Unlocking complementary assets in digital security

An explorative study on the impact of the changing threat landscape and digital security regulation on complementary assets in the financial sector

Kavya Shukla (42111)
Master Thesis
Stockholm School of Economics
Fall 2023
Supervisor: Åke Freij

Abstract

Due to increased risk of cyberattacks, *digital security (DS, hereinafter)* is one of the leading challenges facing organizations today. New ways of working and technologies such as agile and the cloud have accelerated security risks with profound implications. Regulators have taken note of this pertinent issue and have implemented a range of regulations for firms to comply with such as NIS, NIS2, DORA, and GDPR to name a few. However, there is still a lack of clear guidance on organizational best practices to manage DS resources in a constantly evolving threat and regulatory landscape. The information systems literature largely focuses on technical aspects, but the managerial and strategic aspects of DS and related regulation are examined by only a handful of studies with limited focus on both DS threats and DS regulation.

By drawing from management and strategy literature on the resource-based view and dynamic capabilities, this study aims to fill the gap in DS research by using complementary assets as a conceptual framework. Through an explorative, qualitative study, the classification and specification of complementary assets that firms require to address DS related challenges is analyzed. In line with Teece (1986)'s seminal Profiting From Innovation (PFI) framework, complementary assets are specified on a continuum moving from generalized, specialized and finally cospecialized. Intrafirm complementary assets are classified in the areas of manufacturing and distribution. Adding to Teece's PFI framework, relational complementary assets are identified at the interfirm level.

The empirical results highlight that organizations that successfully convert generalized complementary assets into specialized and cospecialized assets are in a better position to address DS threats and regulatory changes. The conversion process is supported by external consultants and AI vendors at the intrafirm level and through external collaborations for interfirm level. Interfirm cospecialized assets were found within and across industries. Finally, this study underscores the importance of orchestration of complementary assets across firm divisions and also highlights the need to determine an optimum level of (co)specialization.

Keywords: digital security, cybersecurity, complementary assets, dynamic capabilities

Acknowledgements

Firstly, many thanks to Åke Freij, my thesis supervisor, for guiding me through the research and thesis process. Your flexibility to meet and discuss with me, your feedback, and your comprehension of my enquiries were invaluable in enabling me to perform this research. I would also like to extend my sincerest appreciation to the 27 anonymous interviewees who made this study possible through sharing their experiences and views on digital security in their respective firms. Your insights have made the work on this thesis deeply inspiring. Finally, thank you to my family and also to my friends who provided immensely helpful comments and interesting perspectives throughout the process.

Table of contents

Definition of core terms used

Term	***Definitions used in this study***
Information Systems (IS)	*"A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information." (NIST, 2023)*
Cybersecurity	*"Cybersecurity is used as an all-inclusive term referring to the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect interconnected environments" (R. von Solms & van Niekerk, 2013)*
Digital security	*"Digital security addresses the core elements of cybersecurity but additionally incorporates a dimension of resilience and security by embedding security in the business and in all of the related business dimensions and organizational factors as a whole alongside machines, people, objects,and processes" (Schinagl & Shahim, 2020)*
Dynamic capabilities	*"Mechanisms to integrate, build, and transform internal and external competencies to address rapidly changing environments" (Teece, 2007)*
Complementary assets	*"Complementary assets refer to the resources, capabilities, and assets that are needed to profit from an innovation. These can encompass any asset that facilitates the commercialization of an innovation, such as financial assets, complementary technology, intangible assets, management capabilities, or market knowledge" (Teece, 1986)*
Information Technology (IT) assets	*"IT assets are the integral components of the organization's IT environment used for storage, management, control, display and data transmission" (NIST, 2023).*

Incidents	*"A single event or a series of linked events unplanned by the financial entity that compromises the security of the network and information systems, and have an adverse impact on the availability, authenticity, integrity or confidentiality of data, or on the services provided by the financial entity."* (DORA, 2023)
Vulnerabilities	*"A weakness, susceptibility or flaw of an asset, system, process or control that can be exploited." (DORA, 2023)*
Agile methodologies	*"The agile methodology is a project management approach that involves breaking the project into phases and emphasizes continuous collaboration and improvement. Teams follow a cycle of planning, executing, and evaluating." (Atlassian, 2023)*
Cloud technologies	*"Cloud computing means having the ability to store and access data and programs over the internet instead of on physical servers. Businesses of any size can harness powerful software and IT infrastructure to become more agile." (Salesforce, 2023)*
Legacy systems	*"An ICT system that has reached the end of its lifecycle (end-of- life), that is not suitable for upgrades or fixes, for technological or commercial reasons, or is no longer supported by its supplier or by an ICT third-party service provider, but that is still in use and supports the functions of the financial entity." (DORA, 2023)*

1. Introduction

"Not only is the threat landscape evolving continuously, but also the regulatory landscape. There are new regulatory requirements such as NIS, [then] NIS2, DORA in the financial sector. So, I think that challenges can be categorized in two different categories: the threat landscape and regulatory landscape." – Interviewee 20

Digital strategies are at the forefront of innovation and transformation strategies, reducing distance between the digital and the physical world (Nylen & Holmstrom, 2015) often with profound security implications (Blum, 2020). Close coupling of digitalization with everyday business has also led to increased attention to security and resilience of digital systems. Instead of being an isolated technological issue, digital security has become a strategic business challenge (Kaplan et al., 2019; Blum, 2020). As organizations seek to digitalize, significant security threats can arise, resulting in fundamental challenges between the business's need to digitalize and the security team's responsibility to protect the organization alongside existing operating models and IT practices (Kaplan et al., 2019). Technology brings new risks that must be addressed from regulatory, organizational, and cybersecurity perspectives. This new approach requires new forms of functional collaboration and resource configurations (Begozzi et al., 2023). Both researchers and practitioners emphasize the need for insight on how organizations can build their *digital security (DS, hereinafter)* assets alongside other strategic and business initiatives.

The proliferation of the Internet has led to globalized, interconnected business with an increased number of time critical services, many levels of infrastructure and a shift in view of actors (Caralli et al., 2010). There is a widening gap between digital security (DS) and digital transformation despite increased investment in the former - ongoing development in digital transformation is taking place at a much faster pace than improvements in DS (Blum, 2020). The pursuit of threats can seem endless as what organizations have not solved in the past is coming back to threaten them. In the early days of the Internet, the threat landscape was not very complex, but this has changed in the last decade due the interconnectedness of actors (Blum, 2020; Schneier, 2015).

Digital transformation demands more cybersecurity, not just because it means “more IT” but also “riskier IT” since newer technologies such as mobile devices, social networks, cloud computing and artificial intelligence (AI) have emerged but often without adequate security built into them (Blum, 2020). A number of high-profile incidents have drawn attention to this issue. In March 2023, Swedbank, one of the largest banks in the Nordics and Baltics was fined 850 million SEK for having a “lack of internal controls” in place during a change of IT systems (Finansinspektionen, 2023). This resulted in halted transactions where almost one million customers had incorrect balances in their accounts, and were unable to make payments (Finansinspektionen, 2023; Rasmussen, 2023).

More recently, in October 2023, Avanza, a Swedish online bank that offers investment and saving services, also went through a similar issue. Customers were unable to log in to their accounts for several hours as a result of a Distributed Denial-of-Service (DDoS) attack (Axelsson, 2023) where malicious actors overload the traffic of a website with more requests that the server can handle (Cloudflare, n.d.).

Other prominent examples include the NotPetya ransomware attack (McQuade, 2018) and more recently, disruption in services of the Swedish grocery chain, Coop also due to ransomware (Thorsell, 2021). These events highlight gaps in implementation of digital security and the need to take a holistic, organization-wide perspective instead of an isolated focus from a technological standpoint taken by practitioners and information systems researchers alike (Schinagl et al., 2022).

New regulatory frameworks and guidelines have been implemented internationally at the EU level in response to rapid and inventive cyber threats and cyberattacks (Butler et al., 2023; Calliess & Baumgarten, 2020). There has been significant push from regulators for organizations to address gaps in their security policies and processes. However, disseminating these new compliance requirements from the regulation into existing IT assets and related resources has posed challenges for firms. Many established firms have highly complex and interconnected systems that have been operational for decades, making it difficult for them to assess the scope and impact of new regulation on existing IT assets, policies and procedures (Clark-Ginsberg & Slayton, 2019; de Vaujany et al., 2018).

Over the years, there has been a focus on technical aspects of security to prevent incidents from happening. Organizations have improved exponentially at tracking threats and offering cybertraining to employees with a more preventative mindset but detecting and responding are not enough. Instead, digital security should be part of day-to-day work, but many organizations still struggle with this due to fragmentation, despite having better regulatory guidelines and tools to understand the threat landscape. European Union Agency for Cybersecurity (ENISA) singles out ransomware, malware, threats against data, denial of service and others as the main threats facing organizations due to their widespread occurrence and the significant impact resulting from the realization of these threats (see Fig. 1). This list is not exhaustive but presents an overview of the current threat landscape (ENISA, 2023).

Fig. 1 Primary threats facing firms, adapted from ENISA Threat Landscape 2023

1.1 Research gap and research question

The organizational aspects of DS have so far been under-researched in the field of Information Systems *(IS, hereinafter)* despite its undeniably critical role in firms (Dhillon et al., 2021a; Schinagl et al., 2022; Schinagl & Shahim, 2020). Previous research on DS places a large emphasis on technical aspects and IT controls with less focus on how they should be leveraged from a managerial and strategic point of view (Mbanaso et al., 2023; Schinagl & Shahim, 2020). There has so far been limited research into how DS and accompanying regulation influences firm resources and capabilities. Increased regulation and evolving threats highlight

the need for strategic guidance since existing literature lacks clear guidance on organizational best practices to manage DS resources in a constantly evolving threat landscape.

Within management and strategy literature, there is limited understanding of underlying mechanisms on how dynamic capabilities are built, expressed and transformed within firms which is compounded in the context of digital transformation (Chirumalla, 2021; Teece, 2018). An illustrative quote from Teece (2018) further emphasizes this problem:

> *"Complements are pervasive throughout the economic system, and particularly in technology development and business transformation. Nevertheless, they are frequently ignored. However, they are central in PFI. Perhaps their neglect can be blamed on Schumpeter (1942), who stressed that "new combinations" of artifacts organized by the entrepreneur brought gales of creative destruction. While emphasizing the substitution of new products for old, he did not stress that, with complements, a rising tide can lift many boats. In the PFI framework, complements need to be considered with more granularity in order to illuminate value capture issues, particularly the ramifications of digital convergence."*

This study takes a disaggregated view of complementary assets in line with prior empirical research to determine the different roles these assets have in the exploitation of core technologies. Answering calls from both IS and strategy researchers, this study aims to advance the theoretical understanding of how DS complementary assets can be useful for companies in increasing their resilience to cyberattacks while being compliant to new regulatory frameworks. Moreover, this study further seeks to examine how DS develops in organizations alongside other business and technological IT processes in organizations. Considering the aforementioned purpose and gaps in existing literature, the following research question has been formulated:

- *RQ: How do firms adapt their complementary assets to deal with digital security challenges arising from a constantly evolving threat and regulatory landscape?*

To answer this research question, I reviewed existing literature on dynamic capabilities, arriving at complementary assets as a suitable conceptual framework capturing the nature and interrelationships between these assets. Studies demonstrate that complementary assets are a suitable perspective to investigate how certain assets need to be transformed or reconfigured to exploit new business opportunities in times of digital and regulatory change (Butler et al., 2023; Chirumalla, 2021; Sköld et al., 2020).

1.2 Expected contribution

This study has a twofold contribution to the literature by studying the intersection between dynamic capabilities and digital security and consequently filling a research gap within each respective field. This paper enriches extant research on RBV and dynamic capabilities by focusing on complementary assets, specifically those in relation to digital security. Antecedents of dynamic capabilities, namely complementary assets, are also examined in this research as they help to explain why certain resources are more likely to support firms in coping with regulatory change. Besides features of the resources themselves, RBV emphasizes the way an organization deploys its resources. Overall, research into antecedents of dynamic capabilities such as selection and orchestration of underlying complementary assets remains limited and fragmented without a clear consensus (Ceipek et al., 2021).

1.3 Delimitation and scope

Since this research aims to study RBV and complementary asset related aspects of DS and not technical aspects, specific attributes of DS itself are not deemed relevant. Thus, this study takes a collective view of DS incorporating different perspectives of the term. Detailed definitions of underlying technologies are also not described in detail for the same reason as the aim of this study is not to provide IT solutions to mitigate vulnerabilities in systems.

1.4 Research outline

Previously discussed problematization, purpose, and research question are explored using a qualitative, explorative approach involving “knowledgeable agents” from various organizations in the financial sector working closely with DS. The study adopts an abductive approach that alternates between theory and empirical data. The results are presented thematically according to the conceptual framework followed by an analysis and discussion of the implications of these findings to tie back to the research question. Finally, the study discusses potential limitations and suggests directions for future research. The study is divided into the following sections (i) Introduction, (ii) Literature Review, (iii) Methodology, (iv) Findings, (v) Analysis, and (vi) Conclusion.

2. Literature review

This section starts by reviewing the literature on the resource-based view in *(2.1)* and complementary assets in *(2.2)* to establish the theoretical basis of this study and its primary research stream. This is followed by a discussion of relevant literature from the field of digital security in *(2.3)* to create a deeper understanding of the key problem. I compare various conceptualizations of complementary assets and how they can be used as a lens to analyze the interplay between digital security and the nature of a firm's complementary assets in *(2.4).* Lastly, the conceptual framework is introduced in *(2.5).*

2.1 Resource-based view

This section starts by defining RBV and dynamic capabilities. In applying complementary assets as a conceptual lens, the *resource-based view (RBV)* of the firm is taken, necessitating a discussion of the theoretical implications of the RBV and its applicability to the field of IS.

2.1.1 Resource-based view

According to the RBV, the firm is viewed as a collection or bundle of resources, commonly defined as the stock of available factors that the firm owns and controls (Dierickx & Cool, 1989; Wernerfelt, 1984). These resources are heterogeneously distributed across firms, similar to the pieces of a "jigsaw puzzle" (Penrose, 2009). Taking a broad definition, resources can be tangible (e.g., plants, equipment, natural resources, raw materials, finished goods) or intangible (e.g., knowledge, information, processes, firm attributes, information). In this view, the firm's rationale is to use these resources, combining these resources into products and services in such a way that returns are maximized over time (Barney, 1991; Wade & Hulland, 2004). Combining and recombining these resource bundles enable the firm to design and execute strategies that improve efficiency and effectiveness as well as generating competitive advantages (Barney, 1991; Newbert, 2007). An organization's superior performance is attributable to its unique, valuable, rare, inimitable and non-substitutable capabilities that enable the organization to perform activities more efficiently and effectively than its competitors (Wade & Hulland, 2004). The RBV assists managers in understanding how the firm's assets can be used to improve its performance. Hamel & Prahlad (2006) argue that the broad understanding of the term resource

implies that past experiences, organizational culture, and competencies can be critical for the firm's success.

The first mentions of RBV in the information systems literature began to appear in the mid-1990s to identify single sets of resources that contributed to business value. Ross et al. (1996) identified various assets related to humans, technology and relationships as IT assets to be central. This was complemented by the findings of Bharadwaj (2000) that included include IT infrastructure and IT-enabled intangibles. Numerous subsequent studies in IS (Nevo & Wade, 2010; Seddon, 2014) and digital transformation (Chirumalla, 2021; Witschel et al., 2023) have taken the RBV view of the firm.

2.1.2 Dynamic capabilities

One critique of the RBV is that it does not fully explain how competitive advantages can be gained in rapidly changing environments since it takes a static view of the firm and its capabilities (Eisenhardt & Martin, 2000; Helfat & Peteraf, 2015). Teece (2007) argues that the RBV does not fully capture "how firms develop or acquire new resources and manage them over time" in response to rapid, uncertain contexts. The dynamic capabilities perspective is built on the notion that competitive advantage originates from unique configurations of resources that are created through strategic processes (Eisenhardt and Martin, 2000). Firms require dynamic capabilities related to sensing, seizing and transforming (Teece, 2007; Chirumalla, 2021). Sensing addresses identifying and responding to opportunities and threats (Teece, 2007). Seizing relates to taking advantage of those opportunities. Finally, transforming capabilities requires keeping the organization competitive by transforming its assets. Teece's view on complementary assets predominantly focus on the second activity, seizing, by providing decision rules for "how entrepreneurs can act to seize the moment."

Understanding dynamic capabilities requires a thorough understanding of the firm's underlying work processes (Eisenhardt & Martin, 2000). Dynamic capabilities are impacted by the firm's organizational processes, systems, and structures to manage its business in the past (Teece, 2007). Teece further elaborates that the order for implementing dynamic capabilities is consequential, as they are often combinations of simpler capabilities and related routines, some of which may be foundational to others and must be learned first. Yet, the research on building

these enabling capabilities in digitally transforming environments is limited (Chirumalla, 2021; Teece, 2018).

Having resource endowments alone does not guarantee competitive advantages or firm performance; the firm must possess distinctive capabilities to better utilize its resources (Lai et al., 2010). Dynamic capabilities can be distinctive resources and capabilities that are required to achieve competitive advantage (Johnson et al., 2017). Typically, these linked resources and capabilities are referred to as "core competences" that remain unique because they comprise a bundle of constituent skills and technologies rather than a discrete skill or technology (ibid). Managers are encouraged to concentrate on building core capabilities, but these are not always easily identifiable from other supplementary assets (Chirumalla, 2021; Lai et al., 2010)

There is still a research gap in the antecedents of dynamic capabilities, specifically in *digital* complementary assets (Ceipek et al., 2021; Teece, 2018a) and consequent regulatory changes relating to these assets. The basic theoretical constructs offered in the PFI model provide some clarity to this issue (Pisano, 2006). Previous studies have established the pivotal role of complementary assets but the role of complementary assets during periods of regulatory change and changing digital environments is underexplored with the exception of a few studies (Andronikidis et al., 2021; Ceipek et al., 2021; Sköld et al., 2020).

2.2 Complementary assets

This subsection discusses the conceptualization of complementary assets and related literature highlighting the role of complementary assets in firms.

2.2.1 Definition of complementary assets

Teece first proposed the concept of complementary assets in 1986 as part of his seminal Profiting from Innovation (PFI) theoretical model. The extant literature in economics and strategy at the time made no mention of complementary assets. Very broadly, complementary assets are defined as:

> *Complementary assets refer to the resources, capabilities, and assets that are needed to profit from an innovation. These can encompass any asset that facilitates the commercialization of an innovation, such as financial assets, complementary technology, intangible assets, management capabilities, or market knowledge (Teece, 1986).*

The PFI argues that the success of innovations, to a lesser extent, relies on the innovator's market share, "but [rather] to the (complementary) asset structure of the innovator, management's market entry timing decisions, and contractual structures employed to access missing complementary assets." Choices with respect to sourcing missing complementary assets are dependent on the asset positioning of other market participants, and on the intellectual property protection available.

While the PFI framework and complementary assets precede the literature on dynamic capabilities, there are "cursory" traces of "dynamic capabilities thinking" since complementary assets might represent capabilities because if the firm did not have certain complementary assets, they would need build or source them externally (Teece, 2006). The PFI framework in a certain sense also "anticipates critical aspects of the dynamic capabilities" framework, more specifically the value that can be derived from the orchestration of cospecialized assets (ibid). In a sense, the ability to build and/or buy and then combine cospecialized assets that yield scope economies can be seen as a dynamic capability (ibid).

Furthermore, the inclusion of intangible assets in this definition is in line with the RBV. Teece (2006) demonstrates that the PFI can also be applied to intangible assets such as IT technologies that are discussed in this paper. The main tenet of the PFI framework (Teece, 1986) is that successful commercialization of technology requires the technological knowledge in question to be used and deployed in conjunction with complementary resources. In a follow-up article, Teece (2018) argues the need for increased investigation and scrutiny of complementary assets in digital contexts. He further states that digital security challenges induce an additional dimension of complexity to this analysis.

2.2.2 Importance of complementary assets

Complementary assets play a crucially important supporting role with regards to a firm's dynamic capabilities but are also essential for successful commercialization of a firm's innovations. Accessing complementary assets has a direct impact on a firm's dynamic capabilities and its propensity to innovate (Jacobides et al., 2006). Complementarities involve the exploitation of the relationship between multiple elements that impose a significant challenge in terms of managing resources purposefully towards innovation (Andronikidis et al., 2021). Certain assets may exert their full potential only through the interaction with other co-existing assets that firms may or may not have at their disposal. Therefore, "examinations of the role of complementary assets as isolating mechanisms for value capture" are required according to Teece (1986).

Technology can be conceptualized "as a special kind of expert knowledge and processes" (Ceipek et al., 2021) and this is used as the basis of this study. A growing stream of research has demonstrated the importance of complementary assets in technological exploitation (Bianchi et al., 2014). Technological exploitation refers to a wider managerial function, which focuses on the expected benefits accrued through implementation, absorption and operation of technology within the firm which includes incremental developments, process improvements and marketing (Cetindamar & Phaal, 2023). Success in achieving the organization's mission relies on critical dependencies between organizational goals and objectives, services, and associated high-value assets (Caralli et al., 2010).

Similarly, complementary assets can also play a supporting role in technological diversification (Ceipek et al., 2021; Chiu et al., 2008). Technological diversification concerns the entry of new technological areas, which bring inherent, inevitable risks and uncertainties that may prevent investments in innovation to being converted to final products (Cooper, 1983; Granstrand & Oskarsson, 1994). However, these can be mitigated by complementary assets in areas such as capital, distribution and marketing (Chiu et al., 2008). Some issues, such as the link between technological diversification and performance outcomes, have been studied extensively (Miller, 2006). In contrast, other topics, such as the antecedents of technological diversification, have received less attention (Ceipek et al., 2021).

In line with the constantly evolving nature of security threats, the dynamic capability view does not take the market, or the product as given, but as objects of strategic reconstitution, emphasizing the key role of strategic management in appropriately adapting, integrating, and re-configuring internal and external organizational skills, resources, and functional competences towards changing technological conditions (Cetindamar et al., 2009; Teece, 2018).

2.3 Digital security

DS can be viewed as subset of Operational Resilience *(OR, hereinafter)* as the latter includes policies relating to business continuity, backing up and restoring data in the event of failure, etc. while DS deals with the mitigation of threats and vulnerabilities (Caralli et al., 2010; ENISA 2023). OR is defined as the processes and related practices by which an organization designs, develops, implements, and controls strategies for protecting and sustaining high value (i.e., organizationally critical) services, related business processes, and associated assets (Caralli et al., 2010; Blum, 2020).

2.3.1 Definition of digital security

This study takes a taking a holistic view of DS that covers the major subsections of the IS security literature to address its objectives of analyzing the nature and deployment of DS assets that organizations require. In most IS literature, the various definitions of security are used interchangeably and a clear consensus on the distinctions between IT security and cybersecurity is still emerging. Cybersecurity is used as an all-inclusive term and refers to:

> *The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect interconnected environments* (R. von Solms & van Niekerk, 2013).

In other words, cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment originating from networked Internet technologies, extending beyond firm boundaries of the firm to include users (ibid). The general security objectives comprise of the CIA triad which stands for confidentiality, integrity and availability (B. von Solms & von Solms, 2018; R. von Solms & van Niekerk, 2013). IT security, on the other hand, includes both software, hardware and other underlying technologies. Cybersecurity includes a broad range of incidents encompassing cyberbullying, terrorism, ransomware and other harmful consequences not just to organizations but also to users from malicious actors. Nevertheless, at its core, all security is about the protection of assets from the various threats posed by vulnerabilities. The vast majority of security processes usually involve the selection and implementation of security controls (also known as countermeasures) that reduce the risk posed by vulnerabilities and incidents.

Since there are many overlapping elements between cybersecurity and IT security, this study chooses to address the wider field of DS and not limit itself to subsections such as cybersecurity, information security and IT security. DS itself broadens the section of cybersecurity and IT security by incorporating the organizational dimension while the other definitions mainly focus on IT assets, technologies and processes, making DS highly appropriate and suitable to use in this study.

DS promotes that security should not be left to IT professionals alone but rather align with business strategy to improve assimilation and cascading of security practices and policies throughout the organization (Schinagl & Shahim, 2020; Schinagl et al., 2022). Thus, DS goes beyond the definition of cybersecurity by incorporating the organizational and societal aspects of cybersecurity and does not focus purely on technical aspects. In that regard, DS can be defined as:

Digital security addresses the core elements of cybersecurity but additionally incorporates a dimension of resilience and security by embedding security in the business and in all of the related business dimensions and organizational factors as a whole alongside machines, people, objects, processes, etc. (Schinagl & Shahim, 2020)

To date, most research that intersects between the organizational aspect of security also uses a similar delineation to empirically study the phenomenon using DS as the main topic of interest (Liu et al., 2020; Schinagl et al., 2022b). Using the wider definition DS is also in alignment with the call with IS to simplify and merge the various definitions for simplicity and clarity (B. von Solms & von Solms, 2018).

The overall state of literature in the field of DS, IT security and cybersecurity can be considered intermediate, having generated a substantial amount of theoretical and empirical work in technical domains such as frameworks and technical security controls to counter digital security risks. However, significant research gaps persist in the areas of implementation and governance of DS practices (Schinagl et al., 2022). Review articles highlight that existing research is highly normative and prescriptive, taking a static, one-size-fits-all and top-down approach limiting opportunities for practical and strategic implementation (Dhillon et al., 2021; Schinagl et al., 2022). Moreover, current DS research does not provide enough empirical and theoretical insight to support organizations overcoming poor performance in DS implementations (Diesch et al., 2020).

A lack of understanding under what conditions DS investments can be leveraged successfully hampers the ability of organizations to successfully exploit and diversify their technology. DS is seen as a cost rather than source of competitive advantage in many organizations, which is also the case for other IT related complementary assets (Hughes, 2006). The successful deployment of IT projects in an organization requires wide investment in a range of

complementary assets to support the technology but there is a significant time the lag between IT investment and business outcomes, making it difficult to disentangle causal impacts of DS related complementary assets (Hughes, 2006; James et al., 2013). Similarly, complementary assets do not generate any revenues for the company, differentiating them from core assets and innovations (Zhou, 2019).

2.3.2 Regulatory change

Overall, details in regulation are sometimes seen as a hindrance to innovation (Clark-Ginsberg & Slayton, 2019; Freij, 2020, 2022). On the other hand, studies have shown that using regulation more efficiently or from different angles can result in strategic advantages for firms (Sköld et al., 2020; Freij, 2022). Regulatory change can often influence the impact of technology, leading to concerns about balancing regulatory change impact with business innovation. Having received substantial scrutiny from regulators, DS is no exception to this.

Several researchers also highlight the lack of research within the field of IS with regards to resources need to address digital regulation, limiting the understanding of critical risks and issues (Clark-Ginsberg & Slayton, 2019; de Vaujany et al., 2018). Butler et al. (2023) note that certain industries such as health care and the financial sector have a considerable level of field-specific regulation focused on IT artefacts and their design and use.

The design of IT assets involves a regulatory dimension, but this process is rarely recognized and made visible in related studies. Existing IS literature also lacks a consensus on the role and adaptability of IT assets in the continued expansion and maintenance of exponentially complex rule sets. Many efforts to manage cyber risks are based on a "top-down" management approach, with the objective to encourage system designers and operators to adopt best practices (Paté-Cornell et al., 2018). However, there is limited guidance on how firms should achieve this. A number of general, regulatory documents are available on DS but often they lack specific considerations of capabilities and core technologies.

2.3.3 Changes to DS assets due to the regulatory and threat landscape

Conversely, having complementary assets can create difficulties for firms when navigating technological discontinuities (Bei, 2019; Cozzolino & Verona, 2022; Jacobides et al., 2006). Firms with established complementary assets might be too deep into an industry to be aware of the gradual shifts or are constantly facing the choice of whether to continue their existing path or to try a new direction. This true even in the context of IT and DS assets.

This also influences continuities and trajectories of DS related complementary assets that firms subsequently adopt. DS regulation, similar to prior IT regulation, is deeply embedded in and now relays most organizational practices at scale and depth (de Vaujany et al., 2018) The use of such capacities during regulation manifests itself through an ongoing materialization of rules toward organizational practices whereby rules become related, conveyed, and eventually embedded into IT assets (ibid).

2.4 Classification and specification of DS complementary assets

Teece (1986) proposes that that the commercialization of any technological achievements is inseparable from the support of assets in multiple areas. For the purpose of this study, manufacturing, distribution and relational assets are examined due to their highlighted importance in IS and DS literature in line with the research question.

The main contribution of Teece's PFI framework is providing a taxonomy around the specification of complementary assets and technologies, namely generalized, specialized and cospecialized complementary assets. These definitions have been upheld in empirical research (Bianchi et al., 2014; Sköld et al., 2020; Cozzolino & Verona, 2022).

2.4.1 Manufacturing complementary assets

Manufacturing is required to convert inventions into marketable products (Teece, 1986) and the absence of complementary technologies can result in the failure of the entire system (Teece, 2006). The original PFI framework outlines these capabilities in the context of traditional manufacturing firms but lacks guidance on how firms can leverage complementary assets in digital firms. Within the IS literature, manufacturing technologies can be classified as: Operation Technology (OT) and Information Technology (IT). OT has supports value creation

and manufacturing processes involving physical devices, and software required to control and monitor processes while IT combines all necessary information processing and technologies (Giannelli & Picone, 2022; Maleh, 2021). Gradually, OT and IT have converged to introduce a number of advantages, such as higher degree of flexibility, scalability and efficiency in the coordination of advanced services and processes (Kure et al., 2022).

On the other hand, the increased reliance on IT creates new opportunities for cyberattacks and increases the vulnerability of those systems, which is exacerbated by the criticality of these systems and infrastructures. Continuously evolving security risk requires more proactive security strategies to attain resilience in addition to the existing reactive approaches (Baskerville et al., 2014). In addition, AI also has strong potential to provide real-time prevention, detection, and recovery measures of technical systems with higher accuracies than traditional methods (Lee, 2020).

2.4.2 Distribution complementary assets

Distribution complementary assets relate to the marketing and sales networks used by financial service organizations to sell their products. Distribution assets, such as sales forces and branches, connect customers with innovations (Teece, 2006; Sköld et al., 2020). A variety of assets and competences are essential to this process and may not always be present in-house (Teece, 1986). In some instances, they may be accessed through contractual agreements, adding a dimension of risk through “dependencies” (ibid).

Moreover, within distribution assets, service networks are necessary to support processes such as repair, maintenance, and after-sales services (Dietl et al., 2009; Tripsas, 1997). Technology and digital business activities create a significant change in the way organizations interact with customers (Schingal & Shahim, 2020). Customers are also demanding increased security and privacy in product offerings (Blum, 2020). Thus, DS is crucial in gaining the trust of customers. Consequently, DS strategies are likely to be unsuccessful if the wider customer experience is not taken into consideration.

2.4.3 Relational complementary assets

Dyer & Singh (1998)argue that RBV in its traditional form takes an overly internal view of the firm as resources might be outside the span of firm boundaries. They may be “embedded in inter-firm resources and routines with the potential to generate relational rents”. Thus, complementary assets can be synergistic in nature (Bianchi et al., 2014) and leveraging the complementary resources with that of alliance partners and outside firms can generate relational rents (Dahlander & Wallin, 2006; Dyer et al., 2018). This becomes increasingly relevant as the perspective on DS shifts from intra- to interorganizational (Diesch et al., 2020; Kure et al., 2022; Schinagl & Shahim, 2020).

Jacobies et al. (2006) further argue that complementary assets be cospecialized at both the firm and industry level describing the latter as “architectures” between multiple firms rather than dyadic relationships. The PFI framework suggests that there is a market for know-how. When complementary assets are idiosyncratic and cannot be obtained through marketplace transactions, alternate forms of organization are required instead. In the same vein, Dahlander and Wallin (2006) find that participation in open-source software developer communities can be used a complementary asset for firms to accelerate open innovation in a firm. Community based complementary assets cannot be acquired through the market. Instead, they require continuous participation, interaction and learning (ibid). To gain access and legitimacy firms deploy employees to interact with other participants in the community (ibid).

2.4.4 Specification of complementary assets

Complementary assets can be generalized, meaning that they are not tailored in any way to the core technology. Such assets provide little or no competitive advantage to a firm, as such assets are readily available in the marketplace or easily developed by the firm itself (Teece, 1986; Teece, 2006; Sköld et al., 2020). Generalized assets are akin to the “fungible resources” mentioned by Penrose (1959). In Penrose's theory of the growth of the firm, certain assets are fungible and can be leveraged to support diversification (Teece, 2006). However, these generalized resources are an essential foundation for subsequent specialization or cospecialization (Chiu et al., 2008; Sköld et al., 2020).

note that there is a continuum between resources that are specialized to a particular setting and generalized resources that can be applied more broadly in many environmental settings. According to Teece's PFI framework, complementary assets can be specialized or cospecialized, building on the generalized complementary asset (Teece, 1986, 2006). Specialized assets are those which are unilaterally dependence between the core technology and complementary asset or vice versa (ibid). Certain complementary assets can be co-specialized where both the complementary asset and the core technology are bilaterally dependent on one another (ibid). The level of specialization to the core technology is an important decision (Teece, 1986; Jacobides et al., 2006).

Specialized and co-specialized complementary assets are difficult to access in the marketplace due to transaction cost issues associated with asset specificity and small numbers bargaining (Ceipek et al., 2021; Chiu et al., 2008). It is these specialized or co-specialized complementary assets that generate competitive advantage for firms (Teece, 1986; Sköld et al., 2020). When innovation depends on specialized complementary assets for successful commercialization, a firm with proprietary access to such assets will outperform competitors who do not have access to such assets (ibid). Specialized and cospecialized assets are more difficult to replicate than generalized complements (Teece, 1986; Teece 2006).

Helfat & Lieberman (2002) state that individual resources and capabilities fall "on a continuum between those that are very narrowly specialized to particular settings" and "those that are broadly applicable in virtually any setting" where specialized firm resources and capabilities are specific to particular settings, and therefore are useful in only a limited range of environments. In contrast, generalized resources and capabilities can be applied more broadly in many environmental settings. This can lead to discontinuities if the dominant paradigm changes substantially due to changes in the market or the regulation, requiring firms to reinvest in a new set of complementary assets (Cozzolino & Verona, 2022).

2.5 Conceptual framework

There is a noticeable lack of academic literature linking DS with the field of strategy and management as shown in Table 1. This study uses complementary assets as a sensitizing concept to act as an interpretative device that sets the direction for data collection and sensemaking of the concept of DS.

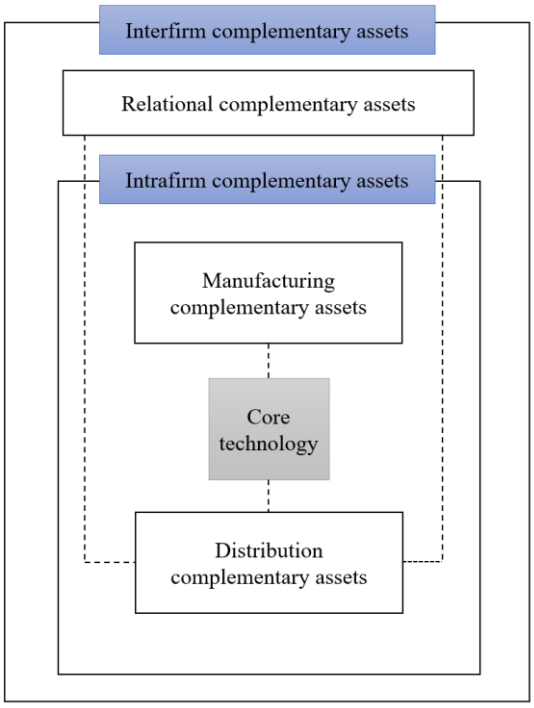
Table 1: Overview of identified research gaps

Identified research gaps	***Amongst others highlighted by***
Digital security from a managerial perspective	*Diesch et al., 2020; Schinagl & Shahim, 2020; Shin & Lowry, 2020; Dhillon et al., 2021; Schinagl et al., 2022; Bulter et al., 2023*
Complementary assets in (1) regulatory change (2) digital transformation or technological change	*(1) Teece, 2018; Sköld et al., 2020; Freij, 2022; Freij, 2022 (2) Teece, 2018; Andronikidis et al., 2021; Ceipek et al., 2021; Cozzolino & Verona, 2022*

The proposed conceptual framework is inspired by the classification and specification of complementary assets used by Sköld et al. (2020) to study the impact of regulatory change and the DS threat landscape. Some key additions have been made in line with the research question. This study adds "relational complementary assets" to the classification of complementary assets within the proposed framework in order to capture interfirm and industrial architectures in place. This is in agreement with Teece (2006) who argues that the PFI can be extended with "a second circle to envelope the first" in recognition of the role of relational technologies as well as that of supporting institutions such as regulators and standard setting bodies. For comparison, Teece's original framework can be found in Appendix 1.

The three specifications of complementary assets are assessed in parallel to assess their collective impact on manufacturing, distribution and relational complementary assets. As a result, the extended conceptual framework as proposed in the findings sections aims to explore the relationship between DS and the nature of the needed complementary assets to improve understanding of DS in light of the changing threat landscape and regulatory environment to achieve the research aim. Finally, in order close the identified research gaps, Figure 2 depicts the conceptual framework used in this study based on insights from the literature review and with the overarching research question in mind.

Fig. 2: Conceptual framework used in this study where the dotted lines indicate the specialization of the complementary asset to the core technology and vice versa. An updated version of framework will be presented in the findings section.



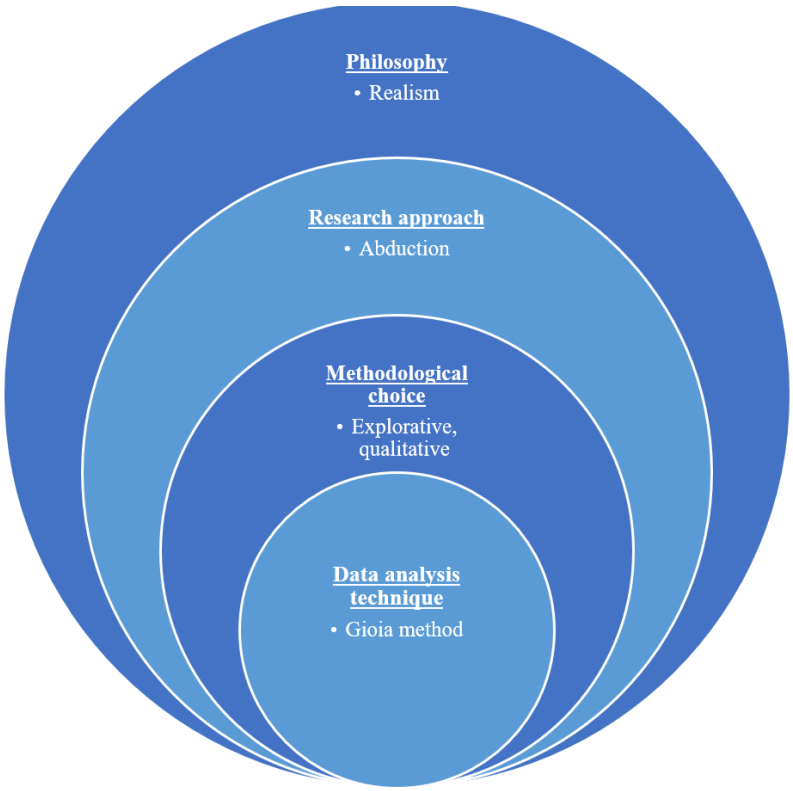
3. Methodology

This section describes the research approach and methodological choices taken by this thesis. First, *(3.1)* elaborates the reasoning behind the selection of the research method while illustrating the fit between the research question and the research purpose. I also discuss the rational for the qualitative case study and the abductive method in *(3.1).* Subsequently, I describe the data collection in terms of interviewee selection and the interview process *(3.2)* followed by a description of how the data was analyzed in *(3.3)* and reflections on the ethics and the quality of the method in *(3.4)*.

3.1 Methodological fit

Figure 3 depicts the method used in this thesis, which is adapted from (Saunders et al., 2019). Different elements of the research method must be coherent and consistent to systematically answer the research question of this thesis. In addition, the research philosophy, approach and method must align with the research objectives and data.

Fig. 3 Research onion adapted from Saunders et al. (2019)



3.1.1 Research philosophy

Since this study aims to understand how organizations build their complementary assets in the context of DS, I chose a realist lens. There are two levels of realism: direct and critical (Saunders et al., 2019). Direct realism takes a purely objective stance and suggests that the world is relatively unchanging (Saunders et al., 2019). Critical realism posits that reality is stratified, mediated, and emergent, incorporating multiple levels of reality, such as the empirical, the actual, and the real. These levels are influenced by causal mechanisms, structures, and agents, and that can change over time and space (Bhaskar, 1978; Tsang, 2014). This differs from positivism, which presupposes that reality is objective and observable, or interpretivism, which investigates subjective meanings and experiences. Therefore, critical realism is suited to this thesis because its aim is explaining how reality works rather than predicting or describing it.

Moreover, realism is also appropriate to this study because unobservable factors such as processes and knowledge are examined. To summarize, ontologically, realism assumes that there is an objective reality. Epistemologically, critical realism assumes modified objectivism, recognizing that human perception and interpretation play a role in our understanding of reality, addressing some of the issues with direct realism (Mingers et al., 2013; Tsang, 2014; Saunders et al., 2019). However, critical realism is not without its shortcomings. Critical realism further states that reality exists independently of individual perceptions but knowledge of it can be fallible and partial (Bhaskar, 1978; Tsang, 2014).

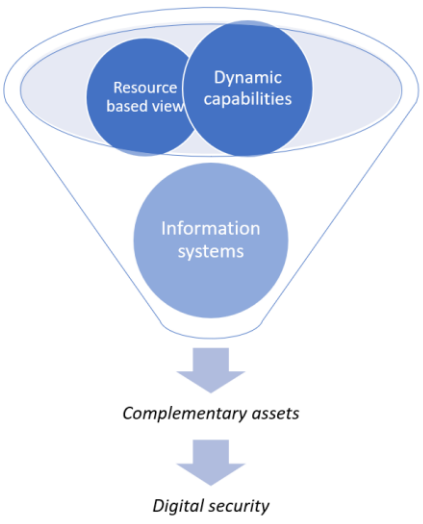
Thus, adopting critical realism also requires a researcher to question their own assumptions with an openness to alternative explanations and evidence. Having worked in the area of compliance at a Nordic payment institution equipped me with transferrable insights into this topic, allowing me to move beyond theorizing (Daft, 1983). At the same time, this can also lead to biased perspectives. Measures taken to address this are discussed further in Section 3.5.

3.1.2 Research approach

Initially, an inductive approach was considered whereby empirical data is used to construct theory. However, after developing an initial feeling for the field of DS through early interviews, the abductive approach was selected since this purpose of this study is not to test existing theory but rather understand how it has evolved due to ongoing changes in the threat landscape and regulatory change.

Since there is a noticeable lack of academic literature about the organizational and managerial aspects of DS, I use concepts from various theoretical domains (Fig. 4). The key literature that this paper builds on is that on the RBV and dynamic capabilities with complementary assets as a sensitizing concept, while drawing on DS related concepts from the IS literature to explain the empirical phenomenon. Since IS research takes a multidisciplinary and cohesive socio-technical view of various perspectives, valuable insights into the topic of DS can be obtained by examining concepts from the field of IS (Butler et al., 2023). The multi-theoretical lens used in this study can be depicted as a funnel where broader theories are first identified and then a narrow research focus is identified (Mbanaso et al., 2023). The funnel strategy supports the sense-making process of the theory, allowing the researcher to filter ideas encountered in the literature and deconstruct the problem under investigation (ibid).

Fig. 4: Research funnel used in the sense-making of the theory and the literature based on Mbanaso et al. (2023)



Researchers can benefit from an initially defined construct to enable enhanced understanding and to provide a platform for the initial design of theory development (Awuzie & McDermott, 2017; Eisenhardt, 1989). Observing that concepts from the field of complementary assets had a high degree of relevance and fit with the research question, they were used to guide the collection of empirical data.

Because abduction entails working with theory and empirics simultaneously, it allows for surprising empirical findings (Timmermans & Tavory, 2012). By alternating back and forth between theory and observation at multiple stages, a holistic understanding of the research question can be obtained. In addition, this study becomes more relevant by mirroring reality as closely as possible (Bryman & Bell, 2015). Under the abductive approach, the researcher can revise theoretical choices after initial observations.

3.1.3 Methodological choice

Qualitative methods using a realist lens are well-positioned to construct propositions and identify structured interactions between complex mechanisms (Mingers et al., 2013). Thus, a qualitative approach is used to gather contextual knowledge at the intersection of DS and complementary assets, as there is limited research and theory connecting the two. This study is primarily exploratory as the purpose is to identify and clarify the nature of DS while providing new insights. An exploratory approach is taken to generate new theoretical insights and contribute to existing research.

After carefully considering methodological fit with the research question and objective, a qualitative study was deemed more suitable than a quantitative one since this paper seeks to answers explorative "how" questions (Saunders et al., 2019; Yin, 2016). Despite the quantifiability of the theoretical lens of this study, a deeper level of understanding of intangible DS complementary assets can be discovered through a qualitative methodology (Schinagl et al., 2022). Interrelationships between specializations of complementary aspects do not easily lend themselves to quantitative datasets as theory lags behind in the operationalization of these variables (Bianchi et al., 2014; Ceipek et al., 2021). Because DS is a confidential topic, organizations are less likely to share their internal insights on this topic, creating challenges in data collection in the form of in-depth single firm case studies or quantitative surveys involving

multiple firms. Establishing face-to-face contact with the interviewees was thus deemed necessary to create a sense of trust and to ensure their participation.

Case studies, into one or multiple firms, could also lead to highly normative findings as organizations tend to tailor their DS strategies based on their individual resource availability, market position and product offerings. Certain individual organizations in the financial sector were deemed suitable but it became evident that conducting a multiple case-study into a few firms would prevent me from being sufficiently detailed in my findings, reducing my ability to develop a holistic understanding of a complex phenomenon such as DS. Therefore, a qualitative method based on multiple, expert interviews is highly suited to the collection of complex detailed data with high exploratory potential (Saunders et al., 2019).

3.2 Data collection

The data collection aims to provide a holistic overview of how various actors perceive phenomena related to DS in their organizations. To collect the main body of research data, semi-structured interviews with field experts in a variety of roles were conducted. Additionally, triangulation with secondary sources such as industry reports, whitepapers and regulatory documents was conducted to fact-check and validate empirical findings (Robinson, 2014).

3.2.1 Pre-study

A pre-study consisting of 3 semi-structured interviews was conducted (Flick, 2018).The goal of this pre-study was to learn more about the field of DS to narrow down the research question and assess the fit of complementary assets as a sensitizing concept. During the pre-study and initial interviews, it became clear that digital security was one of the most important concerns facing practitioners today. The focus of this study was then narrowed down to DS to understand relevant challenges from a theoretical and empirical perspective. Selecting DS within the wider area of OR was also in line with the funnel approach taken within the field of IS (Mbanaso et al., 2023). Additionally, the pre-study also provided a valuable opportunity to test the interview questionnaire and make necessary revisions to its composition. Although no new insights were obtained during the pre-study, the research direction and reliability of the study were greatly improved (Flick, 2018).

3.2.2 Interview sample

The primary objective of this study is to understand how organizations deploy and manage DS complementary assets. After selecting relevant sensitizing concepts to best explain the observed phenomenon and to construct the theoretical framework, I identified actors that were the most knowledgeable of changes in the DS landscape as a result of digital transformation and regulatory change. The interviews were then structured in-depth to explore DS challenges faced by organizations and find recurring themes that match the complementary asset perspective. Interviews with experts have great potential since it allows for the discovery of the implicit dimensions of expert knowledge (Döringer, 2021).

The decision to interview selected "knowledgeable agents" in many organizations (Döringer, 2021; Gioia et al., 2013), rather than many individuals in few organizations was made for several reasons. First, the implementation and management of DS related complementary assets is carried out by a few informed individuals. In the case of financial service organizations, all interviewees were involved in various DS at their respective firms. Similarly, the consultants interviewed also had close contact with these "knowledgeable agents" at various firms in the industry. Second, throughout the research, access to several individuals in one organization turned out to be difficult as many individuals working in this area had busy schedules and were reluctant to share information about colleagues due to confidentiality reasons. The disadvantage of this is limited understanding of the interplay between DS and relevant variables such as organizational culture, firm resources, overall strategy, etc. However, understanding a few contexts in depth can yield more insights than studying many superficially, given time and budget constraints faced by researchers (Bryman & Bell, 2015).

It is essential for representations of the phenomena to provide accurate and meaningful reflections of the shared views of industry participants (Jacobides, 2005). Thus, a diversified sample of consultants, industry practitioners and critical 3rd party service providers performing different functions was need. Interviewees were selected using purposive sampling based on their relevance to the research topic instead of their representativeness of the overall population. As suggested by Flick (2018), minimal contrast sampling is used to find "core of the variation in the field". Thus, interviewees have similar profiles and seniority at their organizations. Schinagl et al. (2022) remark that existing DS research can be supplemented

with a broader range of both business and security participants from a wide cross-section of organizations. This is also echoed by Hall et al. (2020).

Thus, a wide range of actors in different organizations were contacted (Rubin & Rubin, 2011) Interviewees were identified through internet search and initial contact was made with them through LinkedIn. All interviewees, with the exception of Interviewee #13, were from the financial sector but data from Interviewee 13 was used in the analysis for its deep insights as the respondent has worked extensively with DS during their career and presently leads the Global IT Security strategy at a global mining firm based in Sweden.

All in all, a total of 30 interviews was conducted, of which 3 were exploratory pre-study interviews and 27 were in-depth data collecting interviews (see Appendix 2). The interviews ranged from 20 to 75 minutes, which could be considered an appropriate length to avoid fatigue amongst participants while still having in-depth conversations (Yin, 2016). Anonymity was ensured to facilitate open and truthful discussions about potentially sensitive topics such as DS policies and procedures (Bryman & Bell, 2015).

3.2.3 Interview process

Following the abductive research approach, which recommends collecting general information on a certain subject, semi-structured interviews using open-ended questions were conducted (Bryman & Bell, 2015). Semi-structured interviews allow the researcher to be open-minded towards interviewees while steering the discussion towards common themes and topics. At the start of the interview, a brief small talk was initiated to establish a rapport and sense of comfort with the interviewee (Rubin & Rubin, 2011). The background of the study and author were also explained. Additionally, interviewees were asked for their consent to record before the interview, to which the majority agreed. Extensive notes were taken for those interviews that were not recorded. The interviews were held in English, recorded, and transcribed using the built-in function of Microsoft Teams. Nevertheless, all transcripts were reviewed and adapted afterwards to ensure correctness and consistency before using them for data analysis.

The questionnaire was built on findings from the literature and preliminary theories but was adapted throughout the entire collection process based on emergent findings. For instance, several interviewees mentioned challenges related to cloud security, so this was added to the

questionnaire. The order of the questions was also flexible, enabling me to ask for clarification or further details when required (Rubin & Rubin, 2011; Bryman & Bell, 2015). Furthermore, each interview was conducted individually in order to avoid group effects or social desirability bias (Bryman & Bell, 2015). To avoid inducing a bias in the answers, the researcher did not refer to answers given by other interviewees.

The interviewees were held online on Microsoft Teams due to geographical distance of the interviewees as well as time and budgetary constraints. All interviews were held with cameras turned on, facilitating trust with interviewees while ascertaining body language and facial cues. However, research confirms that in-person interviews are only slightly better than videoconferences, creating reassurance that the interview design would help achieve the objectives of this study (Irani, 2019; Khan & MacEachen, 2022).

There was also a risk of interview misinterpretation since only one investigator was conducting the interviews. Credibility and trustworthiness in the data presentation was ensured by regularly sharing and discussing observations with other students. Following Flick (2018), a data point was included in the analysis only if more than one interviewee had independently mentioned it. Since I was the only person conducting the interviews, it was necessary for me to listen to the interviews multiple times to perform a deep analysis and reassess insights from the interviews to ensure that important insights had not been overlooked or misinterpreted.

While the number of interviews was not established at the outset of the study, interviews were conducted until saturation was reached when it was evident that additional discoveries could not be made (Bryman & Bell, 2015). After the 22nd interview, a few new insights emerged but, after the 27th it was evident that additional learnings would be limited. At this point, I conducted the final interview and concluded that saturation was attained.

3.3 Data analysis

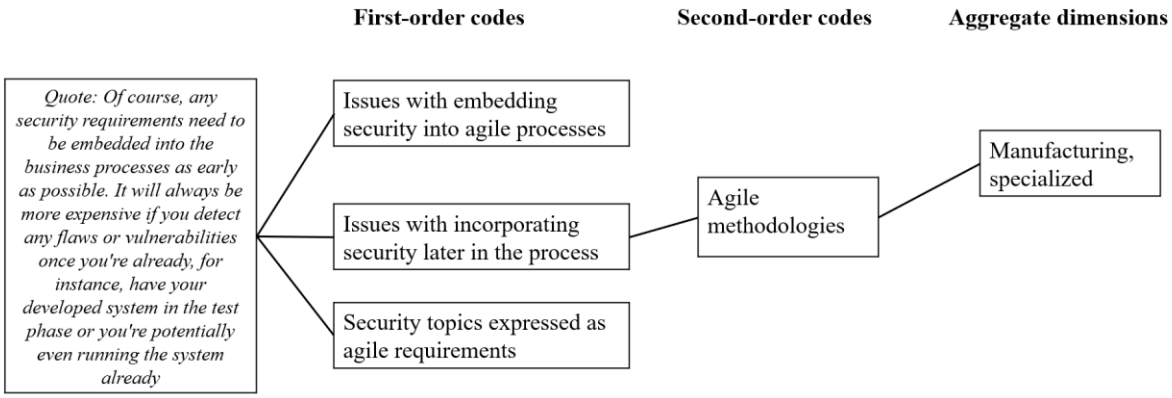
During the early stages, an inductive approach had been considered for this study, where greater emphasis was placed on empirical findings that existing theory. Therefore, Gioia's grounded theory approach was used as starting point. However, after choosing complementary assets as the theoretical lens, a more abductive and reflexive approach was taken in line with Gioia et al. (2013) who state that *"the research process might be viewed as transitioning from "inductive" to a form of "abductive" research."*

Data analysis and processing began as soon as the first interviews had been conducted. By carrying out the data collection and analysis in parallel, it was made possible to sufficiently process the vast volume of text and information, adapt the interview guide in light of emerging findings while ascertaining data saturation (Eisenhardt, 1989). The findings were triangulated using industry reports, whitepapers and company-specific websites. After each interview, I spent approximately 15 minutes summarizing and documenting key insights when the information was still fresh in mind (see Appendix 3, post-interview questions). In the first phase, first- and second-order constructs were coded in line with Gioia et al. (2013) where the first-order constructs focused on preserving the integrity of the exact phrases and terms used by the interviewees. These first-order constructs were then condensed into more theory-centric second-order constructs with a higher level of abstraction.

Then, I compared the first-order codes to merge similar categories, and group them into relevant areas. To find deeper meanings in what the interviewees said and thus capture their so-called "*lebenswelt*", special attention was given to not only what the interviewees said but also how they said it. An exemplary mapping of the constructs and aggregate dimensions in the form of overarching themes, is shown below in Figure 5.

Finally, as overarching themes emerged using the abductive approach, I iterated between the empirical findings and the theory to develop a robust theoretical framework using empirical data gathered in the interviews. The aggregate dimensions refer to the various classifications and specifications of complementary assets, as these broadly describe DS related complementary assets used by organizations in the financial sector. These are used to describe the findings in Sections (4.1) – (4.4).

Fig. 5 Excerpt from the data structure



3.4 Empirical setting

The reason for studying DS specifically in the Swedish financial sector was threefold. First, Teece (2007) stresses that certain business environments favor the creation and integration of dynamic capabilities such as industries fully exposed to opportunities and threats associated with rapid technological change. Moreover, resources and capabilities must be adapted and recombined in response to new digital technologies to satisfy evolving requirements. Bearing in mind these aspects, the financial services industry provides a suitable setting for this study. With technological development, cyber threats and vulnerabilities become more widespread, accelerating the risk of cyberattacks in the Swedish financial sector (IMF, 2023). Financial fraud and data theft are the main motivation behind attacks. Sweden has become extremely dependent on electronic means of payment (ibid). Less than 10 percent payments are in cash in 2020, falling from 39 per cent in 2010, and many businesses no longer accept cash (ibid).

Second, an industry where regulatory change plays a significant role and has associated demands for compliance is the financial services industry (Freij, 2020; Jacobides & Winter, 2005; Sköld et al., 2020). The financial services sector has historically been highly regulated due to high crisis risk in case of failure for wider society (Krüger & Bruachle, 2021). More than many other industries, the financial sector and its systems are highly interconnected and interdependent – a "single point of failure" can easily impede service delivery of other participants in the financial system (Calliess & Baumgarten, 2020). A serious IT incident in a corporation can quickly spread and impact society at large, which is especially pronounced in Sweden due to the interconnectedness of financial sector participants (Finansinspektionen,

2022). The debate on regulatory requirements has been prevalent in the financial industry since its very inception and thus compliance of firms, especially with digital regulation can be seen as highly mature (Blum, 2020). Ongoing regulatory changes in response to changing technological trends imply a need for changed DS complementary assets.

The risk of cyberattacks is especially pronounced in the Swedish financial sector due to the high levels of digitalization and interconnectedness of participants (IMF, 2023). Financial fraud and data theft are the main motivation behind attacks. The adoption of cloud-based software and infrastructure services has accelerated these risks. Sweden has become extremely dependent on electronic means of payment (ibid). Less than 10 percent payments are in cash in 2020, falling from 39 per cent in 2010, and many businesses no longer accept cash (ibid).

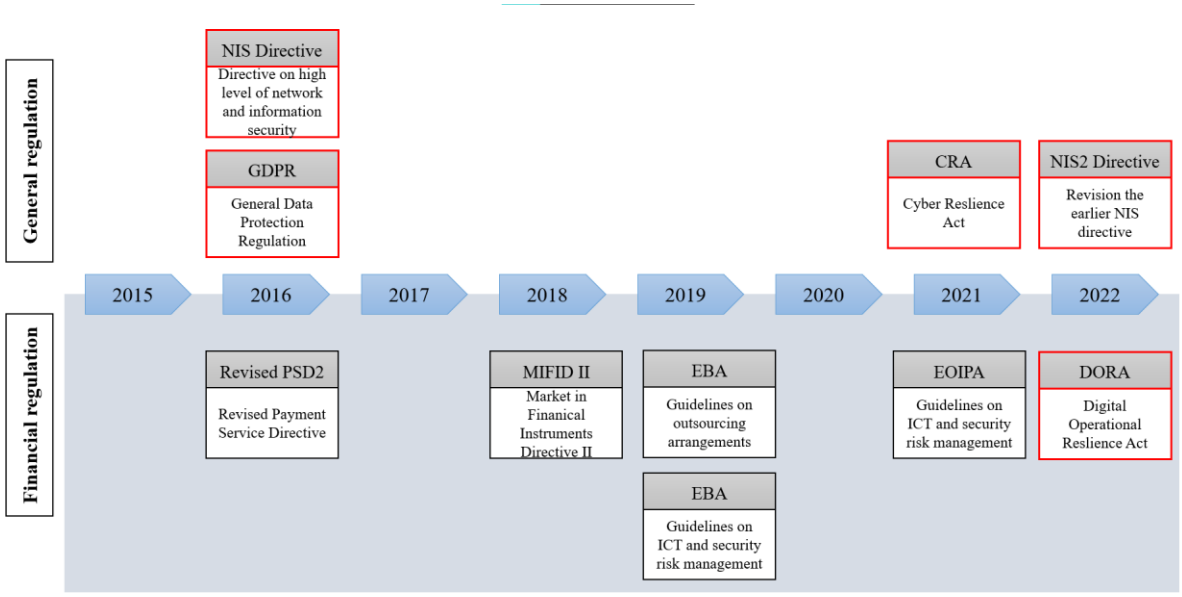
Third, the level of appropriability is also an important determinant of complementary assets (Pisano, 2006). In the financial services industry, whenever a new product or service is offered on the market, others not only copy it very quickly, but often introduce an improved service since they have some time to assess the strengths and weaknesses of the original service (López & Roberts, 2002). Therefore, in "weak" appropriability regimes such as the financial sector where imitation is relatively easy from both a technical and legal standpoint, protecting revenue from innovation has historically required privileged access to co-specialized assets (Pisano, 2006; Sköld et al., 2020b). This differs compared to firms operating in strong appropriation regimes where firms can rely on licensing and other contractual arrangements to extract rents from their innovation without access to such assets (Pisano, 2006; Bianchi et al., 2014).

3.4.1 Overview of regulation discussed in this study

The two most important and far-reaching pieces of legislation are the NIS Directive and the General Data Protection Regulation (GDPR), both passed in 2016. Both pieces of legislation are limited in scope by focusing on specific topics (such as data protection in the case of GDPR). In addition to these general standards, sector-specific standards for the financial sector are further specified through so-called Regulatory Technical Standards (RTS) and other guidelines by the European Banking Authority (EBA) to ensure a consistent implementation in member states (Krüger & Bruachle, 2021). Thus, EU regulation is also widely applicable to Swedish firms and is hence discussed in detail.

Among these RTS, the one with the most far-reaching impact is the Digital Operations Resilience Act (DORA), which is the first regulation of its kind in the EU. The five pillars of DORA explicitly set rules on IT risk-management, incident reporting, resilience testing and IT third-party risk monitoring (EBA, 2022). Firms must also live up to compliance standards such as ISO 27001, which provides a list of requirements for the information security management system and considers risk management as a core component for the overall security management (Kure et al., 2022). Compliance standards such as ISO differ from regulations, but firms must have these certifications as they provide assurance to customers that standardized best practices are followed (ISO, n.d.)

Fig 6. Timeline and overview of general and sector specific DS regulation (not exhaustive). regulations in red boxes are within the scope of this study.



EBA = European Banking Authority; **EOIPA =** European Occupational and Institutional Pensions Authority

Importantly, significant penalties and fines can be incurred if regulations are not adhered to as shown in Table N below. For instance, non-compliance with DORA can result in penalties of up to 2% of annual worldwide turnover (EBA, 2022). The penalties for breach of the Cyber Resilience Act (CRA) and the NIS2 directive also amount to similar losses in revenue(Chee, 2020). In addition to fines, companies can also face reputational losses because these regulations allow authorities to name individual members of executive management if non-compliance by the financial entity can be attributed to specific individuals (Long et al., 2023).

3.5 Quality of the study

Researchers must ensure quality considerations such as trustworthiness and ethical considerations when conducting a qualitative study. In terms of credibility, transferability, and dependability of this study and its findings, I adhere to the guidelines outlined by Lincoln and Guba (1985). Furthermore, utmost efforts were taken to assiduously follow Gioia's methodology on conducting qualitative studies.

3.5.1 Credibility

Credibility in qualitative research is akin to internal validity in quantitative research, where it measures how well the research outcome mirrors the reality of the phenomenon under study (Bryman & Bell, 2015). This ensures that believable theories and insights are generated. To account for credibility, as mentioned in the previous section, triangulation was done using multiple data sources and various theories (Saunders et al., 2019). A holistic view of DS complementary assets was obtained by interviewing a diverse profile of experts. Lastly, taking an abductive approach maintained the focus on relevant aspects of DS and complementary assets, continuously adapting and challenging underlying assumptions.

3.5.2 Transferability

Transferability relates to the external validity of the study and outlines the degree to which a certain study can be transferred to other setting or cases (Lincoln & Guba, 1985).During the interview process, thick descriptions were obtained by asking open-ended, unambiguous questions during the semi-structured interviews and by giving interviewees the possibility to reflect on and explain DS phenomena in their own words. Deeper meanings were then sought in the subsequent transcription and coding process.

3.5.3 Dependability

Dependability refers to the reliability and trustworthiness (Bryman & Bell, 2015) and it pertains to the steadiness of research results over time (Lincoln & Guba, 1985). Prolonged engagement is preferred to understand the variations of a phenomenon in the course of time (Saunders et al., 2019). By considering the time and resource constraints of the study, respondents were asked to describe their experience in terms of the development of DS over time and at different organizations that they worked with over their career, introducing an element of longitudinal interviewing (Bryman & Bell, 2015). Overall, this approach increases the probability that this research produces the same conclusions as if conducted in another time (Lincoln & Guba, 1985). To further ensure dependability, extensive records of the research process were kept mapping all relevant information and creating future recollections of the process. To a certain extent, the academic supervisor acted as an external auditor during regular meetings by asking clarifying questions and accessing the latest changes in the research process.

3.5.4 Ethical considerations

Substantial efforts were made to ensure that this study was conducted responsibly and respectfully. This was particularly important as DS topics are highly confidential. Any identifying information of the interviewees was anonymized to prevent the disclosure of internal insights on this topic. Thus, personal data such as name, employer and gender were anonymized to maintain integrity and compliance with GDPR. Only the most essential information about the respondents is described to ensure transferability.

Interviewees had informed consent, i.e., they were made aware of the purpose of the study, process, and of their right to withdraw at any time (Bryman & Bell, 2015). All participants were informed twice of their anonymity in the invitation emails and at the start of the interview. They were further reassured that interview data collected would not to be used beyond the purpose of this study.

4. Empirical findings

This section covers the main takeaways gained from the empirical data, divided into four main topics in line with the background and the conceptual framework. The background and context of the empirical problem are presented in *(4.1)*. The nature of DS complementary assets in relation to their classification and specification is described in *(4.2 – 4.4)*. Finally, an overview of DS complementary assets is presented in *(4.5)* with regards to the two dimensions of interest. Finally, the data table is introduced in *(4.6)* to provide further evidence of my findings.

4.1 Background and context

Cyberattacks are becoming more prevalent in the financial sector. These attacks are much more frequent than before and often information about these attacks is not disclosed publicly. The pervasive and harmful nature of threats requires better alignment of processes and technologies to address these threats:

"It [cyberattacks]happens more often than you think. The thing is that we have to be careful when you say that it doesn't happen so often because the information is not always public or on the Internet. Often, these incidents are resolved internally." – Interviewee 4

"Organizations need to have better processes to work with than what they usually have. They have very simple processes, which is not enough to really understand risk."
- Interviewee 12

While this is a pressing issue, there are many trade-offs to cybersecurity strategies. The informants concede that "it is expensive to maintain a strong, cybersecurity posture in perpetuity" and that "organizations cannot be 100% resilient" in their operations thus a "risk-based approach" was mentioned by many of the interviewees. More broadly, the risk-based approach is underpinned by calculated risks and the ability to restore function should adverse events occur within an organization:

"It's a calculated risk, this is what you want to base your cyber security on. What if an intrusion only hits one of our contained environments? What do we do then, how much loss can we handle in terms of minutes or lost transactions?"- Interviewee 10

Generally, DS remains a topic that is left to IT teams and there is less dialogue across various divisions. A lack of understanding of DS between IT teams and the business can also lead to siloed approaches, as is illustrated by the following quote from Interviewee 14:

"You need to make sure that business takes lead into the technology questions. You need to be able [to] from a business perspective to write good requirements and have a dialogue around these requirements ongoing. The business needs to set these rules around how long the data needs to be stored, who has access to it, [etc]."

4.1.1 Scale of services and operations

The growing scale of services provided by large organizations also induces complexity in mapping out where DS complementary assets should be deployed.

"We were using many different methods. As IT owner of [bank], I was responsible for 3600 apps on Windows and Linux. I was overseeing 40,000 servers which had to be updated every month and protected from vulnerabilities. Without system segmentation, viruses and trojans can be quite easy to propagate. It takes a lot of effort to segment this especially in big organizations such as ours." – Interviewee 4

As the quote above illustrates, there could be gaps or "blind spots" in the oversight of IT assets as a large number of systems and integrations need to be monitored. Further alignment with system owners in different parts of the firm is needed. This creates further security challenges for organizations to address when deploying specialized and cospecialized assets since the setup of organizations can vary depending on the number of products and geographies that they operate within. In such cases, having leaner operations can sometimes be an advantage:

"Smaller businesses have less complex business models and are less exposed to the incidents and other countervailing forces." – Interviewee 23

"Small operations are better positioned to fulfill these standards. Larger businesses have more complex operations, more business deviations and legacy IT environments. Small organizations have people that are security aware, but the in-depth know-how is missing in small organizations [due to] lack of resources and expertise" – Interviewee 13

Finally, in light of regulations, firms need to further specialize (and cospecialize) their core IT assets since the extent of the regulation varies by the business areas within which the firm operates. Changes in the regulation can also lead to discontinuities in DS complementary assets, often with limited use for previously compliant assets:

"There is no single legislation for all financial institutions. There are multiple standards that apply to different subsectors in different contexts, which entails an analysis of requirements unique to each firm. This leads to a complex and confusing regulatory landscape with limited overlaps, which could lead to discontinuities in technological assets." – Interviewee 1

4.2 Manufacturing complementary assets

The respondents mentioned a combination of generalized, specialized and cospecialized assets in relation to manufacturing. They also mentioned the use of external providers and AI solutions to facilitate the cospecialization process. Since both collaborations with the IT consultants and external providers are dyadic in nature, affecting only intrafirm IT assets and technology, for simplicity, this study does not classify them as relational assets.

4.2.1 Generalized DS complementary assets

At a basic level, most organizations employ static tools to test the level of security in the code that they release and analyze the behavior of products. They also conduct dynamic analyses and test and review weaknesses to further protect against cyberattacks. These are usually IT processes that most organizations have in place as part of their routine "cyber hygiene" practices and are comparable to generalized complementary assets where neither the complement nor the core technology are specialized towards each other.

Organizations have some form of generalized security tools and processes in place that are in compliance with applicable regulation. Without generalized DS assets, firms risk major compliance and IT risk issues:

"Every organization must follow EU regulation such as GDPR to take action and protect confidential data." – Interviewee 8

"ISO27001 states technical controls and gives a good baseline for antimalware, antivirus and phishing is quite important." – Interviewee 23

These generalized assets are usually built based on guidelines from the regulation, but further specialization and cospecialization of both the core technologies and DS assets is needed for organizations to be fully secure from a DS perspective as stated by several interviewees:

"I have this thought around regulation, law and IT [that] when it comes to what regulation puts in the place, it is the bare minimum of what you have to do. The problem is that, in my opinion, businesses should aim for a much higher level than what is in the standards. Putting the bar high should be a business priority in a business. We should put the bar high from the beginning." – Interviewee 14

"You need to build this into each resilience and security process and technology, and this is comparable to the "Covid vaccine". It protects you but additional measures are needed to be secure." – Interviewee 4

4.2.2 Specialized DS complementary assets

With regards to manufacturing assets, unidirectional specialization of the core technologies was required to incorporate DS. Specialized assets in two main areas were mentioned most frequently by interviewees. These were agile technologies, classifiable as IT and legacy systems, classifiable as OT. These are discussed in the following subsection. Several organizations in the financial sector have started using agile methodologies in their ways of working. DS by its very nature goes against the adaptable and flexible nature of agile since DS imposes restrictions and controls that hamper product development and testing:

"The central part of working in an agile way is that you just quickly can create proof of concepts quickly to demonstrate different things, but this might have security implications. Inserting security into this modern way of working can be quite difficult." – Interviewee 16

Agile principles provide an effective method to recognize internal quality issues in software requirements, architecture, coding, and testing but there is a lack of fine tuning towards DS at the organizational and business level. Working with agile methodologies, the level of DS adoption in agile processes needs to be tailored to the business risk. Incorporating these requirements into the core technology in terms of mapping business risk requires a degree of specialization of the core agile methodologies. Security requirements can be expressed in the form of technical debts, which are defined as IT results and metrics that determine the areas towards which further software development should be directed:

When expressed as "security technical debt", the management of security risk and addressing the underlying quality issues can gain increased visibility and can be better communicated between developers, security experts, [and] the management. – Interviewee 21

Almost all the interviewees strongly emphasized the importance of incorporating DS early in the development process, especially when working with agile methods. Thus, having an overview of complementarities throughout the process is essential:

"I would say it's up to 640 times cheaper when I take care of this at the beginning of the development stage. I don't have to refactor, refactor and refactor afterwards. If you take an ongoing enterprise architecture perspective, whether it is for a software or hardware, you can make this cheap, you can make this happen on whatever platform you produce. This is the biggest oversight problem that people do." – Interviewee 14

"A success factor for us that we've been on, not an early stage, but quite early stage when going to the agile world. We've been trying to build security in processes." – Interviewee 6

"Of course, any security requirements need to be embedded into the business processes as early as possible. It will always be more expensive if you detect any flaws or vulnerabilities

once you're already, for instance, have your developed system in the test phase or you're potentially even running the system already." – Interviewee 15

Manufacturing skills are tailored to specific innovations, these particular assets may not easily be transferred to another technology e.g., when changing from legacy systems. This also impacts DS assets. Operating older systems also means that more vulnerabilities would be present in the system:

"The software that you're running might be so old that you can't even upgrade the operating system or the database and that means you are stuck with old vulnerabilities and security threats, imposing a major threat for your operation." – Interviewee 4

Since the systems have been in place for such a long time, firms opted to specialize the legacy technologies to fulfill regulatory requirements:

"Depending on what kind of legacy technologies that they bring with them in their back book, there is 30 to 40 years of technology investments perhaps. And of course, the strategies then become more complex, since in order to be compliant to cannot only focus on new things, you will need to handle all the old stuff as well, which adds a lot of complexity in what you need to implement. Transforming legacy systems to meet these new requirements can be extremely challenging." – Interviewee 25

However, the trend to modify legacy systems to meet DS requirements is likely to change in the future, potentially requiring new forms of specialization, partly due to vulnerabilities in legacy systems and also due to changing business requirements. Organizations are trying to move away from legacy systems and rely more on modern architectures:

"Some of the bigger banks have already started changing their core banking systems. For example, [major Nordic bank] is allocating 7 million SEK for a core banking replacement project. I think those systems do need to be upgraded, but then it's a matter of determining where to start. But this is gaining executive attention." – Interviewee 7

Finally, the possibility to adapt the DS asset to the core technology is also available to firms even when it is sourced externally by specifying these needs to vendors:

"It is possible to issue your own development needs to the supplier. In the next release we like to see certain features." – Interviewee 28

"You can see an enormous variety of providers with services attached to it. You can buy firewalls and attached services. There is a full suite here. For more complex services, there are service support packages that you have to buy at least once." – Interviewee 13

4.2.3 Cospecialized DS complementary assets

Since investments in the specialization of DS assets are cumulative in nature, changes in regulations require adaptation of product functionality and IT systems. The process of transforming generalized assets to cospecialized assets can be facilitated by external consultants in some cases, exemplified by the quote below from Interviewee 8:

"Building ongoing security monitoring tools can be expensive, it's a nightmare. It would take a lot of money to build a team, educate them and get necessary certifications. But a consultant can give you this solution, support your organization and ask you what type of services you want. If you want to implement threat analysis, security testing, digital forensics, reverse engineering, etc. All these things that go through the monitoring tools that take a lot of energy - I would recommend taking them externally."

In addition, organizations find it difficult to translate regulatory requirements into their processes and systems as highlighted by Interviewee 25:

"I think there is a lack of structure capital in terms of how you take the incoming and new requirements and transform the [regulatory] text into something that is executable at the team level. How do you take the text in the law and then go down to the ones that are designing and implementing something is a challenge."

To address this pertinent issue, Artificial Intelligence (AI) tools are emerging and gaining traction as a means to translate regulations into IT requirements that are specific to the company, facilitating cospecialization of DS complements and the core technology:

"There are one or two people working at legal and you know that they don't have time to read 6000 pages of documents. Here I think that AI can make a huge difference in doing a gap analysis. We [major IT services provider] have created an AI that can read the documents and then read the [IT] environments to see [what] needs to be done. You can automate this, and you can even have the controls running daily." – Interviewee 18

Interviewee 18 further adds that these tools can also be used to enhance DS compliance of legacy systems as well:

"The core mainframe system at banks is challenging to work with but our tool translates all the compliance rules and regulations into technical controls that will be performed. Then, it will deliver a result in the dashboard, and you can see their status, these many controls are needed and these many are green and so on."

To summarize, external AI tools can be beneficial in facilitating the cospecialization process, especially in assessing the impact of regulatory change on "complex technological stacks" as well as resulting discontinuities. Using AI as a complementary asset can in turn lead to DS issues but this is not considered to be within the scope of this study.

4.3 Distribution complementary assets

In this area, generalized and specialized solutions were described most frequently. Cospecialized complementary assets were not mentioned by respondents as external providers with fixed offerings were used in the distribution process, especially when using the cloud. Consequently, firms had limited control over changes that could be made to the DS asset. A similar reasoning as manufacturing complementary assets was applied when discussing the dyadic nature of partnerships and transfer of technologies.

4.3.1 Generalized DS complementary assets

Several informants mentioned the use of outsourced, third-party cloud technology in the storage and computation of customer data. They also cited security and privacy threats of data leaving the organization to be one of the most challenging aspects within the area of distribution. There are control and transparency risks when sensitive data of users leaves the organization. While organizations have data management and access controls in place, using the cloud requires additional security considerations and these standard controls might not be sufficient. Thus, a different set of complementary resources are needed. Cloud service providers have basic security configurations available but often the expertise to set these up might be absent in organizations:

"You need to configure your cloud solution; it's not configured in a secure way by default. So, you need to have the competence to configure that." – Interviewee 21

Since there are a limited number of cloud providers, additional "concentration risks" also emerge where firms are "locked-in" with certain providers as there are limited number of firms that specialize in the provision of cloud services called "hyperscalers":

"The downside with the cloud is lock-in. Looking at Microsoft Azure, using both security and compliance tools leads to a bias. In security, we talk about separation of duty. There have been some questions about having the same vendors and the same people doing compliance checks on the environments." – Interviewee 1

"Providers are becoming more complex. How they are all put together is becoming more complex. You will have concentration risks. You know, everyone utilizes Microsoft Azure. Microsoft gets hacked or there's a problem, suddenly everyone has a problem.". – Interviewee 11

These concentration risks also pose additional challenges for organizations as DORA stipulates changes to the provision of cloud services:

"I would say the biggest thing right now that everyone is very worried about is inside the DORA framework that will become active in 2025 and it's one article saying that you must have an exit plan out of your cloud vendor within 6 months." – Interviewee 18

Organizations need to embed DS and resilience considerations into their procurement process when working with cloud vendors at a high level. As a result, security demands on the providers of services such as the cloud as well as other sub providers to achieve regulatory compliance would be much higher. Shifting from current providers are needed:

"If you have a component that is cybersecurity related, then regulatory requirements are such that the company that bought that component now cannot use it because it's not secure as a result of a sub resiliency act [such as] DORA, NIS2, etc."- Interviewee 23

4.3.2 Specialized DS complementary assets

Certain providers offer specialized cloud service for organizations operating in the financial sector. In this case, either core technologies or cloud DS assets are unidirectionally specialized according to security. Some clients also use on-prem solutions that only store information locally for their server backups alongside virtual clouds, requiring changes to the core technology:

"Taking Operational Technology systems, those are critical in many cases. You cannot put them on the cloud. Some of our systems on premise and some on the cloud, but many organizations developed a new IT strategy to categorize, OK, these are our most critical systems, and they have to be on prem." – Interviewee 20

With regards to organizations delivering security updates to their customers, organizations also have "lifecycle management policies" that allow them to incorporate new DS solutions into existing offerings with included support and updates for current customers. In these cases, the

DS asset is specialized towards the core technology. This includes updates and patches to existing systems in accordance with the standards established within ISO 27001:

"You will have to take care of lifecycle management. You will have to patch and update the asset. You will also need to manage the application locally from a functional, business perspective, which may sometimes even have a geographical dimension." – Interviewee 2

Additional encryption and layers of security are needed as organizations work with cloud technologies. Encryption can be facilitated by distributed ledgers, for instance. These were often "agnostic" security solutions that were "loosely coupled" with underlying technologies to ensure interoperability and compatibility with the systems of as many clients as possible. In other words, these were "plug and play" solutions. For example, Interviewee 19, working at a distributed ledger services provider explains as follows:

"While we try to work with host systems and adapt to our clients, we stay away from specific solutions since systems have to be interoperable for the dynamic flow of information."

This is also echoed by a representative of the security and compliance suite provided by one of the major IT players:

"It can run on any platform, and we can scan any data both from our security portfolio but also from our compliance portfolio. We do not store any data. We only send metadata for processing. Our strategy of being hybrid and agnostic makes us unique." – Interviewee 18

The empirics suggest that specialization took place within both internally and externally sourced DS assets. Specialization of the core technology to incorporate security for the end users was also mentioned. Finally, security updates to the DS asset were also disseminated to the customers to meet service level obligations stipulated in contracts with customers.

4.4 Relational complementary assets

Relational assets concern industry level assets that involved cospecialization and coordination efforts between multiple actors. In most cases, the relational assets were cospecialized to various degrees. Generalized and specialized assets were not mentioned by the respondents. Presumably, since firms collaborated with multiple actors to orchestrate and build these assets, they had strong selection policies in place with the actors and this drove the cospecialization process. Furthermore, by its definition, since relational assets involve multiple actors, cospecialization had to take place for these DS complementary assets to materialize. Thus, generalized and specialized assets are not discussed below.

4.4.1 Industry level collaborations around the sharing of incident and threat information

New ways of collaborating are needed as various roles are being updated and changed over time. Cross-industry collaboration can also be highly relevant for creating DS policies and frameworks to gain knowledge about different processes to improve DS. Best practices can be shared to improve the overall resilience of all actors:

"The key to success is to join various professionals with various backgrounds and skills – it is a lot about a collaboration effort. This is the main challenge. One does what they are best at, but they do not look at what others do." – Interviewee 2

Several informants also stressed that these collaborations are not limited to the financial sector, and they named the example of Combient. Created by Marcus Wallenberg and a former Ericsson executive, Mats Agervi, the aim of Combient was to keep up with the rapid movement of technology, and how it affected not only IT departments but entire organizations. One of the topics raised in these forums was that of cybersecurity amongst other such as AI, machine learning, scaling agile organizations, etc. A group of leading Swedish organizations connected to the Wallenberg family were the pilot organizations to be included in this collaborative network. Non-competing industry leaders shared assets and knowledge to work together on the transformation of relevant IT issues.

Over time, the network has expanded to include 30+ large enterprises further supported by an ecosystem of universities and startups. Collaborations with academia were also mentioned by other interviewees facilitate knowledge sharing between actors, thus, to improving offerings and products within DS:

"We are active within academia where we can share necessary lessons learnt and improve ways of working with revealing company secrets. We have published a lot of our research in journals such as IEEE." – Interviewee 19

Collaborations were also found within public sector organizations operating in the financial sector. This was done between the regions and local organizations across the country to increase overall resilience and share key DS learnings. Collaborations with other national organizations were also described:

"We generally share security related information with other regions through SKR since we work with them the most closely. We do not work with the private sector as much because of the confidential and sensitive work that we do. We also work with governmental organizations in other countries but at a very high level."– Interviewee 6

Looking at the financial sector, many firms are currently working together to share information about incidents and threats with other firms in the sector. While this has been beneficial for banks, further improvements can be made in the level of transparency and level of sharing. Organizations might be reluctant to share this information due to concerns about free riders who may benefit from this information.

Enriching the statements of previous respondents, numerous interviewees also highlighted the role of information sharing in preventing and mitigating incidents. This is currently not done optimally as described by Interviewee 14:

"Banks, for example, need to flag early incidents or near misses on their infrastructure, but also business processes, to make sure that organizations can address any vulnerabilities if there is a critical incident going on in the banking infrastructure, so other banks aren't attacked."

Sharing of information about incidents is also being made mandatory with the upcoming rollout of DORA, indicating convergence between industry practices and regulations. This is already in place to some extent with current ISO compliance standards but is not mandatory:

"Some types of cooperation are more challenging. In an ideal world, when there is an incident at one company, they immediately flag it to others. But there is an incredible liability that comes with this and all kinds of reputational costs and other costs. So that type of cooperation is more difficult, but I think that regulatory changes might help create kind of a trustworthy framework where you can share that information." – Interviewee 23

Discussion forums to discuss the impact of the regulation can also help navigate discontinuities even with policy and process related discontinuities:

"When you need to interpret a new regulation or a new legislation, you might want to create policies and the writing aspect of it, it's quite time consuming. So, it's good to have a group that can distribute the type of work you might have by sharing experiences."- Interviewee 2

The learnings from these forums then require further adaptation of the core technology as well as manufacturing and distribution complementary assets. Nevertheless, participation in these forums needs to be balanced as firms cannot be overinvested in multiple forums as this leads to dilution of the knowledge exchange:

"Effort is needed to get value out of these forums. You cannot have too many forums. Thus, a balance is essential." – Interviewee 25

4.4.2 Digital identity solutions

A number of interviewees stated that digital identities was a persistent problem faced by organizations and is best explained as follows:

"The reason we stress digital identities is that if and when you feel very certain that you have assigned a digital identity to someone that should have this identity then you are in a position where you can manage and control access and authorizations, etc. in a more secure way. The critical part here is to whom you provide the digital identity." – Interviewee 13

To address the problem of verifying digital identities, various actors have pooled together their expertise and resources to create solutions to address this problem. One such example is BankID, which was formed following the introduction of the eIDAS regulation in the early 2000s. Various banks formed a consortium with the objective of developing BankID. In 2002, the company Finansiell ID-Teknik was founded, which continued the work of this bank consortium. This company is responsible for maintaining and developing the product further. The banks both own and resell BankID, and over 6000 organizations currently use the services of BankID today. There are other vendors as well that offer digital identity solutions. Organizations might be obligated by the authorities to have multiple methods. These other solutions might not be cospecialized and are outside the financial industry (e.g., Freja ID in healthcare). Therefore, the main digital identity solution discussed in this study is BankID.

BankID holds the dominant position in the Swedish digital identity market. Over time, BankID has been adopted through synergistic cospecialization processes. Similar to cloud solutions described above, BankID also takes an "agnostic" approach to maximize interoperability with different systems and services. The difference between cloud solutions and BankID is that some changes to the core technology are needed to use the latter with existing services. This indicates bidirectional specialization, suggesting co-specialization of the two.

Collaboration was deliberately sought to help make BankID a success instead of the banks individually creating their own digital identity solutions. This also fostered everyone's interest and willingness to create further use cases for digital proof of identity, such as Mobil BankID, which can be used on smartphones. This boosted the uptake of BankID – almost 95% of the Swedish population has BankID.

Advances in digital identity solutions have supported the innovation and creation of new payments services such as Swish, which started in 2012 as a cooperation between six of the largest banks in Sweden and was then scaled to involve other banks. Swish is a payments solution that facilitates real-time transfer of money and has also emerged from the banks' joint development efforts. Mobil BankID ensures security within the Swish app. At present, Swish has 8.4 million users and has processed 500 billion SEK in the previous year.

The examples of BankID and Swish highlight that security was not seen as competition but rather as a central interest of all participants. Furthermore, digital identity solutions, in turn, have evolved to keep up with ongoing market demands to develop features with commercial value while keeping DS policies at the forefront:

"We are obligated to make sure that our [digital identity] products are developed in a safe and secure way. Security is within our DNA, and it is our priority one in pretty much everything we do." – Interviewee 26

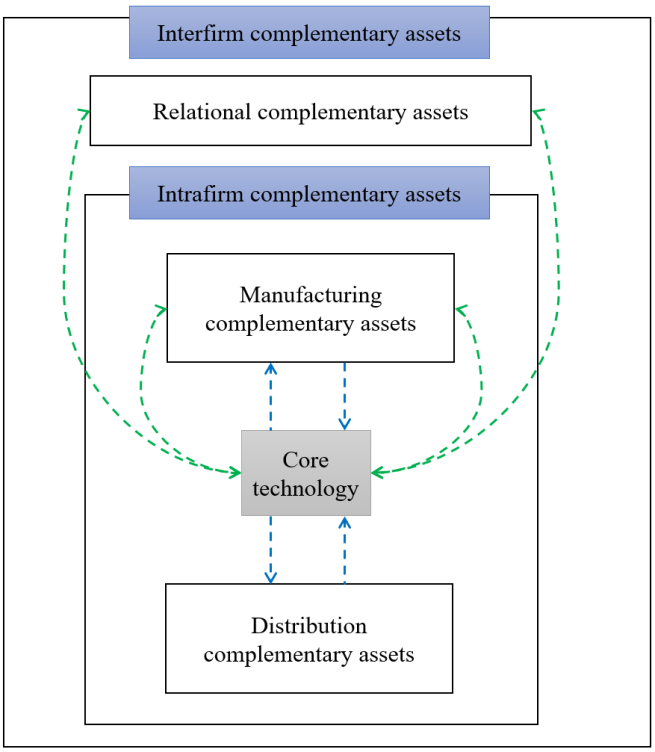
Lastly, within digital identity initiatives, trust between the actors continues to be the cornerstone of these collaborations and is an important factor in driving future initiatives:

"You can see this with the eKrona and the digital euro. You also have it in the digital identity initiative – trust aspect between the actors is key." – Interviewee 25

4.5 Summary of empirics

To summarize the empirics, firms leveraged all three specifications of complementary assets in the area of manufacturing assets. With regards to distribution complementary assets, generalized and specialized solutions were used most frequently. Cospecialized complementary assets were not mentioned, presumably due to technological limitations in making changes to the technologies provided by external service providers. Interfirm elational complementary assets were mainly cospecialized in nature. The updated conceptual framework is depicted below in Figure 6. By building generalized complementary assets, organizations can then use these as a base for building cospecialized and specialized assets as regulatory changes occur. The regulation allows practitioners to develop a baseline level of DS compliance within their organizations. It is important to have baseline tools and frameworks, but they need to be specialized and cospecialized incrementally.

Fig. 6: Updated conceptual framework to show the interrelationships and specializations of the complementary assets. Green lines indicate bidirectional co-specialization, blue lines indicate unidirectional specialization in the direction of the core technology or the DS asset. Generalized assets are not depicted since they are not a part of the original PFI framework. However, they are discussed as part of the findings to highlight the dynamic and transformative nature of complementary assets.



5. Analysis

This section begins by examining differences between intrafirm and interfirm complementary assets. The interdependencies between internal complementary assets are discussed in *(5.1)* followed by an analysis of how the firms internally orchestrate complementary assets in *(5.2).* Subsequently, interfirm complementary assets are analyzed in *(5.3).* Finally, the analysis section is summarized in *(5.4).* Although additional connections might exist among these themes, the analysis is focused on the portrayed interrelationships.

5.1 Dependencies between internal complementary assets

Traditionally, complementary assets have been described as distinct firm level assets with well-defined positions in the value chain according to Teece (1986) within the PFI framework. However, in agreement with Dahlander and Wallin (2006), the findings of this study reinforce that the value chain becomes fragmented in the case of IT assets. Organizations have diverse sets of IT artifacts and networks, which increases the complexity of organizational contexts. This requires multifaceted capacities to drive organizational change at a broad operational scope (Clark-Ginsberg et al., 2019; de Vaujany et al., 2017). This also complicates the set of complementary assets that firms require. The more regulatory frameworks that are applicable to an organization, the higher the complexity in linking. These frameworks need to work in tandem to create synergies across different assets and geographies. Designing and implementing the frameworks can be challenging due to huge gaps in what the regulation states and how to structure the process. The ambiguity of the regulations can introduce challenges in the cospecialization process as both core technologies and DS complements need to be tailored to specific requirements through a risk analysis process, but the steps companies needed to take to do this are unclear.

Interviewees further highlighted the importance of having a "holistic" view of DS complementary assets alongside other processes to map out dependencies across various IT assets. This allows organizations to work on different frameworks in parallel by considering the "breadth" of the systems when implementing internal DS complementary assets instead of focusing on limited areas:

"I'm not saying that you should not think about security in depth, but the first thing is to think of the breath. Everything is more spread out and the challenge is having something that covers all areas well enough." – Interviewee 2

For example, a number of respondents highlighted that when moving data into the cloud, necessary considerations had to be made to manufacturing assets and complements in parallel to mitigate vulnerabilities when data is transferred to external servers, especially in the case of legacy systems which had limited functionality with cloud enabled technologies.

In the same vein, security can be viewed as a chain which is only secure as the weakest link – security is a process in that sense rather than a product (Schneier, 2015). This is especially important because convergence between various technologies can compound the effect of attacks and make tracing the source of attacks significantly complicated. Thus, a better overview of tools and processes as well interconnections between manufacturing and distribution DS complementary assets are needed, as exemplified by the following quotes:

"The security boundary is weakening. Because when we put this technology in place, everything is connected. But it also means that the attack vector [in terms of] how these systems can be hacked and attacked has a massively increased rate." – Interviewee 15

"You need to be secure everywhere – if you have an API that is 99% but 1% is exposed you open up to the non-linear effects of intrusion. The compliance way of thinking is challenging when pivoting and mapping other systems." – Interviewee 23

5.1.1 Discontinuities due to regulatory change

The findings of this study align with those of Sköld et al. (2020) that complementary assets of a generalized nature are a prerequisite for building co-specialized and specialized assets when regulatory changes occur. Some complementarities can persist over time but deviating from these complementarities becomes difficult due to the loss of interoperability (Jacobides et al., 2006). While there are some areas of overlap, many complementary assets and processes need to be reconfigured to be DS compliant and this requires substantial effort. This is also true for DS assets as new regulation is introduced. AI can support this process for manufacturing assets with the emergence of new services but can often be expensive and introduce additional DS risks as data leaves the organization.

Furthermore, the findings also suggest that anticipating certain regulations can facilitate the adoption of regulatory requirements. Organizations carry out a detailed assessment of upcoming regulation within the legal team and monitor the threat landscape so they can create the necessary changes within their systems in advance. This illustrates the monitoring of technological knowledge, in this case at the individual firm level. By leveraging these capabilities, organizations can anticipate significant trends and changes to regulation and pinpoint gaps that present promising opportunities. This alludes to sensing dynamic capabilities that can be utilized in concert with seizing capabilities (Teece, 2007).

5.2 Orchestration of complementary assets

The importance of asset orchestration, especially of specialized and cospecialized assets is supported in the empirics, corroborating the findings of Teece (2006, 2018) and Sköld et al (2020). Asset orchestration involves the acquisition, assembly, and coordinated deployment of resources (Helfat & Liebermann, 2002). Different complementary assets vary in their moderating roles and finding an appropriate balance among all assets can be difficult.

The empirical data illustrates that the size, composition, and interactions of networks systems, tools and processes can lead to unique firm level responses to the standards (Clark- Ginsberg & Slayton, 2019). Thus, it is key to identify the “optimum” level of required specialized and cospecialized complementary assets to generate maximal advantages for a firm (Teece, 2006).

The empirics suggest that matching the appropriate level of DS with a firm's industry environment can be considered as a firm's dynamic capability "to integrate, build, and reconfigure internal and external competences to address rapidly changing threat and regulatory environment".

Seizing capabilities are also most closely linked to complementary assets, which is also validated by the findings of this study. The effective use of internal resources to create valuable timesaving and value generating processes and actions is an essential aspect of seizing capabilities (Teece, 2006), which is also observable in the case of DS. When used in concert with the aforementioned regulatory sensing capabilities, firms can successfully transform or reconfigure these capabilities to keep up with changes in the threat and regulatory landscape. Teece (2006) argues that seizing capabilities in isolation are not sufficient, despite seizing capabilities being the most closely linked to complementary assets. The presence of sensing and transforming capabilities in the empirical findings further validates the point.

5.2.1 Internal and external collaborations

Teece (1986)'s original PFI framework highlights the crucial role of knowledge integration and knowledge conversion. Firms can deploy complementary assets and combine them with knowledge under weak appropriability regimes to increase the potential success of their innovations. More specifically, it is evident from the empirical data that authority and expertise are resources that have a key impact in enabling DS within firms, especially when converting generalized assets to specialized or cospecialized complementarities. Thus, the resource base in the form of skilled experts and security professionals is an important enabler of DS in firms. This observation regarding DS complementary assets is congruent with previous research on knowledge resources that enable digital projects (Teece, 2018; Andronikidis et al., 2021). Dedicated teams with the necessary know-how to carry out DS projects are essential for a firm to understand compliance and regulatory requirements. Furthermore, knowledgeable employees can effectively communicate DS policies to internal stakeholders, increasing the effectiveness of DS implementation within an organization.

However, recruiting qualified security experts can be difficult as "IT experts can be much more expensive that other kinds of specialists and often this expertise is difficult to find in the market." Thus, organizations might have to rely on external consultants and solution providers

to implement DS solutions. Teece (2006, 2018) suggests that firms supply the missing pieces through their competencies. Firms start from mapping out their existing DS resources and then identify what is missing. To prevent full reliance on internal resources for the implementation of DS, the respondents states that organizations need the capability to acquire knowledge and skills externally and to integrate them effectively into the organization. Companies are focusing on building long-term strategic relationships with technology experts with complementary resources and competencies. Thereby, it is possible to optimize the current technological portfolio while using external DS services and partners to strengthen the overall security posture of the firm.

The empirics further validate the findings of Dahlander & Wallin (2006). The challenge for organizations is not deciding which part of the integrated value chain to own but to decide which resources in a dissolving value chain are necessary to own in order to be able to maximize the output of internal DS resources. Although capabilities can be acquired, integrating an unrelated capability into an existing organization is challenging at best, leading to "disastrous" consequences (Teece & Linden, 2017). This is underscored within DORA guidelines where increasing responsibilities are placed on vendors and suppliers, where firms can face huge fines if the procurement process is not detailed enough. Additionally, having vendors that have not been through sufficient security screening "can introduce new vulnerabilities into the firm."

5.2.2 Lack of organizational alignment

DS complements alone are insufficient in achieving compliance and resilience in the long term, as additional complementary assets are needed for this. The respondents highlighted IT experts and system owners within firms as a crucial asset when fostering DS within different business units. Implementing DS is the result of coordination efforts across various divisions. In relation to DS, interviewees referred to this as "alignment between technical, business and legal parts of the organization". Organizational divisions must develop and utilize DS complementary assets quickly and efficiently. In this regard, the problem of interdivisional coordination arises, such as jointly managing DS assets and tools, sharing information between divisions, or gathering a corporate task force of individuals drawn from multiple divisions to address DS-related issues (Lai et al., 2010).

Previous studies also highlight cultural disconnects between developers, engineers, and compliance teams that create issues when digital security measures are added on after software development is complete (Hall et al., 2020; Schinagl & Shahim, 2020; Schinagl et al., 2022). To combat these issues, firms must find ways to overcome organizational factors that affect secure software development and related complements. Having the necessary expertise to successfully deploy DS complements in processes and align various stakeholders in the firm can itself be viewed as a complementary asset or dynamic capability. Thus, within the group of DS complementary assets, technical and organizational controls such as specific processes and documents can be included. This is in line with the definition of DS because it incorporates other organizational and human factors beyond just IT systems and assets.

The informants state that this is improving with executive teams taking a greater interest in security, but DS is not given the same level of attention as other complementary assets relating to financial resources. The cost of security risks is not clearly defined, and this can sometimes be challenging to underpin due to the complex impact on IT assets. This is partly attributable to the fact that DS does not generate revenues for firms and is seen as "a cost-center instead of a profitable unit". This is further highlighted by Interviewee 18:

"So, we would, say, like try to install this tool instead and being proactive instead of reactive and take some of that money you're paying in fines today and invested into the tool and also try to invest into new technologies and try to do something useful with that money instead."

Thus, developing a proactive and more business-oriented view of DS also helps gain management attention by tying DS requirements to business opportunities. Regulatory requirements have been expanding over the past decade but "the key is not only to be compliant but learn how to use these frameworks for doing better business."

5.2.3 Timely implementation of complementary assets

If security is integrated into existing business processes, security becomes more natural and self-evident and eventually able to be institutionalized throughout the firm (Schinagl et al., 2022). Following this perspective, DS should be considered and embedded in every new initiative, business product or process. Integrating DS complementary assets in the early stages

of the design process has multiple advantages. First, when DS complementary assets are implemented in the early design stages, it leads to more efficiency in the innovation process and reduces the degree to which security hinders business innovation (Diesch et al., 2020; Schingal & Shahim, 2020; Schinagl et al., 2022). Second, investing in DS complements earlier also results in long term cost savings because it is less costly to implement security in products or processes during the design period so that products do not have to be rebuilt or adapted before they are launched. This also prevents expensive delays and latency since "surprises from unexpected changes are mitigated" and development teams can focus on profitable and marketable features instead. Third, latency toward implementing security features increases over time to the point that adding security after the fact becomes unfeasible (Schinagl et al., 2022). Security latency is described by respondents as "the time needed to actually implement security in relation to the total development process".

5.3 Interfirm complementary assets

5.3.1 Joint interfirm responses to regulation

Industry level cospecialized assets are not just technical in nature based on "the path-dependent evolution of firm's capabilities" but can also be shaped by external factors such as legal and regulatory standards (Jacobides et al., 2006). This is evident from the examples of eIDAS and DORA. In relation to eIDAS, locally influenced actions of individual actors combined to create emergent systemic outcomes. Despite concerns about competitiveness, publicly disclosing information regarding an innovation and its complementarities may help establish a technological standard and dominant product within the industry (James et al., 2013). Currently, BankID dominates the digital identity market in Sweden because of its ease of use and interoperability across multiple products and systems.

Creating an ecosystem or network of partners is needed to invent and create collaborative new offerings and partnerships. This is not limited to networks between companies within the financial sector but can also include academia and other firms outside the financial sector. In addition, DORA makes the sharing of information regarding incidents and vulnerabilities mandatory across firms to create a stronger threat response at the industry level. Having these processes in place makes the adoption of DORA less time and resource intensive.

5.4 Summary of analysis

Organizations in the financial sector converted existing generalized assets into specialized assets (Chiu et al., 2008; Sköld et al., 2020) in order to be capable of offering products and services that were compliant with DS regulation. The generalized controls and tools used for DS might not vary across firms but the ways in which they are implemented and built into various processes and internal systems varies drastically across organizations. In that sense, the codified knowledge and frameworks that organizations use around DS could be viewed as a vital seizing dynamic capability that is unique to certain firms. These sensing capabilities need to be combined with corresponding regulatory sensing and transforming capabilities which corresponds with the findings of Teece (2006).

When knowledge of DS was not always present internally, external consultants were instrumental sources of knowledge in the cospecialization and specialization process to build internal complementary assets. This corresponds to existing perspectives regarding dynamic capabilities, which considers the complementary asset providers of a company, both inside and outside said organization, as an essential part of commercializing innovations (Teece, 2006, 2018; Andronikidis et al., 2021; Ceipek et al., 2021).

Information sharing networks about threats and incidents within the financial sector firms, academia and other companies represent important relational assets. They address current and future DS challenges optimally through a cluster of complementary assets. Shared resources and expertise also facilitate cospecialization, which is not possible solely with internal resources and capabilities due to increasing complexity resulting from the DS threat landscape and regulatory uncertainty. This was beneficial to individual firms as they were able to access to crucial complementary assets while simultaneously reaping benefits from the increased division of labor and increased cospecialization opportunities (Dahlander & Wallin, 2006).

However, the selection of suitable partners is also crucial for these collaborations to yield valuable output. Thus, a balance must be achieved between efforts to acquire and build interfirm (relational) and intrafirm (manufacturing and distribution) complementary assets.

6. Conclusion

This section presents the answers to the research question *(6.1)*. Based on these, I elaborate the theoretical contribution and practical implications of this thesis *(6.2 - 6.3)*. Lastly, I discuss the limitations of this study and areas for future research in *(6.4)*.

6.1 Answering the research question

This thesis attempts to answer the following research question:

How do firms adapt their complementary assets to deal with digital security challenges arising from a constantly evolving threat and regulatory landscape?

Therefore, the classification and specification of complementary assets were empirically researched in relation to intrafirm and interfirm complementary assets. The level of specialization varied for the three classifications of complementary assets when dealing with digital security challenges marked by a constantly evolving threat and regulatory landscape. At the intrafirm level, firms leverage both specialized and cospecialized manufacturing complementary assets and specialized distribution complementary assets. Timely implementation of DS complementary assets was found to be of utmost importance. The importance of external partners in the cospecialization process of the manufacturing assets was observed where external consultants were involved in obtaining the knowledge to convert generalized assets to specialized and cospecialized assets.

At the interfirm level, relational assets were cospecialized to share knowledge and create new digital identity solutions. Organizations can increase their preparedness against cyberattacks by sharing knowledge about threats and incidents with participants both from within and outside the industry. The empirical findings suggest that orchestration of cospecialized assets is vital due to the blurring boundaries between the classified complementary assets and the core technologies. Furthermore, a balance or “optimum” level of specialization and cospecialization is needed. This balance is determined by each firm based on its unique resources and capabilities for both the intrafirm and interfirm complementary assets.

6.2 Theoretical contribution

The findings of this study are of relevance to both the strategy literature and to the field of IS since concepts from the latter are used to establish the importance of DS in firms. The theoretical contributions of this study are fourfold. First, this study primarily answers the call from Teece (2018) to analyze how complementary assets are redeveloped in changing digital environments. In alignment with previous research on the role of cospecialized and specialized assets, this study finds support for the notion of orchestration put forward by Teece (2006; 2018) and Sköld et al. (2020).

Second, the explorative nature of this study also allows for a disaggregated and componential view of complementary assets, responding to the request by Ceipek et al. (2021) to provide practical and theoretical insight into the required level of specialization of complementary assets. This study also differs from previous studies since it draws from the highly digitalized financial sector, whereas extant research on complementary assets have been conducted in physical product companies with the exception of Sköld et al. (2020).

Third, the proposed conceptual framework extends that of Teece (1986) by adding an additional dimension of relational complementary assets. Teece (1986) argues that firms should begin with identifying missing competencies and then supplying them through integration or contractual strategies. However, the emergence of new modes of organization and interfirm collaboration is not captured within Teece (1986)'s original PFI framework and subsequent studies that use complementary assets as a conceptual lens. In this regard, this study sheds light on the decreasing importance of owning and building complementary assets within the firm when they can be sourced economically through alliances and collaboration without losing proprietary information.

Lastly, and most significantly, by bridging IS concepts and strategy literature, the study makes key theoretical contributions to both research fields by introducing DS concepts to complementary assets and dynamic capabilities, and vice versa. This study establishes the importance of considering DS from the viewpoint of multiple stakeholders. Moreover, by substituting the financial sector with other organizational and industry contexts, the proposed conceptual framework can also be utilized to understand other underlying effects and thus explore DS in a wider range of settings.

6.3 Managerial contribution

Closely connected to the theoretical contributions, this study has important practical implications for all firms, even non-financial sector firms. Organizations invest vast amounts of time, money and resources on DS compliance issues. Digital solutions and processes sourced externally from outside vendors and consultants are one way to reduce these compliance costs. Managers can structure and perform their analysis of DS complementary assets according to the examples provided in Section 4 and 5. They represent a comprehensive continuum moving from generalized to specialized and cospecialized complementary assets. This is assuming that complementary assets can be matched to the distinct categories and specifications outlined in this study. The empirical findings and analysis provide firms with a basis to understand what complementary assets they own and which ones are currently missing. Likewise, firms need to measure the combined effect of the three specifications continuously to ensure the balance and appropriate set of complementary assets over time.

6.4 Limitations and future research

First, a greater number of representatives from each firm should be interviewed. Since there are less than two interviewees from the same firm, crucial aspects might not have been uncovered. This is a substantial limitation as this study concerns concepts that are shared across organizations. The limited number of interviews from the same firm could represent overly simplified generalizations when conclusions are inferred for the entire organization. To mitigate this, a comparative study using Eisenhardt's comparative case method would enable a deeper understanding of the topic. Future research on complementary assets should further explore the identified relationships between the second-order themes and constructs. Additionally, firm-level studies into DS complementary assets can be used to further analyze and decompose the microfoundations and modes of organization that are required for firms to successfully implement DS.

Second, follow-up interviews could also have enhanced the findings of this study as some aspects of DS and complementary assets only manifest over time. Thus, this study represents cross-sectional snapshots. While triangulation of the findings was performed against regulatory reports and whitepapers from multiple years to address this limitation, a longer study timeframe would have yielded richer data. Longitudinal insights into the phenomenon of complementary

assets and DS over time can generate highly relevant conclusions. Researchers with the capabilities and resources to study firms in multiple contexts could follow DS complementary assets in firms over time.

Third, the distinction between core and complementary assets in this study assumes that the two are neatly dichotomous and distinguishable in practice. This is especially significant in the context of IT assets which are characterized by overlaps across intrafirm processes and also in the value chain of developing IT assets. Thus, methods to ascertain the optimum level of classification and specification of complementary assets is not addressed within this study as the data does not sufficiently capture this phenomenon. Further studies are, thus, required to underpin this balance. Mixed methods studies involving both quantitative and qualitative methods could be applied to answer this question. Researchers with more time and resources could potentially gather data from a larger set of organizations and provide practical insights into measuring optimum levels of specialization numerically while supporting their results with qualitative insights into the interrelationships between the complementary assets.

Finally, this thesis' approach gives certain depth and practical insight into how DS complementary assets are built in the context of the financial sector. However, this potentially limits the study's applicability in certain regulatory contexts. It would be interesting to apply the presented framework in the context of a different industry with different regulations.

6.4.1 Mismatch between research question and theory

To answer the research question, complementary assets were used as a sensitizing concept. The theory of complementary assets functions more as a framework to classify certain elements than as a standalone framework. Theories related to diffusion models could have been better suited for understanding differences in the implementation of digital security across firms.

In addition, further discussion of disruptive innovation would have enhanced the thesis further since complementary assets are closely linked to this concept. Such assets are difficult to imitate because they are path dependent and arise as a result of specific firm choices and characteristics (Teece, 2018; Sköld et al., 2020). In the absence of complementarities, imitators are unable to replicate innovations (Teece, 1986). Acknowledging this limitation, in-depth comparative studies of a few imitator and innovator firms would have been more suitable. However, finding participants given the limited duration of the thesis term made it difficult to

build mutually trustworthy relationships with representatives of financial sector firms. If time had permitted, I would have done this in a second, round of follow-up interviews with certain participants to ascertain the competitive advantages yielded by building complementarities.

6.4.2 Mismatch between theory and method

As mentioned above, finding "knowledgeable agents" was a challenge. The consultants interviewed in this study are either business or technical experts. However, participants acknowledged the use of consultants was crucial in implementing digital security practices within their companies. Thus, consultants were also interviewed in this study, but a wider range of stakeholders could have enriched the results of this study.

Moreover, explaining one specific technology was also not feasible as digital security is required for most IT services within the financial sector. This would also vary substantially across companies. The emphasis of the thesis was not of technology but rather on the managerial aspects. This is also in line with the identified research gap. Finally, the Gioia method is used to analyze the data, but alternatives could also have been considered.

6.4.3 Mismatch between research question and method

It was also mentioned during the thesis defence that a study going back to the historical origins of when these systems were created going as far back as 1960s. Given the time frame and resource constraints of the master's thesis, this was out of scope for two reasons (1) finding participants with the requisite knowledge was not feasible as conducting a longer longitudinal study would require more follow-up interviews and access to the companies which might not have been granted.

References

Andronikidis, A., Karolidis, D., & Zafeiriou, G. (2021). Reflections on grounding firm innovation and viability [Article]. *European Management Journal*, *39*(1), 2–8. https://doi.org/10.1016/j.emj.2020.11.003

Awuzie, B., & McDermott, P. (2017). An abductive approach to qualitative built environment research [Article]. *Qualitative Research Journal*, *17*(4), 356–372. https://doi.org/10.1108/QRJ-08-2016-0048

Axelsson, J. (2023, October 10). Nya problem för Avanza – utsatt för ddos-attack. *Dagens Industri*. https://www.di.se/live/nya-problem-for-avanza-utsatt-for-ddos-attack/

Barney, J. (1991). Firm Resources and Sustained Competitive Advantage [Article]. *Journal of Management*, *17*(1), 99–120. https://doi.org/10.1177/014920639101700108

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response [Article]. *Information & Management*, *51*(1), 138–151. https://doi.org/10.1016/j.im.2013.11.004

Bei, X. (2019). Trademarks, specialized complementary assets, and the external sourcing of innovation [Article]. *Research Policy*, *48*(9), 103709. https://doi.org/10.1016/j.respol.2018.11.003

Bharadwaj, A. S. (2000). A Resource-Based Perspective on Information Technology Capability and Firm Performance: An Empirical Investigation [Article]. *MIS Quarterly*, *24*(1), 169–196. https://doi.org/10.2307/3250983

Bhaskar, R. (2008). *A Realist Theory of Science* (1st ed.). Routledge.

Bianchi, M., Frattini, F., Lejarraga, J., & Di Minin, A. (2014). Technology Exploitation Paths: Combining Technological and Complementary Resources in New Product Development and Licensing [Article]. *The Journal of Product Innovation Management*, *31*(S1), 146–169. https://doi.org/10.1111/jpim.12198

Blum, D. (2020). *Rational Cybersecurity for Business* [Book]. Springer Nature. https://doi.org/10.1007/978-1-4842-5952-8

Bryman, A., & Bell, E. (2015). Business research methods: Oxford University Press. *American Journal of Sociology*.

Butler, T., Gozman, D., & Lyytinen, K. (2023). The regulation of and through information technology: Towards a conceptual ontology for IS research [Article]. *Journal of Information Technology*, *38*(2), 86–107. https://doi.org/10.1177/02683962231181147

Calliess, C., & Baumgarten, A. (2020). Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective. *German Law Journal*, *21*(6), 1149–1179. https://doi.org/10.1017/glj.2020.67

Caralli, R. A., Allen, J. H., Curtis, P. D., White, D. W., & Young, L. R. (2010). Improving Operational Resilience Processes: The CERT Resilience Management Model. *Socialcom*, 1165–1170. https://doi.org/10.1109/SocialCom.2010.173

Ceipek, R., Hautz, J., De Massis, A., Matzler, K., & Ardito, L. (2021). Digital Transformation Through Exploratory and Exploitative Internet of Things Innovations: The Impact of Family Management and Technological Diversification [Article]. *The Journal of Product Innovation Management*, *38*(1), 142–165. https://doi.org/10.1111/jpim.12551

Cetindamar, D., & Phaal, R. (2023). Technology Management in the Age of Digital Technologies [Article]. *IEEE Transactions on Engineering Management*, *70*(7), 2507–2515. https://doi.org/10.1109/TEM.2021.3101196

Cetindamar, D., Phaal, R., & Probert, D. (2009). Understanding technology management as a dynamic capability: A framework for technology management activities [Article]. *Technovation*, *29*(4), 237–246. https://doi.org/10.1016/j.technovation.2008.10.004

Chee, F. Y. (2020, December 16). *Companies may face 2% fine for breaching EU cybersecurity rules*. Reuters. https://www.reuters.com/article/eu-cybersecurity-idUSKBN28Q1NS/

Chirumalla, K. (2021). Building digitally-enabled process innovation in the process industries: A dynamic capabilities approach [Article]. *Technovation*, *105*, 102256. https://doi.org/10.1016/j.technovation.2021.102256

Chiu, Y.-C., Lai, H.-C., Lee, T.-Y., & Liaw, Y.-C. (2008). Technological diversification, complementary assets, and performance [Article]. *Technological Forecasting & Social Change*, *75*(6), 875–892. https://doi.org/10.1016/j.techfore.2007.07.003

Clark-Ginsberg, A., & Slayton, R. (2019). Regulating risks within complex sociotechnical systems: Evidence from critical infrastructure cybersecurity standards. *Science & Public Policy*, *46*(3), 339–346.

Cloudflare. (n.d.). *What is a DDoS attack?* Cloudflare. Retrieved December 4, 2023, from https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

Cooper, R. G. (1983). A process model for industrial new product development [Article]. *IEEE Transactions on Engineering Management*, *EM-30*(1), 2–11. https://doi.org/10.1109/TEM.1983.6448637

Cozzolino, A., & Verona, G. (2022). Responding to Complementary-Asset Discontinuities: A Multilevel Adaptation Framework of Resources, Demand, and Ecosystems [Article]. *Organization Science (Providence, R.I.)*, *33*(5), 1990–2017. https://doi.org/10.1287/orsc.2021.1522

Daft, R. L. (1983). Learning the Craft of Organizational Research [Article]. *The Academy of Management Review*, *8*(4), 539–546. https://doi.org/10.5465/amr.1983.4284649

Dahlander, L., & Wallin, M. W. (2006). A man on the inside: Unlocking communities as complementary assets. *Research Policy*, *35*(8), 1243–1259. https://doi.org/10.1016/J.RESPOL.2006.09.011

de Vaujany, F.-X., Fomin, V. V, Haefliger, S., & Lyytinen, K. (2018). Rules, Practices, and Information Technology: A Trifecta of Organizational Regulation. *IDEAS Working Paper Series from RePEc*, *29*(3), 755–773.

Dhillon, G., Smith, K., & Dissanayaka, I. (2021a). Information systems security research agenda: Exploring the gap between research and practice [Article]. *The Journal of Strategic Information Systems*, *30*(4), 101693. https://doi.org/10.1016/j.jsis.2021.101693

Dhillon, G., Smith, K., & Dissanayaka, I. (2021b). Information systems security research agenda: Exploring the gap between research and practice [Article]. *The Journal of Strategic Information Systems*, *30*(4), 101693. https://doi.org/10.1016/j.jsis.2021.101693

Dierickx, I., & Cool, K. (1989). Asset Stock Accumulation and Sustainability of Competitive Advantage [Article]. *Management Science*, *35*(12), 1504–1511. https://doi.org/10.1287/mnsc.35.12.1504

Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers [Article]. *Computers & Security*, *92*, 101747–21. https://doi.org/10.1016/j.cose.2020.101747

Dietl, H., Royer, S., & Stratmann, U. (2009). Value Creation Architectures and Competitive Advantage: Lessons from the European Automobile Industry [Article]. *California Management Review*, *51*(3), 24–48. https://doi.org/10.2307/41166492

DORA. (2023). *Digital Operational Resilience Act (DORA)*. https://www.dora-info.eu/article-3/

Döringer, S. (2021). "The problem-centred expert interview". Combining qualitative interviewing approaches for investigating implicit expert knowledge [Article]. *International Journal of Social Research Methodology*, *24*(3), 265–278. https://doi.org/10.1080/13645579.2020.1766777

Dyer, J. H., & Singh, H. (1998). The Relational View: Cooperative Strategy and Sources of Interorganizational Competitive Advantage [Article]. *The Academy of Management Review*, *23*(4), 660–679. https://doi.org/10.2307/259056

Dyer, J. H., Singh, H., & Hesterly, W. S. (2018). The relational view revisited: A dynamic perspective on value creation and value capture [Article]. *Strategic Management Journal*, *39*(12), 3140–3162. https://doi.org/10.1002/smj.2785

EBA. (2022). *The Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554* . https://www.digital-operational-resilience-act.com/

Eisenhardt, K. M. (1989). Building Theories from Case Study Research [Article]. *The Academy of Management Review*, *14*(4), 532–550. https://doi.org/10.5465/amr.1989.4308385

EISENHARDT, K. M., & MARTIN, J. A. (2000). Dynamic capabilities : What are they? [Article]. *Strategic Management Journal*, *21*(10–11), 1105–1121.

ENISA. (2023). *ENISA THREAT LANDSCAPE 2023*.

Finansinspektionen. (2023, March 15). *Swedbank receives a remark and an administrative fine*. https://www.fi.se/en/published/sanctions/financial-firms/2023/swedbank-receives-a-remark-and-an-administrative-fine/

Flick, Uwe. (2018). *An introduction to qualitative research* (6th edition) [Book]. SAGE Publications.

Freij, Å. (2020). Using technology to support financial services regulatory compliance: current applications and future prospects of regtech [Article]. *The Journal of Investment Compliance*, *21*(2/3), 181–190. https://doi.org/10.1108/JOIC-10-2020-0033

Freij, Å. (2022). Regulatory change impact on technology and associated mitigation capabilities [Article]. *Technology Analysis & Strategic Management*, *34*(12), 1418–1431. https://doi.org/10.1080/09537325.2021.1963426

Giannelli, C., & Picone, M. (2022). Editorial "Industrial IoT as IT and OT Convergence: Challenges and Opportunities" [Article]. *IoT*, *3*(1), 259–261. https://doi.org/10.3390/iot3010014

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking Qualitative Rigor in Inductive Research [Article]. *Organizational Research Methods*, *16*(1), 15–31. https://doi.org/10.1177/1094428112452151

Granstrand, O., & Oskarsson, C. (1994). Technology diversification in "MUL-TECH" corporations [Article]. *IEEE Transactions on Engineering Management*, *41*(4), 355–364. https://doi.org/10.1109/17.364559

Helfat, C. E., & Lieberman, M. B. (2002). The birth of capabilities: market entry and the importance of pre-history [Article]. *Industrial and Corporate Change*, *11*(4), 725–760. https://doi.org/10.1093/icc/11.4.725

HELFAT, C. E., & PETERAF, M. A. (2015). MANAGERIAL COGNITIVE CAPABILITIES AND THE MICROFOUNDATIONS OF DYNAMIC CAPABILITIES. *Strategic Management Journal*, *36*(6), 831–850. http://www.jstor.org/stable/43897807

Hughes, A. (2006). The transforming power of complementary assets [Article]. *MIT Sloan Management Review*, *47*(4), 50.

IMF. (2023). Sweden: Financial Sector Assessment Program–Technical Note on Cybersecurity Risk Supervision and Oversight. In *2023*. https://www.imf.org/en/Publications/CR/Issues/2023/04/05/Sweden-Financial-Sector-Assessment-ProgramTechnical-Note-on-Cybersecurity-Risk-Supervision-531869

Irani, E. (2019). The Use of Videoconferencing for Qualitative Interviewing: Opportunities, Challenges, and Considerations [Article]. *Clinical Nursing Research*, *28*(1), 3–8. https://doi.org/10.1177/1054773818803170

ISO. (n.d.). *ISO and policy makers*. Retrieved December 4, 2023, from https://www.iso.org/iso-and-policy-makers.html

Jacobides, M. G. (2005). Industry Change through Vertical Disintegration: How and Why Markets Emerged in Mortgage Banking [Article]. *Academy of Management Journal*, *48*(3), 465–498. https://doi.org/10.5465/AMJ.2005.17407912

Jacobides, M. G., Knudsen, T., & Augier, M. (2006). Benefiting from innovation: Value creation, value appropriation and the role of industry architectures [Article]. *Research Policy*, *35*(8), 1200–1221. https://doi.org/10.1016/j.respol.2006.09.005

Jacobides, M. G., & Winter, S. G. (2005). The co-evolution of capabilities and transaction costs: explaining the institutional structure of production [Article]. *Strategic Management Journal*, *26*(5), 395–413. https://doi.org/10.1002/smj.460

James, S. D., Leiblein, M. J., & Lu, S. (2013). How Firms Capture Value From Their Innovations [Article]. *Journal of Management*, *39*(5), 1123–1155. https://doi.org/10.1177/0149206313488211

Johnson, G. (2017). *Exploring strategy* (R. Whittington, K. Scholes, D. Angwin, & P. Regner, Eds.; Eleventh Edition) [Book]. Pearson.

Kaplan, J., Richter, W., & Ware, D. (2019). Cybersecurity: Linchpin of the digital enterprise [Article]. In *McKinsey Insights*. McKinsey & Company, Inc. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-linchpin-of-the-digital-enterprise

Khan, T. H., & MacEachen, E. (2022). A furnished house without walls: Examining the work and health support systems of self-employed workers in Ontario, Canada [Article]. *Safety and Health at Work*, *13*, S201–S201. https://doi.org/10.1016/j.shaw.2021.12.1380

Krüger, P., & Bruachle, J. (2021). *The European Union, Cybersecurity, and the Financial Sector: A Primer*. https://carnegieendowment.org/2021/03/16/european-union-cybersecurity-and-financial-sector-primer-pub-84055

Kure, H. I., Islam, S., & Mouratidis, H. (2022). An integrated cyber security risk management framework and risk predication for the critical infrastructure protection [Article]. *Neural Computing & Applications*, *34*(18), 15241–15271. https://doi.org/10.1007/s00521-022-06959-2

Lai, H.-C., Chiu, Y.-C., Liaw, Y.-C., & Lee, T.-Y. (2010). Technological Diversification and Organizational Divisionalization: The Moderating Role of Complementary Assets [Article]. *British Journal of Management*, *21*(4), 983–995. https://doi.org/10.1111/j.1467-8551.2009.00630.x

Lee, I. (2020). Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management [Article]. *Future Internet*, *12*(9), 157. https://doi.org/10.3390/fi12090157

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. Sage, Thousand Oaks.

Liu, C.-W., Huang, P., & Lucas, H. C. (2020). Centralized IT Decision Making and Cybersecurity Breaches: Evidence from U.S. Higher Education Institutions [Article]. *Journal of Management Information Systems*, *37*(3), 758–787. https://doi.org/10.1080/07421222.2020.1790190

Long, W., Cuyvers, L., & Quarthilo, J. (2023, May 8). *New EU Cyber Law for the Financial Services Industry with Significant Impact on ICT Service Providers*. Sidley. https://datamatters.sidley.com/2023/05/08/new-eu-cyber-law-for-the-financial-services-industry-with-significant-impact-on-ict-service-providers/

López, L. E., & Roberts, E. B. (2002). First-mover advantages in regimes of weak appropriability: the case of financial services innovations [Article]. *Journal of Business Research*, *55*(12), 997–1005. https://doi.org/10.1016/S0148-2963(01)00200-4

Maleh, Y. (2021). IT/OT convergence and cyber security [Article]. *Computer Fraud & Security*, *2021*(12), 13–16. https://doi.org/10.1016/S1361-3723(21)00129-9

Mbanaso, U. M., Abrahams, L., & Okafor, K. C. (2023). Adopting a Funnel Strategy and Using Mind Mapping to Visualize the Research Design. In U. M. Mbanaso, L. Abrahams, & K. C. Okafor (Eds.), *Research Techniques for Computer Science, Information Systems and Cybersecurity* (pp. 39–58). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-30031-8_4

McQuade, M. (2018, August 22). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. Wired. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Miller, D. J. (2006). Technological diversity, related diversification, and firm performance [Article]. *Strategic Management Journal*, *27*(7), 601–619. https://doi.org/10.1002/smj.533

Mingers, J., Mutch, A., & Willcocks, L. (2013). Critical Realism in Information Systems Research [Article]. *MIS Quarterly*, *37*(3), 795–802. https://doi.org/10.25300/MISQ/2013/37:3.3

Nevo, S., & Wade, M. R. (2010). The Formation and Value of IT-Enabled Resources: Antecedents and Consequences of Synergistic Relationships [Article]. *MIS Quarterly*, *34*(1), 163–183. https://doi.org/10.2307/20721419

Newbert, S. L. (2007). Empirical research on the resource-based view of the firm: an assessment and suggestions for future research [Article]. *Strategic Management Journal*, *28*(2), 121–146. https://doi.org/10.1002/smj.573

Nylen, D., & Holmstrom, J. (2015). Digital innovation strategy: A framework for diagnosing and improving digital product and service innovation [Article]. *Business Horizons*, *58*(1), 57–67. https://doi.org/10.1016/j.bushor.2014.09.001

Paté-Cornell, M. -Elisabeth, Kuypers, M., Smith, M., & Keller, P. (2018). Cyber Risk Management for Critical Infrastructure: A Risk Analysis Model and Three Case Studies [Article]. *Risk Analysis*, *38*(2), 226–241. https://doi.org/10.1111/risa.12844

Penrose, Edith. (2009). *The Theory of the Growth of the Firm.* (Christos. Pitelis, Ed.; 4th ed.) [Book]. Oxford University Press, Incorporated.

Pisano, G. (2006). Profiting from innovation and the intellectual property revolution [Article]. *Research Policy*, *35*(8), 1122–1130. https://doi.org/10.1016/j.respol.2006.09.008

Rasmussen, L. (2023, March 15). *Swedbank receives $82 mln administrative fine over lack of IT control*. Reuters. 05/11/2023https://www.reuters.com/business/finance/swedbank-gets-82-mln-administrative-fine-2023-03-15/

Robinson, O. C. (2014). Sampling in Interview-Based Qualitative Research: A Theoretical and Practical Guide [Article]. *Qualitative Research in Psychology*, *11*(1), 25–41. https://doi.org/10.1080/14780887.2013.801543

Rubin, H. J., & Rubin, I. S. (2011). *Qualitative interviewing: The art of hearing data.* Sage.

Saunders, M. (2019). *Research methods for business students* (P. Lewis & Adrian. Thornhill, Eds.; Eighth edition) [Book]. Pearson Education.

Schinagl, S., & Shahim, A. (2020). What do we know about information security governance? [Article]. *Information and Computer Security*, *28*(2), 261–292. https://doi.org/10.1108/ICS-02-2019-0033

Schinagl, S., Shahim, A., & Khapova, S. (2022). Paradoxical tensions in the implementation of digital security governance: Toward an ambidextrous approach to governing digital security [Article]. *Computers & Security*, *122*, 102903. https://doi.org/10.1016/j.cose.2022.102903

Schneier, B. (2015). *Secrets & Lies: Digital Security In a Networked World* (15th ed.). John Wiley & Sons Incorporated.

Seddon, P. B. (2014). Implications for strategic IS research of the resource-based theory of the firm: A reflection. *The Journal of Strategic Information Systems*, *23*(4), 257–269. https://doi.org/https://doi.org/10.1016/j.jsis.2014.11.001

Sköld, M., Freij, Å., & Frishammar, J. (2020a). New Entrant or Incumbent Advantage in Light of Regulatory Change: A Multiple Case Study of the Swedish Life Insurance Industry [Article]. *European Management Review*, *17*(1), 209–227. https://doi.org/10.1111/emre.12345

Sköld, M., Freij, Å., & Frishammar, J. (2020b). New Entrant or Incumbent Advantage in Light of Regulatory Change: A Multiple Case Study of the Swedish Life Insurance Industry [Article]. *European Management Review*, *17*(1), 209–227. https://doi.org/10.1111/emre.12345

Taylor, P., & Lowe, J. (1997). Are functional assets or knowledge assets the basis of new product development performance? [Article]. *Technology Analysis & Strategic Management*, *9*(4), 473–488. https://doi.org/10.1080/09537329708524298

Teece, D. J. (1986a). Profiting from technological innovation: Implications for integration, collaboration, licensing and public policy. *Research Policy*, *15*(6), 285–305. https://doi.org/10.1016/0048-7333(86)90027-2

Teece, D. J. (1986b). Profiting from technological innovation: Implications for integration, collaboration, licensing and public policy. *Research Policy*, *15*(6), 285–305. https://doi.org/10.1016/0048-7333(86)90027-2

Teece, D. J. (2006). Reflections on “Profiting from Innovation” [Article]. *Research Policy*, *35*(8), 1131–1146. https://doi.org/10.1016/j.respol.2006.09.009

Teece, D. J. (2007). Explicating dynamic capabilities: the nature and microfoundations of (sustainable) enterprise performance [Article]. *Strategic Management Journal*, *28*(13), 1319–1350. https://doi.org/10.1002/smj.640

Teece, D. J. (2018). Profiting from innovation in the digital economy: Enabling technologies, standards, and licensing models in the wireless world [Article]. *Research Policy*, *47*(8), 1367–1387. https://doi.org/10.1016/j.respol.2017.01.015

Teece, D. J., & Linden, G. (2017). Business models, value capture, and the digital enterprise [Article]. *Journal of Organization Design (Aarhus)*, *6*(8), 1–14. https://doi.org/10.1186/s41469-017-0018-x

Thorsell, K. (2021, September 17). *IT-attacken mot Coop: ”Verkligheten är något annat än träning”*. Ingenjören. 05/11/2023https://ingenjoren.se/2021/09/17/it-attacken-mot-coop-verkligheten-ar-nagot-annat-an-traning/

Timmermans, S., & Tavory, I. (2012). Theory Construction in Qualitative Research: From Grounded Theory to Abductive Analysis [Article]. *Sociological Theory*, *30*(3), 167–186. https://doi.org/10.1177/0735275112457914

TRIPSAS, M. (1997). UNRAVELING THE PROCESS OF CREATIVE DESTRUCTION: COMPLEMENTARY ASSETS AND INCUMBENT SURVIVAL IN THE TYPESETTER INDUSTRY [Article]. *Strategic Management Journal*, *18*(S1), 119–142. https://doi.org/10.1002/(SICI)1097-0266(199707)18:1+<119::AID-SMJ921>3.0.CO;2-0

Tsang, E. W. K. (2014). Case studies and generalization in information systems research: A critical realist perspective [Article]. *The Journal of Strategic Information Systems*, *23*(2), 174–186. https://doi.org/10.1016/j.jsis.2013.09.002

Valerio Begozzi, Matteo Oldani, & Francesca Terrizzano. (2023). The growing importance of digital risk governance [Article]. *Risk Management Magazine (Online)*, *18*(2), 27–36. https://doi.org/10.47473/2020rmm0126

von Solms, B., & von Solms, R. (2018). Cybersecurity and information security – what goes where? [Article]. *Information and Computer Security*, *26*(1), 2–9. https://doi.org/10.1108/ICS-04-2017-0025

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security [Article]. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Wade, M., & Hulland, J. (2004). Review: The Resource-Based View and Information Systems Research: Review, Extension, and Suggestions for Future Research [Article]. *MIS Quarterly*, *28*(1), 107–142. https://doi.org/10.2307/25148626

Wernerfelt, B. (1984). A Resource-based View of the Firm [Article]. *Strategic Management Journal*, *5*(2), 171.

Yin, R. (2016). *Qualitative Research from Start to Finish* (2nd ed.). The Guildford Press.

Appendix 1 Teece (1986) framework of complementary assets

Fig A2.1 Complementary assets needed to commercialize an innovation, adapted from the original framework by Teece (1986). Teece (2006) argues the need to add relational assets to this framework

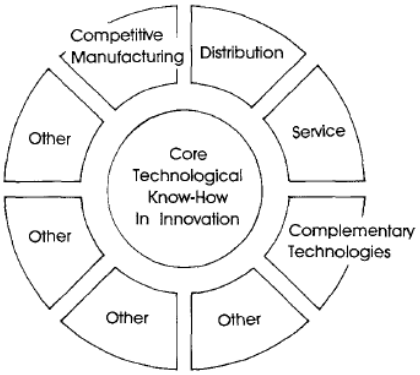
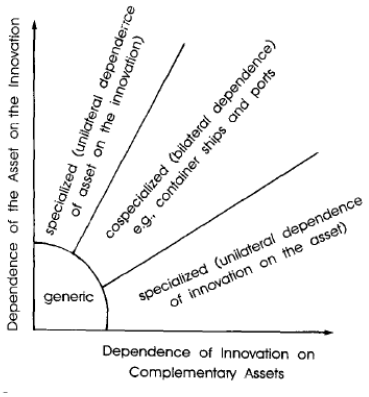


Fig A2.2 Generalized, cospecialized and specialized complementary assets, adapted from the original framework by Teece (1986)



Appendix 2 List of interviewees

Interviewee	Role	Interview date	Interview length (hh:mm)
1	Independent consultant working with governance, risk and compliance	2023-10-04	00:59
2	Senior consultant working with cybersecurity digitalization specifically in the financial sector	2023-10-06	01:10
3	Business development at blockchain digitalization company	2023-10-11	00:25
4	Chief Innovation Officer at major Swedish insurance firm	2023-10-16	01:01
5	Senior Business Developer at Nordic bank	2023-10-16	00:30
6	IT-security specialist and Data Security (GDPR) Coordinator at government agency	2023-10-17	00:50
7	Chief Information Officer at Swedish investment firm	2023-10-18	00:42
8	Cybersecurity specialist providing external security services	2023-10-18	00:45
9	Senior cybersecurity consultant	2023-10-18	00:55
10	Senior cloud specialist at Nordic bank	2023-10-19	00:57
11	Project manager at IT consulting firm	2023-10-20	00:50
12	Former Chief Information Security Officer at insurance firm	2023-10-20	00:52
13	Head of Global IT Security at a global mining and construction company	2023-10-20	01:08
14	Information & Cybersecurity advisor; Chief Information Security Officer at distributed ledger solutions provider	2023-10-23	01:15
15	Consultant at cybersecurity consultancy firm	2023-10-23	00:49
16	Chief Information Security Officer at investment firm	2023-10-25	01:19
17	Senior Information Security Consultant	2023-10-25	01:01
18	Business development director of compliance solutions at major global firm	2023-10-26	00:50
19	Head of digtial assets at distributed ledger solution provider	2023-10-26	00:48
20	Senior Manager at consulting firm working with cybersecurity projects	2023-10-27	00:58
21	Freelance penetration and security tester	2023-10-30	00:45
22	Compliance manager and Data Protection Officer at regional bank	2023-10-31	00:35
23	Business consultant working with cybersecurity projects	2023-10-31	01:02
24	Former head of cloud implementation at major Swedish bank	2023-11-02	01:03
25	Senior consultant working in the area of data privacy	2023-11-07	00:32
26	Chief Technical Officer at Swedish digital identity company	2023-11-07	00:25
27	Senior leadership role in cross-functional IT implementation at regional insurance provider	2023-11-09	00:44

Appendix 3 Interview questions and post-interview questions

Sample interview questions for the main interview

Introduction

- Presentation of author
- Presentation of thesis and its general purpose
- Presentation of formal information around participation
    - Participation is voluntary.
    - You have the right to cancel the interview at any time without explaining why.
    - The company, interviewee name, and role will be anonymised.
    - Ask for approval to record the interview to later transcribe it excluding any personal data. Any questions before we begin?

Background information

- How would you describe your role at your current company or firm?
- How long have you worked in this field and what were your previous experiences?

DS related questions

- How would you describe the current security threats and challenges facing the industry? Has anything changed in the past few years?
    - How are companies dealing with these threats?
- How do companies prepare for regulatory changes such as DORA, NIS 2, etc.?
- How do companies build these capabilities and frameworks?
- What internal capabilities are used in the context of DS?
- What external capabilities are used in the context of DS?
- Are there any industry level collaborations present around DS? If yes, then could you please elaborate further.

Drivers and barriers

- What challenges have you faced when implementing DS policies?
- How have you overcome them and what were your learnings in the process?

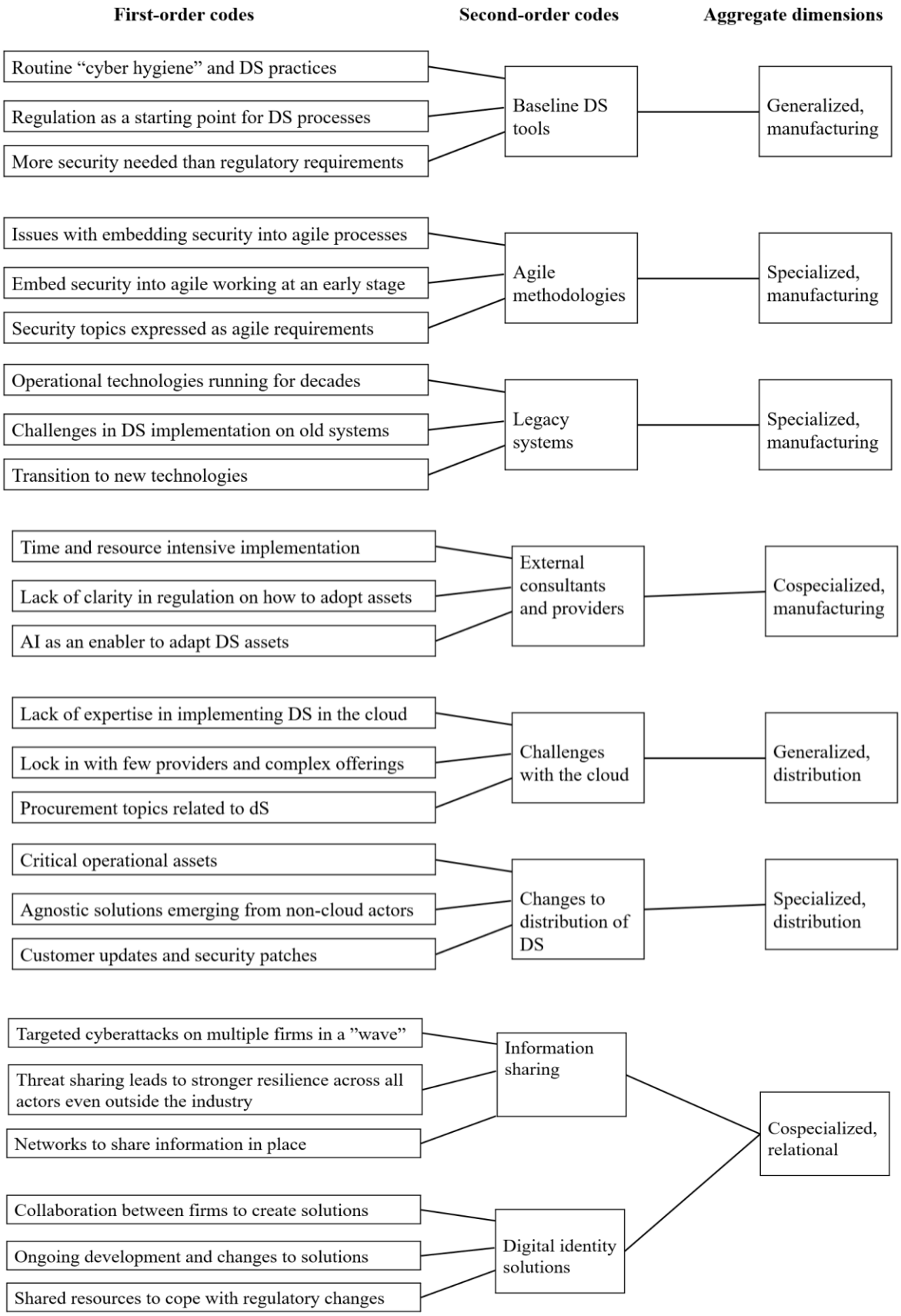
Outro

- Have I missed anything? Is there anything you would like to highlight that I might have missed regarding the topic?
- Can I reach out to you in case I have follow-up questions in the future?

Post interview questions

- How did the interview go?
- What were the key learnings?
- Feelings about the interview: did it open new any avenues of interest?)
- Setting of the interview

Appendix 4 Data structure



Appendix 5 Data table

The data table below is presented to provide additional support to the empirics, offering supplementary quotes to the first-order and second-order codes.

Data supporting interpretations	
Aggregate dimensions	*First order themes & representative quotations*
Background & context	*"Even in a big company, there are incidents happening in one department that other department never finds out about." – Interviewee 16* *"DDos and phishing attacks have become more sophisticated. This requires updated tech and learning. It is quite hard to implement these lessons." – Interviewee 1*
Manufacturing, generalized	*"In terms of cyber security, [the regulation] gives an organization the incentive to start working risk based [and] in a more systematic manner because if you fail to do so, the worst case could be you will get huge fines." - Interviewee 20* *"Regulations are a great base, but they are [a] low baseline of the most important things to put in place. They let you follow a framework that makes sense." – Interviewee 10* *"I would say that it is very important, I would say that that, the regulation is the foundation that you base your work on." – Interviewee 2*
Manufacturing, specialized	***Challenges with agile methodologies*** *"Traditionally [agile] has not worked well with [security]. Developers are the least security aware employees. They do not know how to develop code in a secure way. Security champions are needed to help*

	explain how to develop secure software." - Interviewee 20
	Early implementation of agile
	"If you just look at Netflix as a company, on the surface, they are just providing you streaming services, but there some extremely interesting technology choices that they've done deep in their systems from the start." – Interviewee 7
	"Afterwards security is more expensive, therefore the focus should be security by design, early in the process. Explicit requirements should be code and scan things in the pipeline. Testing should be done as part of the production environment." – Interviewee 23
	Challenges with legacy systems
	"We started as a bank more less, but of course implications are much more complex with an IT stack that is over 50 years old. I don't know how many generations of IT we have. This is the case for most banks in this region." – Interviewee 10
	"There is lack of expertise when it comes to understanding the security aspects legacy systems because the knowledge is no longer in the firm." – Interviewee 27
Manufacturing, cospecialized	***Regulatory uncertainty***
	"DORA is complex and hits broadly since it has different takes than that of previous ICT regulation. The previous regulation explains to a large extent to what to do, but they were not quite as granular as DORA. We need to take a number of aspects into account building new things." – Interviewee 3

External consultants

"PCI DSS requires external testing of vulnerabilities. There are plenty of time and resource constraints when firms do this testing internally. This will now become mandatory with DORA." – Interviewee 21

AI tools

"AI tools, especially in the regtech area can level the playing field." – Interviewee 2

"AI tools have to be tailored to the function. You can reuse the same AI engine, but some tailoring takes place for different products and for different purposes. The AI can then optimize itself using the data it collects." – Interviewee 16

"Going froward, we should try to automate as much as possible. It's better to have built in security so we do not rely on humans and leave room for error. AI can steer and guide humans." – Interviewee 13

Distribution, generalized

Cloud technologies

"With the migration to cloud, we need to to know exactly what we're doing and that we're doing the right thing. And also [we are] integrating into all of the things we move, and this has to be to the right parts of the organizations. We set a new chain of events into motion so what if we have a disaster, right?" – Interviewee 10

"Cloud security is an extremely relevant topic. There is an entire field around this that has emerged and is growing rapidly." – Interviewee 20

"Legislators ask for separation of duty and separation of the data in different sources since there is a high focus on security. This is an issue with the cloud." – Interviewee 27

Distribution, specialized	***Encryption*** *"We need to have open systems. Our systems have to be interoperable to work with other distributed ledger solutions." – Interviewee 5* *"We have proxy servers in the middle that only send metadata outside the firm." – Interviewee 1* ***Specialized cloud solutions*** *"Of course, if you have a competence gap in terms of actually understanding the code that the old legacy systems are running on that would be a risk. But then you have to integrate these systems into a modern IT infrastructure. Cloud based can also be a challenge. So, you need to create specialized solutions."- Interviewee 27* *"Looking at Operation Technology Systems of the systems, those are very critical in many cases very critical, and they have to be on-premises only. Otherwise, we face very serious security and compliance risks" – Interviewee 1* ***Procurement considerations*** *"If you look at DORA, an entire article covers security in procurement so many of our clients are requesting support to establish a process where they can assess risks prior to the onboarding of the vendor." – Interviewee 20* ***Service packages*** *"There are an enormous variety of providers with services attached to it. For more complex services, there are service support packages that our clients have to buy at least once." - Interviewee 1*

Relational assets: information sharing	***Barriers to sharing information*** "It's for a good cause, but it can be painful." ***Benefits to sharing information*** *"If information is collected centrally, there is less of the free-riding problem. We can potentially stop bigger attacks or even campaigns of attacks. There is a monoculture of Windows and Linux servers in many firms so there is less variation in technology. Sharing early indicators can prevent risks before they even develop." – Interviewee 23* ***Information sharing networks*** *"We work with the large banks in this region. We collaborate with them, and we also collaborate with the number of different organizations. We report incidents to MSB, and we also report to suppliers such as Microsoft." – Interviewee 10* *"Whoever it affects, we cooperate with a number of different networks around cybersecurity and resilience networks as well. And we are working with our competitors as well the big banks so some of this is in place for DORA." – Interviewee 3* *"Our [global consulting] firm has networks of CISOs from the client companies that we work with. They participate regularly in information sharing groups. They are from all around the world." – Interviewee 20*

	Balance in sharing information *"You cannot move around all your data, but you should be able to share some of your data. It is important to consider the opportunity costs." – Interviewee 27*
Relational assets: Digital identity solutions	***Cospecialized interfirm solutions*** *"We use a toolbox of identity systems, payment services, identity management and data storage solutions from multiple providers. We combine this to create digital and digital identities for anything that can be uniquely identified in a transparent manner." – Interviewee 19* *"Many countries look at what the Swedish financial sector has achieved as the standard for digital identities. I think the success of this is driven by the many strong partnerships." – Interviewee 5*