The role of cybersecurity in hospital procurement processes: Key factors

Rutger van Baren
Delft University of Technology

Abstract

Cybersecurity is important to hospitals and patients alike and is becoming more important as healthcare is experiencing more cybercrime over time. It is partially the result of complex interactions during procurement, but little research has been done into these interactions and what room they allow for inclusion of cybersecurity. The goal of this research is to *explore the key factors that influence the role of cybersecurity in hospital procurement processes*. Nine semi-structured interviews were conducted with hospital cybersecurity experts. Using a combination of a purchase process model and complex decision-making framework and semi-grounded theory techniques, five key factors and their interrelations were identified: supplier-hospital relationship, knowledge exchange and retention, alternative purchase processes, cloud transition and conflicting priorities. These factors influence the decision power of hospitals and their internal departments before and after signing off on a purchase.

1 Introduction

A study found that 94% of healthcare institutions had been targeted by cybercrime [13] and since then, the number of healthcare data breaches has been increasing at a high rate [30]. The healthcare sector is lagging behind others in protecting its main stakeholder (patients) in cyberspace [23]. In the meantime, the confidentiality, availability and integrity of healthcare data and systems are under threat and further improvement of cybersecurity in healthcare is needed. However, this is not a trivial task, as cybersecurity is the result of many different interacting elements in the technological [37], human [28] and organisational [27] domains, making it a complex problem. Additionally, factors specific to the healthcare sector such as extreme resource constraints and highly fragmented governance structures [29] further complicate efforts for improvement.

Cybersecurity in healthcare is an active research topic, but previous recommendations for improvement have focused on integrating cybersecurity at suppliers and improving cybersecurity of existing systems within organisations. In between these moments lies an important moment where systems are evaluated and selected: the procurement process. Previous research concluded that "procurement is a key process shaping the IT environment of modern hospitals and, as such, should be at the forefront when it comes to meeting cybersecurity objectives" [9].

The main research question in this paper is: *Which key factors influence the role of cybersecurity in procurement in healthcare?* Based on a procurement process framework that can capture complex interactions in decision-making, interviews are conducted and analysed using semi-grounded theory techniques. This paper focuses on hospitals because they are the most complex healthcare institutions [30].

Section 2 covers related work on cybersecurity and procurement. In Section 3, a theoretical framework is derived form a purchase process model and complex decision-making framework. Section 4 discusses the research methods used to collect and analyse the results, which are presented in Section 5.

2 Related work

2.1 Cybersecurity and healthcare

On the technical side, systems with long lifecycles result in a legacy of outdated operating systems and software, leaving vulnerabilities such as misconfiguration and security holes [37]. It can sometimes be remedied by patching those older systems, but patching itself is often difficult due to disruption of the organisational workflow [37] and the extremely high number of systems that need to be patched and the variety of these systems [23]. Medical devices often contain proprietary software, meaning healthcare IT teams are unable to access the internal software at all [5] and even if they could, many of them cannot support onboard cybersecurity measures due to a lack of processing capacity [37].

Aside from technical issues, human behaviour or error accounting for the majority of cyberattacks [28]. Medical staff especially sees cybersecurity measures as a barrier [23]. According to the European Commission "raising awareness of staff working in healthcare settings on security and data privacy is important to reduce cybersecurity vulnerabilities and exposure" [10]. 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" [8]. Security measures can compromise the real-time performance of a system, for example by frequently requiring users to log in [2]. 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" [24].

Aside from operational staff, "hospital management support is essential for user compliance with information security policies" [23]. Assuming support is there, organisations focus on intentional consequences of intentional actions, as opposed to unintentional consequences of intentional or unintentional actions [27]. 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. These risks are easier to define and easier to mitigate through technology. Cybersecurity through technological measures is the focus in cybersecurity, both for researchers [30] and organisations [25]. When mitigating a risk, organisations must believe the benefits will exceed the costs, but the returns on cybersecurity investments are subject to high uncertainty [14], as estimating the benefits of an investment is difficult [18].

There is a misalignment of incentives between patients and hospitals [31]. He states that hospitals do not suffer direct consequences from a data breach, but patients do. Hospitals are concerned with the suitability and costs of new systems, which reduce the role of cybersecurity in the procurement process [15]. 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 [30]. This directly contradicts Moore's perspective, as hospitals do experience direct consequences and can therefore be said to have incentives for cybersecurity that align with those of their patients.

Different approaches have been used to research improvement of cybersecurity in healthcare. From a sector-wide view six avenues for improvement have been suggested [21]: 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 [5], that a more preventative and proactive approach to cybersecurity is required [3] and that cybersecurity must be integrated into healthcare processes [29].

2.2 Cybersecurity and procurement

Dominant procurement models view purchase processes as a series of discrete events and focus on either business actions, decisions or strategic activities [4]. In an effort to improve cybersecurity by design for energy delivery systems, common sector-specific cybersecurity procurement language can benefit its role [17], aiding 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". 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 [7]. 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 [9]. 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"). From a decision-making view, 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 [26].

2.3 Decision power

Having established the importance of decisions in procurement, several new considerations arise in the context of procurement.

On the buyer side, purchasing authority often resides with a hospital department's leadership. The inclusion of cybersecurity considerations during procurement happens at their discretion. They may make a purchasing decision without properly considering cybersecurity implications, due to overconfidence in their own decision-making ability [11] or because they lack the relevant skill set to evaluate trade-offs [16]. Such a situation may result in disregarding cybersecurity as a criterion or in blind purchases of cybersecurity solutions without much discernible vision [1]. 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 cybersecurity, they are made to degrade it instead. This role reversal illustrates an adverse impact on a hospital's ability to pursue cybersecu-

rity 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, then their purchasing decisions may reflect this by ignoring warnings from cybersecurity personnel. Thus, department leadership potentially plays a large role in cybersecurity 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 [34]. The low amount of suppliers makes it hard to foster competition, which is the main goal of the procurement system [7]. 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 [32]. 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 [12]. However, the current market structure appears to offer little incentive to suppliers to improve their product's cybersecurity features, 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 [35].

Pressure from local interests can drive deviations from procurement procedures [20]. For example, suppliers tend to approach department leadership directly, getting a head start on any formal purchase processes [22]. 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 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?

3 Theoretical framework

To analyse cybersecurity in procurement processes, a new framework was synthesised from the cyclical ENISA purchase process model [9] and a complex decision-making framework [33].

Purchase process models generally view procurement as a series of decisions (decision-making), business activities (tactical/operational) or strategic activities (strategic) [4]. None of these variations account for complex interactions between outside and inside influences, preferring to model the process as a static thing. The ENISA procurement process model was chosen for its relevance to both hospitals, procurement and cybersecurity. This tactical/operational model consists of eight steps: analysing business needs, identifying and collecting requirements, preparing the request for proposal or tender, evaluation received proposals, negotiating and awarding, signing the contract, contract supervision and lessons learned. This final step emphasises the cyclical nature of purchases, where past experiences can contribute to future purchase processes.

The complex decision-making framework has two dimensions: exogenous/endogenous to separate internal and external influences, and structural conditions/actor-oriented explanations to separate environment from actors. This framework was originally developed for political decision-making. To examine its fit with the research topic, it was used to categorise findings from literature. A dominant focus on structural conditions was discovered, so the choice was made to focus on actor-oriented explanations in the new framework. The resulting framework 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 framework is included in Figure 1.

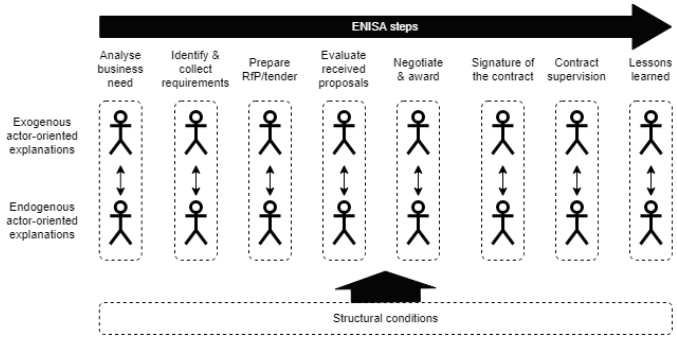

Figure 1: Combined analysis framework

4 Method

Qualitative data was gathered using semi-structured interviews with experts in cybersecurity in healthcare. Interviewees were sourced over LinkedIn and personal networks of the researcher and supervisors. Interview candidates were selected based on their organisational role (Chief Information Security Officer or similar) and their involvement with cybersecurity, healthcare and procurement.

Based on the theoretical framework, an initial set of interview questions was made to establish the key factors that

influence cybersecurity in procurement. These were subsequently refined after the second interview. These changes were mainly motivated by repeated mentions of alternative purchase processes, cybersecurity importance and supplier resistance and cooperation. The original and new sets of interview questions are included in the Appendix.

This research was approved by the Human Research Ethics Commission of Delft University of Technology (reference number: 1247). Informed consent was obtained from all interviewees prior to recording. Interviews were recorded and transcribed and the transcripts were sent to interviewees for review and approval. The recording failed in two interviews. In these cases, the transcript was substituted with the researcher's notes. Approved transcripts and notes were coded using techniques from semi-grounded theory, since the interviews were inherently based on existing research.

Using a method for estimating saturation [19] based on the number of new themes identified per interview, the final run of interviews provided 3% new information compared to the first four interviews. Assuming an information threshold of 5%, this estimate indicated that thematic saturation had been reached, providing an argument that the number of conducted interviews was sufficient.

5 Results

Using semi-grounded theory techniques, five key 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.

5.1 Supplier-hospital relationship

The supplier-hospital relationship is characterised by an imbalance in decision power in favour of suppliers. hospitals generally prefer known suppliers. When 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. This can start to influence the procurement process during requirement collection, as the requirements may be formulated to fit the supplier or may not be formulated at all, shortening the process.

Lock-in Sticking with a supplier for a longer time can result in a supplier lock-in, which refers to a situation where switching to another supplier is not feasible. In this situation, hospitals 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. Supplier lock-in can be the result of high switching costs. Hospitals have complex systems with long lifecycles and connect these to a variety of specialised equipment. Their replacement requires changes throughout other connected systems, making switching costs prohibitively high. This problem worsens over time, increasing the strength of the lock-in. The other side of supplier lock-in is the lack of suppliers to switch to, rendering hospitals unable to reap the benefits of supplier competition.

Hospital responses Hospital use two strategies use to increase their ability to influence the final purchase decision: bloc formation and knowledge exchange. Since knowledge exchange is a theme of itself, it will be discussed in the respective section. Bloc formation refers to group purchasing behaviour [32], 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.

Differences between suppliers Suppliers vary in their cooperation with hospitals. Results indicated distinctions based on size and maturity. Regarding size, cooperation is a matter of willingness for larger suppliers. For smaller suppliers, cooperation depends on their ability, as they have limited resources and tend to focus these on functionality over other demands. Cybersecurity maturity is the degree to which cybersecurity is a part of a supplier's offerings. 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. A noncooperative attitude in negotiations could be an attempt to avoid having to implement cybersecurity measures.

5.2 Knowledge exchange and retention

Hospitals are increasingly gathering and sharing cybersecurity knowledge, to the direct benefit of cybersecurity as well as their position in negotiations with suppliers. In the context of procurement, three kinds of knowledge are exchanged between hospitals:

- 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.

Besides exchanging knowledge, hospitals are improving their ability to retain it. This involves recording experiences and learning lessons from previous mistakes, and mainly serves to improve the purchase process itself. This takes the form of process guidance tools such as purchase dossiers, standardised requirement lists and process flow diagrams. Lessons learned during purchase processes can then be used to improve them, creating a feedback loop of continuous process improvement.

There is room for improving knowledge exchange. 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. Knowledge retention in hospitals can also be improved. For example, previous experiences with known suppliers are not recorded explicitly and hospitals do not perform post-purchase evaluations of suppliers.

Knowledge exchange and retention affect 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.

5.3 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.

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. 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. Increased 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.

5.4 Cloud transition

Some suppliers are transitioning to the cloud, forcing their clients to move with them, potentially through supplier lock-in. Some hospitals had a strict policy against cloud services, with one mentioning a "stigma around cloud". The attitude of hospitals towards cloud services is improving and adoption is increasing and the choice during proposals no longer defaults to on-premise solutions. The topic of cloud transition revealed multiple closely interlinked sub-themes: control, cus-

tomisability, transferring cybersecurity responsibility, vendor specialisation, cost-effectiveness and convenience.

Control and customisability Control is the extent to which a hospital can manage or interact with the cloud service. Control is important in dictating patching schedules and is closely related to customisability. 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 can make a cloud transition too expensive, as the integration may require many costly changes on the hospital side. 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 centres 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.

Cost-effectiveness and convenience Cloud solutions are convenient because they allow for contractually moving responsibility for processed data to the cloud vendor. As cloud services do involve sending sensitive data to third parties, some hospitals subject a transition to the cloud to careful consideration. On the other side, some hospitals harbour a more passive attitude towards cybersecurity which might best be described as "It's their problem". Another element of convenience is the ability of a vendor to specialise. Cloud service providers are responsible for managing and maintaining their systems only. Cloud services are designed for remote access, while on-premise solutions might involve "shooting a hole in your firewall". 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. This allows hospitals to achieve more with the same investment, increasing the cost effectiveness of the cloud service.

The overarching considerations for cloud transitions 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. 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)?

5.5 Conflicting priorities

The final theme 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 can show signs of 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 distance between customer and suppliers need not be an issue, as too much conflict can cause suppliers to lose a customer, incentivising cooperation to a degree. Still, suppliers do not have the same incentives for cybersecurity as hospitals. The resulting misalignment of priorities can cause conflict between these actors during negotiation and contract supervision. 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.

Internal Aside from conflict between suppliers, actors within a 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 all aspects of security and the latter only with availability. 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. 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 temporarily align.

Conflict between internal actors boils down to a trade-off between patient care and security. 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.

5.6 Interrelation of key factors

Having established the key factors that influence the role of cybersecurity in procurement, the next step is describing the interrelations between these factors. The interrelations are shown in Figure 2.

Knowledge exchange - 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

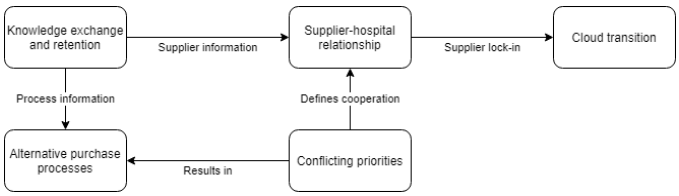

Figure 2: Interrelations between key factors

grip on purchase processes, hospitals can gain more control over purchases that bypass the regular process.

Conflicting priorities - 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 - 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 - 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.

Supplier-hospital relationship - 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.

6 Discussion

Supplier-hospital relationship Previous research highlighted the importance of endpoint complexity [23] and legacy IT [37], 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. The results implied a lack of suppliers, which makes competition between them less likely [7]. Previous research resulted in similar findings [34], pointing to alignment of the findings in this research with existing literature. A new finding was the use of knowledge exchange to obtain decision power or cooperation of a supplier in negotiations. The distinctions between suppliers were not encountered in other literature. The notion that there is a difference between small and large suppliers in the development of their products is somewhat supported, as 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 [36]. The two reasons for noncooperation (willingness and ability to cooperate) were not explicitly mentioned in previous literature. The tendency of hospitals to build relationships with suppliers aligns with previous findings [7].

Knowledge exchange and retention Research has advocated for improved threat information exchange between hospitals see [21] and the results mentioned a significant improvement in this area in the last five years. The other two kinds of information are being shared less. The exchange of process information can help in spreading best practices as demonstrated by previous efforts [9]. The use of supplier information for gaining decision power in negotiations was not encountered in previous literature. Prior to the interviews, this research did not find evidence of the importance of knowledge retention within hospitals. Some 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.

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 [22]. 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 [16].

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 [23]. 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.

Conflicting priorities The importance of management support for compliance to security policies is recognised in previous research, and conflict between internal departments to some extent. While not cited directly as conflict, organisational complexity and internal politics have been identified as important factors in cybersecurity [23]. The priorities in the conflict between the IT and Medical departments did represent a previously identified trade-off between smooth operation and high cybersecurity levels [6]. 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.

7 Conclusion

Five key factors that influence the role of cybersecurity in procurement as well as several underlying themes were found in this research: supplier-hospital relationship, knowledge exchange and retention, alternative purchase processes, cloud transition and conflicting priorities. These factors impact the role of cybersecurity in procurement by affecting relations with suppliers or the purchase process itself. While the findings did echo previous research, several new findings emerged. The importance of knowledge exchange about suppliers in the procurement process provides a new avenue for improving the role of cybersecurity in procurement. Additionally, the link between increased connectivity and visibility of alternative purchase processes was not recognised in previous research but holds promise for the inclusion of cybersecurity in the future. Finally, the importance of aligned priorities between internal hospital departments and between hospitals and suppliers highlights a need for clear communication between actors. These results contribute to ongoing efforts to improve cybersecurity in hospitals by highlighting new factors in procurement and their effect on decision power. Providing resource-constrained organisations like hospitals with new means to achieve higher levels of cybersecurity can benefit patients and hospitals alike by ensuring healthcare provision continuity in an evolving digital threat landscape.

The use of interviews with hospital personnel made 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 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. Only one interviewee was not directly associated with a hospital, which may have resulted in a biased sample.

Based on the findings, the following recommendations are made:

- **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 balance decision power between suppliers and hospitals.

- **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.

- **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.

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 cybersecurity challenges. A final avenue for

future research is scaling this research to the sector, to assess if the findings hold for the majority of hospitals.

References

[1] Chon Abraham, Dave Chatterjee, and Ronald R. Sims. Muddling through cybersecurity: Insights from the u.s. healthcare industry. *Business Horizons*, 62(4):539–548, jul 2019.

[2] Uchenna P. Daniel Ani, Hongmei (Mary) He, and Ashutosh Tiwari. Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. *Journal of Cyber Security Technology*, 1(1):32–74, nov 2016.

[3] Salem T. Argaw, Juan R. Troncoso-Pastoriza, Darren Lacey, Marie-Valentine Florin, Franck Calcavecchia, Denise Anderson, Wayne Burleson, Jan-Michael Vogel, Chana O'Leary, Bruce Eshaya-Chauvin, and Antoine Flahault. Cybersecurity of hospitals: discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making*, 20(1), jul 2020.

[4] Jenny Bäckstrand, Robert Suurmond, Erik van Raaij, and Clive Chen. Purchasing process models: Inspiration for teaching purchasing and supply management. *Journal of Purchasing and Supply Management*, 25(5):100577, dec 2019.

[5] Lynne Coventry and Dawn Branley. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, 113:48–52, jul 2018.

[6] Ricardo Siqueira de Carvalho and Danish Saleem. Recommended functionalities for improving cybersecurity of distributed energy resources. volume 1, pages 226–231. IEEE, 2019.

[7] Francesco Decarolis and Cristina Giorgiantonio. Public procurement of healthcare in europe: The case of medical devices. *Rivista di Politica Economica*, 104:4, 2015.

[8] Adenekan Dedeke. Cybersecurity framework adoption: using capability levels for implementation tiers and profiles. *IEEE Security & Privacy*, 15(5):47–54, 2017.

[9] Athanasios Drougkas, Dimitra Liveri, Antigone Zisi, and Pinelopi Kyranoudi. Procurement guidelines for cybersecurity in hospitals. Technical report, European Union Agency for Cybersecurity (ENISA), February 2020.

[10] European Commission. Topic: Raising awareness and developing training schemes on cybersecurity in hospitals, 2018.

[11] Nathanael J. Fast, Niro Sivanathan, Nicole D. Mayer, and Adam D. Galinsky. Power and overconfident decision-making. *Organizational Behavior and Human Decision Processes*, 117(2):249–260, mar 2012.

[12] FDA. Cybersecurity, March 2020.

[13] B. Filkins. SANS health care cyberthreat report: widespread compromises detected, compliance nightmare on horizon, February 2014.

[14] Eric A. Fischer. Cybersecurity issues and challenges: In brief. Congressional Research Service, August 2016.

[15] Saira Ghafur, Emilia Grass, Nick A Jennings, and Ara Darzi. The challenges of cybersecurity in health care: the uk national health service as a case study. *The Lancet Digital Health*, 1(1):e10–e12, 2019.

[16] Jennifer L. Gibson, Douglas K. Martin, and Peter A. Singer. Priority setting in hospitals: Fairness, inclusiveness, and the problem of institutional power differences. *Social Science & Medicine*, 61(11):2355–2362, dec 2005.

[17] Ed Goff, Cliff Glantz, and Rebecca Massello. Cybersecurity procurement language for energy delivery systems. In *Proceedings of the 9th Annual Cyber and Information Security Research Conference on - CISR '14*. ACM Press, 2014.

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

[19] Greg Guest, Emily Namey, and Mario Chen. A simple method to assess and report thematic saturation in qualitative research. *PLOS ONE*, 15(5):e0232076, may 2020.

[20] Lisa Hansson and Johan Holmgren. Bypassing public procurement regulation: A study of rationality in local decisionmaking. *Regulation & Governance*, 5(3):368–385, may 2011.

[21] Health Care Industry Cybersecurity Task Force. Report on improving cybersecurity in the health care industry. Technical report, 2017.

[22] HIMSS Analytics. Hospital decision makers study, May 2013.

[23] Mohammad S Jalali and Jessica P Kaiser. Cybersecurity in hospitals: A systematic, organizational perspective. *Journal of Medical Internet Research*, 20(5):e10059, may 2018.

[24] Iacovos Kirlappos, Simon Parkin, and M. Angela Sasse. Learning from "shadow security:" why understanding non-compliant behaviors provides the basis for effective security. In *Proceedings 2014 Workshop on Usable Security*. Internet Society, 2014.

[25] Saurabh Kumar, Baidyanath Biswas, Manjot Singh Bhatia, and Manoj Dora. Antecedents for enhanced level of cyber-security in organisations. *Journal of Enterprise Information Management*, ahead-of-print(ahead-of-print), oct 2020.

[26] Andre Kushniruk, MarieCatherine Beuscart-Zéphir, Watbled, Alexis Grzes Elizabeth Borycki Ludivine, and Joseph Kannry. Increasing the safety of healthcare information systems through improved procurement: toward a framework for selection of safe healthcare systems. *Healthcare Quarterly*, 13:53–58, September 2010.

[27] Claire Laybats and Luke Tredinnick. Information security. *Business Information Review*, 33(2):76–80, jun 2016.

[28] Masike Malatji, Annlizé Marnewick, and Suné von Solms. Validation of a socio-technical management process for optimising cybersecurity practices. *Computers & Security*, 95:101846, aug 2020.

[29] Guy Martin, Paul Martin, Chris Hankin, Ara Darzi, and James Kinross. Cybersecurity and healthcare: how safe are we? *BMJ*, page j3179, jul 2017.

[30] Alexander McLeod and Diane Dolezel. Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems*, 108:57–68, apr 2018.

[31] Tyler Moore. The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection*, 3(3-4):103–117, dec 2010.

[32] Jean Nollet and Martin Beaulieu. The development of group purchasing: an empirical study in the healthcare sector. *Journal of Purchasing and Supply Management*, 9(1):3–10, jan 2003.

[33] Jon Nyhlén and Gustav Lidén. Methods for analyzing decision-making: a framework approach. *Quality & Quantity*, 48(5):2523–2535, jul 2013.

[34] Persistence Market Research. Global Market Study on Cardiac Pacemaker: North America Regional Market to Register a Declining CAGR of -1.4% Between 2016 and 2024, November 2016.

[35] Sylvestre Uwizeyemungu, Placide Poba-Nzaou, and Michael Cantinotti. European hospitals' transition toward fully electronic-based systems: Do information technology security and privacy practices follow? *JMIR Medical Informatics*, 7(1):e11211, 2019.

[36] Ernest W. Walker and II. Petty, J William. Financial differences between large and small firms. *Financial Management (pre-1986)*, 7(4):61, 1978.

[37] Patricia Williams and Andrew Woodward. Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *Medical Devices: Evidence and Research*, page 305, jul 2015.

A Initial interview questions

- 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?
- 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?
- How many offers do you typically get for a purchase?
- Who evaluate these proposals?
- What are their interests in selecting a proposal?
- How are different proposals evaluated?
- Who can block or promote a final decision?
- Who has the final say on selecting a supplier?
- Who is responsible for the contract?
- Is there an evaluation process for contracts?
- Who is responsible evaluating contract performance?
- If yes, could you explain this process?
- How do previous experiences inform supplier selection in future contracts?
- How do previous experiences inform setting requirements in the future?

B Revised intervew questions

- What kind of role does cybersecurity play in new purchases?
- Who are involved in setting the requirements for new purchases?
- How do they affect the set of requirements?
- What kind of requirements are these?
- Do purchases sometimes deviate from the proper process?
- What is the effect of that?
- How are different proposals evaluated?
- Who evaluate received proposals?
- What are their interests in selecting a proposal?
- How important is cybersecurity compared to other criteria?
- What drives the increasing importance of cybersecurity?
- How does regulation factor into this process?
- How do suppliers react to your requirements?
- Are they willing to cooperate?