Evaluating a Cybersecurity Operations Center Implementation Program in a Regional Healthcare System: Challenges and Lessons Learned

W. Alec Cram
University of Waterloo
wacram@uwaterloo.ca

Ian McKillop
University of Waterloo
ian@uwaterloo.ca

Abstract

In an effort to address escalating cybersecurity risks, healthcare organizations are increasingly turning to shared service operations centers to help coordinate day-to-day cybersecurity activities, such as training, incident response, and policy management. This research examines an early-stage program to establish a series of cybersecurity operations centers within a large, regional, publicly funded healthcare system. Over 13 months, the authors acted as expert advisors on the project and simultaneously undertook an ethnographic study, including a review of project documents, observation of stakeholder meetings, and an examination of 29 interview transcripts. The results of our analysis highlight the challenges facing healthcare leaders seeking to implement operational cybersecurity initiatives. In particular, we highlight tensions that emerged related to the oversight structure, guiding framework, performance management, and initiative validation. Our analysis points to a series of responses that healthcare leaders can undertake to avoid common pitfalls and achieve positive outcomes from such projects.

Keywords: Healthcare, cybersecurity, operations center, qualitative, ethnography.

1. Introduction

The healthcare sector faces a relentless barrage of cybersecurity threats, including ransomware attacks, theft of confidential data, and employee negligence (Adams, 2022; Balasubramanian, 2022; Foy, 2023). Ongoing cost pressures and staffing shortfalls further exacerbate the difficulties in assembling an adequate cybersecurity defense. Reports indicate that successful cyberattacks have a direct impact on the quality of medical care, including delayed procedures, additional complications, and increased mortality (Devi, 2023; Ponemon Institute, 2022).

In an effort to address these concerns, healthcare leaders are increasingly strategizing approaches to implement technical solutions, policy guidelines, training initiatives, and control standards to acute care hospitals, primary care clinics, and long-term care facilities. Particularly in publicly funded health systems, government leaders are often motivated to leverage economies of scale to (at least partially) centralize operational cybersecurity activities through a shared service model to ensure a baseline standard of activities across a complex and multi-tiered set of facilities, while also being mindful of cost limitations.

We sought to undertake an in-depth investigation of one region's approach to dealing with this tension.[1] Over a 13-month period, spanning February 2022 to March 2023, the authors acted as expert cybersecurity advisors to a five-person team tasked with evaluating a project consisting of the design and implementation of cybersecurity operations (CYOP) centers in the region. The aim of the evaluation was to identify the strengths and weaknesses of the program; assess the opportunities, lessons learned, and best practices from the project; and determine if the project provided benefits to the broader regional health system.

The authors' role as both project team members and academic researchers, provided a unique opportunity to observe and participate in the CYOP program evaluation not only to aid the regional health system but also to analyze the challenges and lessons learned that could be of use to other healthcare leaders, cybersecurity practitioners, and researchers.

During the project, we were provided full access to project documentation, stakeholder meetings, and interview transcripts. We leveraged this data to investigate two research questions. First, we asked: *What are the governance challenges inherent in designing and implementing a multi-tiered*

[1] Due to confidentiality restrictions, the authors are unable to disclose the name or location of the case setting.

URI: https://hdl.handle.net/10125/106834
978-0-9981331-7-1

cybersecurity operations initiative in a publicly funded healthcare system? Second, we asked: *How can healthcare leaders tasked with overseeing such initiatives avoid common pitfalls and achieve positive outcomes?*

Our results pointed to four key governance challenges, revolving around the oversight structure, guiding framework, performance management, and initiative validation. Competing tensions within each of these challenges present key decisions for healthcare leaders, to which we provide suggestions for action. Our study contributes to the growing academic literature on the factors that present risks to cybersecurity initiatives in a healthcare context. We also provide tangible guidance to healthcare leaders facing difficult cybersecurity governance choices.

In the next section, we highlight concepts from the cybersecurity governance literature, as well as from past research focusing on healthcare cybersecurity. Next, we describe our research approach. We then outline the findings from the project evaluation, alongside our own insights on challenges and lessons learned. Finally, we discuss the consequences of our observations and conclude with opportunities for future research.

2. Background

Broadly, cybersecurity refers to "the process of protecting information by preventing, detecting, and responding to attacks" (National Institute of Standards and Technology, 2018, p. 45). One important element of this process is cybersecurity governance, which represents the leadership, organizational structures, and processes that seek to protect an organization's information assets (Johnston & Hale, 2009). Cybersecurity governance is concerned with the strategic elements (e.g., sponsorship, risk assessment), managerial/operational elements (e.g., policies, program management, user management), and technical elements (e.g., incident management, systems development) (Da Veiga & Eloff, 2007; Hepfer & Powell, 2020). Indeed, recent viewpoints of Maleh et al. (2021) and Yusif and Hafeez-Baig (2021) reiterate that cybersecurity governance encompasses cybersecurity strategy, as well as related elements of compliance, risk management, standardized processes, and senior leadership oversight.

Several models of governance in the technology context are explored in past literature, including a centralized model (i.e., decision-making and budgeting concentrated centrally), a decentralized model (i.e., decision-making and budgeting is made at a unit/divisional level, with little coordination across units), and a federated model (i.e., decision-making and reporting is split between a centralized group and autonomous groups) (Brown & Grant, 2005; Symons, 2005; Williams & Karahanna, 2013). Regardless of the model choice, effective cybersecurity governance can enhance strategic alignment of IT and business objectives, as well as organizational resilience, though past literature paints a wide-ranging collection of critical success factors (Abraham & Sims, 2021; AlGhamdi et al., 2020).

2.1. Cybersecurity in the healthcare sector

Cybersecurity issues in the healthcare sector have garnered increased attention as the quantity and severity of attacks have increased in recent years (Offner et al., 2020). Aging infrastructure, connected medical devices, and a weak cybersecurity culture contribute to the unique risk factors of the industry (Ahmed et al., 2019; Garcia-Perez et al., 2023). Indeed, healthcare organizations tend to have a large volume of sensitive patient data (both personal and health-related) that can be readily monetized by attackers, which serves to attract the interest of malicious actors (Bhuyan et al., 2020).

Healthcare organizations are most commonly targeted via infrastructure attacks (e.g., distributed denial of service), ransomware attacks, and social engineering attacks (e.g., phishing) (Nifakos et al., 2021). Cybersecurity within a healthcare context presents an escalated set of consequences relative to a "typical" business, due to the potential to impact patient care (Ahmed et al., 2019; Tully et al., 2020). In cases where a significant cybersecurity incident occurs in a healthcare setting, a recent report indicates that 28% impact emergency care and 17% cause serious patient harm (HIMSS, 2020).

Healthcare organizations are heavily targeted on the basis that they often represent "soft" targets due to fragmented governance and limited resources (Coventry & Branley, 2018; Martin et al., 2017). Relative to other sectors, healthcare organizations tend to invest only 1%-2% of the annual budget on IT, compared to 4%-10% in other industries (Ghafur et al., 2019). From this annual IT budget, average healthcare organizations spend only about 5% on cybersecurity (Skahill & West, 2021), while almost a fifth of healthcare organizations spend 2% or less of their IT budget on cybersecurity (HIMSS, 2020). With the demand for cybersecurity staff already extremely high (Segal, 2022), this low level of investment can place healthcare organizations in the situation of being unable to pay market rates for qualified experts (Martin et al., 2017) or get access to the necessary cybersecurity tools (HIMSS, 2020).

Although external parties, such as hackers, pose significant threats to healthcare organizations, both negligent insiders (e.g., a nurse who unintentionally shares a system password) and malicious insiders (e.g., a hospital that sells patient information) pose at least as great a risk to confidentiality, integrity, and availability (Ghafur et al., 2019; HIMSS, 2020).

Cybersecurity governance in large, publicly funded healthcare organizations tends to be challenging due to both size and complexity. For example, in the UK, the "healthcare sector comprises many thousands of distinct entities, and clear accountability and responsibility for cybersecurity at a national level are lacking" (Martin et al., 2017, p. 2). This context presents oversight challenges; however, "reducing variation in resource availability makes the whole system less vulnerable – a few hospitals with low resources for cybersecurity threaten the entire infrastructure of health care" (Jalali & Kaiser, 2018, p. 1).

Broadly, the healthcare cybersecurity literature has largely focused on highlighting the distinct threats and vulnerabilities facing the industry. Although some general recommendations (e.g., Bhuyan et al., 2020; Jalali & Kaiser, 2018) have been proposed, they tend to avoid the higher-level oversight perspective of the governance literature. In the following section, we outline how we approached these governance elements through an in-depth case study of a CYOP program within a large, regional, publicly funded healthcare system.

3. Research approach

The authors conducted the research using an ethnographic approach, which refers to a methodology characterized by in-depth fieldwork where researchers are immersed in the social and cultural context of a phenomenon (Myers, 2009). Ethnography can provide rich, in-depth insights into organizational aspects of information systems by cultivating a deep understanding of a problem domain that can result in the ability to challenge assumptions (Myers, 1999). Indeed, ethnography has a rich history within the information systems literature, both as seminal works (e.g., Orlikowski, 1991; Zuboff, 1988) and as recent works that focus on contemporary topics (e.g., Ens et al., 2023; Kumar et al., 2022).

Our approach differs from a (single site) case study approach in three ways: duration, data, and engagement. First, since our study took place over a 13-month period, it allowed us to embed ourselves more deeply into the project and the lives of participants than we could have in a traditional case study that would be conducted over a shorter period. Second, whereas case studies typically draw on only interviews or documents, ethnographies supplement these approaches with participant observation and engagement. We were in regular communication with the project evaluators and stakeholders (e.g., over 400 emails were exchanged throughout the course of the project with the researchers) and worked alongside the team to make sense of the project, its challenges, and how to assess its value for the healthcare system's leadership. Third, whereas a case study researcher remains an organizational observer (Yin, 2009), this project permitted the researchers an opportunity to actively engage with our subjects and participate as project team members in the CYOP project evaluation, as well as in the generation of recommendations to guide future directions of the program. Baskerville and Myers (2015) refer to this approach, which represents a more active engagement of the researcher in the field, as design ethnography. Although we recognize the potential bias that could emerge from serving as both a core project team member and as a researcher, we note that both our role as project evaluators and researchers were independent from the core activities of the CYOP project itself (i.e., neither the evaluation nor research concerned our own actions).

3.1. Data collection

The evaluation team was provided with a collection of project documents and conducted a series of semi-structured interviews with cybersecurity specialists, project leaders, and partner organization representatives. The authors were provided access to this data, in order to support the evaluation team's assessment of the overall project.

In total, 144 documents were provided to the researchers, including project plans, status reports, technical standards, readiness plans, and training materials. These documents consisted of 1,283 pages.

Additionally, 29 interviews were conducted by the evaluation team with cybersecurity specialists (4 interviews), project leaders (9 interviews), and partner organization representatives (16 interviews). The interviews had an average length of 35 minutes and generated a total of 574 transcribed pages.

In addition to the program documents and interview transcripts, the authors were actively engaged in observing and interacting with project team members and the evaluation team throughout the project. This included participating in a total of 28 (virtual) meetings, covering over 23.5 hours, during the project evaluation.

3.2. Data analysis

Throughout the project, case notes were maintained by the authors that recorded our observations emerging from the document review, project meetings, and interview transcripts. We iteratively reviewed new data as they became available and incrementally refined our observations and insights. As patterns emerged in the data that challenged our assumptions, that prompted us to think differently about CYOP governance, or that highlighted valuable guidance for practitioners, the authors discussed these patterns and made note of them. We returned to these patterns as more data were collected to further refine, challenge, and build the resulting conclusions.

Two project deliverables were created and delivered to management during the course of our fieldwork, which were separate from our research findings but were nonetheless important contributions to our thought process: an interim report in late 2022 and a final report in early 2023. As the authors were participating in the creation of these deliverables as expert advisors, the interim report provided us with a temporal separation between the midpoint and end of the project, which prompted us to establish some preliminary observations at the beginning of the project that we were able to refine during the second half of the project. This was particularly helpful because the observations were not only shared between the author team but also discussed at length with the evaluation team, as well as with the management team of the region's healthcare system, who provided feedback and validation of the observations. As a result, we were able to clarify and enhance our own insights, based on the perspectives of key stakeholders.

4. Findings

In this section, we first provide a brief outline of the CYOP project, followed by the observations and insights that emerged from our analysis.

4.1. CYOP project overview

In early 2019, a professional services firm was engaged by the regional healthcare system to complete a cybersecurity assessment. An overall cybersecurity model emerged from this assessment, consisting of a three-tier framework, based loosely on the concepts outlined in the NIST's *Framework for Improving Critical Infrastructure* (2018). As part of the assessment, a recommendation was also made to establish a CYOP program, as well as a governance structure to oversee its activities. The program to implement the CYOP centers was initiated shortly afterwards.

Beginning in February 2022 and continuing through March 2023, the authors served as expert (cybersecurity) advisors to a five-member team that had been tasked with evaluating an early-stage project consisting of a series of CYOP centers in a large, regional, public healthcare system. The evaluation team had been asked to evaluate the strengths and weaknesses of the project; the opportunities, lessons learned, and best practices; and the benefits that the CYOP centers provided to the overall health system.

Broadly, the project consisted of the creation of several designated CYOP centers. Each center consisted of a lead organization (a hospital or network of hospitals) that was tasked with providing critical cybersecurity capabilities to a set of partner organizations. Each center was located in a distinct geographical location in the region. In total, almost half of the region's hospitals were included as members during the project, alongside numerous smaller healthcare providers, such as long-term care organizations, community care organizations, primary care clinics. Each center encompassed a single lead organization and an average of 12 additional partner organizations. The overriding goal of the CYOP structure was to reduce redundancy, leverage shared cybersecurity services more effectively, and provide centralized cybersecurity oversight.

Government funding was provided over a two-year period to each of the CYOP centers, while central coordination of the overall project was facilitated through a subunit of the region's healthcare system. Leadership of the team overseeing the project consisted of a Vice President of the Cybersecurity Program, Director of the Information Security Office, and a Cybersecurity Program Manager. The CYOP center program was intended to advance cybersecurity maturity for the region and reduce the duplication of effort via a shared services model. A key goal of the project was to determine if a CYOP structure could reduce costs associated with cyber incidents. If this was found to be the case, a potential expansion (i.e., more CYOP centers, more partner organization coverage) of the program was possible at a later date.

4.2. Governance challenges

We identified four primary governance challenges that emerged in our analysis of the CYOP project: the oversight structure, guiding framework, performance management, and initiative validation. Each of these challenges is outlined in the following sections, which leverage our ethnographic approach toward the social and cultural context of the organization's stakeholders. In particular, we highlight a series of corresponding tensions that represent the principal governance challenges that emerged during the CYOP project.

4.2.1 Oversight structure: Centralized vs decentralized. As with many complex organizations, the healthcare system under investigation struggled to determine the appropriate balance between a centralized cybersecurity governance structure, in which decision-making and control could be consolidated within a small leadership team, and a decentralized structure, in which local healthcare entities were provided autonomy to make decisions that were right for them.

The solution implemented by the leadership was to divide a set of 45 cybersecurity capabilities among a centralized oversight unit, a series of regional CYOP centers (i.e., that formed the basis for the project), as well as a collection of local entities and partners (i.e., hospitals, community care organizations, long-term care organizations, and primary care facilities). This three-tier model was circulated widely as the accepted structure for implementing and governing cybersecurity operations. However, in our stakeholder discussions and observations, there was often uncertainty around what the proposed structure actually represented. For example, "identity management" and "incident response" capabilities were listed as both a shared central-regional responsibility and a shared regional-local responsibility. Separately, a "cyber reporting and metrics" capability was listed as a central responsibility and a regional responsibility, but was depicted differently than other shared responsibilities. The lack of explanation on what each of the capabilities represented or how to interpret the model led to a good deal of stakeholder confusion. One of the interviewees noted the following:

> *The concern I have from that [model] is that there's still things that have to happen locally in there, that I don't know how a regional center can manage, right? There still needs to be either a very strong centralized team or a very well-coordinated federated team…But going to this federated model, where there's people that are in the regions and in the single sites, I just don't know if the model describes well enough how the roles and responsibilities are going to be shared and the differences that happen between the small sites. So, for example, a small site might have somebody that can deliver on-site training, but another site might not be able to. How is the regional model going to deal with that sort of inconsistency?* (Cybersecurity Specialist #1)

Additionally, the governance structure revealed a power imbalance between the regional CYOP centers and the underlying participant entities. Since the project design was primarily top-down in nature, individual hospitals expressed concern that they weren't being consulted on the aspects of cybersecurity that were important to them. One interviewee expressed the following:

> *I would like to see more guidance when it comes to the governance. I've got a group of member sites [and] I'm struggling to determine where representatives from each of those sites can meaningfully contribute to the governance of the [CYOP center]. That is something that I'm struggling with and our CISO is working on, but has not come to a decision. We don't have committees established for procurement or we don't have committees established for vulnerability management. Those are the kinds of things that we are working toward at this point and time.* (Partner Organization Representative #1)

4.2.2. Guiding framework: Structured vs adapted. The CYOP program drew on NIST's (2018) framework for improving critical infrastructure cybersecurity, primarily in terms of the five core functions (i.e., identify, protect, detect, respond, recover), as well as the underlying control categories. Although stakeholders generally appreciated the structure inherent in the framework, concerns were raised in terms of the lack of discussion and consultation in arriving at the adoption decision. One interviewee highlighted their frustration as follows:

> *I've been looking for them to help make sure that our [regional CYOP centers] are sharing and working together. In a way, the [regional centers] have been doing that independent to [the central CYOP center]. And they did some things, like they said, "Hey, we're all going to use the NIST framework." Wonderful. You decided, you didn't leave it up to us to decide. Perfect. You told us what tool we're going to use to monitor it in. Perfect. You've now told us you're going to go out to market and find us another tool. Perfect.* (Partner Organization Representative #4)

Other stakeholders pointed out the potentially false sense of security that the use of frameworks like NIST can provide:

> *So, NIST, it's good because it's better to have a framework than not to have a framework. But, for me, if I see somebody that is not doing well on NIST it's a good sign because I know what they're talking about. If it's somebody that's doing super well on NIST then that's a red flag for me…So, I think in a way it's a dangerous framework because it gives a very big false sense of security, because the organization that struggles will look through it and say, "Yeah, I got that, I got that"; they look like they go well and then their senior management team or their board will just like lower their flag, "We're all good, look at how mature they are." It's too rudimentary I think for that.* (Project Leader #5)

The overriding governance challenge here is that, on the one hand, a structured framework provides uniformity and consistency, but on the other hand, it offers a lack of flexibility and possibly a poor fit with an organization, its culture, and its processes.

4.2.3. Performance management: Formal vs flexible. Demonstrating the achievement of performance expectations was a key element of the project, both to track progress and to inform funding decisions for the future of the CYOP initiative. Several forms of performance management were undertaken, including monthly status reports prepared by each CYOP center and a baseline self-assessment questionnaire on the current status of cybersecurity controls at each local entity. Additionally, the overall program evaluation served as a holistic performance management exercise.

The status reports took the form of one-page dashboards, with a listing of key activities completed, upcoming activities, status ratings (e.g., denoting green, yellow, red), and milestone progress. The milestones were listed in terms of the NIST framework categories (e.g., identify, protect, detect), but were very general (e.g., incident response, training) and contained few measurable indicators or details of the underlying steps.

Similarly, a questionnaire was used to identify process and technical gaps, relative to the NIST framework. Maturity scores were generated, alongside recommendations on the highest risk areas to focus on.

One of the key governance challenges with such a distributed, self-reported approach is the reliability and comparability of the collected data. Part of the issue was the wide variance of participant familiarity with cybersecurity issues (e.g., a large urban hospital with trained staff and a set of cybersecurity tools, versus a small, rural hospital with very few IT staff and little cybersecurity expertise). Inevitably, where a less mature site is found to have more significant gaps to fill compared to a more advanced site, they will receive additional attention. Although this is helpful to improve the poorest performers, it does little to help the average (or better) performers advance. One interviewee summarized this view as follows:

> *The [CYOP program] has been focused on those who are further behind. So, [each partner organization is] pushing for certain things; things that in the case of [our larger organization], have already been done.* (Partner Organization Representative #9)

Another challenge was the ability to compare consolidated performance results across the CYOP centers. One interviewee framed the difficulty as follows:

> *For our region, I've assigned one guy to be doing this [performance management] stuff…So, that person is going to be my litmus test to say. "Within the region I know that this is apples to apples," but outside of my region, if another CYOP [center] has gone and interpreted the questionnaire totally differently than my person, you might get inconsistent data as far as [if] the status is truly of an apple over there or is it more of an orange.* (Project Leader #3)

One mechanism used to attempt to even the playing field was the identification of nine "critical controls" that each CYOP center was to fulfil. These nine controls were selected based on an evaluation of the current healthcare threat landscape. However, compliance with these controls was encouraged on a "best-effort" basis (rather than mandated and audited for compliance).

Throughout the project, recognition of the importance of setting project-wide key performance indicators was noted by stakeholders, but no comprehensive, formal listing of measurable indicators was established.

4.2.4. Initiative validation: External vs internal. Due to the publicly funded nature of the healthcare system examined in this study, fiscal accountability and funding restrictions associated with projects such as the CYOP initiative were heavily scrutinized. Alongside this financial spotlight is the importance of stakeholder perceptions that the project is producing benefits for the healthcare system overall. Indeed, demonstrating this tangible progress was of critical importance for CYOP leaders in order to secure the funding necessary to extend the program's duration through 2023. Due to the relatively short timeline of the project, CYOP leadership was almost entirely focused on pursuing short-term targets that could be pointed to as clear progress rather than longer-term initiatives that might not produce results within the project timeline.

For example, during the project, many CYOP centers elected to allocate their available funds to purchasing cybersecurity tools and hiring staff, rather than undertaking more complex and time-consuming processes such as developing cybersecurity policies or designing cybersecurity training programs. Although this is not unexpected, it points to the challenges in overseeing projects with short-term financial commitments but longer-term performance targets. That is, the region's CYOP project was intended to determine if such a shared service model could provide cost reductions alongside more effective cybersecurity management. However, due to the limited timeframe, CYOP centers were incented to demonstrate results that could be perceived as achieving these objectives, but without providing them with the resources to fully allow for such progress to take place. Quick wins, such as purchasing a new tool, can therefore be easily highlighted in a status report, despite there not (yet) being sufficient evidence in place to demonstrate either its effectiveness or contribution to cost savings.

These short-term wins served as small demonstrations of legitimacy to the overall project. Similar mechanisms that sought to demonstrate that the project was operating as intended were the reliance on external resources, including the NIST framework, and a professional services firm that assisted in the creation of the region's cybersecurity model. By pointing to these industry-accepted norms, it added weight to the argument that the project was going in the right direction.

However, the evaluation team pointed out that simply relying on the NIST framework or engaging consultants does not necessarily lead to optimal outcomes. As noted above, the cybersecurity model used by the region (and created by the consultants) was difficult to understand and lacked sufficient detail, whereas the NIST framework was being employed in a somewhat piecemeal fashion.

Overall, this short-term mindset led to questions about the capability of the CYOP centers to facilitate sustained benefits, in the event that funding was cut or reduced in the future. One interviewee noted the following:

> *The resources to do the work are difficult and the sustainment of those [CYOP centers] is what always comes into question. How are we going to be able to keep this up after the funds dry up? That comes up repeatedly and advocating that in some way…would be valuable because we came out of the pandemic and all the hospitals are stressed for cash. How do we do this, yet they realize security is imperative? It's part of what we have to do. So how do we carve [it] out? It's a struggle, right? Do I really want to carve out money and reduce how much I'm funding clinical [care]?* (Project Leader #2)

4.3. Avoiding pitfalls and achieving positive outcomes

Our second research question asked how healthcare leaders tasked with overseeing cybersecurity initiatives can avoid common pitfalls and achieve positive outcomes. For each of the four challenges noted above, we propose corresponding guidance for cybersecurity leaders in the healthcare sector. Our observations are summarized in Table 1.

Table 1. Governance Challenges & Lessons Learned

Governance Challenges	**Lessons Learned**
Oversight structure	Federated model with clearly articulated roles and responsibilities.
Guiding framework	Consult widely and determine alternatives; communicate with stakeholders on what/why/how the framework will be used.
Performance management	Establish measurable key performance indicators (KPIs) early in the project, using a sliding scale (e.g., minimum, target, stretch). Refine KPIs as necessary.
Initiative validation	Set minimum funding periods to five years, to enable assembling the people, processes, and technology to provide long-term benefits.

In response to the first identified governance challenge (balancing a centralized and decentralized structure), we propose that a federated model where standards are centrally defined, but autonomy and resources are provided to local entities, is the most appropriate approach in healthcare settings such as the one we studied, due to the variance in terms of size and cybersecurity maturity of the participating entities. However, a clearer plan that explicitly articulates the roles and responsibilities of the participants in more detail is imperative to more effectively communicate and coordinate the related activities.

The second governance challenge focused on the role of a guiding framework in terms of a structured adoption or one that is adapted. On the one hand, a framework such as NIST provides a well-accepted foundation on which to build cybersecurity operations. On the other hand, the NIST framework is complex and detailed, vastly exceeding the scope of the CYOP program. We propose that although selected aspects of NIST are a perfectly reasonable choice to underpin the program, other alternatives (e.g., COBIT, SANS CIS) could have been considered and discussed more widely with stakeholder groups. After a decision is made on the framework, a more explicit articulation from the leadership team on what elements of the framework are to be used, why these elements will be used, and how exactly they will be used would allow a more consistent understanding across the various stakeholder groups.

The third governance challenge concerned the tension between a formal and flexible performance management approach. In the context of our case, having a single set of targets would have been of little use due to the range of participant maturity levels. However, some measurable targets would have been welcomed, even if they needed to be refined as the project progressed. In order to account for the range of participants, a simple sliding scale of KPIs could have been established, starting with a "minimum" level that all entities should comply with, moving on to a "target" level that demonstrates an extended level of maturity, and continuing to a "stretch" target for those more advanced entities.

Finally, the fourth governance challenge considered the validation of the CYOP program initiative. The publicly funded model of the healthcare system under review presented particular challenges due to the limited duration funding period. We propose that funding for cybersecurity initiatives in a healthcare setting should be no shorter than five years to allow for leaders to reasonably assemble the building blocks necessary to enable a sustainable set of processes, people, and technology. Funding periods with shorter durations only serve to incent short-term strategizing, which does not adequately serve the broader objectives of a robust cybersecurity management program.

5. Discussion

Our findings point to four key tensions that threatened the CYOP implementation project. Based on our analysis, tensions emerged in relation to the oversight structure, the guiding framework, performance management, and initiative validation.

The identified concerns echo some of the risk management and resourcing observations raised by Bhuyan et al. (2020) and Jalali and Kaiser (2018); however, our focus on a publicly funded system, rather than a mixed, public-private system such as in the United States, provides a distinct financial and regulatory perspective.

In particular, the size of the initiative (each of the CYOP centers encompassed an average of 12 additional partner organizations, such as hospitals) and the wide variation of cybersecurity maturity represented an acute governance challenge. This challenge was compounded by the multiple layers of decision-making authority, starting with the regional government, then flowing down to the regional healthcare leadership, cybersecurity leadership, and partner organization (e.g., hospital) leadership. Although cybersecurity issues were widely accepted as a legitimate risk across these leadership levels, the multiple layers contributed to a somewhat slow and disjointed oversight process.

However, the recognition that a cohesive, integrated process is required to mitigate cybersecurity risks within the most vulnerable partner organizations shows that projects such as the one we examined is a step in the right direction. As one of the interviewees put it:

> *Within the cybersecurity world, we have some common restraints. We can't find enough people; it's hard to find talent, retain, recruit and build that expertise for what we can pay for the expertise. We're limited in our funding and our salary bands. So, if we're not working together in this, we're going to fail.* (Cybersecurity Specialist #3)

However, from a governance perspective, our findings suggest that the general IT governance challenges associated with a federated model appear to also apply in both a cybersecurity and healthcare context. That is, coordination between the central unit, regional CYOP centers, and partner organizations is critical to facilitate alignment and reduce the likelihood of wasted resources. Indeed, the four governance challenges identified above, mirror the four categories of structural change identified by Williams and Karahanna (2013): coordinating structure and context (oversight structure), outer context (guiding framework), inner context (performance management), and power and politics (initiative validation).

As one of the main objectives of the project was to enable a sharing of common cybersecurity tools and services, those organizations that were trailing in maturity were provided the support necessary to advance. An interviewee noted this in the following way:

> *The smaller organizations, they just they don't have the dedicated cybersecurity staff…they don't have the funding to have that dedicated staff. So, this is where they benefit the subject matter expertise at the centralized level.* (Partner Organization Representative #2)

However, the successful expansion of such initiatives relies heavily on the adequacy of coordination processes. Williams and Karahanna (2013) frame the concept of coordination within a federated governance model as "the ongoing process of integrating information, resources, activities, and people across different interdependent parts of an organization to accomplish enterprise goals" (p. 936). As cybersecurity maturity of the more undeveloped partners is raised to a minimum level, CYOP objectives should expand to push the more advanced partners to supplement their maturity. As well, the CYOP initiative represents just one of the many cybersecurity capabilities that are important for the healthcare sector (e.g., others include data privacy, architecture, and access management). The region needs to provide long-term funding, expand the program to all partner organizations, and stimulate innovation and agility in their cybersecurity management initiatives.

5.1. Limitations and future research

As with any research, our study includes limitations that present opportunities for future study. First, we focus on a CYOP program in a publicly funded regional healthcare system. We recognize the uncertain generalizability that our findings might have for other healthcare organizations operating in different locations and with different characteristics. In response, we encourage future research to undertake similar evaluations at different sites in order to verify if the same findings can be confirmed. Second, our ethnographic approach relied on the collection of documents, observation of meetings, and review of interview transcripts over an extended period of time. Although ethnographies can provide rich insights into the social and cultural norms of an organization, alternative methodologies, such as surveys or experiments could provide alternative insights that could supplement or challenge our findings. We encourage cybersecurity researchers in the healthcare space to employ such methodologies in order to extend our findings.

6. Conclusion

Over the course of a 13-month ethnographic study, the authors acted as expert advisors to a team tasked with evaluating an early-stage project to roll out a series of CYOP centers in a large, regional, publicly funded healthcare system. Through a review of project documents, observation of stakeholder meetings, and an examination of 29 interview transcripts, we highlight four key governance challenges that faced organizational leaders: oversight structure, guiding framework, performance management, and initiative validation. We highlighted a series of recommended responses that healthcare leaders can undertake to learn from the case and facilitate positive outcomes from cybersecurity initiatives.

7. References

Abraham, C., & Sims, R. R. (2021). A comprehensive approach to cyber resilience. *MIT Sloan Management Review, 62*(4), 1-4.

Adams, K. (2022, December 18). What we learned from cybersecurity attacks in healthcare in 2022. *MedCityNews*. https://medcitynews.com/2022/12/what-we-learned-from-cybersecurity-attacks-in-healthcare-in-2022/

Ahmed, Y., Naqvi, S., & Josephs, M. (2019). *Cybersecurity metrics for enhanced protection of healthcare IT systems* 13th International Symposium on Medical Information and Communication Technology, Oslo, Norway.

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers & Security, 99*(-), 1-39.

Balasubramanian, S. (2022, October 24). Cybersecurity must become a top priority in healthcare. *Forbes*. https://www.forbes.com/sites/saibala/2022/10/24/cybersecurity-must-become-a-top-priority-in-healthcare/?sh=32b3172f23b5

Baskerville, R. L., & Myers, M. D. (2015). Design ethnography in information systems. *Information Systems Journal, 25*(1), 23-46. https://doi.org/10.1111/isj.12055

Bhuyan, S. S., Kabir, U. Y., Escareno, J. M., Ector, K., Palakodeti, S., Wyant, D., Kumar, S., Levy, M., Kedia, S., Dasgupta, D., & Dobalian, A. (2020). Transforming healthcare cybersecurity from reactive to proactive: Current status and future recommendations. *Journal of Medical Systems, 44*(98), 1-9. https://doi.org/10.1007/s10916-019-1507-y

Brown, A. E., & Grant, G. G. (2005). Framing the frameworks: A review of IT governance research. *Communications of the Association for Information Systems, 15*(38), 696-712. https://doi.org/10.17705/1CAIS.01538

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

Da Veiga, A., & Eloff, J. H. P. (2007). An information security governance framework. *Information Systems Management, 24*(4), 361-372. https://doi.org/10.1145/1655168.1655170

Devi, S. (2023). Cyber-attacks on health-care systems. *The Lancet Oncology, 24*(4), E148. https://doi.org/10.1016/S1470-2045(23)00119-5

Ens, N., Hukal, P., & Jensen, T. B. (2023). Dynamics of control on digital platforms. *Information Systems Journal, Forthcoming*, 1-22. https://doi.org/10.1111/isj.12429

Foy, B. (2023). The outlook for healthcare cybersecurity in 2023. *Security*. https://www.securitymagazine.com/articles/98755-the-outlook-for-healthcare-cybersecurity-in-2023

Garcia-Perez, A., Cegarra-Navarro, J. G., Sallos, M. P., Martinez-Caro, E., & Chinnaswamy, A. (2023). Resilience in healthcare systems: Cyber security and digital transformation. *Technovation, 121*, 1-11. https://doi.org/10.1016/j.technovation.2022.102583

Ghafur, S., Grass, E., Jennings, N. R., & 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. https://doi.org/10.1016/S2589-7500(19)30005-6

Hepfer, M., & Powell, T. C. (2020). Make cybersecurity a strategic asset. *MIT Sloan Management Review, 62*(1), 40-45.

HIMSS. (2020). *2020 HIMSS cybersecurity survey*. Healthcare Information and Management Systems Society.

Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in hospitals: A systematic, organizational perspective. *Journal of Medical Internet Research, 20*(5), 1-17. https://doi.org/10.2196/10059

Johnston, A. C., & Hale, R. (2009). Improved security through information security governance. *Communications of the ACM, 52*(1), 126-129. https://doi.org/10.1145/1435417.1435446

Kumar, M., Singh, J. B., Chandwani, R., & Gupta, A. (2022). Locating resistance to healthcare information technology: A bourdieusian analysis of doctors' symbolic capital conservation. *Information Systems Journal, 32*(2), 377-413. https://doi.org/10.1111/isj.12357

Maleh, Y., Sahid, A., & Belaissaoui, M. (2021). A maturity framework for cybersecurity governance in organizations. *The EDP Audit, Control, and Security Newsletter, 63*(6), 1-22. https://doi.org/10.1080/07366981.2020.1815354

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: How safe are we? *British Medical Journal, 358*(-), 1-4. https://doi.org/10.1136/bmj.j3179

Myers, M. D. (1999). Investigating information systems with ethnographic research. *Communications of the Association for Information Systems, 2*(23), 1-20. https://doi.org/10.17705/1CAIS.00223

Myers, M. D. (2009). *Qualitative research in business & management*. SAGE Publications.

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors, 21*(5119), 1-25. https://doi.org/10.3390/s21155119

Offner, K. L., Sitnikova, E., Joiner, K., & MacIntyre, C. R. (2020). Towards understanding cybersecurity capability in australian healthcare organisations: A systematic review of recent trends, threats and mitigation. *Intellignce and National Security, 35*(4), 556-585. https://doi.org/10.1080/02684527.2020.1752459

Orlikowski, W. J. (1991). Integrated information environment or matrix of control? The contradictory implications of information technology. *Accounting, Management & Information Technology, 1*(1), 9-42. https://doi.org/10.1016/0959-8022(91)90011-3

Ponemon Institute. (2022). *Cyber insecurity in healthcare: The cost and impact on patient safety and care.* https://www.proofpoint.com/us/cyber-insecurity-in-healthcare

Segal, E. (2022, April 6). Continued security staff shortages are making businesses more vulnerable to cyberattacks: Report. *Forbes*. https://www.forbes.com/sites/edwardsegal/2022/04/06/continued-security-staff-shortages-are-making-businesses-more-vulnerable-to-cyberattacks-report/?sh=15a8ec3b7157

Skahill, E., & West, D. M. (2021). *Why hospitals and healthcare organizations need to take cybersecurity more seriously*. Brookings. https://www.brookings.edu/blog/techtank/2021/08/09/why-hospitals-and-healthcare-organizations-need-to-take-cybersecurity-more-seriously/

Symons, C. (2005). *IT governance framework*. Forrester.

Tully, J., Selzer, J., Phillips, J. P., O'Connor, P., & Dameff, C. (2020). Healthcare challenges in the era of cybersecurity. *Health Security, 18*(3), 228-231. https://doi.org/10.1089/hs.2019.0123

Williams, C. K., & Karahanna, E. (2013). Causal explanation in the coordinating process: A critical realist case study of federated IT governance structures. *MIS Quarterly, 37*(3), 933-964. https://doi.org/10.1089/hs.2019.0123

Yin, R. K. (2009). *Case study research: Design and methods*. SAGE.

Yusif, S., & Hafeez-Baig, A. (2021). A conceptual model for cybersecurity governance. *Journal of Applied Security Research, 16*(4), 490-513. https://doi.org/10.1080/19361610.2021.1918995

Zuboff, S. (1988). *In the age of the smart machine*. Basic Books.