwoorden voor verschillende mensen, dat geeft niet teveel gedoe?
I: Nee. En sterker nog, als een apparaat afgevoerd wordt, dan zit nog steeds dat wachtwoord en account daarin. We moeten apparaten afvoeren via een stichting, dat heeft te maken met dat CE-verhaal. Die neemt dan het eigenaarschap over van ons. Dan zouden wij een soort leverancier worden van iemand anders die die apparatuur zou kunnen gaan gebruiken. Dat willen we niet. Dus we hebben daar een tussenpartij voor. Veel medische apparatuur wordt nog wel eens naar Afrika of andere landen gestuurd voor hergebruik. Dat kan ook prima. Dan zorgen wij er wel voor dat we ook weer die wachtwoorden wijzigen en dat die wachtwoorden meegegeven worden met de apparatuur. Nooit dat dat een wachtwoord is wat wij in gebruik hebben.
R: Dan heb ik nog een vraag over cloud-based systemen. Bent u daar ook mee bezig geweest?
I: Nee, wij houden eigenlijk binnen de medische techniek, de cloud-based apparatuur buiten de deur op het ogenblik.
R: En wat drijft die beslissing?
I: Het is vaak zo dat cloud-based apparatuur hun data, wat data is van ons, over de patiënt, naar de cloud van de leverancier stuurt. Dan kan je er gebruik van maken. Dat is een beetje, bij ons geldt onbekend is onbemind. We zijn er nog niet aan toe denk ik. Wij willen de data gewoon in huis hebben, op onze eigen systemen, onze eigen storage, binnen ons eigen EPD. Daar koppelen we op dit moment geen cloud-oplossing aan.
R: Dus dat is echt een beleid?
I: Ja, zeker. Het enige wat wel gebeurt is, bij bijvoorbeeld robotisering op de OK, daar is bij het gebruik van de OK-robot iemand van de leverancier die de diagnostische gegevens van de apparatuur, dus geen patiëntgegevens, direct ontvangt. De leverancier ziet direct of het apparaat een fout constateert, in de apparatuur zelf. Stel er is een lamp kapot, of een meetbord kapot, dan wordt dat direct gesignaleerd en dan kan de leverancier direct ingrijpen.
R: Dan wilde ik ook nog iets weten over de aanbestedingen. Daar komen criteria bij kijken, die stel je zelf. Zijn daar bepaalde dingen die zwaarder wegen, vaak, dan anderen?
I: Ja, binnen een pakket van eisen worden altijd wegingen aangebracht.
R: Zijn die consistent, zijn het vaak eisen die de arts zelf stelt die voor gaan?
I: Dat is lastig. In zoverre lastig: bij het maken van een pakket van eisen neemt Inkoop de leiding. En Inkoop schakelt een aantal partijen in. Zoals ons vanuit de Medische Techniek, maar ook ICT met hun eisen. Dan wordt specifiek gekeken naar de noodzaak die de afdeling heeft. Als het dan aan het netwerk aangesloten wordt, gaat ICT daar het pakket van eisen aanvullen. Daar kunnen wensen in staan, maar ook lock-out criteria. Bijvoorbeeld dat een apparaat een firewall heeft. Als het product dat dan niet heeft, dan sluiten we die leverancier uit.
R: U noemde ook dat sommige aanschaffen niet helemaal volgens het boekje verlopen. Ik kan mij voorstellen dat zo'n requirement van zo'n firewall er niet goed doorheen is gekomen.
I: Ja.
R: Hoeveel gebeurt dat? Hoeveel last heeft u daarvan?
I: Dat gebeurt op het ogenblik niet heel erg veel. Dat is echt met hele grote systemen, en over het algemeen ken je wel de leverancier en het systeem al. Wij komen geen situaties tegen waarin het slecht of helemaal niet geregeld is. En we hebben ook, binnen ICT, over die medische netwerken, dat zijn eigenlijk virtuele netwerken waarbij er een firewall tussen staat. We hebben wel apparatuur die bijvoorbeeld niet voldoet aan de virusbeschermingseisen die wij stellen. Of apparaten die niet geüpdatet kunnen worden, omdat de leverancier nou eenmaal aangeeft dat zij niet willen dat er updates op worden gedraaid. Daar zijn we niet blij mee, want die zorgen voor een risico. Wat we dan doen is dat we die apparatuur in een geïsoleerd virtueel netwerk zetten, met een intrusion protection system: een systeem wat constant monitort of er verkeerde data wordt gegenereerd.
R: Dus die apparaten bevinden zich op een gesegregeerd netwerk?
I: Ja. Komt er een virus los uit zo'n apparaat, dan wordt dat netwerktechnisch gestopt. En dan wordt het apparaat geïsoleerd van de rest. Maar goed, dat zijn de uitzonderingen, alhoewel we wel uitgaan dat we bepaalde apparatuur in dat soort geïsoleerde netwerken zetten.
R: Ik heb nog één vraag voordat ik ga afronden. Is er nog iets waarvan u denkt dat het belangrijk om te noemen als we het hebben over cybersecurity in ziekenhuizen? Iets wat ik vandaag nog niet gedekt

heb?
I: Je probeert als organisatie de ontwikkelingen op dit gebied bij te houden. Er is nog een soort cybersecurity-platform waar wij bij aangesloten zijn. Wij zijn daar als medische techniek ook bij betrokken geweest. Wij volgen daar seminars en dat soort zaken, om onszelf op de hoogte te houden. Je loopt met dat soort zaken altijd achter op de technieken die ontstaan bij criminelen. Dat is voor ons lastig. Je probeert jezelf altijd te beschermen.
R: Dus dat is voor u een soort derde partij waar u die kennis inwint?
I: Ja.

B.3. Transcript 3

Researcher designated ”R”, interviewee designated ”I”.
R: Voordat we van start kunnen, heb ik nog een korte formaliteit. Ik heb het consent-formulier doorgestuurd. Stem je ermee in dat ik je data van dit interview verwerk zoals vernoemd in dat formulier?
I: Ja.
R: Dan hebben we dat gehad. Laten we maar beginnen met een introductievraag. Kun je me wat vertellen over jouw positie binnen jouw organisatie, en je ervaring met inkoop in ziekenhuizen?
I: Ja. Mijn positie hier bij [organisatie] is eigenlijk tweeledig. Dat komt omdat we nog een vrij kleine organisatie zijn. Ik vervul hier de functie van Information Security Officer. dat is verantwoordelijk voor de interne beveiliging. Daarnaast ben ik Security Specialist. Dat betekent dat ik andere incidenten afhandel bij zorginstellingen, en alle vragen beantwoord rondom cybersecurity die men heeft. En daar zitten dus onder andere vragen tussen over inkooptrajecten, leveranciers en dergelijke. Dat is denk ik het relevante stukje van mijn werkzaamheden voor jouw onderzoek.
R: Kun je voor mijn begrip misschien een voorbeeld geven van de vragen die jou dan gesteld worden?
I: Ja. Je kan je voorstellen dat een partij bezig is met het inrichten van een meer volwassen security-organisatie. Daartoe willen ze wat SIEM-tooling (Security Information and Event Management) in huis hebben om al die events bij elkaar te brengen, om daar wat analyse op te doen en alertering op te zetten. Om te kijken of er geen gekke dingen in de organisatie gebeuren. En in zo’n geval zouden ze dus bij ons met de vraag kunnen komen: ”Hebben jullie ervaring met verschillende SIEMs (Security Information and Event Management) of andere deelnemers?” ”Hebben jullie daar een voorkeur in?” ”Is het koppelbaar met deze en deze systemen?” ”Hoe kan ik dat het beste inrichten?”. Dus het kunnen hele diverse vragen zijn.
R: Dat loopt dus sterk uiteen. Dat is dus kennis die ze helemaal niet in huis hebben, of ze zoeken aanvullende kennis?
I: Vaak aanvullende kennis. Het verschilt heel erg per instelling wat het niveau is, en waar het onderzoek wordt gedaan. Sommige partijen laten dat voor een groot deel over aan een Inkoopafdeling. Andere partijen die zitten in dat inkoopproces, daarbij is de afdeling Inkoop maar een klein onderdeel. Voor de rest zoeken ze zelf uit wat nodig is en vervolgens passeert het in een proces. Er zit ook vaak een stuk change-organisatie om een nieuw product dat wordt ingekocht, ook in te brengen in de organisatie. Dat verschilt dus heel erg. Heel af en toe spreek ik iemand die echt van Inkoop is. Dat heeft voornamelijk betrekking op hun eigen aansluiting bij ons. Maar de meeste vraag komt van security-medewerkers in de organisatie, die een soort adviesvraag bij ons neerleggen.
R: En hoe zie je dit ontwikkelen? Gebeurt dit steeds meer? Of zie je dat organisaties steeds meer zelf weten?
I: Op wat betrek je dat?
R: Of ze steeds meer van die security-kennis zelf in huis halen.
I: Dat is een interessante vraag. Ik denk dat de zorgsector wel aan het groeien is qua volwassenheidsniveau [van security], maar de meeste zorginstellingen hebben nog wel een heel lage hoeveelheid medewerkers dat enkel en alleen zich richt op security. Dat wil zeggen dat een ziekenhuis van 2000+ FTE, die zou één CISO hebben, en misschien nog een security-manager die zich wat meer operationeel bezighoudt. En verder ligt een groot deel van de verantwoordelijkheid bij beleidsmakers, kwaliteitsmanagers en IT. Iemand daarbij fulltime aantrekken, die ook security doet, dat zie je niet heel vaak. Maar wij hebben natuurlijk contact met alle ziekenhuizen in Nederland, dus als daar een wijziging is in het personeelsbestand ten aanzien van security, dan krijgen wij dat doorgegeven omdat wij de dienstverlening daarop moeten aanpassen. Dat gebeurt op zich wel regelmatig. Er komt dus wel nieuw personeel bij. Of ik daar een trend in zou kunnen ontwaren, durf ik niet te stellen.

R: Uit een ander interview heb ik al vernomen de integratie van security-requirements, dat sommigen ervaren dat dat steeds meer gebeurt. Dat je daar steeds minder omheen kan. Maar de markt is niet altijd zo. Een RfP (Request for Proposal) loopt niet altijd zo dat je altijd de ruimte hebt om verschillende suppliers aan te spreken. Hoe zitten die suppliers met cybersecurity? Zijn zij bereid daarin tegemoet te komen? Zijn zij ermee bezig?
I: Ik denk dat dat ook iets groeiends is. Ik denk da leveranciers in het medisch gebied, medische IT dus, software en hardware, dat die daar steeds meer mee bezig gaan omdat de vraag ook meer aanwezig is. Dan wordt het op een gegeven moment ook financieel interessant. Als je meedoet aan een RfP en je concurrent doet wel iets met security, en je verliest daardoor een opdracht, dan gaat het op een gegeven moment in de portemonnee iets doen. Het verschilt heel erg per partij. Sommige leveranciers zijn al behoorlijk wat verder, die hebben een hele baseline al ingericht. Daar hoef je ook niet gekke dingen van te verwachten. Aan de andere kant zie je dan weer bij wat kleinere leveranciers vaak, of bij partijen die traditioneel voornamelijk helemaal in de interne organisatie zaten, met geen enkele koppeling.... Op een netwerk bijvoorbeeld, dat die daar bar weinig aandacht aan hadden besteed. Maar ja, het hele cybersecurity-gebeuren in de wereld krijgt meer tractie, en dat zorgt ervoor dat ook bij kleine partijen het op den duur gemeengoed gaat worden. En wat daarnaast een driver bij is, is.. in de zorgsector, afhankelijk van wat je doet.. Er zijn bepaalde typen wetgeving die je verplichten om maatregelen te nemen, of bezig te zijn met een security-framework. In de zorg is dat de NEN-7510. Die roept ook wel iets over beveiligingsmaatregelen in soft- en hardware. En ook hoe je met leveranciers moet omgaan. Dat bepaalde eisen moeten worden gesteld, omdat het anders een risico vormt. Dus we zien ook wel in onze deelnemersgroep dat soms een deelnemer aan een andere deelnemer vraagt... We hebben een soort community voor hen. Dat die vraagt van ”We zijn bezig met deze leverancier en die doen iets heel vreemds op het gebied van security. Heeft iemand anders dit ook gezien?” Soms melden ze dat bij ons als een Responsible Disclosure melding. Dan gaan we met de leverancier in conclaaf. En het verschilt heel erg per leverancier hoe ze daar mee omgaan. Ik denk dat [betrekking van leveranciers] groeiend is. Of ik je daar harde statistiek voor zou kunnen geven, dat denk ik niet. Maar het is wel het gevoel dat bij mij heerst.
R: Dus op die manier worden er wel lessen uitgewisseld?
I: Ja. Wij brengen bijvoorbeeld de CISO’s, maar ook het technisch personeel in zorginstellingen, die brengen we bij elkaar. En we faciliteren overleg op het gebied van security. Zeker richting leveranciers kan dat heel waardevol zijn als je bepaalde security-eisen hebt en je een soort bloc kan vormen met elkaar - omdat in het verleden en nu soms ook nog wel eens gebeurt, dat een leverancier tegen een zorginstelling zegt: ”je bent de enige die hier een punt van maakt. 99% van andere klanten doen hier niet moeilijk over.”
R: Dus dat is een stuk pushback vanuit de leverancier?
I: Ja, en dat is dan in de praktijk misschien helemaal niet zo. Dan stellen ze die vraag en dan zeggen drie andere partijen: ”dat hebben wij ook meegemaakt.” Dan kan je actie gaan ondernemen omdat je daarbij de leverancier feitelijk betrapt op een actie die misschien niet kan of mag. Dat helpt natuurlijk ook, als dat vaker voorkomt, dan trekken mensen ook hun conclusies.
R: En in het licht van de Medical Device Regulation die geupdatet wordt - dat is uitgesteld naar volgend jaar - Ik geloof dat daarin ook een stuk strictere eisen staan voor medische apparatuur, ook met betrekking tot cybersecurity. Leveranciers zouden er dus wel mee bezig moeten zijn. Merk je dat dat een issue voor ze is?
I: Dat verschilt dus heel erg per organisatie. Als wij een Responsible Disclosure melding doen, met zorginstellingen bij een leverancier, dan is de reactie heel wisselend. De ene partij die krijgt zo’n melding binnen en zegt: ”dat is geen probleem want dat stuk software hoort in een aparte Virtual Local Area Network te staan, dus er is geen enkele reden dat dat communiceert met X.” Andere mensen zeggen: ”ja, dat kan best zijn, maar toch hoort een verbinding tussen punt A en punt B ten alle tijden beveiligd te zijn, einde discussie.” Dan is dat natuurlijk even de vraag wat de correcte visie is. Waar mogelijk maken we daar gebruik van internationale standaarden van het classificeren van dergelijke kwetsbaarheden. Zoals bijvoorbeeld met het Common Vulnerability Scoring System. Daar kan je een beetje objectief aangeven of een kwetsbaarheid in een product een bepaalde score haalt. Dat haalt dan soms wel een beetje de wind bij een leverancier uit de zeilen. Als je dat duizend keren per jaar doet, zoals wij dat doen, dan heb je op een gegeven moment wel een redelijk gevoel voor wat de ernst is van een probleem.
R: En dat soort metingen of evaluaties worden meegenomen door ziekenhuizen als zij een RfP sturen

en dat gaan evalueren?
I: Niet op die manier. Het traject dat ik beschrijf heeft meer betrekking op, als een leverancier al een dienst levert waarin vervolgens een kwetsbaarheid wordt ontdekt, dan komt het wel eens voor dat, voordat die dienstverlening operationeel is, men een Proof of Concept (PoC) draait waarbij zaken aan het licht komen. Ook dat is een verschil tussen zorginstellingen. Sommige draaien wel een PoC en anderen niet. Daar wisselt het inkoopproces en dat hele traject ervan over de linie. Dat verschilt heel erg. Ik denk wel dat een aantal, of ik weet dat een aantal partijen, als onderdeel van hun inkoopproces, ook kijken of er al kwetsbaarheden bekend zijn in een stuk software, die ze willen aanschaffen. Of dat die een track-record hebben van heel veel kwetsbaarheden. Maar dat is een minima die dat doet.
R: Dat wordt dus wel gedaan, maar niet veel dus?
I: Dat is mijn indruk ja. Nogmaals, daar heb ik geen harde cijfers voor.
R: Als we dan kijken naar, als er iets ingekocht is, dan heb je een traject erna dat iets in gebruik is. Ik begrijp dat jullie daar dus ook wel mee te maken hebben. Dat jullie dan alsnog een melding versturen. Hoe wordt daarop gereageerd vanuit het ziekenhuis? Weten die wat ze ermee moeten?
I: Dat verschilt ook weer per instelling. In de regel wel. [mijn organisatie] heeft, ik denk in de afgelopen drie jaar, wel een behoorlijke positie daarin ingenomen. Tot op het niveau dat als wij adviseren om per direct een applicatie uit te zetten, dat het gros van de instellingen dat ook direct doet. Omdat wij dan een inschatting zouden maken dat het gebruik van die applicatie echt totaal onveilig is. Een voorbeeld daarvan kan Citrix zijn, van afgelopen jaar. Als wij daartegen adviseren, dan is er een hele goede kans dat dat wordt opgevolgd. Als wij een beveiligingsadvies sturen voor een bepaald product in de medische IT, dan wordt dat in bijna alle gevallen behoorlijk serieus opgepakt, afhankelijk van de ernst. Dan gaat het mee in óf het reguliere patchproces, óf er wordt een uitzondering gemaakt en ze gaan buiten hun reguliere patchwindow een apparaat updaten of mitigerende maatregelen en/of workarounds in plaats zetten. Dat is ook ons doel, om voor hen die schifting te doen, in de beschikbare informatie, wat het juiste handelingsperspectief is. En daarbij heb je natuurlijk altijd wel te maken met de variabelen van een instelling zelf. Als daar vragen over zijn, dan bellen we gerust even met ze om uit te vragen hoe de situatie bij een specifieke instelling is en wat het beste advies daar zou kunnen zijn om mee om te gaan. Bijvoorbeeld: je kan wel een kwetsbaarheid in een product hebben, maar als in een specifieke instelling dat apparaat nooit aan iets anders is aangesloten en dat nooit het geval zal zijn, dan neemt je attack surface behoorlijk af. Dan kan een risico-afweging zijn om te zeggen: ”nou ja, het patchen van dit apparaat kost meer moeite of is meer risicovol dan dat het oplevert, dus we doen het niet.” Maar dat is een afweging aan de instelling. In principe geven wij een algemeen advies en waar instellingen dat prettig vinden, gaan we één op één met ze in conclaaf.
R: Kom je vanuit jouw positie ook wel een in contact met de wijdere groep die apparaten inkopen in het ziekenhuis? Waar ik vooral naar vis is, spreek je ook wel eens artsen of dergelijk ziekenhuispersoneel?
I: Nee.
R: Okee. Waar ik een beetje heen wil is, binnen dat inkoopproces is cybersecurity dus relatief nieuw. Ik ben benieuwd of je een gevoel had hoe belangrijk men dat acht? Hoeveel prioriteit krijgt dat?
I: Nog heel even terugkomend op je eerdere opmerking dat het relatief nieuw i**I**: Dat is heel erg afhankelijk van de instelling. Sommige instellingen zijn al lang bezig met een information security management-framework. Die zijn misschien al gecertificeerd tegen de NEN-7510. Die hebben dat misschien al tien, zo niet meer jaren in place om bepaalde eisen te stellen aan een leverancier. Terwijl juist andere partijen net beginnen met een Excelsheet die ze aan een leverancier aanbieden van ”Vul dit eens in”. Dat even vooropgesteld. En wat was je tweede vraag?
R: Wat voor prioriteit geniet cybersecurity naast andere requirements?
I: Dat ligt heel erg aan de, dat klinkt misschien vreemd, maar dat ligt vaak aan de positie en het mandaat dat aan de CISO wordt gegeven in de organisatie. En natuurlijk ook het stukje persoonlijke expertise van die persoon. We hebben een aantal van onze deelnemers waarbij de CISO eigenlijk onder de IT-manager is gepositioneerd. Daardoor zie je wel eens dat er wat slagkracht mist. Dan wordt de CISO soms geïnformeerd, of die probeert zichzelf te betrekken bij X. Terwijl andere organisaties, daar zit de CISO meer op het board-level, of direct onder de CIO. Die heeft daardoor meer inspraak in het aanpassen van processen. Dat wil zeggen dat, in sommige instellingen, een CISO een inkoopproces kan stoppen op het moment dat het niet voldoet aan de gestelde eisen. Of als men er niet uit kan komen, dat wil zeggen dat de leverancier niet kan of niet wil tegemoetkomen aan bepaalde eisen.. Afhankelijk van wat de CISO daarin te zeggen heeft, kan het zomaar zijn dat een inkoopproces dan stilvalt. In andere gevallen rent de CISO als het ware achter het inkoopproces aan en deelt zoveel mogelijk

papieren uit aan het inkooptraject, in de hoop dat leveranciers, in ieder geval voor zijn administratie, wat willen invullen. Om zo een beetje grip op de zaak te krijgen. Dus het verschilt heel erg per instelling welke prioriteit dat heeft. Dus bij sommigen is het een harde nee als ze er niet aan voldoen, en bij anderen komt het eigenlijk na het besluit, komt security nog even langs met: ”Voldoen jullie hieraan of niet?” Divers landschap.
R: En in de situatie waarin security dan iets minder meetelt, geeft dat dan ook meer moeilijkheden voor IT?
I: Ik denk niet dat ik daar data over heb. Ik kan me vanuit functioneel oogpunt heel goed voorstellen dat, los van security en functionele eisen, als je hebt afgesproken dat in jouw hele omgeving alle verbindingen ten minste met TLS-1.2 (beveiligingsprotocol) worden gedaan, en een stuk software of hardware heeft alleen oudere ciphersuites die hij ondersteunt, dan zal IT er waarschijnlijk een mouw aan moeten passen. Maar dat gaat dan vaak ook weer denk ik hand in hand. In de zin van, als bij het inkoopproces security al niet zo’n dingetje is, dan zullen bepaalde andere security-eisen in de organisatie ook niet zo krachtig zijn. Maar dat is een aanname.
R: Dan nog even terugkomend op het moment als een apparaat of systeem al in gebruik i**I**: Weet je of er ook evaluatietrajecten voor apparatuur of systemen worden uitgevoerd? Of die er zijn? Worden jullie daarbij betrokken?
I: Of dat voor soft- of hardware gebeurt, dat weet ik niet. Wat wij wel eens terugkrijgen is dat men een soort vulnerabilityscan op het interne netwerk doet of laat doen, waarbij dan bepaalde stukken soft- of hardware naar voren komen. Voor het één-op-één, dus voor één type hardware of stuk software, dat weet ik niet. Het komt wel eens voor dat iemand zegt: ”Wij zijn aan het PoCen (Proof of Concept runnen) met een tool” of ”We hebben dit al enige tijd in huis, en we zijn nu een vulnerabilityscan aan het doen, en dat hele apparaat dat kapt er mee als er een scan langskomt”. Dat is niet zo netjes als dat gebeurt, en dan heb je dus wel iets van een evaluatie van een product, maar op een zijdelingse manier. Of ze het per stuk doen, weet ik niet.
R: Dan heb ik ook nog een paar vragen over cloud-based systemen. Kun je misschien iets vertellen over waarom mensen de keuze maken om voor een cloud-based optie te gaan, in plaats van iets in-house?
I: Dat kan een aantal redenen hebben. Een ervan is capaciteit van de IT-afdeling. In een ziekenhuis van 2000-2500 FTE is een IT-organisatie ergens tussen de 50-100 man. Dus een substantieel aantal mensen. En dat is een bepaalde kostenpost. Je moet ze opleiden, dus in sommige gevallen kan het gewoon kosteneffectief zijn om veel van je IT-infra uit te besteden of in de cloud te hangen. Daarnaast hebben ook veel cloudpartijen en datacenters die gebruikt worden, die hebben dat als core business. Daardoor kunnen ze zich veel meer focussen op het dichtdraaien van systemen, het certificeren van hun infra tegen allerlei beveiligingseisen en beschikbaarheidseisen.
I: Dat kan ertoe leiden dat een cloudpartij betere voorwaarden kan creëren voor een ziekenhuis die dat niet als core business heeft. Laat staan het certificeren ervoor. Dus dat heeft redelijk wat aanlokkelijke kanten voor veel instellingen, omdat ze een deel niet meer zelf hoeven te doen, en het soms, in ieder geval voor de eerstkomende vijf á tien jaar, ook wel goedkoper kan uitvallen. Dus het zijn wel overwegingen. Maar er zit nog wel een stigma omheen in mijn ervaring. Ik denk niet dat veel ziekenhuizen aan de klok hangen dat ze hun EPD in de cloud hebben hangen.
R: Ik ben ook wel benieuwd: als zo’n organisatie dan wel voor een cloud-based oplossing gaat... Hoe zien zij dan die cybersecurity? Je noemde net dat die organisatie zelf dan veel beter in staat is om dat te doen. Is dan de houding van het ziekenhuis van: ”nou, dat is dus hun probleem?”.
I: Nee. eigenlijk alle partijen die ik ken, die een EPD in de cloud hebben staan, die zijn daar erg voorzichtig mee te werk gegaan. Logisch natuurlijk, zou je denken. Maar die hebben wel uitgebreide trajecten gehad. Voor implementatie kan zo’n traject rustig twee jaar duren. En dan is daar uitvoerige discussie over de beschikbaarheidseisen, hoe wordt data beveiligd, hoe gaat de backup gebeuren, is er een failover-system [backup kloon systeem], staat het in twee datacenters, is er certificering aanwezig. Het gevoel van ’over de schutting gooien’ heb ik niet geproefd. Dat wordt wel stevig begeleid, in mijn ervaring.
R: Dat zijn dus ook requirements die van tevoren bij zo’n cloud-based aanschaf ook naar voren komen? Dat wordt vanuit de koper gesteld?
I: Ja. In het voorbeeld wat ik schets, heeft dat betrekking op EPD. Of dat traject even scherp is bij andere applicaties, dat weet ik niet. Maar, de meeste partijen die een deel van de infra in de cloud hangen, die hebben wel afspraken en beleid rondom de afweging of iets in de cloud moet of dat het

intern moet gebeuren, en wat de eisen daar dan voor zijn.
R: Dan heb ik nog een vraag over het initiëren van zo'n hele aankoop. Is het ook wel eens zo dat een aankoop echt puur cybersecurity-gemotiveerd is?
I: Ja, dat komt dan ook vaak vanuit het security-team. Stel, men begint met het pen-testen [penetratie-testen] van een aantal interne applicaties in de interne organisatie, of het scannen van kwetsbaarheden. Vervolgens wordt er met de leverancier gepraat: "we zien dit en dit, kan dat worden opgelost?" en de leverancier die is daar niet zo receptief voor, dan wordt er wel eens de vraag gesteld of er een misschien een vervangend product voor is dat wel in 2020 leeft. Om die security goed te doen. Dat komt voor.
R: Dus dat is in die zin wel, het kan echt een motivatie zijn?
I: Ja.
R: Ik heb het hoofdgedeelte hiermee wel gedekt. Ik heb nog een laatste vraag voor je. Zijn er nog andere factoren die nog niet echt benoemd zijn vandaag, die de cybersecurity in dat inkoopproces beïnvloeden?
I: Compliance. Wet- en regelgeving. Als je persoonsgegevens in een systeem verwerkt, dan komt de AVG om de hoek kijken. De AVG die heeft ook onderdelen die vragen om passende beveiligingsmaatregelen. Als je een BSN-nummer in de zorg verwerkt, dan moet je iets met de NEN-7510. Dat betekent een heleboel dingen, en onderdeel daarvan is dus ook een goed inkoop- en leveranciersrelatietraject. Het kan zomaar zijn dat een deel van de motivatie van cybersecurity zo'n inkooptraject is. "We willen compliant raken aan deze normering en de juiste beveiligingsmaatregelen hebben. Dat betekent dat het inkoopproces onder de loep moet worden genomen. Dat kan ook nog een driver zijn om daarmee aan de slag te gaan.
R: Dankjewel. Dan heb ik voor de informatie die ik zocht, dus ik ga afsluiten.

B.4. Transcript 4

Researcher designated "R", interviewee designated "I". Note: Some sections of the recording of this interview were of poor quality and could not be transcribed.
R: Dank voor je tijd vandaag. Eerst nog wat formaliteiten. Als het goed is, heb ik je een formulier toegestuurd met hoe ik de verzamelde data ga verwerken. Geef je hierbij toestemming dat dat ik je data verwerk zoals op dat formulier staat?
I: Ja.
R: Laten we beginnen met een achtergrondvraag. Kun je me wat vertellen over je functie en je ervaring met inkoop binnen ziekenhuizen?
I: Ja. Ik zit al vier jaar binnen [organisatie] als Senior Inkoper, waarvan drie jaar als IT Inkoop.
[...]
R: Dankjewel. Het is misschien handig om een voorbeeld te pakken van een inkoopproces waar je bij betrokken bent geweest. Kun je zo'n proces noemen?
I: Op dit moment ben ik bezig met het aanschaftraject van een softwareproject voor de...
R: Kunt u dat herhalen? De verbinding viel even weg.
I: Ik ben bezig met [de aanschaf van] een intrusion detection-tool.
R: Kun je me wat vertellen over de redenen om met deze aankoop te starten?
I: Binnen [organisatie] hebben we sinds drie jaar geleden een EPD draaien. Om dat draaiend te krijgen hebben we tien jaar daarvoor een ICT-freeze gehad. We hebben nu dus een flinke berg werk te doen.
[...]
I: We gaan een softwarepakket voor Security Information and Event Management aanschaffen
R: Wat voor pakket van eisen wordt daaraan gekoppeld? Wie komen daarbij kijken?
I: PvE, daar hebben we een Lead Architect, [...], er zit een Security Officer bij, iemand van privacy, Inkoop, [...], het hoofd van de Medische Techniek, een Solutions Architect, dus het is een hele keur aan mensen die direct betrokken worden bij zo'n zaak. Ook de leverancier is wel betrokken, [...].
R: Dat zijn flink wat verschillende partijen. Is het de afdeling Inkoop die dit coördineert en zorgt dat elke partij op het juiste moment wordt aangesproken?
I: Nee, we hebben gekozen om dit als ICT-afdeling zelf helemaal geïmplementeerd te krijgen. [...] Bij Medische Microbiologie is aangegeven dat ze [...]. Dat verzoek hebben ze gedaan bij de afdeling ICT. Die hebben een hele zware implementatie gehad. Het aanschaffen van het pakket is niet zo moeilijk, het is echt het organiseren en implementeren van het pakket waar de focus op zit. Er zit een zware

ICT-kant op, een zware organisatorische component, een zwaar security-deel. Daardoor is er ook een projectleider op gezet. [...]
R: Naar hoeveel verschillende opties wordt bij zo'n aanschaf gekeken?
I: Dat ligt sterk aan wat we willen aanschaffen. We hebben met deze infectie-preventietool, daar is het maar net hoe we dat specificeren. Als je zegt: "ik wil technisch een beetje investeren, want ik wil dit en dat pakket met en die specificaties", dan heb je dus technische specificaties waarmee je enkel en alleen maar bij een bepaalde leverancier terechtkomt. [...] Als je dan functioneel specificeert, dat is dus eigenlijk veel meer dat je gaat nadenken over de functies die je wil... Stel je zegt: "ik ben gewend om met dit programma te werken", dan hoor je vaak zeggen: "ik wil DAT". Als je iets functioneel gaat specificeren, dan moet je weer gaan nadenken van: "we hebben dit programma, wat moet dat nou eigenlijk doen?" "Hoe formuleer ik dit leverancier-neutraal?" "Klopt datgene wat we hebben opgeschreven?". Dan zie je dat de eindgebruiker niet goed in staat is om in functionaliteiten te beschrijven.
R: Die zijn dus meer geneigd te specificeren op een specifiek product?
I: Ja. [...] Zeker bij een universitair ziekenhuis...
[Call was interrupted and resumed]
The recording of the resumed call was inaudible and impossible to transcribe. Included below are the personal notes made during the interview:

- Procurement process is structured using procedures and guidelines, but these are not always followed.
- External motivation for purchase can come from suppliers selling an upgrade to an existing system.
- Explicit mention of technical specification lock-in, and supplier lock-in.
- Interview subject prefers cloud-based services, because this transfers responsibility for services to the supplier.
- Decision to outsource to cloud-based or run something in-house lies with tech department.
- Hospitals are a "collection of businesses".
- Ways to divide these 'businesses' are: university/education vs medical services, medical vs support, others.
- Organisation described as network organisation. Challenge is finding and connecting the right people. Governance is a big challenge in this context.
- Priorities in procurement lie with patient care, privacy and security, and after a set of criteria come the interests of the Purchasing department. Well-developed contracts and reasonable pricing are not the most important.

B.5. Transcript 5

Researcher designated "R", interviewee designated "I".
R:Voordat we beginnen, moet ik wat formaliteiten afwikkelen. U heeft het toestemmingsformulier toegezonden gekregen. Stemt u ermee in dat ik dit interview verwerk zoals aangegeven op dat formulier?
I: Ja.
R: Top, dankuwel. Ik zou graag beginnen met een paar achtergrondvragen. Kunt u mij vertellen wat uw functie is binnen uw organisatie, en wat uw ervaring met inkoopprocessen is?
I: Mijn functie binnen [mijn organisatie] is Chief Information Security Officer. In de afgelopen 15 jaar ben ik onder andere ook IT-manager geweest. In [mijn organisatie] zie ik regelmatig zaken voorbij komen qua beveiliging en privacy, in het proces van de aanschaf.
R: Dankuwel. Dat proces van aanschaf, daar bel ik dus vandaag over. Mijn doel is een goed beeld krijgen van het verloop van dat proces, en hoe ver ziekenhuizen zijn met de integratie van cybersecurity daarin. Kunt u voor mij een voorbeeld noemen van een recente aanschaf waarin cybersecurity een factor was? Het mag er ook een zijn waarin dat niet per se zo was.

I: Dat is niet zozeer het probleem. Het probleem is dat ook cybersecurity geadresseerd wordt als ik er niet bij betrokken ben, omdat we dat inmiddels in het proces verweven hebben.
R: Dat zit al geïntegreerd?
I: Ja.
R: Hoe ziet die integratie er dan uit?
I: Dat is dusdanig gevormd dat de afdeling Medische ICT een standaard programma van eisen (PvE). Dat standaard PvE, daar zitten ook de cybersecurity-onderdelen in verweven. Bij alle aanschaf wordt bij ons cybersecurity meegenomen.
R: Dus in het standaard PvE zijn daar requirements voor gesteld?
I: Ja.
R: Weet u toevallig ook wat voor requirements dat zijn? Is dat certificering, of eigen definities misschien?
I: Toevallig hebben we recent een revisie gehad. Ik kan heel even kijken of ik die erbij kan halen. Het heeft onder andere te maken met de versies van de besturingssystemen. Wij stellen minimale eisen aan de besturingssystemen in het PvE. Ik moet even door deze lijst heen lopen, want ze staan niet als zodanig genoemd als security-eis.
R: Als vervolg op de eis over de versies van het besturingssysteem: hoe reageren suppliers als je dat soort eisen stelt?
I: Dat is verschillend. Met name aan de medische kant is het nog vaak een probleem. Medische systemen worden eigenlijk van oudsher opgeleverd as-is. Ze kennen een goedkeuringstraject van een jaar of vijf, dus worden ze bijna altijd standaard met verouderde software geleverd. Tenminste, dat was in het verleden zo. Dat wordt beter en beter. Het komt steeds minder vaak voor dat we daar uberhaupt iets mee moeten doen. Dit is wel een eis waar we de kansen hebben om wat aanvullende maatregelen te treffen als het niet mogelijk is. Dus de eerste keus is een leverancier die wel aan die eisen voldoet, maar stel dat alle leveranciers niet aan die eisen kunnen voldoen, dan zullen we moeten gaan onderhandelen wat wel mogelijk is en dan zie je vaak dat er maatregelen worden getroffen ofwel zijn. Dat is bijvoorbeeld hardening: dan is het misschien een iets ouder besturingssysteem, maar dusdanig uitgekleed dat daar heel veel andere functionaliteiten 'uitgesloopt' zijn. Dat zie je bij een leverancier als Siemens. Dat neemt heel veel risico's weg. Soms worden aanvullende hardware- of softwarecomponenten geïnstalleerd, door de leverancier, die ook die maatregelen vervangen van het bijwerken [van software]. Of we besluiten zelf om bepaalde maatregelen te treffen - dan moet je denken aan segmentering of het inbouwen van een intrusion prevention system.
R: U noemde een trend dat het wel iets beter gaat met de security aan de leverancierskant. Wat zijn daar de drijfveren achter geweest?
I: Ik ben in [jaar] begonnen met het PvE, om daar die securityzaken in te adresseren. Toen stonden ze daar echt heel raar van op te kijken. Dan kreeg je meer vragende ogen dan wat anders, en was het bijna altijd onderhandelen van "wat bedoel je dan?". Overigens wel een voordeel, want dan ben je tenminste al aan het onderhandelen. Dus daar helpt het al in. En "jullie zijn de enigen die dit vragen", dat zou best kunnen dat we enige waren die dit vroegen. Dat laatste argument hoor ik al jaren niet meer, "jullie zijn de enigen die dit vragen". Dat is er echt uit. Dat argument wordt niet meer gebruikt. Ik heb wel het idee dat het door de markt komt, omdat collega's met mij leveranciers daarom vragen. Ik moet wel zeggen, de komst van de AVG heeft daar ook een flinke boost in gegeven, omdat vaak het contract vergezeld moet worden van een (data)verwerkingsovereenkomst. Daarin moeten maatregelen bij gedefinieerd worden en dan staat het ineens zwart-op-wit. Dan moeten ze aangeven dat ze technische en organisatorische maatregelen getroffen hebben om de beveiliging goed te regelen, omdat ze compliant moeten zijn met de ISO-27001 of NEN-7510. Dan zullen ze moeten steken of snijden. Het is eigenlijk beiden. Ik zag het al ingezet toen het echt de markt was, maar regulering vanuit de overheid heeft een flinke boost gegeven. Die boost komt voor medische apparatuur trouwens net zoveel uit de VS. In 2017 heeft de Food & Drug Administration daar al een duidelijke uitspraak over gedaan, dat het bijwerken van software geen reden is om een apparaat niet goed te keuren, of andersom, dat je goedkeuring ook niet mag gebruiken om te zeggen "daarom patchen we niet". Dat maakt dan wel indruk op Amerikaanse leveranciers.
R: Die moeten dan aan de lokale regulatie voldoen en dat echoot dus door overzees?
I: Ja, we hebben natuurlijk te maken met veel Amerikaanse leveranciers in de medische wereld.
R: Als het gaat om de aankoop van een medisch apparaat, wie zijn er allemaal bij betrokken bij het overwegen van verschillende ontvangen proposals?

I: Als het echt gaat om een medisch apparaat, dan zijn daar de klinisch fysici in de lead. Zij betrekken daar de klinische informatici bij. Het zijn meer de informatici-managers, moet ik zeggen. Maar ook medisch-technici en natuurlijk de aanvrager, degene uit het proces zelf, die het product nodig heeft. Zodra het bepaalde netwerkcomponenten betreft, dan wordt het overlegd met de IT-architect. Dan specifiek vaak de IT-architect die ook security in zijn portefeuille heeft, omdat het netwerkcomponenten zijn en netwerken en security gaan vaak hand in hand. Als het er discussies zijn, dan wil ik er ook nog wel eens bij betrokken worden - dus als een leverancier niet wil of niet kan, et cetera.
R: Hoe zit dat met leveranciers die al equipment bij jullie hebben staan? Genieten die voorkeur?
I: Dat zou ik niet weten.
R: Als er naar verschillende proposals wordt gekeken, wat voor criteria komen daarbij kijken, en hoe zwaar wegen die ten opzichte van elkaar?
I: We hebben eisen en we hebben wensen. Dat is het zo'n beetje. Verder zijn ze niet veel belangrijker of minder belangrijk. Wat het wel is, is dat er eisen zijn waarover we in gesprek kunnen gaan als er alternatieven zijn. Het is heel moeilijk om daar een keihard statement in te nemen, omdat je eigenlijk de risico's weg wil nemen. Vaak kun je risico's op meer dan één manier wegnemen. Vaak gebruik je ook wel meer dan één manier, je wedt niet op maar één paard. Dat zit op het technisch vlak. We hebben het eerder gehad over het patchen, maar het betreft ook de security die op endpoints wordt geïnstalleerd. Of een stapje verder, of het systeem geschikt is om vulnerability-scanning te pareren. Als wij ons netwerk gaan afscannen of er gevoelige apparatuur op staat, dat die apparatuur dan niet daar alleen al op onderuit gaat - dat is in het verleden nog wel eens gebeurd met medische apparatuur. Maar ook de mogelijkheid tot een testomgeving is belangrijk, zodat je niet direct in je productieomgeving in hoeft. Dat kan inhouden dat een medisch apparaat de mogelijkheid heeft om bepaalde waarnemingen naar een product door te sturen, of dat er zelfs een testapparaat beschikbaar wordt gesteld. Dan hangt af van wat we aanschaffen. Een PET-scan, waar we er maar één van hebben, dan zeggen we niet "laten we op voorhand maar eentje extra nemen zodat we wat kunnen testen". Met echografen, waar we er heel veel van hebben, daar gebeurt dat bijvoorbeeld wel.
R: Als een apparaat is aangeschaft en in bedrijf is, is er dan een evaluatietraject? Worden bijvoorbeeld security-aspecten gemonitord?
I: We ondernemen wel wat stappen. Om te beginnen, als een apparaat aangeschaft is, dan zal het geïmplementeerd moeten worden en dan passeert het ons change advisory board. Die gaan onder andere kijken of er aan alle randvoorwaarden voldaan is, en of de planning past in de andere wijzigingen die doorgevoerd worden. Zo voorkomen we dat we twee grote wijzigingen tegelijkertijd in een weekend plannen. In die board heb ik ook een plek. Dus voordat iets geïmplementeerd wordt, zie ik het design nog voorbij komen, zie ik of alle risico's in kaart gebracht zijn. Dat doe ik zelf. Dat is een wekelijks overleg waarin we dat voorbij zien komen. Die beveiliging wordt opgenomen in ons information security managementsysteem. Alle maatregelen die nieuw getroffen worden, worden daarin opgenomen. Er wordt ook op gezette tijden opnieuw uitgevraagd of [die maatregelen] nog actueel zijn. Dat is een geregeld mechanisme. Ongeregeld is het vulnerability scanning of een penetration test, maar ook een audit op een afdeling, waarin we kijken, ongepland of meer ongestructureerd, of alles er nog goed bij staat en aan de juiste eisen voldoet.
R: Dus dat soort maatregelen zijn niet zozeer op een specifiek apparaat gericht, maar geconcentreerd per afdeling, als ik het goed begrijp?
I: Ja. De reguliere maatregelen die er zijn, zijn het patchmanagement - we hebben een cyclus waarin we elke maand de nieuwe uitgekomen patches beoordelen en testen, en uitrollen op diverse apparaten. Dat geldt voor medische maar ook voor niet-medische apparatuur. Er loopt ook nog een stroom vanuit z-CERT. Als wij een advisory krijgen van z-CERT dat er een kwetsbaarheid zit in een systeem, dan wordt die bij ons bekeken door de IT-architect en mijzelf. Wij bepalen dan of er een noodzaak is om die sneller op te vangen dan met het reguliere patchregime. Dan wordt dat als risico aangemerkt en dat wordt dat ook in dat wekelijks overleg met de change advisory board bekeken. Dat wordt dan geklassificeerd, en als het nog sneller moet, als we denken dat het om een heel groot risico gaat, dan lopen we langs die procedure en hebben we een versnelde uitrol om een kwetsbaarheid te verhelpen. Dat is hooguit één keer per jaar.
R: Ik wil nog wat vragen over dat patchmanagement. Vroeger is dat nog al eens moeilijk geweest omdat suppliers lastig deden over toegang verschaffen op hun apparaten. Is dat inmiddels veranderd?
I: Daar is wel duidelijk een trend in zichtbaar. Je ziet meer en meer software-oplossingen komen. Waar in het verleden een PACS-systeem [medisch röntgenbeeldensysteem] geleverd werd met service en

kosten en alles erbij als zijnde één aanschaf, daar zie je nu meer dat wij eigen apparatuur, eigen installaties mogen doen en dat er dan los software op gezet wordt die het regelt. Dat zie je duidelijk ontstaan. De tweede trend die je ziet ontstaan, is dat er veel meer gebruik wordt gemaakt van cloud-applicaties, dus dat de leverancier verantwoordelijk is voor het patchregime. Wat we ook nog steeds zien, is dat wij bepaalde apparatuur in huis hebben, die onderhouden wordt door leveranciers.
R: En hoe gaat dat in zijn werk? Sommige apparatuur is niet goed beschikbaar om te patchen.
I: Dat is een kwestie van plannen.
R: Het lukt wel, om dat tijdig te regelen.
I: Ja, de spoedzaken wel, als het nodig is, is het nodig en dan wordt er tijd voor vrijgemaakt. Het is ook maar zelden dat het patchen van een systeem een paar uur duurt. Meestal hebben we het over een paar minuten ofzo. Het is ook niet zo dat we 247 in operatie zijn. Plekken genoeg waar je na vijf uur vooruit kunt, of in het weekend vooruit kunt, of tussen de middag. Daar valt vrij veel mee te doen. Het is niet makkelijk, het moet allemaal ingepland worden. Je kunt niet zomaar een behandeling stoppen. Meer en meer zijn we daarin naar vaste momenten aan het gaan waarin we patchen, omdat beter te reguleren.
R: Dat is met de supplier te coördineren?
I: Zeker, nou ja, de meer volwassen suppliers komen zelf met een maintenance schedule. Op die vaste momenten komen zij langs om patches te installeren. Als er spoed is, dan ga je langs alles, maar dan is het ook spoed.
R: Dus er zit een schifting in suppliers in volwassenheid?
I: Ja, zeker.
R: Sommige suppliers schikken zich dan meer naar jullie schema, of ze hebben geen capaciteit? Waar zit dat verschil in?
I: Dat is vrij divers. Je hebt de wat grotere leveranciers die heel hautain zijn en zeggen: ”It’s our way or the highway”. Die heb je erbij. Je hebt ook hele grote leveranciers die klantgericht meedenken en juist meer met ons werken. Het is niet per se dat groot dat beter of slechter doet dan klein. Het is wel dat het bij de grotere een kwestie is van wel of niet willen, en bij de kleinere gaat het om wel of niet kunnen. Dus de incentive om niet mee te werken is anders.
R: Ik wil graag nog inhaken op het thema ’cloud-based’. Wat drijft de beslissing om iets cloud-based te gaan, tegenover iets on-premises te gaan doen?
I: Een belangrijke is wanneer een leverancier zegt: ”We stoppen met het on-premise aanbieden en we gaan alleen maar cloud-based aanbieden”. Een andere reden is wie het systeem kunnen patchen. De derde reden is het beschikbaar maken van de apparatuur of software buiten de contouren van het ziekenhuis. Als je denkt aan thuisdialyse-apparatuur, dan is het veel makkelijker om die aan een cloud-applicatie te linken, dan om een gat te schieten in je firewall om te zorgen dat je met een datacenter kan verbinden.
R: Dus dan ligt de securityverantwoordelijkheid ook sterk bij de cloud provider?
I: Nou, de verantwoordelijkheid ligt bij het ziekenhuis, want wij zijn verantwoordelijk voor de data. Wij verleggen dat naar de leverancier; we stellen eisen aan die leverancier en we toetsen die eisen op gezette tijden. Dat gaat niet heel diep, maar wij vragen het liefst certificaten op dat leveranciers geaudit zijn. Ook op gezette tijden testen wij, vrij eenvoudig, hoe de basissystemen erbij staan: of ze gepatcht zijn of niet, dat kun je aan de buitenkant vrij goed zien.
R: Ik wil ook nog ingaan op het uitwisselen van kennis. Ik begrijp dat z-CERT daarin onder andere een rol speelt. Als je kan kiezen tussen verschillende suppliers, in hoeverre worden dan informatie of ervaringen van andere ziekenhuizen gebruikt?
I: Wat gebeurt, is dat wij onderling overleggen: ”heeft iemand al ervaringen met een dergelijk product” en zo ja, welke? Dan zit je een stap eerder, en moet de leverancier uberhaupt nog gekozen worden. Dat is hetgene wat het meest gebeurt.
R: Dat is dan productspecifiek, of gaat dat ook meer algemeen over suppliers?
I: Meestal is het productgericht, dus van ”wie heeft er al ervaring met zulk soort producten?”. Daar wordt dan vanzelf de leverancier meegenomen die daarbij hoort. Ook andersom gebeurt dit. Als je al een leverancier in huis hebt dan willen we ook nog wel eens uitwisselen hoe je een leverancier zo ver krijgt dat hij meewerkt. Of we vragen of iemand iets al voor elkaar heeft gekregen. Wat we ook doen, is vragen of iemand anders een leverancier al eens heeft getest. Dan hoef je dat niet nog een keer te testen. Daar zijn zowel leveranciers als ziekenhuizen bij gebaat.
R: Dus onder andere worden testprestaties onderling uitgewisseld en daar wordt waarde aan gehecht?

I: Ja.
R: Als er voor een cloud-oplossing wordt gegaan, waar in het proces gebeurt dat? Kan dat een uitgangspunt zijn, of is het meer één van de overwogen opties?
I: Dat laatste vooral.
I: Er is wel een shift naar de eerste variant, dat je ziet dat cloud in sommige gevallen een voordeel heeft voor de functionaliteit, maar dat is nog niet zo vaak. Als je die thuisdialyse neemt, dan is het functioneel makkelijker om te doen, maar eerlijk gezegd, meestal is het aanbod-gedreven. We kiezen daar dus niet echt zelf voor, maar het is wat een leverancier aanbiedt.
R: Stel je koopt een medisch apparaat, dan is de afdeling die dat aanvraagt daar een onderdeel van. Hoe kijken zij tegen die security-eisen aan?
I: Lastig. Hoe verder je teruggaat in de lijn, hoe meer mensen gefocust zijn op de functionaliteit. Security is geen functionaliteit, dat is meer een continuïteitsvraagstuk. Daar zijn ze niet in geïnteresseerd. Ze snappen het steeds beter, moet ik zeggen, dat is wel duidelijk zichtbaar. Datzelfde geldt ook voor privacy. Maar het is niet hun eerste prioriteit, die zit in de functionaliteit. Veel van de beslissingen over security worden ook wat verder in het traject genomen. Dat wordt door wat techneuten genomen en die gaan wel met de leverancier om tafel om te zorgen dat als een apparaat er dan komt, dat het dan veilig komt. Daar zijn de aanvragers niet altijd bij betrokken, maar soms heeft het wel een financiële impact, dat we daarin meer op hun budget drukken, omdat er wat security-features bij moeten komen.
R: Komt het voor dat aankopen dat security-traject niet goed doorlopen?
I: Ja. Dat wordt ook steeds minder, omdat het net steeds strakker gespannen wordt. Dat zie je bijvoorbeeld ook met dat change advisory board. Heb je het verkeerd aangeschaft, dan moet het vervolgens geïnstalleerd worden en krijg je daarna de deksel op je neus. Dan heb je budget gekregen voor één bedrag en gaan ze daarna zeggen dat daar nog een gelijke som bovenop moet aan security-maatregelen. Dan moet je terug naar de Raad van Bestuur om extra geld te vragen, en dat vinden ze helemaal niet leuk. Dus dat passeren van de procedure wordt steeds minder. Eerlijk is eerlijk, het gebeurt nog wel.
R: Loopt dat proces meer direct tussen de afdeling en de supplier?
I: Nee, het proces wat ik omschrijf is vooral als het ICT-gedreven is. Als het niet ICT-gedreven is, of als je zegt dat je de afdeling ICT niet per se nodig hebt, dan wil het nog wel eens fout gaan. De afdeling ICT heeft een eigen inkoper, die snapt dat allemaal. Je zou natuurlijk een cloud-applicatie kunnen aanschaffen zonder de IT-afdeling erbij te betrekken. Als je dan een inkoper hebt, een reguliere inkoper, die dat niet door heeft gehad [dat ICT betrokken moest worden], dan kun je nog wel daartegenaan lopen. Of als een medisch specialist uit eigen zak dingen betaalt, dus niet vanuit het budget van het ziekenhuis. Meestal als het ziekenhuis het moet betalen, dan gaat het wel goed. Vrij gevestigde specialisten kunnen ook dingen aanschaffen.
R: Wat voor apparatuur moet ik dan aan denken?
I: Dat is dan niet zozeer apparatuur, meer software. Als het apparatuur is, dan is het goed geregeld. Dat heeft ook met veilige toepassing van medische techniek te maken. Daar brandt niemand zich aan. Daarin worden ook veel zorgen uit handen genomen. De aanvragers hebben een hekel aan al die regeltjes, maar dat wordt in dat proces ook aan hen weggenomen. Dus het heeft ook voordelen om het via het reguliere proces aan te schaffen.
R: Hoe wordt binnen het ziekenhuis over de cloud gedacht? Sommigen zijn fan, anderen zijn terughoudend.
I: Hoe ik dat zelf zie, of hoe onze organisatie dat ziet?
R: De organisatie.
I: De organisatie gaat langzaam wat meer de kant van cloud op. Er wordt niet meer standaard gekozen voor on-premise. Waar dat in het verleden wel zo was, moest alles on-premise en moesten leveranciers zich af en toe in de gekste bochten wringen om het in de cloud te krijgen. Dat is wel omgedraaid. Als er nu een goed cloud-product is, dan kan daarvoor worden kozen.
R: En uw eigen mening?
I: Er zitten grote voordelen aan cloud, maar dan heb ik wel een voorkeur voor de private cloud, en niet de public cloud. Daarmee heb ik wat meer moeite. Dat is vooral eigenbelang - ik heb veel meer moeite om public cloud te controleren dan om private cloud te controleren.
R: Dan heb ik tot slot nog een wat algemenere vraag. Zijn er nog elementen die de security in het inkoopproces beïnvloeden, die we nog niet benoemd hebben?
I: Nee, volgens mij niet.
R: Daarmee is het dan denk ik voldoende voor mij, dus dan ga ik afsluiten.

B.6. Transcript 6

During this interview, the recording program failed. Instead of a transcript, the researcher's notes from the interview are provided below:

- Interviewee is a hospital CISO. He is responsible for information security within the hospital. He is currently working on getting the hospital certifiec for NEN7510, which is based on the ISO 27001 norm. Among other responsibilities, he is involved in controlling cybersecurity for an internet-exposed service that the hospital provides.
- The hospital employs [a large company] who provide a SOC-service (Security Operations Center). That is a form of active network security monitoring.
- Integration of cybersecurity in the purchase process is limited.
- This hospital uses a set process that includes risk analysis. If the risk analysis shows any high risks, then this may warrant performing a Business Impact Analysis as a follow-up.
- In most Programs of Requirements, IT requirements are included.
- This hospital schedules annual penetration tests. These are provided by either an external party or even by the supplier of a specific product.
- An example of a monopolized service had to do with an organisation that provided EDI (Electronic Data Interchange) between the hospital and general practitioners. There used to be only one such provider, monopolizing this service. This hospital went looking for another party to provide this service, to break up the monopoly position of this provider and obtain more favourable conditions. They were joined by several other hospitals at this new EDI provider.
- One monopolistic party was bought out by an investment firm, which resulted in them doubling their prices. They were in a position to do this because of their monopoly.
- This hospital engages in knowledge exchange with other hospitals, among other sources through Z-CERT.
- The interviewee cited a cultural conflict between the general IT department and the Medical IT department. In the context of cybersecurity, the IT department is focused on mitigating newly found vulnerabilities or threats. The Medical department is mostly concerned with ensuring equipment remains operational. The interviewee stated that Medical IT sees updates or patches as risks, quoting a mentality of ”If it's working, then don't touch it”. Both communicate to get things done, but all of the above sometimes results in a feeling of ”Here they come again”.
- Previously, this hospital pursued a minimum of connectivity of equipment. Now, devices are increasingly connected and patched. This shift was caused by the 2017 FDA ruling about medical device patching.
- Smaller suppliers usually focus on functionality, not on non-functional requirements like cybersecurity.
- The interviewee observed a trend where these smaller players are disappearing due to being unable to conform to new regulation. The interviewee explicitly mentioned European certification (CE) as a factor. The result is that only larger players remain.
- Hospitals are increasingly entering into cooperation with larger suppliers, meaning they purchase primarily equipment from that supplier.
- When large suppliers are asked about cybersecurity, some have a standard answer ready and are willing to cooperate. Others enter into a discussion and push back strongly.
- Large suppliers with answers ready about security features often specific offers to deal with it. These offerings range from security features being included in the standard product, or can take the form of additional costs to enable patching.

- Involved parties in setting requirements are (among others) requesting department, requesting department management, facility director, financial personnel.
- The interviewee mentioned not always getting his way (thereby not satisfying his requirements). When that happens, additional measures are taken, the risk is insured against, or the risk is accepted.
- This hospital has vulnerability scans performed one or more external parties.
- Cloud services are mostly application-level systems, of the SaaS type.
- The interviewee mentioned cloud services can often be too expensive.
- Cloud services are sometimes engaged when specialized knowledge is needed that the hospital can't otherwise source by itself.
- Cybersecurity responsibility lies with the hospital and is contractually moved towards the cloud provider.
- There is no periodical evaluation of suppliers. The interviewee did indicate a desire to start doing this.
- Motivation for going to cloud-based solutions comes from suppliers moving their product into the cloud. Sometimes they offer a cloud solution and an on-premises version, sometimes they shift to offering their services exclusively cloud-based.

B.7. Transcript 7

Researcher designated "R", interviewee designated "I".
R: Kun je me wat vertellen over je positie binnen je organisatie en je ervaring met cybersecurity?
I: Zeker. Ik ben de CISO van het […] ziekenhuis. Ik zit sinds [een paar jaar] bij dit ziekenhuis. Ik had zelf geen ziekenhuiservaring voordat ik hier begon. Ik kom grotendeels uit het bedrijfsleven. Ik heb bij [een groot accountingbedrijf] gewerkt, en twee jaar bij een hele grote bouwonderneming. Altijd aan de security-kant. Security en compliance, en ook de hardcore technische kant. Ik ben [lange tijd] infrastructure manager geweest bij [bedrijf]. Daarna heb ik als security officer gewerkt, en ik zat in het second line of defence-team voor security en compliance voor Europa. Nu dus voor het eerst in het ziekenhuis, en ik val als CISO rechtstreeks onder de Raad van Bestuur, en ik rapporteer aan de voorzitter van de Raad van Bestuur, en ik zit ook samen met de privacy-mensen - Twee privacy-officers en een FG (Functionaris Gegevensbescherming). En daar bestaat het team eigenlijk uit. Dat is de structuur en zo ben ik daar terechtgekomen.
R: Dankjewel, dat is duidelijk. Kun je me wat vertellen over, als er een nieuw apparaat of systeem in het ziekenhuis wordt gekocht – wat voor vorm neemt cybersecurity daarbij aan?
I: Dat is wel tweeledig. Als je kijkt naar de AVG/GDPR, en dat is voor mij ook een grote… Redding wil ik niet zeggen, maar het helpt natuurlijk enorm mee met de borging van de informatiebeveiliging en privacy in het inkoopproces. Tijdens het inkoopproces is dat.. we kijken echt naar de borging van de juridische kant. Ik wil er trouwens wel bij benoemen, één van de grootste problemen die je hebt bij zo'n ziekenhuis, en ik denk dat je dit ook van andere collega's hebt gehoord, het is dat het vrij moeilijk is om ten eerste grip te krijgen op het inkoopproces. Dus wij zien dat er best wel veel contracten.. ik wil zeggen werden, maar dat het is nog steeds worden.. afgesloten met externe partijen, waarbij we dan toch te laat of niet worden aangekaart. Dus in de eerste instantie is het zo dat, we hebben een aparte inkooporganisatie. Die inkooporganisatie haakt ons eigenlijk altijd aan, maar het kan dus voorkomen dat HR op eigen initiatief iets inkoopt en dan hebben wij daar geen zicht op. Met betrekking tot de medische apparatuur, dat verloopt ook natuurlijk via de regels van de medische technologie. Daar zijn ook gewoon afspraken over. Ik heb goede contacten met de klinisch fysicus die gaat over de inkoop van die apparatuur. Die haakt ons eigenlijk altijd aan bij het inkoopproces. Wij kijken dus altijd mee naar de technische kant. Om een voorbeeld te geven: ik heb over twee uur een meeting met [leverancier], die natuurlijk heel veel apparatuur bij ons regelt. En het sluitstuk is uiteindelijk de verwerkingsovereenkomst en het DPIA (Data Protection Impact Assessment) die we natuurlijk uitvoeren. En op basis van die gegevens kan ik nog aanvullende informatiebeveiligingsmaatregelen laten toepassen.

R: Je noemde het net al: het gebeurt nog wel eens dat dingen gekocht worden en dat je daar dan niet bij betrokken wordt. Wat voor effect heeft dat achteraf? Hoe wordt daarmee omgegaan als er toch problemen ontstaan op het gebied van cybersecurity?
I: Dat hangt er wel vanaf. Wij kijken ook bij het inkoopproces, bij nieuwe systemen of applicaties, wat voor data gaat daarnaartoe? Wat voor informatie wordt er gedeeld? Is het een kritisch systeem, of staan er niet zoveel persoonsgegevens en vinden we dat dan een wat minder kritisch systeem? Op basis daarvan kijken we wel naar de apparatuur, naar de systemen. Komt er iets voorbij wat wat minder kritisch is, dan proberen we achteraf nog in ieder geval een verwerkingsovereenkomst en DPIA met die partij af te sluiten. Is het nou daadwerkelijk dat er iets gedaan is met een partij die bijvoorbeeld rechtstreeks in ons EPD (Elektronisch Patiëntendossier) iets kan doen – wat echt wel een redelijke impact op de privacy en informatiebeveiliging heeft – dan kunnen we ook desnoods het project of de applicatie stilleggen. Dat is gelukkig nog niet voorgekomen. Maar gaat dat langs ons heen en worden wij geïnformeerd.. Ik kan wel een voorbeeld geven, dat werkt wat beter. Een voorbeeld is dat HR nu, in verband met CoViD, extern een e-learningmodule heeft aangeschaft, en dus een partij heeft gevraagd van “Kunnen jullie dat voor ons maken?”. Dat is gebeurd, en die partij heeft al onze e-mailadressen van alle verpleegkundigen gekregen, en een mailtje gestuurd met “Jullie hebben nu toegang tot die omgeving, en kunnen hier een CoViD-training volgen.” Daar zitten wel gevolgen aan, want die partij heeft dan al onze e-mailadressen. We waren daar niet over geïnformeerd, en dat gaan we nu nog rechttrekken door middel van een DPIA en een verwerkingsovereenkomst. Daarbij kijk ik dus vooral naar de informatiebeveiliging. Maar zal het zo zijn dat we opeens een rechtstreekse koppeling hebben met een partij die iets in ons EPD gaat doen, dan zijn wij ook in staat om te zeggen: “Dit kan nu niet, dit moet stopgezet worden.” Het hangt wel van de kwalificatie van het systeem af, die dan ingekocht is.
R: Als we het hebben over aankopen waar je wel bij betrokken bent, daar komen veel verschillende criteria bij kijken en cybersecurity vormt daar een onderdeel van. Hoe belangrijk wordt cybersecurity gevonden, naast alle andere criteria?
I: Dat wordt als belangrijk gezien, gelukkig. Wel nu wat meer dan toen ik begon. Vroeger toen was dat nog niet zo. Toen was de CISO-rol er ook niet voor het ziekenhuis. Dat is een nieuwe rol en ik probeer daarin ook op een politiek handige manier ervoor te zorgen dat mensen dat ook inzien. Wij doen dat ook door middel van awareness-trainingen. Dus wij hebben trainingen die we voor het hele personeel uitrollen via een SaaS-applicatie (Software as a Service), waarbij we ook zeggen: “Er komt een nieuwe applicatie of een leverancier wil iets doen bij ons, let erop dat je alle informatiebeveiliging borgt en dat je wel met privacy contact opneemt.“ Dus.. wat was de vraag?
R: Hoe cybersecurity zich verhoudt tot andere criteria.
I: Dus op die manier, door middel van privacy en informatiebeveiliging en awareness-trainingen wordt dat dus wel gezien en wordt de meerwaarde gezien. Plus ook nog eens een keer, dat als er incidenten zijn, wat ook gewoon voorkomt niet alleen bij ons maar ook bij externe partijen, dan communiceren we daar ook bewust over. We zorgen dat we dan op intranet ook een bericht plaatsen. Dit is er gebeurd bij die leverancier, bent u bekend ermee dat dit impact heeft op informatiebeveiliging? En dat we het nog melden bij een aparte cybermailbox. En je ziet dat, door die awareness te verhogen, dat dat er wel voor zorgt dat mensen er meer rekening mee houden.
R: Je noemde daarbij incidenten communiceren en awareness-trainingen. Zijn er nog andere vormen waarmee die awareness wordt vergroot?
I: Presentaties, dus door middel van voor grote groepen met mensen staan. Toen ik net begon, hadden we groepen van honderd mensen die we ’s avonds dan een uur lange presentatie gaven, een halfuurtje privacy en een halfuurtje informatiebeveiliging. En daar was dit dan ook een onderdeel van. Dus ik gaf altijd aan dat bij Inkoop van iets, informeer ons en haak ons aan. Een sterke proef voor ons is de inkooporganisatie. Alle contracten daar worden ondertekend door één manager die verantwoordelijk is voor inkoop. Die weet dat dit ook gewoon een onderdeel daarvan is, dus die haakt ons wel altijd aan bij grote kritische projecten.
R: Voor het formele proces, dan loopt dat dus wel netjes?
I: Ja, maar je moet er rekening mee houden, zoals ik net al zei… We zitten natuurlijk met een erfenis, dat we dit in het verleden gewoon niet gedaan hebben en dat het niet geborgd is want er was nog geen AVG. Toen was er wel andere wet- en regelgeving, maar toen hadden bijvoorbeeld niet een DPIA. Dus ja, voor oudere contracten… Je hebt systemen die staan al vijf tot tien jaar in het ziekenhuis, daar hebben we nog wel een inhaalslag te maken. Je blijft altijd verrast worden door dingen die ingekocht

worden waar je dan niet van tevoren over was geïnformeerd, dat blijft wel voorkomen.
R: En die erfenis, die contracten die dat stukje missen, hoe wordt dat nu anders gedaan? Dat zijn de DPIA's?
I: Goede vraag. Wat we doen is, als organisatie ben je ook verplicht om een register van verwerking te maken. Je moet weten waar je informatie staat, waar je persoonsgegevens staan, hoe ze beveiligd zijn et cetera. We zijn bezig, daar zijn we bij lange na nog niet, daar ben ik open en eerlijk over, dat het register van verwerking, daar zou je ook een kolom DPIA moeten hebben en in de DPIA vragen we dan ook om cybersecurity-maatregelen. En of er een verwerkersovereenkomst is. Bij die twee moet eigenlijk een vinkje staan. In de ideale wereld, dat gaat nog een paar jaar duren, dan hebben we een lijst, een verwerkersovereenkomst, met een sluitend stuk met al die informatie. Maar daar zijn we nog lang niet, moet ik eerlijk zeggen.
R: En dat is dan iets waar jij zelf je voornamelijk mee bezighoudt?
I: Het is altijd een tandem. Het is altijd zo dat de DPIA, die kan ik naar de leverancier sturen, maar dat kan ook een privacy officer doen. Maar de beoordeling gebeurt altijd met zijn tweeeën, want in die DPIA worden privacyvragen gesteld, en informatiebeveiligingsvragen. Dan hebben we altijd een korte call dat we een halfuurtje bij elkaar gaan zitten, en dat we gaan bepalen van "Is dit genoeg? Willen we meer weten?". En mochten we meer willen weten, dan gaan we weer het gesprek aan met de leverancier, zoals vanmiddag met [leverancier], en dat kan een paar keer voorkomen totdat we een goed evenwicht hebben gevonden.
R: De leveranciers, daar wil ik ook nog op inhaken. Hoe gedragen die zich, zijn die bereid mee te werken of mee te denken?
I: Goede vraag. Dat varieert, en dat hangt helemaal af van het volwassenheidsniveau van de leverancier. We hebben wel eens te maken met partijen die, bij wijze van spreken, net beginnen en nog hun computersystemen… tegenwoordig niet meer in de meterkast maar in de cloud hebben gezet, maar gewoon slecht hebben beveiligd. Dat heb ik meegemaakt met leveranciers. Dan probeer ik ze wel altijd te helpen door adviezen te geven wat ze kunnen verbeteren en dat we ook niet zomaar hun applicatie gaan gebruiken zonder dat die zaken zijn verbeterd. Dat moet je denken aan Two-Factor Authenticatie, vulnerability scanning op hun systemen, het patchen. Dat komt gewoon voor dat leveranciers dat niet goed onder controle hebben. Er zijn partijen die hoeven we helemaal niet te vertellen hoe ze het moeten doen, want die sturen meteen al hun policies en richtlijnen, en daar mag je van uitgaan dat ze het goed regelen. Dan gaat het meer aan de juridische kant, dat de contracten dat op de letter bepalen. Maar als je het technisch gaat uitvragen hebben ze het meestal wel goed geborgen.
R: Dus dat zit hem in het volwassenheidsniveau?
I: Ja.
R: Zie je daarin ook een schifting tussen kleinere en grotere suppliers?
I: Ja, de startups, de kleinere partijen, die zijn dus over het algemeen wat minder secure, om dat zo maar te noemen. De wat grotere bedrijven dus wel, maar goed, we hebben ook redelijk grote bedrijven die ook al jaren bestaan, waar we dan toch af en toe wat aanvullende maatregelen moeten treffen.
R: Dan heb ik nog een vraag over cloud services. Je ziet dat veel zorginstellingen meer in de cloud gaan doen. Wat drijft die beslissing eigenlijk?
I: Dat vind ik dubbel. Je hebt natuurlijk je eigen IT en je hebt IT die aangeboden wordt door leveranciers. Je ziet nu voornamelijk bij ons dat de IT die wordt aangeboden door leveranciers, die bevindt zich voornamelijk in de cloud. Een concreet voorbeeld: ons urenregistratiesysteem was vroeger gewoon een server in ons eigen datacenter. Dat is nu een SaaS-applicatie. En dan staat het automatisch in de cloud en dan hoeft IT daar weinig mee te doen. Dan komt het wel voorbij mijn bureau. Zelf, als ziekenhuis zijnde, hebben we nu nog de policy om niet onze core systemen richting de cloud te verplaatsen. Dus het geldt wel voor leveranciers-gedreven applicaties, maar ons EPD staat bijvoorbeeld nog gewoon in ons eigen datacenter.
R: Dat is een stuk voorzichtigheid, of onbekend is onbemind?
I: Het is wel een strategische keuze. Het is wel vanuit het verleden door IT geadviseerd aan de Raad van Bestuur, om dat niet te doen. Ik merk wel in [de afgelopen jaren] dat er wel erg veel druk wordt uitgeoefend door [leverancier], die regelmatig bij ons op bezoek is. Dat probeert ons aan [hun programma] te krijgen, maar dat programma daar heb je weinig aan als je verplegend personeel bent, want dan zit je niet zoveel daarmee te werken. Maar er wordt wel erg veel druk uitgeoefend om richting cloud te gaan. De keus is nog steeds wel van onze eigen IT om dat on-premise te houden. Maar ik denk wel dat dat gaat veranderen in de toekomst.

R: Zou je daar een gok kunnen doen over de termijn?
I: Ik denk dat we heel snel naar een hybride oplossing toe gaan. Met andere woorden, dat we wel sommige zaken via bijvoorbeeld de [programma] van [leverancier] gedeeltelijk gaan doen, omdat bepaalde tooling die we nodig hebben om het veilig te krijgen, wat ook een advies van mijn kant geweest is binnen IT en richting de Raad van Bestuur… Er is bijvoorbeeld je hele mobile device management, je endpoint protection. Je ziet dat veel meer zaken… veel artsen werken nu thuis, verpleging heeft ook vaak een telefoon met allerlei applicaties erop, dat moet allemaal veilig worden gemaakt. Daar kan je zelf allerlei tooling voor inkopen, maar [leverancier] biedt daar tegenwoordig gewoon standaardoplossingen voor. Dus ik verwacht dat wij meer naar dat soort oplossingen gaan bewegen. Dan zit je al gedeeltelijk in de cloud. We zullen niet zo snel onze core IT daarin plaatsen, maar het is wel zo dat bijvoorbeeld [leverancier] bezig is in een samenwerking om hun EPD vanuit de cloud aan te gaan bieden. Dus ik verwacht dat zij binnen vijf jaar ons, redelijk geforceerd, richting cloud gaan dirigeren. Ik heb dat meermalen ook gevraagd bij [leverancier], maar daar geven ze nu nog geen duidelijkheid over. Ik denk wel dat dat hun strategie is.
R: Zo'n EPD, dat wissel je niet zo makkelijk, dus dan kan je niet zo snel zeggen dat je wat anders gaat doen. Dus zou je zeggen dat je dan als ziekenhuis echt geen keuze meer hebt, of gaat zoiets zo sterk tegen beleid in dat je dan alternatieven gaat bekijken?
I: Nou, ik denk dat het probleem voornamelijk zit in het maatwerk. We hebben nu net sinds vorig jaar het standaard EPD, maar we hadden heel erg veel maatwerk. Het probleem met cloudoplossingen is dat je daarop niet heel veel maatwerk kunt toepassen. Ik denk dat daar wel eens een functionele bottleneck in zal zitten. Vanuit cybersecurityperspectief ben ik verder helemaal niet tegen de cloud. Sterker nog, ik denk dat veel zaken, misschien niet beter maar net zo goed geregeld kunnen worden. Je moet ook niet vergeten, een ziekenhuis heeft altijd te weinig geld en te weinig mensen. Wat op IT-gebied dus echt zorgt voor een tekort aan kennis en aan ervaring, waardoor je op cybersecuritygebied af en toe moeite hebt om dingen voor elkaar te krijgen omdat de kennis er gewoon niet is. Dat is wel makkelijker als je dat contractueel kan afdwingen bij een [leverancier], dan ben ik daar wel voorstander van.
R: Dus zou je zeggen dat het een manier is om met hetzelfde geld meer te bereiken?
I: Nee, dat vind ik niet. Ik denk dat we het zelf ook heel erg goed kunnen, als we maar de juiste mensen hebben. Dat vind ik het belangrijkste. Het is niet veiliger, want het is gewoon andermans computer waar je op werkt. Dus het maakt niet uit of het nou bij jou of bij hen staat, de kuren zijn hetzelfde. Ik denk dat je wel hetzelfde beveiligingsniveau moet kunnen halen.
R: Ik wil graag ook nog een vraag stellen over kennis delen met andere ziekenhuizen. Maken jullie gebruik van kennis van andere ziekenhuizen? Spreken jullie die?
I: Wij werken in NVZ-verband samen. We zijn een niet-academisch ziekenhuis. Wij komen via de NVZ minimaal twee tot drie keer per jaar bij elkaar, de CISOs en de FGs. Om kennis te delen en ook andere partijen uit te nodigen om eens wat te vertellen over hoe zij het doen. Zo was er eens een keer iemand van de politie die vertelde hoe zij het doen. Daar ontmoeten we alle collega's. We hebben ook een internetsite bij de NVZ waar we vragen kunnen stellen aan collega's en kennis kunnen delen. Daarnaast heb ik zelf ook informeel contact met mijn directe collega's. die kan ik gewoon mailen en daar kan ik vragen aan stellen.
R: Dus er zijn verschillende lijnen voor?
I: Ja, zeker. We proberen echt aan kennisdeling te doen.
R: Is dat ook iets wat wordt gebruikt in dat inkoopproces? Dus als een leverancier moeilijk doet, dat je dan even uitvraagt hoe een ander iets heeft gedaan?
I: Ja, dat EPD is een voorbeeld. Daar proberen we gezamenlijk in op te trekken. Zowel de FG's aan de juridische kant alsook de CISO's. Logging is een ding bij [leverancier] en als er dingen niet goed zijn, dan praten we daar onderling over. We hebben ook een gebruikersgroep bij [leverancier], waar we ook dan met elkaar bij elkaar komen. Dan bespreken we dat met [leverancier]. Dus we proberen wel een front te vormen. Ik moet wel eerlijk zeggen, dat heb ik ook al met mijn collega's gedeeld, ik vind wel dat dat beter kan. We komen relatief weinig bij elkaar, en op de intranetsite bij de NVZ wordt wel wat gedeeld, maar het zijn altijd dezelfde mensen die dat doen. Dat vind ik wel eens jammer, dat zou wat breder kunnen. Volgens mij hebben we tegen de honderd ziekenhuizen in Nederland, en ik heb vijf collega's waarvan ik weet dat ze actief deelnemen, misschien tien. Nu zijn dat wel twintig tot dertig man totaal hoor, maar uiteindelijk is het maar een derde ongeveer die zijn mond open doet. Dat zou wel wat meer mogen, wat mij betreft.

R: Komt het ook voor dat je bepaalde stukken informatie liever niet deelt met een ander ziekenhuis? Is daar terughoudendheid in?
I: Niet van mijn kant. Ik kan me voorstellen dat niet alle collega's altijd alles delen. Ook op cybersecuritygebied hebben wij een rondje "Code Rood". Daar worden alle cybersecurityincidenten gedeeld, maar alles wat daar besproken wordt, mag niet naar buiten worden gebracht. Ik deel daar wel altijd alles, want ook wij hebben incidenten en ook daar moeten collega's van kunnen leren. Ik kan me voorstellen dat niet altijd iedereen alles deelt, maar ik doe dat wel in ieder geval.
R: Je noemde eerder awareness-trainingen voor personeel om bewustzijn te verhogen. Ik begrijp dat dat dus wel effectief is geweest?
I: Jazeker. Want toen ik net begon, hebben we heel erg gedrukt op het melden van datalekken want dat is voor ons als ziekenhuis van belang. De AVG was net nieuw, mensen kenden het nog niet, dat hebben we echt heel erg benadrukt binnen de organisatie, zowel met die presentaties als via het intranet, als via nu dan die awareness-trainingen, die SaaS-oplossing. Dat zijn wel altijd de hoofdpunten die we daar benoemen. Daar hebben we werk van gemaakt.
R: Voor mijn beeldvorming, dat zijn losse trainingen met personeel in de zaal?
I: Ja, we hebben dus de normale powerpointpresentaties gehad. Dat was dus altijd samen met de FG. Ik deed een verhaal, dan deed de FG een verhaal. Nu hebben we daar een SaaS-oplossing voor. Nu zijn het zeven modules die mensen krijgen. Ze krijgen een mailtje met een uitnodiging. Dan klikken ze op de link en krijgen ze een webpagina voor hun neus. Dan moeten ze meestal twee tot drie minuten informatie ontvangen. Dat doen we over een periode van een paar weken. Dan zijn er verschillende onderwerpen die we behandelen, waaronder ook bijvoorbeeld cloud-oplossingen en inkoop, maar ook het gebruik van het EPD, toetsingcommissie. En hoe meld je een datalek.
R: Dat is dus vrij breed?
I: Ja.
R: Dan heb ik denk ik voor nu genoeg informatie van je gekregen. Als laatste wil ik je nog één vraag stellen: zijn er nog belangrijke invloeden die cybersecurity in ziekenhuizen gaan doen veranderen?
I: Waar mijn voornaamste aandachtspunt zit, en waar ik me, nou niet zorgen om maak, maar ik moet wel zeggen dat ik me daar wel op focus want ik denk dat dat tussen nu en vijf jaar voor ziekenhuizen een issue gaat worden, wat ik nog niet goed onder controle heb en dat moet wel als CISO, dat is het Internet of Things. Daarmee bedoel ik het aantal apparaten wat op de markt gebracht gaat worden om thuis metingen te doen, ECG's te kunnen maken, hartmonitoring. Dat soort zaken, dat gaat zeker met 5G een enorme vlucht nemen. Daar heb ik wel mijn, niet twijfels, maar dat moeten we wel goed onder controle zien te houden. Dat in combinate met de cloud… Het is nu al complex, de structuur van een ziekenhuis. Wederom, ik heb jarenlang in het bedrijfsleven gelopen, daar heb je gewoon KA, dat is kantoorautomatisering. Dat is vrij plat. Toen ik voor het eerst in het ziekenhuis kwam, als je dan kijkt naar de netwerkarchitecturen en de systemen die daar staan, dat is al retecomplex [sic]. Laat staan als je binne vijf jaar, zeker binnen tien jaar, de cloud en Internet of Things erbij moet betrekken. Dan heb je echt wel een uitdaging. Daar zit voornamelijk mijn focus, dat ik denk van: "ja, hoe gaan we dat goed onder controle krijgen?". Maar dat maakt het ook leuk.
R: Dankjewel. Dan ga ik afronden. In ieder geval dank voor je tijd vandaag.
End of transcript.

B.8. Transcript 8

Researcher designated "R", interviewee designated "I".
R:Wat is je functie binnen jouw organisatie en wat is je ervaring met cybersecurity?
I: Ik ben sinds [een aantal] jaar CISO in [organisatie]. Ik ben daarvoor [jaren] lang verantwoordelijk geweest voor alle ICT en Medische Techniek in hetzelfde ziekenhuis. Ik heb om motiverende redenen besloten daaraan een andere wending te geven. Daarmee ga ik van een lijnmanager naar meer een advies- of expertfunctie toe. De verbintenis met ICT mag duidelijk zijn. Uiteraard in mijn vorige rol ook natuurlijk te maken gehad met alles rondom informatieveiligheid, maar vanuit mijn vroegere werkgevers, werkte ik bij [organisatie] enterprise risk services, en daar heb ik mij eigenlijk meer gespecialiseerd in IT-risicomanagement in brede zin. Dus die kennis komt nu ook weer goed van pas in deze nieuwe rol. Het is namelijk een nieuwe rol voor mij, maar het is ook een nieuwe rol voor [dit ziekenhuis]. Wij hadden tot voor kort eigenlijk niet of nauwelijks sturing op het gebied van informatiebeveiliging, privacy al wel iets langer. Dus ook aan mij de taak om dat verder vorm te geven, en daar ook doelen, of de

strategie op af te stemmen.
R:Wat voor vorm neemt de informatiebeveiliging aan? Zijn dat proceswijzigingen, of technische maatregelen?
I: Alles. Uiteindelijk start je gewoon met een beleid, van “hoe wil je dat informatiebeveiliging in het ziekenhuis werkt?” Dat hebben we al wat langer. Je moet nu meer denken dat we naar een ISMS-achtige (Information Security Management System) structuur gaan, waarin je meer een plan & control cyclus gaat krijgen rondom informatieveiligheid met een jaarplan en een roadmap. Met verantwoording en rapportage. Dat is één. Het zit hem ook in technische maatregelen die je gaat nemen. Dat wil niet zeggen dat ze niet al genomen zijn, maar nu ga je daar meer op sturen en focussen. Het zit hem in ten derde ook in de acquirering van nieuwe diensten en producten, dus projecten waarin je probeert aan de hand van een basiskader of raamwerk, een soort acceptatiecriteria te creëren waarlangs je nieuwe producten gaat halen. Het zit hem tot slot in vrijblijvend en niet-vrijblijvend advies, het zit hem in toetsing van onderwerpen, audits. Het is breed.
R:Je had het even over het ontwikkelen van acceptatiecriteria. Zou je daar iets over kunnen uitweiden?
I: Ik was al bang voor die vraag. Het is zo dat, ik vlieg hem vanuit een iets andere hoek aan, denk ik, dan dat je misschien vanuit jouw onderwerp, als zijnde inkoop, bedoelt, maar dit zit er wel dicht tegenaan. Wij hebben als ziekenhuis een lifecycle ontwikkeld rondom ICT-diensten en -producten. Van “Hoe komt iets nou binnen? Hoe voer je daar een adequate risicoanalyse op uit? Hoe ga je vervolgens dat in productie brengen? Wat doe je tijdens die productie? Hoe voer je het ook weer netjes af?”. Tegelijkertijd zie je dat er veel mitsen en maren zijn, wet- en regelgeving en kaders waaraan je je dan moet gaan houden. Dat kunnen externe kaders zijn, wet- en regelgeving bijvoorbeeld, of de e-healthkaders die er voor ons zijn. Het kan ook NEN-7510 zijn. Maar het kunnen ook interne kaders zijn, als zijnde acceptatiecriteria voor ICT-afdelingen, overdracht naar beheer en dat soort zaken. Of aansluitende architectuur, dat kan er ook één zijn. Toen mijn functie geformaliseerd werd - en ik loop daar eigenlijk al een tijdje mee rond, ook vanuit mijn oude functie – constateerde ik al van “Goh, nou hebben we allerlei functionarissen in huis, die zijn helaas niet vertegenwoordigd in één afdeling. Dat zijn allemaal functionarissen die zich bezig houden met kadering van bepaalde onderwerpen. Als wij een nieuw ICT-systeem implementeren, dan zult gij hier hier- en hieraan voldoen. Maar dat vindt het hoofd systeembeheer, dat vindt de privacyfunctionaris, dat vind ik, dat vindt misschien wel de opdrachtgever, de opdrachtnemer, et cetera”. Toen dacht ik van “Dat is onhandig” want elke keer als we dus iets gaan doen, dan komt heel dit riedeltje van mensen, en al die toetsingskaders komen op tafel, en elke keer hoort zo’n projectleider dan van “Wil je hier en hier ook nog even aan voldoen?” of “Weet je nog dat je met dit kader rekening moet houden?”. Dus ik was weer een nieuwe in die lijn, en ik zag het al gebeuren dat ik dan met mijn kadertje van informatieveiligheid weer overal langs moest om te vertellen hoe ze dat moesten doen. Ik heb dus initiatief genomen om dat andersom in te richten. Ik heb gezegd: “Zouden we daar naar een meer centraal controleraamwerk of referentieraamwerk kunnen gaan?” - de term is voor ons discutabel – waarin je zegt van: “We gaan niet als losse functionarissen naar het project toe op ons moment dat wij denken dat het dan goed is om te doen, of dat wij denken van “Let op, hier moeten we nog snel bij zijn!”. Nee, we gaan met elkaar één bron vastleggen, waar we aan de hand van dataclassificatie gaan bepalen welke maatregelen nodig zijn om iets te acquireren en in productie te nemen. Dat leggen we vast in één bron, en dat betekent dat projectmanagers of dadelijk zelfs inkopers, dat die naar die ene bron kunnen kijken op het moment dat zij vinden dat het nodig is. Dus als zij in een contractonderhandeling zitten, kunnen ze hem beetpakken. Of als zij aan het Programma van Eisen zitten, kunnen ze hem beetpakken. En niet dat zij afhankelijk zijn van al die individuen die op hun eigen moment komen. Zij kunnen dat dan zelf bepalen. Ze hoeven ook maar naar één bron te kijken, en die bron is altijd actueel.
R:Dat is dus een ongoing procesverbetering.
I: Ja. Daar zijn we nu net een paar weken mee bezig, om dat van de grond proberen te krijgen. Die lifecycle bestaat al langer, alleen dit wordt onderdeel van die lifecycle.
R:Daarmee wordt dan het verzamelen van requirements op een andere manier ingericht.
I: Ja precies. Daar zitten technische requirements bij, daar zitten dienstenrequirements bij, daar zitten privacy- en informatiebeveiligingsrequirements bij. Daar zou je uiteindelijk ook inkooprequirements aan kunnen toevoegen. Dat je dat helemaal naar voren trekt. Zo ver zijn we op dit moment nog niet.
R:Communiceer je in deze redesign ook met andere ziekenhuizen, om te kijken hoe zij het hebben gedaan?
I: Nou, dat zijn twee verschillende richtingen die je nu beschrijft. Communiceren naar ziekenhuizen is

meer van: “Ik geef het weg”. En hoe anderen het hebben gedaan, dan ontvang je. Ik ben toevallig op het spoor gekomen van een ander ziekenhuis die het ook zo heeft gedaan, dat daar ook mee bezig is. Ik heb eigenlijk dat idee over genomen. Ik heb ook de vraag gehad, van: “We horen dat jullie dit doen, we hebben dit bij jullie gezien, kunnen jullie ons eens vertellen hoe dat werkt?”. Dan zou ik dat overigens zonder meer doen, maar dat is nog in dit geval, voor dit onderwerp, relatief beperkt.
R:Als we dan wat meer kijken naar cybersecurity, worden daarin ervaringen gedeeld met andere ziekenhuizen?
I: Die vraag stel je los van het referentieraamwerk?
R:Ja.
I: Er wordt best wel wat gedeeld. Ik weet niet of je [ander ziekenhuis] al hebt gesproken, maar daar zit je in de lijn van een sectorale cert die we hebben, een Zorg-CERT. Daar zit zowel [het andere ziekenhuis] als [mijn ziekenhuis] in de deelnemersraad. Dus wij zijn lid van de eerste uren. In die zin wisselen we daar altijd wel uit. Dan is er ook nog een gezamenlijke, ik noem het maar een customer managementsysteem, waarin allerlei ziekenhuizen bij elkaar zitten - maar zeker niet allemaal doen ze mee – om in een soort chatbox allerlei ontwikkelingen uit te wisselen. Bedreigingen, risico’s, indicators of compromise. Maar ook recent nog zat ik met een aantal ziekenhuizen in de regio aan de telefoon naar aanleiding van een bedreiging van Emotet (een Trojan malware-programma). Dat we elkaar toch spontaan bellen, en zeggen: “Dit speelt er.” Ik heb ook nog recent contact gehad over SOC-SIEM oplossingen (Security Operations Center-Security Information and Event Management) met een aantal ziekenhuizen. Wij zijn bezig met een softwareselectie van SOC-SIEM. Daar heb ik bij ziekenhuizen informatie opgevraagd, gesprekken gevoerd met een aantal mensen, maar ook over ziekenhuizen gesproken die in hetzelfde vaarwater zitten. En zo wissel je toch wel veel ervaring uit, dus ik kan wel zeggen dat daar best wel wat wordt uitgewisseld, maar je moet er wel gewoon zelf initiatief in nemen en je moet ook open staan voor andere vragen.
R:Is dit iets wat al langer gebeurt, of is dit een meer recente ontwikkeling?
I: Ik denk dat, als je het vraagt rondom, “wordt er veel uitgewisseld tussen ziekenhuizen?”… dan Op ICT-gebied is dat al een heel lange ontwikkeling. Op ICT wordt er eigenlijk niet geconcurreerd. Dat is toch anders dan op zorg, waar het toch allemaal wat moeizamer gaat. Dus de ICT-mensen hebben over het algemeen hele warme contacten. Als het gaat om security, denk ik dat het ook al redelijk lang gebeurt, maar ik denk wel dat, door onder andere de komst van het Zorg-CERT, de ontwikkelingen van de laatste vijf jaar, dat dat wel in een stroomversnelling aan het komen is. Dat het in ieder geval wel meer is geworden.
R:Dus dat is een soort katalysator geweest om die informatiewisseling te faciliteren?
I: Ja, ik denk het wel. Ik denk het wel, want bijvoorbeeld het uitwisselingskanaal… Zorg-CERT bestaat ook nog maar twee en een halfjaar. Dat uitwisselkanaal hadden we daarvoor niet, dus ik denk wel dat er dingen gebeurd zijn die dat versnellen. Daarvoor moest je gewoon je mensen kennen. En ICT-managers die communiceren wel met elkaar, maar het zijn de CISO’s en de ISO’s die natuurlijk echt meer over security gaan.
R:Ik wil ook graag een vraag stellen over suppliers van medische apparatuur of systemen. Binnen de medische wereld zijn die in het verleden soms lastig geweest in de samenwerking. Is dat iets waar je je in herkent?
I: Ja. Ik weet niet precies hoe je dat bedoelt?
R:Dat je dan aankomt met bepaalde security-requirements en dat ze dan nee zeggen.
I: Ja, dat heeft een aantal aspecten. Eén: je hebt natuurlijk sowieso te maken met legacy-systemen, waar je eigenlijk, vanuit de historie, nauwelijks aan kan tornen, maar toch aan gebonden bent. Waar je dan misschien aanvullende maatregelen moet nemen om het toch veilig te houden. Twee: je hebt te maken met dedicated systemen, dus het is een soort black box, of closed-box, oplossing waarbij je apparatuur koopt met een softwarematige oplossing. En dat is bijna één, en dan mag je daar bijna zelf niks aan veranderen, want dan ondersteunt de leverancier niet meer. Dat is een probleem. Drie: dat leveranciers nog maar heel bewust aware zijn [sic] van dat zij mee moeten in deze snelle ontwikkeling, wat betekent dat zij qua patchen, testen, certificeringen misschien ook wel nog een inhaalslag te maken hebben.
R:En zie je dat dat al ingezet wordt?
I: Ja dat zie ik wel. Ik heb toevallig vandaag nog een leverancier aan de lijn gehad, maar dat ging niet over medische apparatuur, maar een beetje een tussenvariant ervan. Die ook wil zeggen: “Wij zijn ook aan het nadenken over hoe we dit nou beter kunnen regelen.” Ik zie dat bij Medische Techniek, er meer

belang gaat komen voor patchen, omdat natuurlijk ook kwetsbaarheden daar toch gewoon in lengte van dagen erin zitten, of er morgen in kunnen komen. Dat medische leveranciers ook weer proactief gaan communiceren over hun kwetsbaarheden, wat ze voorheen eigenlijk ook nauwelijks deden. Er is ook een platform, ik weet even niet meer hoe het heet… Eén of ander platform waar ook allerlei verzamelingen plaatsvinden van kwetsbaarheden in de meeste apparatuur, zodat je daar maatregelen op kunt treffen. Dus ja, dat is wel in gang gezet.
R:Je noemde net ook even dat je gebonden bent aan legacy-apparatuur en -systemen. Kan het ook zo zijn dat security op zichzelf van zo'n systeem een motivatie is om dat te gaan vervangen?
I: Ja, dat kan, maar dan zit je vaak meer gebonden niet zozeer aan de harde technische security, maar meer als gevolg van de discontinuïteit van Operating Systems. Dus ik merk dat de drive om te vervangen wordt eerder ingegeven door een Windows XP en dat soort ongein, dan dat je zegt: "Dit is een zwak systeem, of is onveilig." Dat is mijn gevoel. Het heeft wel een natuurlijke reden, omdat vaak er kennis ontbreekt, de leverancier ook niet transparant is, er ook weinig bekend wordt over kwetsbaarheden in medische systemen. Je moet het eerst weten, dan kun je handelen. Daarnaast is het ook wel zo dat het vervangen is niet 1,2,3 gedaan. Heel veel leveranciers zeggen gewoon: "Als jij daar Windows XP wil vervangen is dat prima, maar dan moet jij een nieuwe MRI kopen, want dit is aan elkaar verbonden. Dat verkopen wij niet los, dat upgraden we niet los. Dus dat is best lastig.
R:Dat is nu nog wel de situatie? De markt is nog wel zo dat dat voorlopig hetzelfde blijft?
I: Ik denk voor medische systemen op dit moment dat dat voor een groot deel nog het geval is, ja.
R:Ik hoor dit van meer kanten, een stuk pushback vanuit de leverancier. Dat die dit niet willen.
I: Ja, is het willen, of is het bewustzijn en het nog niet kunnen? Dat weet ik niet.
R:Dus dat ze überhaupt nog niet ontwikkeld zijn daarin?
I: Nouja, kijk. Nu hebben we tegenwoordig allemaal een computer, met een monitor en een toetsenbord en een muis. Leveranciers komen uit de hoek van de oude machines. Dat is gewoon een heel klein schermpje in het monochroom, met een paar knoppen dat je op reset kunt drukken, aan/uit en dat is het dan. Dus die hele beweging naar penetratie van ICT in de medische wereld en dat dat steeds rijker wordt qua functionaliteit en dat dat meer operating systemen aan het worden zijn met interactie en gebruikers en kwetsbaarheden, dat is ook een trend die zich een aantal jaar geleden pas is gaan inzetten. Waardoor leveranciers zich gaan realiseren van: "Wacht eens even, het is niet meer een ijzeren doos met een PLC erin (Programmable Logic Controller, een soort simpele gespecialiseerde computer), maar er komt inmiddels veel meer bij kijken. Dat brengt ook kwetsbaarheden met zich mee.
R:Is dit dan anders voor jongere of oudere leveranciers? Is daar een scheiding in te maken?
I: Ja, ik denk het wel. Nouja, is het jong en oud, dat weet ik niet. Ik zou niet willen zeggen jong en oud, ik zou het meer willen typeren als nieuwe producten. Ik kan me zo voorstellen, als ik kijk naar nieuwe leveranciers, die nog niet zo lang op de markt zijn, die echt een niche product ontwikkelen, dat die vaak wel heel erg bezig zijn met dit soort dingen. De gevestigde spelers die al lang producten in hun range hebben, die willen wel, en ik denk wel dat ze ook echt aan het veranderen zijn, maar ja, nogmaals, een MRI van een paar miljoen, die heb je niet in drie jaar afgeschreven. Of in vier of vijf jaar. De ontwikkelingen gaan zo snel, je zit toch tien of vijftien jaar aan een medisch apparaat vast.
R:Eén van de ontwikkelingen die we in de zorg zien, is dat er dingen in de cloud worden aangeboden. Ik weet niet of jouw ziekenhuis daar ook iets mee doet?
I: Ja, tot op zekere hoogte wel. 'Dingen' is natuurlijk een heel breed begrip. Waar heb je het dan over? Natuurlijk maken wij gebruik van clouddiensten.
R:Dat is dan wel welkom in het ziekenhuis, er is geen beleid daartegen?
I: Nou ja, je moet wel onderscheid maken in wat je bedoelt met cloud. Want cloud kan zijn dat ik mijn hardware buiten de deur heb gezet, maar alles zelf beheer. Cloud kan zijn dat ik een softwarepakket buiten de deur draai, op eigen hardware, maar beheerd door een andere partij. Zowel de software als de hardware, of alleen de hardware, of alleen de software. Cloud kan zijn dat ik een stuk software koop, of een dienst, waarbij ik me geen zorgen maak over hardware, en dat alles wordt beheerd door een leverancier. Je hebt wel wat varianten. Ik weet niet of je een specifieke variant bedoelt, of gewoon in zijn algemeenheid?
R:In de eerste plaats in zijn algemeenheid, maar het onderscheid is nuttig om te maken. Ik bespeur een graad van controle, die hier het onderscheid maakt. Maakt dat het verschil?
I: Ja, het is controle, maar ook wel weer toch, zoals aan het begin van het gesprek, die veiligheid. Ziekenhuizen vinden het op dit moment nog wel erg spannend en lastig om hun hele EPD's buiten de deur te zetten. Dat heeft zeker met controle te maken, met continuïteit te maken, met beveiliging en

privacy te maken. Maar ik denk uiteindelijk dat dat een onontkoombare richting is die we op moeten gaan. En er zijn ook al ziekenhuizen die het al gedaan hebben. Dat speelt mee. Ik denk ook dat… de business case is daarin toch nog wel een lastige, omdat het niet zo zeer nog zit in hardware of in kennis, dat geloof ik allemaal wel, maar in de gevraagde wendbaarheid en flexibiliteit van ziekenhuizen is zo groot en hoog, dat dat heel lastig is om dat kosteneffectief onder te brengen in een cloudcontract. Met andere woorden: wanneer zet je iets in de cloud weg, als je gewoon zelf controle hebt over je wijzigingen en de boel gewoon de boel kan zijn? Vaak is de praktijk dat wij zoveel moeten wijzigen en aanpassen dat je, als je niet oppast, enorm veel kosten terugkrijgt voor al die wijzigingen en mutaties. Dat is vaak wel een uitdaging. Dus niet elk product of dienst leent zich er zomaar voor in een ziekenhuis om even in de cloud te zetten. Dat gaat wel komen, dat gaat beter worden denk ik. Meer standaardisatie, dat zal wel moeten.
R:Die cloudtransitie, dat is voornamelijk iets wat leveranciers inzetten, of ik dat ook een wens af en toe vanuit het ziekenhuis zelf?
I: Beide. Ik zie leveranciers die zeggen: “Luister, over vijf jaar zitten wij in de cloud en je moet je on-premise oplossingen gaan afbouwen. Wij gaan jou helpen om naar de cloud te gaan”. Die zie ik voorbij komen. Ik zie leveranciers die gewoon beide aanbieden en je kunt een keuze maken. En ik zie dat ziekenhuizen soms heel bewust voor een oplossing kiezen die juist in de cloud zit, omdat het zo lekker effectief is, en je hebt daar geen beheerslast meer van. Ook daar komen alle varianten wel aan bod, afhankelijk van het type product of de situatie die je hebt. Simpel gezegd, als ik een product heb dat ik moet aanschaffen waar ik nog geen kennis van heb ontwikkeld, maar redelijk gestandaardiseerd is, of waar ik bijzondere hardware voor nodig heb, dan kan ik natuurlijk overwegend zeggen van: “Gooi het maar in de cloud, ik heb er geen omkijken meer naar.”
R:Dus cloud kan een manier zijn om het voor jezelf eenvoudig te houden?
I: Ja, of te voorkomen dat je moet investeren in extra kennis. Er zijn allerlei redenen om dat te kunnen doen. Of continuïteit.
R:Ik ben ook wel benieuwd naar, als er een nieuw apparaat wordt aangekocht, komt daar dan enige vorm van training voor de gebruiker bij, voor de arts zelf? Krijgt die iets van een cybersecurity-toelichting als er een nieuw apparaat bij komt?
I: Ik denk dat ik dat antwoord én schuldig moet blijven, én ik denk dat het antwoord over het algemeen ‘nee’ is. Wat wel gebeurt, is dat als het gaat om bewustwording rondom cybersecurity, dan vindt er van alles plaats. Er zijn bijvoorbeeld verplichte trainingen, die je om de drie jaar moet volgen, ook als je net in dienst komt. Er wordt gecommuniceerd, er worden bewustwordingsacties gehouden. Mensen worden gelogd in sommige gevallen. Als mensen thuis op een phishingmail klikken, dan worden ze daar niet zozeer op aangesproken, maar in ieder geval, afhankelijk van de situatie, worden ze in ieder geval even bewust gemaakt van “Let op voor de volgende keer”. Op dat soort manieren wordt wel getraind, maar als je nou zegt “Hier is een nieuw apparaat, wat moet je nou vooral niet doen”, dan denk ik dat het antwoord nee is.
R:Er zijn dus wel bewustwordingsacties, hoe effectief zijn die naar jouw inzicht?
I: Dat is altijd lastig meten, of dat in die zin effectief is. Maar gezien ook de reacties en vragen die er komen, durf ik wel te stellen dat daar zeker wel effectiviteit aan zit.
R:Wat voor vragen komen daarvandaan, en van wie komen die?
I: Dat zijn vragen van gebruikers. Die zeggen van: “Ik heb dit gelezen, hoe moet ik dat nu toepassen?” of “Ik heb dit gelezen, wat een goed verhaal, maar help me even met dit goed vertalen” of “Je hebt dit verteld, ik kan het bij je ophalen, ik wil graag zoveel exemplaren hebben”, of “Jullie hebben een bericht uitgestuurd over phishing, ik heb een phishingmail denk ik gevonden, waar kan ik dat melden?”. Dat soort dingen.
R:Er is wel reactie op die bewustwordingsacties dus?
I: Ik vind van wel.
R:Ik wil ook graag iets weten over de invloed van regulatie. Je hebt de GDPR die enige informatiemaatregelen vereist. Zijn daar nog andere invloed vanuit regulatie of wet- en regelgeving die cybersecurity in ziekenhuizen beïnvloeden?
I: Ja, ik denk dat als je het hebt over de GDPR, heeft dat twee kanten. Het heeft de verwerkingsverantwoordelijke kant, waarbij je zorg wil dragen dat degene die jouw gegevens verwerkt, dat je zorgt dat dat veilig gebeurt, dat het ziekenhuis daar maatregelen voor neemt richting verwerker. Maar het komt ook voor dat wij de verwerker zijn, dan zullen we ook zelf daarin de nodige maatregelen moeten treffen. Dat is een kant. De kant is ook dat er, in de samenwerking met partijen, er steeds meer afspraken worden

gemaakt over hoe we veilig samen kunnen werken. Bijvoorbeeld in al onze inkoopcontracten hebben wij een passage opgenomen rondom informatieveiligheid. Die is wel relatief beperkt, maar hij zit er wel in. Kijk naar zoiets als de NEN-7510, wat natuurlijk ook gaat over privacy en bescherming van patiëntgegevens en medewerkersgegevens tot op zekere hoogte. De AP (Autoriteit Persoonsgegevens), je boetepotentieel, dat als je door cybercriminaliteit geraakt wordt en je hebt daar geen goed verhaal bij of je bent vooral nalatig geweest, dan kan natuurlijk, omdat het vaak over patiëntgegevens gaat, dan loop je risico op boetes. Nou is dit natuurlijk allemaal GDPR, maar ik probeer even de context te schetsen waarin dit dan beweegt. Of er nog echt andere… een simpel voorbeeld: ik krijg ook audits. Een DigiD-audit voor het zorgportaal. Doe je dat specifiek voor cybersecurity: ja, tot op zekere hoogte wel. Er zit ook een pentest (penetratietest) aan vast om te zorgen dat dingen niet misbruikt kunnen worden en gehackt kunnen worden. Dus ook dat zijn wel weer kleine dingen die maken dat je altijd bewust moet zijn en bezig bent met cybersecurity.
R:End at belang van cybersecurity in het ziekenhuis, klopt het als ik zeg dat dat groeiende is?
I: Ja. Ik denk dat je dat wel kunt stellen dat dat groeit. Ik zie dat zowel bij gebruikers, alsook wel bij de Raad van Bestuur. Dat wil niet altijd zeggen dat we alles kunnen, dat overal een ja op komt. Maar er is wel dialoog, en dat is denk ik veel meer dan een paar jaar geleden.
R:Dus dat is in die zin echt een toenemende, een stijgende trend?
I: Ja, dat denk ik wel, absoluut.
R:En hoe zie je dat in de toekomst ontwikkelen?
I: Wat denk ik vooral een uitdaging zal gaan worden, is om het niet alleen te benoemen. Het herkennen is er denk ik wel, maar het erkennen, en daar vervolgens ook je strategie op aan te passen. Want ik denk dat, waar tot voor enige tijd geleden ziekenhuizen misschien wel redelijk gevrijwaard bleven van echte grote hacking-aanvallen, is door corona dat ineens heel anders geworden door statelijke actoren die bij wijze van spreken op zoek zijn naar de CoViD-remedie, om het maar zo te zeggen. Een vaccin. Medische gegevens zijn toch steeds meer waard geworden de laatste jaren. Dat ook wij onderhevig zijn aan gerichte hacking-aanvallen, dat dat betekent dat je daar dus ook gericht op moet gaan investeren en maatregelen moet gaan treffen, of dat nou organisatorische maatregelen zijn, of technische maatregelen. Maar dat betekent gewoon per definitie dat iets in jouw strategie, en iets in jouw capaciteit en in jouw middelen moet naar security gaan. Dat wordt denk ik alleen maar meer. Dat lijkt me op dit moment nog wel de grootste uitdaging, om die balans en die keuze daarin te maken. Want eigenlijk, en dat klinkt misschien heel raar, maar dat geld is er niet omdat er nog zoveel andere dingen moeten in ziekenhuizen.
R:Je hebt hiermee wel de meeste van mijn punten vanuit jezelf al behandeld, dus wat ik denk ik ga doen is een beetje afronden.

End of transcript.

B.9. Transcript 9

Researcher designated ”R”, interview subjects designated ”Ia”, “Ib” (two interviewees answered questions simultaneously.

Note: The primary purpose of this interview differed from the other interviews. The purpose of this interview was to obtain feedback on a set of proposed survey items, whereas the other interviews were focused on the role of cybersecurity in procurement. For this reason, the contents of this interview are different than others.

R:Ik wilde graag met jullie een aantal enquêtevragen langslopen en daarover van gedachten wisselen. De achtergrond voor de enquête is dat deze gericht is op CISO’s, CIO’s, ISO’s en eventueel andere cybersecurityexperts in ziekenhuizen. De naam van die rollen varieert over en weer. Het doel is om te identificeren wat de grootste informatiebehoefte op dit moment is. Dat gaat aan de hand van een aantal vragen, beantwoord met een vijfpuntsschaal. Ik wil jullie graag een moment geven om de vraag te bestuderen, waarna ik wat vragen ga stellen over deze opstelling.
R:Wat is de eerste gedachte die jullie hebben wij deze vragen?
Ia:een ding, je zegt “gedurende of na de inkoop”. Als je het hebt over na de inkoop, hoe zie je dat dan? Als je het al in productie hebt?
R:Als het systeem al in gebruik is. Ik begrijp dat dat een onderscheid is wat jullie waardevol vinden?
Ia:Ik denk dat je dan al te laat bent. Die informatie wil je eigenlijk van tevoren weten.
R:Dus in die zin zou het meer van toegevoegde waarde zijn om het te scopen op alleen voor de inkoop?

Ib:Ja, maar de praktijk leert dat er ook aankopen gebeuren waarbij je alleen maar achteraf wordt geconfronteerd met de feiten, dat er nog een hoop moet gebeuren.
Ia:Dat klopt.
Ib:Maar je zou het voorin willen hebben ja.
R:Zou het waardevol zijn om deze vragen dan te stellen waarbij je onderscheid maakt tussen voor en na de aankoopbeslissing?
Ib:Wat ik lees is dat je zegt: hoe belangrijk vind je informatie over bijvoorbeeld cybersecurity threats en risks. Die heb ik eigenlijk tijdens de aankoop maar deels nodig want het is een nieuw product en we gaan ervanuit dat het goed in de markt gebracht wordt. Maar we zien dan dat vooral medische apparaten daarna heel snel achter gaan lopen en niet meer geüpdatet worden. Dus ik denk dat, als je het puur hebt over de informatie over kwetsbaarheden, over bedreigingen, over risico's, over indicators of compromise, dat die na het aankooptraject steeds belangrijker gaan worden, omdat producten steeds vaker achter gaan lopen.
R:Dankjewel. Dan heb ik een vervolgvraag over items. Zijn er items die jullie missen in deze lijst?
Ib:Wat we zien is een trend van leveranciers om een beetje van hun hostingproblemen af te komen. Dat zij steeds vaker zaken als SaaS (Software as a Service) of IaaS (Infrastructure as a Service) gaan leveren. Het is dus niet alleen maar cybersecurity, maar we willen ook graag vanuit informatiebeveiliging weten: "waar we heb je alles ondergebracht en hoe is dat geregeld?". Dus niet zozeer het product maar ook de dienstverlening achter het product. Dat zie je vooral in de e-healthoplossingen, dat mensen thuis dus hun metingen laten verrichten, dat dat vaak met cloudoplossingen gaat. Dus cloud zien wij op dit moment voor onze eigen doeleinden nog niet als primair doel, maar je ziet dat het op deze manier wel binnenkomt.
R:Dat verandert dan ook de vragen die jullie zelf stellen over cybersecurity?
Ib:Ja, je risico ligt ineens anders. Als iemand ineens dingen onderbrengt bij een Amazon of een Microsoft of een Google, dan moet je het risico anders gaan beoordelen.
R:En die informatie daarover? Komt dat voort uit overleg met de desbetreffende serviceprovider?
Ib:Ja.
R:Wordt daarbij wel eens gekeken hoe andere ziekenhuizen iets hebben gedaan? Wordt daar onderling over gecommuniceerd?
Ib:We zien in de praktijk vaak dat die oplossingen bij meerdere ziekenhuizen aangeboden worden. Daar zoeken we zeker, als we dat zien, het contact met andere ziekenhuizen. Je hebt ook nog oplossingen waar we inderdaad samen met andere ziekenhuizen optrekken. Maar het is geen automatisme.
R:Dankjewel. Laten we voor nu even naar de volgende items gaan. Het is hetzelfde lijstje, maar de vraag is of deze types informatie er überhaupt zijn. Sommigen geven aan dat leveranciers soms niet de gewenste informatie willen geven over producten of diensten. Is dat iets waar jullie je in herkennen?
Ib:Ik zou zeggen vooral bij óf de hele grote, óf de hele kleine. De middenrange gaat best goed.
Ia:Ja.
R:Die schifting tussen groot en klein, kan je daar wat meer over vertellen?
Ib:We merken dat dat soms wel en soms niet zo moeilijk is. We hebben een gesprek gehad met Philips, over hoe zij hun zaken in moesten richten zodat het voor ons zo goed mogelijk was. Dat ging echt met mensen uit de top. Maar we zien dat andere leveranciers, die zeggen van: "dit is nou eenmaal het product en zo is het op de markt gezet. Wij hebben geconstateerd dat het veilig is, en andere ziekenhuizen doen dat ook, die hebben dit ook zo gekocht dus je moet maar akkoord gaan". Dat is dan vervelend. Wat je bij hele kleine ziet, is dat ze zeggen: "we hebben de flexibiliteit niet", en "het product wordt tegen een dusdanig lage prijs aangeboden aan jullie, dat wij geen budget zien om aanpassingen te doen". Het gaat vaak over aansprakelijkheid voor risico's. Wij zien producten ook als diensten, dus het kan zijn dat iemand bijvoorbeeld een vragenlijst levert als product aan ons. Dat zij dan zeggen dat het duizend euro kost per jaar, voor die vragenlijsten die de patiënten in moeten vullen. En dat zij maar aansprakelijk zijn voor duizend euro. Zo werkt dat niet, want je kan met een stuk hout een auto van honderdduizend euro kapotslaan, dus aansprakelijkheid is niet het stuk hout.
R:[S1], heb jij hier nog iets aan toe te voegen?
Ia:Wat ik mis, is dat we ook nog wat andere algemene vragen hebben als we leveranciers ondervragen. Of ze verwerkingsovereenkomsten hebben… Meer wat algemene vragen. Of ze een beleid hebben opgesteld, of ze voldoen aan bepaalde normen.
R:Dat is dus bij de leverancier zelf waar je die informatie vandaan wil hebben?
Ia:Ja, dat klopt.

R:Wordt daarin met andere ziekenhuizen gekeken van: “Ze zeggen nee bij ons, hoe ging dat bij jullie?”
Ia:Niet anders dan wat [S2] net uitlegde.
Ia:Ik denk dat het juist te weinig gebeurt.
Ib:Ja, dat denk ik ook.
R:Te weinig kennisdeling met andere ziekenhuizen?
Ib:Ja, alleen als je samen in een traject zit, dan werk je hartstikke goed samen. Maar zodra je een traject aangeboden krijgt of een aanschaf doet, dan zie je dat heel veel ziekenhuizen toch autonoom opereren.
Ia:Je trekt wel met andere ziekenhuizen op, of je gaat vragen van: “hoe hebben jullie het geïmplementeerd en ingericht?”. Meer over functionaliteiten enzo. Als je dan het aanschaftraject ingaat, dan heb je het daar niet over. Je weet ook niet wat anderen betaald hebben.
R:Is dat iets waarbij jullie denken dat dat waarde zou hebben om dat wel te doen?
Ia:Ik denk het wel.
R:Dan een iets meer open vraag. Wat zou een manier zijn om dat de bereiken?
Ia:Wij hebben een inkoopalliantie voor een aantal ziekenhuizen. Ik denk dat daar zeker een taak ligt. Ik denk dat de NVZ er ook wel iets aan mag doen. Wat namelijk gebeurt, is op het moment dat je daadwerkelijk in dat aanschaftraject zit, en je zit vanuit jezelf te opereren, dan kan je geen vuist maken naar een leverancier die het niet goed doet. Want op het moment dat je weet dat van de 115 ziekenhuizen er twintig bezig zijn met een leverancier, dan kan je wel een vuist maken en zeggen: “als je je zaken niet op orde hebt, dan gaat het gewoon niet door”.
R:De inkoopalliantie zelf en NVZ dus.
Ia:Ja, want als je dan nog kijkt naar die eerste vraag, “gedurende of tijdens het traject”. Als er echt [iets aan de hand is], dan zijn er wel gremia, dat je kunt delen “we zijn hier tegenaan gelopen, hebben jullie dat ook ontdekt?”, “hebben jullie dat ook gezien?”, “hoe gaan jullie daarmee om?”.
R:Dus eigenlijk, zodra er conflict is, wordt er gekeken naar hoe andere ziekenhuizen iets doen?
Ia:Ja.
R:Dus conflict is een motivator om die kennis te gaan delen?
Ia:Ja.
R:Dankjewel. De laatste vraag ging over de kanalen die ziekenhuizen gebruiken om kennis te delen met andere ziekenhuizen. Net werd de inkoopalliantie genoemd, NVZ. Zijn daar nog andere kanalen die daarin waardevol kunnen zijn, die een rol kunnen gaan spelen om dit soort kennis uit te gaan wisselen?
Ia:Nee, ik denk dat je het dan breed aan moet pakken. Dit zijn ook de dingen de ik zou noemen, deze kanalen.
R:Dan heb ik hiermee de feedback op de vragen zelf verzameld. Ik wil graag nog een vraag stellen over cloudoplossingen. De motivatie om naar de cloud te gaan, begrijp ik goed dat dat een leverancier is, die dat oplegt?
Ib:Ja, bij veel producten is het dat zij een keuze maken om niet zelf te hosten. Dat is ook voor de kleine en middelgrote een onmogelijkheid om dat op een veilige manier te kunnen doen. Dan zie je dat ze ook inderdaad snel aankomen met een SaaS of IaaS oplossing. Vooral als je een korte termijn een bepaald project draait, met een test, dan is het natuurlijk het beste om dat bij een Microsoft of een Amazon onder te brengen, want dan kan je net zo makkelijk weer ermee stoppen. Anders loopt een investering drie tot vijf jaar door.
R:Is dat dan dus vanuit gemak?
Ib:Ja, kosteneffectiviteit wel. Dat brengt wel de uitdaging mee dat persoonsgegevens en vaak ook bijzondere persoonsgegevens bij een internationaal bedrijf staan, waarbij je dus heel goed op moet letten hoe het beschreven is.
R:Daarmee moet je dan een dataverwerkingsovereenkomst gaan sluiten?
Ia:Ja, dat was dus ook precies waar ik net op doelde, met die algemene informatie. Waar sla je je data op? Dat is zeker wat we van tevoren allemaal willen weten.
R:Daar werken zij aan mee?
Ib:Ja, inmiddels weten ze heel goed wat een verwerkersovereenkomst is. De eerste jaren was het een enorme worsteling.
R:Hoe werd dat destijds ontvangen?
Ib:Nu wordt het vaak al aangeboden. Dat wil niet zeggen dat we het ermee eens zijn, wat ze hebben opgeschreven, maar ze bieden in ieder geval een verwerkersovereenkomst aan. Maar de eerste jaren

was dat, tot een jaar of twee of drie geleden, was dat gewoon lastig. Het was eigenlijk geen onderwerp van discussie.
R:Dat is vrij kort geleden dan.
Ib:Ja, sinds januari 2016 is de Wet Meldplicht Datalekken ingegaan, toen is er heel veel nadruk gelegd op de verwerkersovereenkomst. Uiteindelijk is die altijd al verplicht geweest, alleen is daar nooit zo op gehakt totdat iemand begon over de noodzaak ervan. We zien dat dat wel geholpen heeft in het besef bij leveranciers dat ze het ook goed moeten beschrijven.
R:Voor mijn beeldvorming, de Wet Meldplicht Datalekken, de verwerkersovereenkomst, hoe zijn die aangesloten? Is het zo dat in de verwerkersovereenkomst wordt aangegeven dat je verplicht bent om een lek te melden?
Ib:Ja, daar staat die meldplicht in, maar ook in de wet is ook aangegeven dat je moet documenteren hoe je de afspraken gemaakt hebt. Het middel daartoe is een verwerkersovereenkomst, dus je zag vanaf januari 2016 dat er plotseling mensen als een gek begonnen om verwerkersovereenkomsten te verzamelen. Dat heette toen nog een bewerkersovereenkomst. Terwijl er eigenlijk al een wettelijke plicht was om dat goed te beschrijven. Toen is het duidelijk geworden. Tussen januari 2016 en mei 2018, wanneer de AVG van toepassing werd, zag je een stijgende lijn. Sinds de AVG is iedereen zich ervan bewust dat het zonder niet meer lukt. Dan nog zie je wel eens een keer, de ene keer is het een document waar je echt alles twintig keer door moet lezen omdat het zo complex is opgesteld, de andere keer is het een vodje.
Ia:Maar er is een standaard vanuit de NVZ. Die standaard wordt wel door de meeste leveranciers gebruikt. Dat eisen we eigenlijk ook. Als we een leverancier hebben, dan moet die het volgens die standaard invullen.
Ib:Dat is dus een standaard vanuit de branchevereniging.
R:Dus iedereen die daarbij aangesloten is, maakt daarvan actief gebruik?
Ib:Ja. En leveranciers nu dus ook.
R:Die zijn dat komen te verwachten?
Ib:Ja, die weten dat, als ze dit bij dat [ziekenhuis] hem niet krijgen, dan krijgen ze hem bij de andere wel. Dus ze zullen voorbereid moeten zijn. Het wettelijk kader heeft ons daarin wel geholpen.
R:Die tegenstand in het begin, van leveranciers, hoe zou je zelf uitleggen waardoor zij in staat waren tegenstand te bieden?
Ib:Ze hebben een uniek product vaak. Ze hebben een positie… Je ziet in de pers dat mensen zeggen: “je moet geen Microsoft-producten kopen want Unix is veel veiliger”, dat soort zaken. Maar er zijn leveranciers die hun platform gewoon zo aanbieden, daar is het op ontwikkeld en daar is het medisch gecertificeerd. Je kan niet naar een ander want die heeft dat niet. Die nichemarkt maakt het voor zorginstanties heel lastig.
R:Dankjewel. Ik wilde het voor nu hierbij laten.
[End of transcript]

C

Codebook

Table C.1: The codebook developed during interview analysis.

Code	Cloud transition	Knowledge exchange and retention	Process flow	Structural conditions	Supplier-hospital relationship	Value conflict
Action - Assess financial/legal context						
Action - Control/lead purchase process			X			
Action - Review purchase process			X			
Actor - 3rd party expert			X			
Actor - Board of Directors						
Actor - End users / clinical staff						
Actor - Hospital non-clinical staff						
Actor - IT dept.						
Actor - MedTech dept.						
Actor - Purchasing dept						
Actor - Security officer						
Actor - Supplier						
Cloud - Control	X					
Cloud - Convenience	X					
Cloud - Cost-effectiveness	X					
Cloud - Customizability	X					
Cloud - Example						
Cloud - Hospital attitude	X					
Cloud - Responsibility transference to cloud provider	X					
Cloud - Staff opinion	X					
Cloud - Trend towards cloud-based systems	X				X	
Cloud - Vendor specialization	X				X	
Cybersecurity measures						
Cybersecurity opinion						
DecisionCriteria - Financial						
DecisionCriteria - Technology						
Evaluation on dept. level, not device						
Governance - Complex environment makes finding right people difficult						X

Continuation of Table C.1

Code	**Cloud transition**	**Knowledge exchange and retention**	**Process flow**	**Structural conditions**	**Supplier-hospital relationship**	**Value conflict**
Governance - Cybersecurity importance related to CISO position						X
Governance - Cybersecurity integration in one dept. reflects overall importance in hospital						X
Improper purchase processes			X			X
Interviewee experience						
Knowledge - Adjustments for renewal not structurally collected		X				
Knowledge - Common security standards		X				
Knowledge - Contract performance eval. not standard		X			X	
Knowledge - Cybersecurity expertise (ext.)		X				
Knowledge - Other hospitals' experiences		X				
Knowledge - Prior experience from staff		X				
Knowledge - Process flow documentation		X				
Knowledge - Processing registry		X				
Knowledge - Purchase dossiers to preserve knowledge		X				
Knowledge - Staff cybersecurity awareness		X				
Knowledge - Standardized requirements		X				
Knowledge - Supplier asking customer feedback		X				
Knowledge - Supplier vulnerability history		X				
Knowledge - Suppliers didn't understand security		X		X		X
Knowledge - System vulnerabilities		X				
Market dynamics - Bloc formation to counter supplier				X	X	
Market dynamics - Demand necessitated supplier security growth				X		
Market dynamics - Position incumbents improving				X		
Market dynamics - Security can be argument for switching supplier				X		
Market dynamics - Supplier lock-in				X	X	
Market dynamics - Suppliers using market position to enforce will				X	X	
Medical equipment fails due to scan						
Need to deploy additional measures						
Older systems legacy						
Patchmanagement - Bypass normal process if urgent						X
Patchmanagement - General						X
Patchmanagement - Risk of patching						X
Patchmanagement - Suppliers and hospitals trying to set their own patching agenda					X	X
Process - Requester not part of entire purchase			X			
Process - Review security portfolio			X			
Process - Verify purchase necessity			X			
Process1 - Initiate new purchase			X			
Process2 - Identify requirements			X			
Process3 - Prepare RfP			X			

Continuation of Table C.1						
Code	**Cloud transition**	**Knowledge exchange and retention**	**Process flow**	**Structural conditions**	**Supplier-hospital relationship**	**Value conflict**
Process4 - Evaluate proposals			X		X	
Process5 - Negotiate + award			X		X	
Process6 - Contract signing			X			
Process7 - Contract supervision			X		X	
Process8 - Lessons learned / renewal			X			
Procurement characteristic - Connectivity			X			
Procurement characteristic - Known product implies simpler process			X		X	
Procurement characteristic - Larger purchases warrant more scrutiny			X			
Procurement characteristic - Proof-of-Concept availability			X			
Procurement characteristic - Public procurement elicits multiple suppliers			X			
Procurement characteristic - Risk analysis results			X			
Procurement example						
Regulatory influence - CE documentation				X		
Regulatory influence - FDA				X		
Regulatory influence - GDPR				X		
Resistance to involvement of internal actors in procurement			X			X
Supplier distinctions					X	
Trend - Cybersecurity importance in hospitals increasing		X				X
Trend - Sector security maturity growing				X		
End of Table						

D

Survey mock-up

This survey is part of a study on purchase processes in hospitals and the role of suppliers in them. Previous interview-based research identified five key factors that influence the role of cybersecurity in procurement processes in hospitals. This survey is an extension of that research, and is intended to investigate these factors further by establishing their prevalence across Dutch hospitals.

To extend our research, we are interested in several background characteristics. **Please answer the three background questions below:**

How many beds does your hospital have?	**O** <101	**O** 101-250	**O** 251 to 750	**O** >750
How large is the IT budget in your organisation? (% of total hospital budget)	**O** <1%	**O** 1% to 3%	**O** 3.1%-5%	**O** >5%
What is your your function title within your organisation?	[open question]			

We are interested to learn how suppliers and information flow affects your procurement process. **Therefore, please indicate how often you encounter the following notions in your purchase processes:**

	Never	Rarely	Sometimes	Often	Always
A lack of alternative suppliers to consider	**O**	**O**	**O**	**O**	**O**
High costs associated with switching to another supplier	**O**	**O**	**O**	**O**	**O**
Membership of a purchasing alliance or similar organisation	**O**	**O**	**O**	**O**	**O**
Exchanging information with other hospitals about suppliers	**O**	**O**	**O**	**O**	**O**
A preference in my hospital for known suppliers over unknown ones	**O**	**O**	**O**	**O**	**O**

We found that knowledge exchange and retention are important aspects facilitating the role of cybersecurity in the procurement process. **Please indicate how often you make use of the following information within your purchase processes (before or after the purchase has concluded):**

	Never	Rarely	Sometimes	Often	Always
Supplier information from other hospitals (how to get a supplier to cooperate, security test results, information about cybersecurity measures specific to a supplier)	**O**	**O**	**O**	**O**	**O**
Threat information from other hospitals (threats, risks, vulnerabilities, indicators of compromise, mitigation strategies)	**O**	**O**	**O**	**O**	**O**
Process information from other hospitals (best practices for processes)	**O**	**O**	**O**	**O**	**O**
Records of previous purchases	**O**	**O**	**O**	**O**	**O**
Standardised requirement lists	**O**	**O**	**O**	**O**	**O**
Purchase process management tools (e.g. process flow diagrams, purchase management systems)	**O**	**O**	**O**	**O**	**O**
Previous evaluations of suppliers	**O**	**O**	**O**	**O**	**O**

Our research indicated that conflicting priorities can negatively impact the role of cybersecurity in procurement. **Please indicate how often the following situations occur in purchase processes:**

	Never	Rarely	Sometimes	Often	Always
Hospital staff bypassing regular purchase procedures	O	O	O	O	O
Purchased assets requiring a network connection to function	O	O	O	O	O
Conflicting priorities between the hospital and a supplier	O	O	O	O	O
Conflicting priorities between hospital departments	O	O	O	O	O
IT personnel being engaged after the purchase process has concluded	O	O	O	O	O

Our research revealed that suppliers can be characterised in terms of their willingness and ability to cooperate and cybersecurity maturity. **When you discuss cybersecurity features during negotiations in your purchases...**

	Never	Rarely	Sometimes	Often	Always
Large suppliers are willing to cooperate	O	O	O	O	O
Large suppliers are able to cooperate	O	O	O	O	O
Small suppliers are willing to cooperate	O	O	O	O	O
Small suppliers are able to cooperate	O	O	O	O	O
Large suppliers understand what we want from them	O	O	O	O	O
Large suppliers have the desired information ready	O	O	O	O	O
Small suppliers understand what we want from them	O	O	O	O	O
Small suppliers have the desired information ready	O	O	O	O	O

Previous research has highlighted purchases of cloud-based solutions in hospitals as a special case of purchase processes. The following questions are about these cloud solutions. **Please indicate how much you agree or disagree with the following statements:**

	Strongly disagree	Disagree	Neither agree or disagree	Agree	Strongly Agree
My hospital prefers on-premises solutions over off-premises solutions	O	O	O	O	O
My hospital is more willing to adopt cloud solutions than five years ago	O	O	O	O	O
Cloud solutions help us achieve higher security levels with fewer resources	O	O	O	O	O
Transitions to cloud solutions are forced by suppliers	O	O	O	O	O

In a transition to a cloud-based solution, how important are the following notions:

	Unimportant	Slightly important	Moderately important	Important	Very important
Control (patching access)	O	O	O	O	O
Customisability (ability to adjust the solution to your needs)	O	O	O	O	O
Cost-effectiveness	O	O	O	O	O

Thank you for participation in this survey. Your contribution is appreciated.