A Trade Secrets Framework and Strategic Approaches

Ozcan O.[1], Pickernell D.[2], Trott P.[3]

1 School of Languages and Applied Linguistics, University of Portsmouth, UK; School of Management, Swansea University, UK oleksandra.ozcan@port.ac.uk

2 School of Management, Swansea University, UK d.g.pickernell@swansea.ac.uk

3 School of Strategy, Marketing and Innovation, University of Portsmouth, UK paul.trott@port.ac.uk

Abstract

Trade secrets are key assets for innovative, successful, companies. Compared to other intellectual property (IP), trade secrets require different approaches to protect and embed them into company innovation strategies. Previous literature has not, however, provided a comprehensive evaluation of the strategic approaches towards trade secrets. This paper benefits from a systematic literature review (SLR) method to examine trade secrecy approaches with a theoretical lens using both dynamic capabilities (DC) and resource based-view (RBV) approaches. Fifty articles are carefully selected and examined to build a 'strategic directions and approaches' framework for companies to protect and benefit from their trade secrets. This study therefore offers both academic and practical value by identifying a dynamic, structured, view of available trade secrecy approaches, the foundations for a unified trade secrecy framework, and a future research agenda.

Keywords: Trade Secrecy Approaches, Dynamic Capability, Resource Based-view, Innovation Appropriation.

Managerial relevance statement

This study is relevant for managers and practitioners as it highlights the significance of trade secrecy as a valuable Intellectual Property (IP) protection tool. We provide a comprehensive overview of the trade secrecy approaches found in academic literature at various stages of the trade secrecy management process. Companies considering IP protection approaches can use this information to form an opinion on how to protect their valuable information as a trade secret. Additionally, we stress that IP protection should not be viewed as a standalone function within an organization, but rather as an integral component of the ways through which a business can meet its strategic objectives.

1. Introduction

Trade secrets are quickly outgrowing patents in global usage. In the UK, for example, 70% of companies of various sizes and industries now use trade secrets for the protection of their innovations (Intellectual Property Office (IPO), 2021). Use of such trade secrets allows organizations to free up resources for further innovation and to grow brand value immediately without financial expense (Miric et al., 2019). Trade secrets tend to be more widely used for marketing and organizational innovations, predominantly by manufacturing companies in engineering, textile, chemicals and pharmaceutical sectors (Wajsman and Garcia-Valero, 2017). Service sectors prefer to use trade secrecy for process and customer lists protection due to the unpatentability of some processes, difficulty of monitoring process patent infringement and the potential for reverse-engineering (IPO, 2022).

Unlike patents, however, trade secrets are only valuable when they remain a secret and their protection is weaker when information leakage or spill-over occurs (Hardy,2021). The theft of a trade secret has both strategic and financial consequences for a business that can lead to the overall loss of competitive advantage. The most frequent instances of trade secrecy loss are due to malicious trade secret misappropriation, theft, and cybertheft (Ritala et al, 2015). Indeed, cybertheft alone generates £60 billion yearly losses with potential losses of 1 million jobs in the EU (Basuchoudhary and Searle,2019), and it has become one of the key challenges posed to trade secrecy management in the digital age (Searle, 2021).

Consequently, trade secrecy is gaining the attention of policy makers, particularly through trade secrets disputes. The number of emerging high-profile legal cases on trade secrecy misappropriation (Heraeus v Zimmer, 2022; Qualcomm v Apple, 2017; Motorola Solutions v Hytera Communications,2020) highlight the extent of these issues. Weaknesses in businesses' trade secrecy protection regimes, low levels of business awareness, limitation of employee mobility, cybersecurity, weaknesses of the identification and protection of trade secrets are

among some of the main policy issues in the field of trade secrecy management today (WTO, 2022). Thus, the Intellectual Property Office UK (2021) and World Trade Organization (2022) are among many public policy organizations calling for increased trade secrecy awareness by innovative firms in implementation, safeguarding and breach mitigation of trade secrecy.

Despite its impact on innovation and economic growth, however, trade secrecy is poorly studied (Wajsman & García-Valero, 2017; Kang and Lee, 2022). Prior research on trade secrecy has focused on the choice of Intellectual Property (IP) rights protection approaches, their efficiency, impact on innovative activities (Sofka et al, 2018; Suzuki, 2015; Miric et al, 2019; du Zubielque et al, 2016; Contactor, 2019; Crittenden et al, 2015), human resource management in IP (Hannah, 2007, Hannah et al; 2019); choice of value capture strategies (James et al, 2013); institutional approaches for organizational secrecy (Liebeskind, 1997; Hannah and Robertson, 2015); and impacts of trade secrecy on innovations (Contractor, 2019; Crittenden et al., 2015; Henttonen et al., 2016). Few studies, however, provide a holistic overview of IP appropriability strategies (Bos et al., 2015; Liebeskind, 1997; Hannah et al., 2019; James et al., 2013). More specifically, examination of the previous literature shows a lack of theoretical and practical frameworks for trade secrecy approaches and strategies. Table 1 demonstrates some of the key studies in trade secrecy management.

Table 1. Key literature on trade secret management

Key Literature	Areas of Research	Literature Gap
Kang and Lee (2022)	A dynamic approach to trade secrecy protection in response to employee departure after the adoption of the Application v Hunter decision.	Management lacks knowledge on the variety of trade secrecy approaches. More research is needed to provide a canvas of trade secrecy protection approaches for management in the case of worker departure.
Crittenden et al (2019)	Overview of trade secrecy protection approaches to achieve competitive advantage.	There is a lack of understanding of the value trade secrets represent for organizations. More research is needed to highlight the importance of trade secrecy and the variety of approaches available for trade secrecy protection.
Hannah et al (2019)	Types of value appropriation strategies and secrecy as a knowledge protection strategy.	More research is needed in studying the processes of creation, implementation, protection and change of a trade secret.

Bos et al (2015)	Advantages and disadvantages of trade secrecy; determinants of trade secrecy use; stages and lifecycle of trade secrecy.	Lack of research on the entire process of trade secrecy management. More research needed to understand the processes behind the choice of a trade secret approach over other forms of IP protection, variety of trade secret protection approaches and finally trade secret mitigation.
James at al (2013)	Value capture strategies from innovations and the identification of the conditions for the selection of such value capture strategies.	General lack of understanding of how firms manage value capture strategies throughout the different stages of IP protection.
Liebeskind (1997)	Understanding the types of knowledge, costs of keeping the knowledge protected and approaches of organizational knowledge protection.	More research needed into variety of knowledge protection approaches.

The authors in these studies argue for more research into trade secrecy processes, stages and trade secrecy protection approaches (Liebskind, 1997; Bos et al ,2015; Hannah et al, 2019; Kang and Lee, 2022). The lack of review studies on trade secrecy protection approaches and theoretical frameworks, however, adds to the disadvantaged and overlooked position of trade secrecy as an IP protection approach. Considering these key studies and the research gaps in this field they reveal that there is a lack of knowledge on trade secrecy approaches that can be utilized by management to protect valuable information and mitigate the potential damages of trade secret leakage. Therefore, we aim to address the following research questions:

RQ1: What trade secrecy management approaches are used to protect and sustain innovations?

RQ2: What trade secrecy management approaches are implemented by innovative companies in cases of misappropriation?

Based on the above-mentioned research questions, the aim of this study is to identify strategic approaches and to propose a theoretical framework for trade secrets. To achieve this, a systematic literature review (SLR) approach is used to examine 50 carefully selected studies with two theoretical lenses, dynamic capabilities (DC) and the resource based-view (RBV). The RBV of the firm identifies a specific bundle of complementing tangible and intangible

resources to protect trade secrets as valuable organizational resources. This complements the DC approach, which gives a framework for the processes required when trade secrecy is breached, reconfiguring assets and resources to create a new trade secrecy equilibrium where RBV approaches can again apply (Porter 1981, 1996; Teece, 2007; Hussain & Terziovski, 2016)

The selected methodological approach, with its rich theoretical foundations, allows us to demonstrate the full spectrum of trade secrecy management approaches available in existing literature and contribute to previous studies in a number of ways. We contribute to the studies of Bos et al. (2015) and Hannah et al (2019) by providing a theoretical framework for trade secrets to illustrate available approaches and options to the relevant stakeholders in this field. The work also extends previous findings by providing a stage-based approach using DC theory following the future research directions of Kang and Lee (2022) and Crittenden et al (2019). Finally, we provide future research directions to the relevant academicians in this field, by identifying key gaps in the relevant literature by linking it to the theoretical framework developed based on both DC and RBV theories.

Apart from the contributions to the theory and previous studies, this study also provides practical contributions to this field. The results of the study reveal that there is a large number of available trade secrecy protection approaches for managers to utilize. However, there is also a lack of trade secrecy management understanding in innovative organizations. Therefore, this study reaffirms the need for the development of a comprehensive trade secrecy management framework to be applied by innovative companies through the lifecycle of the trade secret.

In the following section, relevant literature and theories are examined to build the conceptual framework, from both DC and RBV theories. In the method section, the chosen systematic literature review method, the widely accepted PRISMA (Preferred Reporting Items for

Systematic Reviews and Meta-Analyses) process and framework, is illustrated. In the results section, the findings are organised based on the theoretical framework developed in this study. Finally, in the Conclusions, the results are discussed in relation to previous studies, contributions derived and explained in detail, practical managerial and policy implications outlined, the study's limitations identified, and consequent future research directions derived.

2. Background and Relevant Theories

2.1. Background

Trade secrecy is an important mechanism for protection of valuable knowledge created as a result of innovative activity (Hemphill, 2004). According to the World Intellectual Property Organization (WIPO), trade secrets are IP rights on confidential information, which may be sold or licensed (WIPO, 2021). Trade secrets protect confidential information forming a key competitive advantage for the company. It can be technical or commercial information relating to manufacturing processes, designs of computer software, marketing strategies and client lists (WIPO, 2021). The definition of trade secret under the EU Directive 2016/943 is consistent with WIPO, though it does not acknowledge trade secrecy as an exclusive IP right. Both, however, provide trade secrets with equal and harmonised means and levels of protection (Morrison & Foerster, 2017). Under Article 39 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) and Article 2 of the EU Directive 2016/943, to be considered a trade secret the information in question must:

1. Possess commercial value because of its secret properties;
2. Be limited in knowledge to a number of individuals; and
3. Be kept secret by a rightful owner using reasonable steps in the form of confidentiality agreements or other means (TRIPS; 1995; EU Directive 2016/943);

Unlike patents, however, the scope of information covered by trade secrets is unlimited (ICC), 2017). The commercial value requirement applies to potential and actual value (Brant & Lohse,

2014). Therefore, the trade secret protection umbrella extends to experimental work, unreleased products or strategies and information value superseding actual use conditions including failed experiments and "negative know-how". (Brant & Lohse, 2014). Conversely, trade secrets are non-exclusive. Independent discovery and reverse engineering are permissible. (Brant & Lohse, 2014). Hence, it is the responsibility of a trade secret owner to take reasonable efforts to protect the confidentiality of such information.

The amount of such efforts varies according to the extent of technological development and company size: from confidentiality agreements in Small and Medium-sized Enterprises (SMEs) to cyber-theft prevention in large corporations (Brant & Lohse, 2014). Without safeguarding, however, some confidential information disclosure, in the form of unintentional leakage, employee mobility and commercial espionage (Arrow, 1962; Quan and Chesbrough, 2009) is inevitable. It is worth noting, therefore, that despite established trade secrecy protection legislation, the practical details of trade secrecy management are frequently overlooked.

2.2. Theoretical Framework

In the context of trade secrets, both RBV and DC provide theoretical underpinnings. Looking at RBV first, to determine the strategic importance of key organizational resources or capabilities they must possess several qualities described in the VRIO Framework established by Barney (1991), specifically needing to be valuable, rare, inimitable AND organized within the company (Barney 1991, 1995). These characteristics allow a company to extract maximum value from their assets and provide motivation for further innovation (Cohen et al, 2002). The key organizational resources of the innovative companies that satisfy the VRIO framework constitute IP and, in this case, trade secrets (Penrose, 1959). If pursued by the company, trade secrets are an essential part of its IP portfolio allowing appropriation of innovation value (Hannah, 2019).

The RBV, however, underpins trade secrecy only when it is well protected as a key organizational resource. Significantly, trade secrets are often in the form of tacit knowledge accumulated in the minds of employees, difficult to imitate and harder to retain within the company (Polanyi, 1962; Teece et al, 1997). Firms that aim at sustaining their competitive advantage through possession of trade secrets theoretically need to engage in strategic planning to foresee potential threats or changes in the environment that might affect the trade secret (Barney, 1991).

DC theory, however, states that in order to sustain competitive advantage, companies also need to constantly monitor changes in their external environment and adjust their competencies accordingly (Tsortzki, 2014; Barreto, 2010). A rapid and highly innovative environment requires a dynamic appropriability approach (Teece, 2000, Huang et al, 2014). The DC theory therefore fulfils the requirement of trade secrecy mitigation as a result of intentional spill-over, revealing of confidential information or misappropriation. Consequently, we consider a two-fold continuously evolving trade secrecy management approach where a company owning a trade secret needs to consider both the RBV approach to maintaining and protecting existing trade secrets and the DC proactive approach for potential misappropriation. That being said, we also acknowledge theoretical overlapping in the measures taken by companies to sustain their competitive advantage and safeguard trade secrets in light of changing environmental or threat conditions.

Considering this theoretical background, trade secrecy management approaches delineate into one of these two theoretical concepts. Figure 1 demonstrates trade secrecy management approaches arising from capabilities within the organization to contain trade secrets or take measures to avoid loss of valuable information due to internal or external environmental changes.

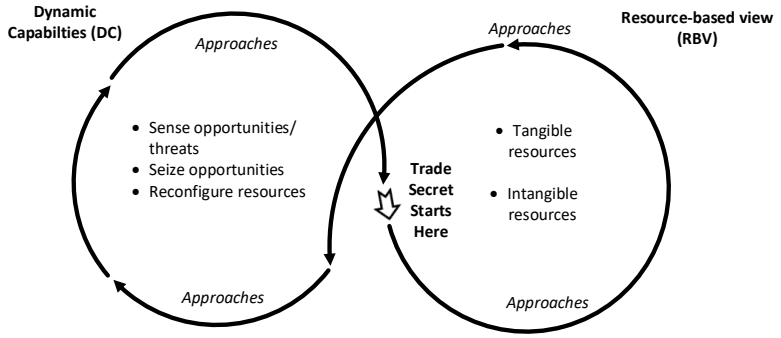


Figure 1. Conceptual Framework for Trade secrecy management approaches

The RBV divides these capabilities into tangible and intangible (Barney, 1991), where tangible and intangible resources are capabilities an organization possesses and applies to protect its trade secrets. Tangible aspects of the RBV entails measures of physical nature taken by such organisations: from organizational actions concerned with administrative and physical control to financial protection measures (e.g. unused debt capacity). Intangible capabilities are focused on protection measures concerned with innovation activities and Human Resource (HR)

management (Barney,1986).

The DC approach entails application of organizational approaches reflecting continuous revision of threats and opportunities and reconfiguration of organizational assets to manage such valuable information (Teece, 2007). Trade secrecy management approaches identified with DC concepts then entail targeted measures taken by an organization to sense, seize or reconfigure assets based on new opportunities or threats to trade secrecy protection.

Figure 1 demonstrates that these trade secrecy approaches are interlinked with each other, forming a complete cycle. The RBV approach seems most relevant to activities undertaken to keep the trade secret, whilst approaches shift into the DC approaches after the environment changes when trade secrecy is breached, the DC approaches then flowing back into the RBV approaches if trade secrecy can be re-established and made viable. The RBV and DC approaches are thus interlinked and constitute a cohesive method to trade secrecy management.

3. Method

To capture relevant studies, grasp their subjects and review findings, the PRISMA approach (Moher et al., 2009) was used in this study. To synthesize data and concepts the principles of thematic analysis of Tranfield et al (2003) and Gioia et al. (2013) and principles of systematic literature review of Rojon et al (2021) and Kunish et al (2023) were used in this study.

Considering other review studies (Bos et al, 2015, James et al, 2013; Liebeskind, 1997), three search engines (Web of Science, Scopus and Google Scholar) were applied to identify eligible studies We then selected keywords for the search, also based on previous literature reviews and main concepts such as “secret” or “secrecy” and “innovat*” or “knowledge protection” or “appropriability” or “strategy*” (Bos et al, 2015). The related notions of “IP” or “intellectual property” or “trade secre* were also included (Holgersson & Aaboen, 2019) (see Figure 2).

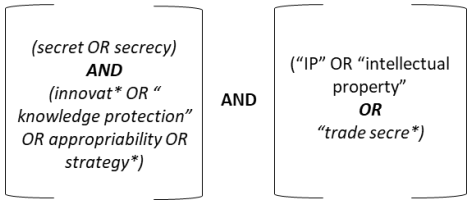


Figure 2. Search Terms

To ensure creation of a manageable set of papers, a number of initial inclusion (and, by definition, exclusion) criteria (supported by referenced previous use) were then applied: (i) the trade secrecy domain spans different areas of research, including business, law and economics. For the purposes of this study, the scope of the literature review and selected studies was limited to the business and management domain, though, if an article from the area of law demonstrates valuable contributions to the research question, it is also included in the pool of selected studies for review (Somaya, 2012); (ii) studies limited to cited works in journals with an impact factor higher than .50 (Bos et al, 2015) (iii) articles limited to empirical research.

These criteria were in line with the PRISMA framework (see Appendix 1). Content examination of title and abstract with subsequent full reading of the selected pool of articles (Pittaway et al., 2004) was then undertaken. During this screening process articles had to include content on one or other of the following criteria to be eligible for the selected pool of studies: 1) Secrecy protection approaches 2) Appropriability mechanisms. Articles examining other appropriability strategies have also been screened and relevant trade secrecy strategy sections of the articles identified and included in the pool (see Figure 3). The quality of the article pool is supported by CABS ranking criteria demonstrated in Table 2. The majority of the publications selected for this study (approximately 75%) possessing 3 or 4* ranking according to the CABS system.

Table 2. CABS ranking of selected articles

CABS Ranking	Quantity	Percentage
4	23	46%
3	14	28%
2	10	20%
1	2	4%
0	1	2%

The approaches to trade secrecy protection and misappropriation mitigation were then identified in the literature by means of systematic literature review in NVIVO, reflected through the conceptual framework based on the RBV of the firm and DC. The identification and tailoring of NVIVO analysis results to the parameters of the RBV and DC theories was derived from the contextual interpretation of research results that initially fit RBV parameters. An additional layer of DC theory interpretation was later identified with the acknowledgement of uncertainties in the environment of the innovating companies implementing trade secrecy. A full overview of the systematic literature review process carried out in this study can be seen in Figure 3.

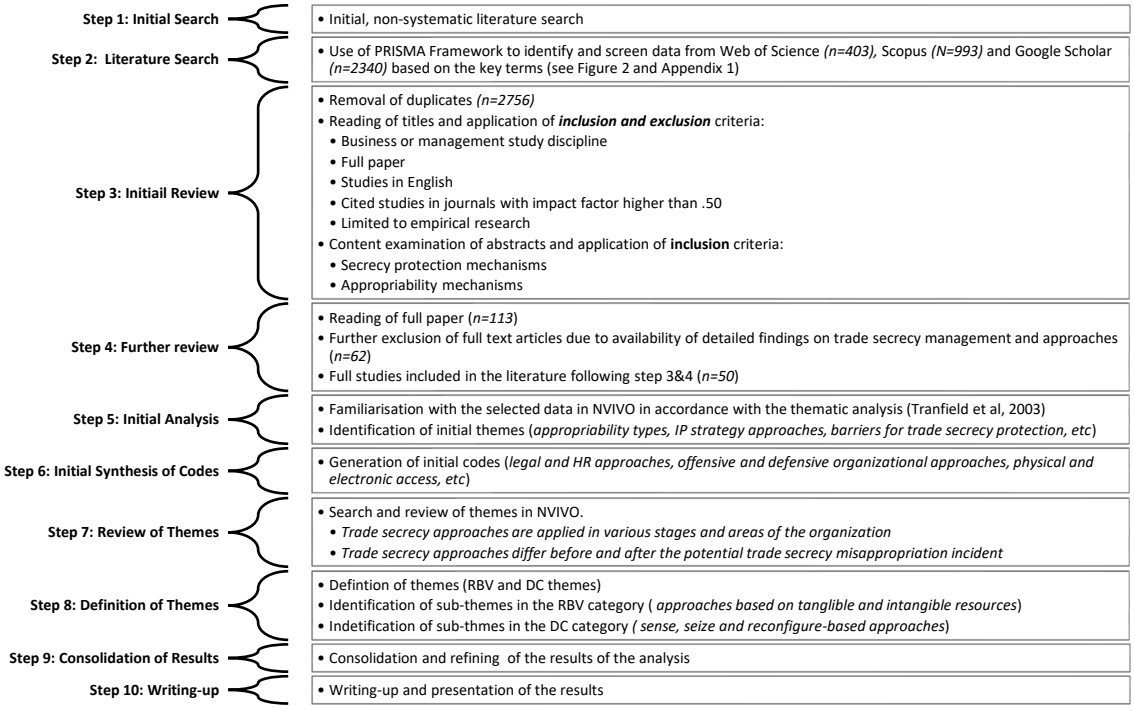


Figure 3. Overview of the SLR process (Adopted from Rojon et al (2021)

Upon completion of all the stages of the thematic analysis, we refined and consolidated the results of the analysis. The presentation of these results is in the following sections.

4. Results

Section 4 represents the findings and provides discussion for each category. First, we provide an overview of the findings (Section 4.1). We then follow with identified trade secrecy strategic approaches within the RBV theoretical framework (Section 4.2) and identified trade secrecy strategic approaches within the DC theoretical framework (Section 4.3.)

4.1. Overview of Findings

Following the conceptual framework and the SLR approach, Figure 4 is designed based on RBV and DC theories. As illustrated, trade secrecy approaches can be managed in an integrated two-fold fashion where the RBV identified approaches flow into the DC approaches in a loop throughout the lifetime of the trade secret. The first element of the mechanism is supported by

the premise of the protection of the most valuable resources as part of the RBV, the second element being the ability to respond to environmental changes, sensing and preventing threats to existing trade secrets and mitigating breach or loss of trade secrets.

The start of a trade secret signals the beginning of the implementation of RBV protection approaches. The approaches remain within the RBV protection umbrella unless there is a change in the environment. Such circumstance lead organizations to re-consider their protection approaches. Re-consideration leads to reconfigured protection approaches and a potential for a new trade secret or reinforcement of the existing trade secret using RBV approaches, whereas failure to react to the change in circumstances can lead to the loss of the trade secret overall.

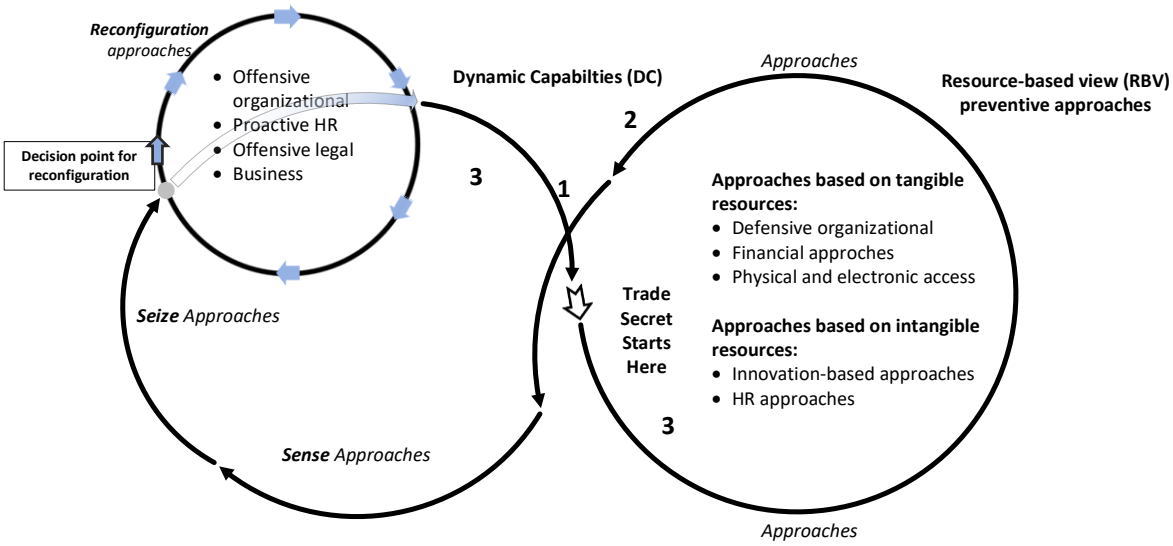


Figure 4. Enhanced Theoretical Framework: Theoretical underpinning of trade secrecy approaches

Figure 4 also demonstrates that a potential disclosure occurrence is a trigger point to re-evaluate the applied measures and move to DC trade secrecy safeguarding approaches. Specifically, once there is an evident threat of trade secrecy breach or an actual occurrence of trade secrecy misappropriation, there are three potential outcomes. These outcomes are specified in Figure 4 with corresponding numbers for each situation, as following:

1. The company loses its trade secret and its competitive advantage. The loop of trade secrecy approaches closes and diminishes.
2. The company loses the trade secret and reconfigures its business to focus on other operations. The loop of trade secrecy approaches closes and diminishes.
3. The company acknowledges the threat or a loss of trade secret after sensing environmental changes; seizes the opportunity and reconfigures its safeguarding approaches with an existing trade secret in mind (decision point for reconfiguration). This scenario puts the company back into the loop of (reconfigured) RBV approaches.

Both RBV and DC protection approaches have been identified as having an array of options. Figure 5 then demonstrates the strategic approaches utilized by the companies for trade secrecy protection under the RBV framework. The RBV approaches include two subcategories based on the type of the resources the company is in possession of in relation to trade secret management. These resource-based sub-categories includes a total of additional 15 sub-sub-categories that characterize approaches companies may undertake to safeguard their trade secrets.

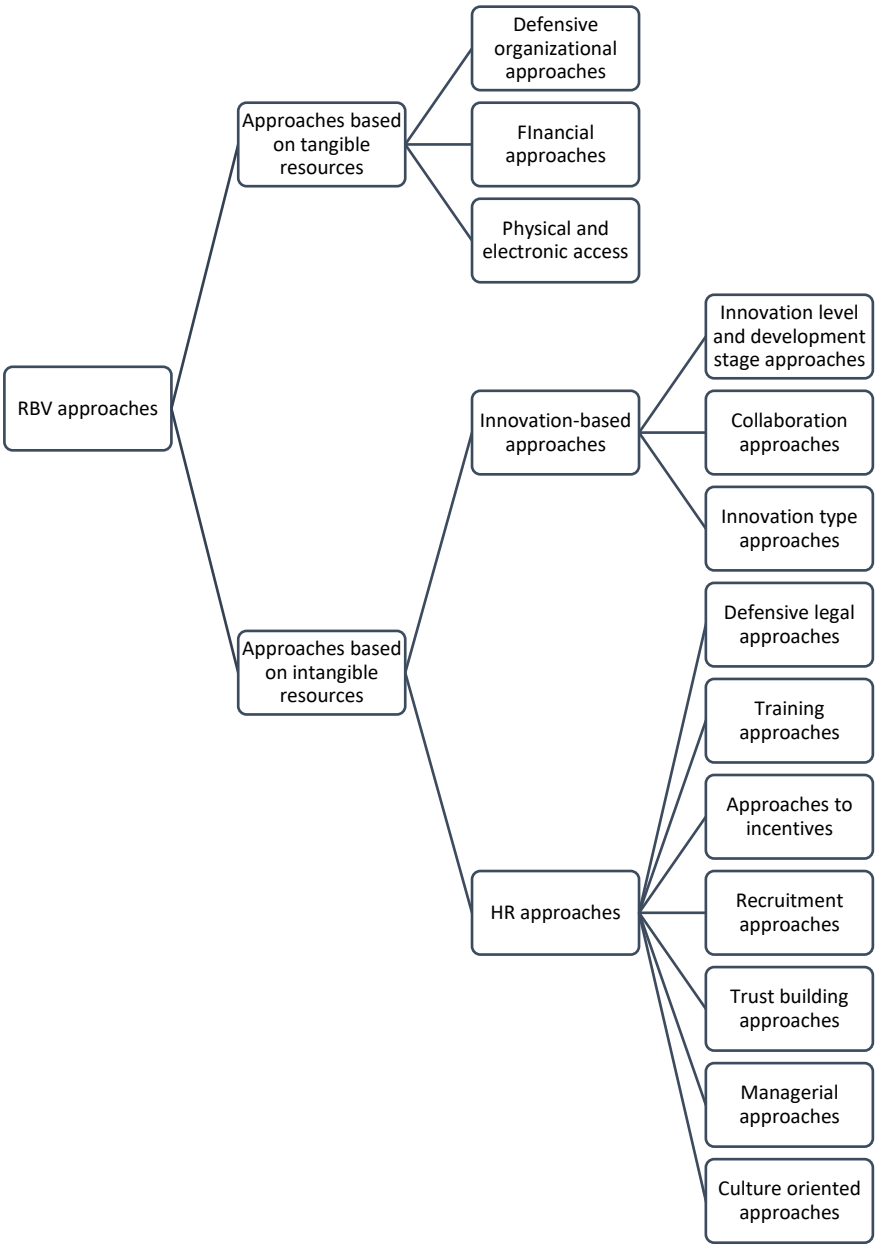


Figure 5. Identified RBV strategic approaches

Figure 6, in turn, embodies the identified strategic approaches applied by companies under the DC framework for both trade secrecy safeguarding and mitigation of threats or breaches. The DC framework includes three subcategories of trade secrecy approaches that are resonant to the DC framework elements: sense, seize and reconfigure. The reconfiguration section also includes four sub-categories of approaches identified in the literature. We now consider each of these categories of identified approaches in detail and in relation to one another.

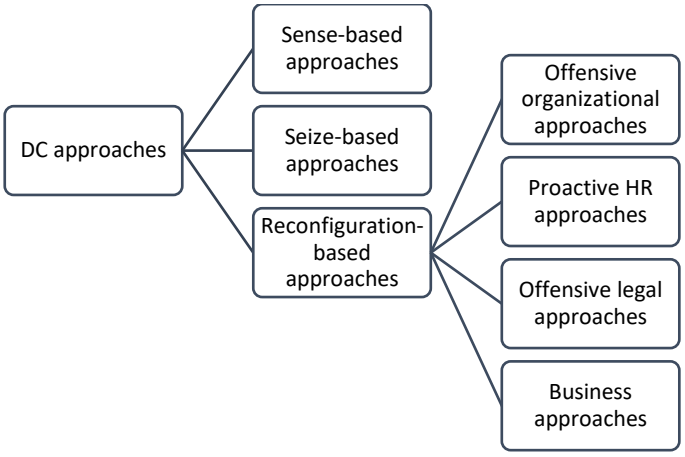


Figure 6. Identified DC strategic approaches

4.2. Resource-based view strategic approaches

Table 3 below demonstrates the map of categories of trade secrecy approaches under the RBV umbrella that companies undertake to safeguard their trade secrets. Considering the conceptual framework of the study these approaches were divided into two categories: i) approaches based on tangible and ii) intangible resources of the firm. Trade secrecy approaches derived from tangible resources are physical access to information, organizational and financial approaches. Approaches derived from intangible resources, conversely, are focused on measures taken through innovation and HR processes within the company.

Our analysis uncovered that out of the vast array of the strategic trade secrecy approaches most attention is given to approaches derived from intangible resources of the firm. In this instance, HR approaches are the most prominent. Whilst they represent a selection of strategic choices, however, there is an evident lack of overall synergy. The approaches are therefore examined as independent phenomena within the innovative organizations with intellectual property.

Table 3. RBV approaches

Main RBV category	Description	Sub-categories	Identified approaches	References
Approaches based on tangible resources	Trade secrecy approaches based on tangible resources are concentrated on strengthening physical and electronic access controls to confidential information within the company; maintaining management and financial capacity for trade secrecy management.	Defensive organizational approaches	*Formal control systems; integrated management information systems; policy and administrative measures within organization; labelling of information 'confidential'; etc.*	Delerue (2010); Collombelli (2020); Elliot (2019); Gama (2019); Manzini and Lazarotti (2016); Solli-Saether et al (2015); McConnahie (1997)
		Financial approaches	*Financial policy instruments; maintenance of unused debt capacity; continuous evaluation of IP asset value; etc.*	Basuchoudhary et Searle (2019); Collombelli (2020); Fredendal et al (2016); McConnahie (1997); Klasa et al (2018);
		Physical and electronic access	*Secure access check points; access to key personnel only; avoidance of written documentation flow; etc.*	Collombelli (2020); Delerue (2010); Elliot (2019); Gallie (2012); Gama (2019); Hannah (2007); Hemphill (2004); Keupp (2010); Sofka et al (2019); Olander (2015)
Approaches based on intangible resources	Trade secrecy strategic approaches based on intangible resources are concentrated around innovation and HR activities of the company. Innovation-based approaches focus on trade secrecy safeguarding during different stages of the innovative process (from ideation to commercialization); innovation level (incremental, disruptive, etc); innovation type (product, process, service) and trade secrecy approaches in	Innovation-based approaches	*Bundles of different IP protection mechanisms (trade secrecy and patenting); trade secrecy, lead time and customer relationship management; localization of information to mother company; trust building, trust leveraging and reciprocity; balance of information sharing; strategic openness; strategic withholding; strategic delaying; knowledge fragmentation;*	de Farla and Sofka (2010); Delerue (2010); McConnahie (1997); Seo et al (2014); Collombelli (2020); Elliot (2019); Gallie (2012); Gama (2019); Hannah (2007); Hemphill (2004); Keupp (2010); Sofka et al (2019); Olander (2015); Zobel et al (2017); Thoma and Bizer (2013); Arundel (2001); Manzini and Lazarotti (2016); Capponi et al (2019); Nelson (2016); McAdam and Marlow (2007), Crass et al (2019);Amara

collaborative processes.			(2008); Crass (2009); Quan and Chesbrough (2009); Hussinger (2006); Lu (2007); Nelson (2016); Leiponen and Byma (2009);
HR trade secrecy strategic approaches are defensive organizational measures that focus on ensuring trade secrecy safeguarding in all areas of HR operations: from recruitment to employment termination. Such measures are recruitment process trade secrecy safeguarding approaches; trust building; employee training; approaches around incentives; managerial approaches; organizational culture-oriented approaches and legal measures.	HR approaches	*Employee willingness, commitment and trustworthiness assessment; employee loyalty and relational contracts; trust building; pecuniary and non-pecuniary incentives (equity-based compensation, ownership participation schemes, long-term compensation packages); deferred rewards; sense of autonomy; social projects involvement; on-the job proactive training techniques (awareness training, hands-on training, informal conversations); formal and frequent reminders; effective management and interpersonal relationships with employees and suppliers; limitation or increase of employee social interaction; legal contracting (confidentiality clauses, non-disclosure agreements, non-compete and assignment agreements).*	Barros (2021); Basuchoudhary and Searle (2019); Contigiani et al (2016); du Zubielqui et al (2016); Elliot et al (2019); Flammer and Kacperczyk (2019); Gallie – Legros (2012); Gonzalez-Alvarez and Nieto- Antolin (2007); Hannah (2007); Keupp (2010); Keupp (2009); Lu (2007); Manzini and Lazzarotti (2015); Marx (2011); Sofka et al (2018); Zobel et al (2017); Delerue and Lejeune (2010); Delerue and Lejeune (2011); Klasa et al (2018); Olander and Hurmelinna-Laukkanen (2015); Hannah (2007); McConnahie (1997); Nelson (2016); Damij et al (2022); Quan and Chesbrough (2009); Hemphill (2004); Collombelli (2020); Solli-Saether et al (2015); Teece (2000); deFaria and Sofka (2010); Amara et al (2008); Fredendall et al (2016); Gans et al (2017); Glaeser (2018); Gonzalez-Alvarez and Nieto-Antolin (2007); Kitchin and Balckburn (1998); Molok et al (2018););

Hussain and
Terziovski (2015);

4.2.1. Approaches based on tangible resources

The first layer of mechanisms within the RBV umbrella identified in the literature are physical and electronic access to trade secrets or confidential information; defensive organizational approaches in managing valuable information and firm's financial approaches with regards to trade secrecy and its safeguarding.

Physical or electronic access to a company's valuable resources pose a great risk to the protection of existing or developing intellectual property. Collombelli (2020) argues effective 'resource-position barriers' are key to appropriation of returns as a result of innovative activity. In this instance, a number of other authors (Hemphill,2004; Hannah, 2007; Sofka 2019; Delerue,2010; Olander (2015)) also claim that secure physical and electronic access check points need to be imposed on research and development (R&D) facilities where trade secrets are mostly concentrated and access granted only to key personnel (Keupp, 2010; Sofka, 2019). Many authors argue for *avoidance of written documentation flow*. (Keupp, 2010; Gama, 2019; Hemphill, 2004). Hempill (2004) and Elliot (2019) support centralized encrypted cyber security protocols where network and communication are limited to employees based on their areas of involvement and security clearance.

Another category of identified approaches based on tangible resources are *defensive organizational approaches*. These establish formal control systems and integrated management information systems including: policy and administrative measures (Barney, 1991). Elliot (2019) and Solli- Saether et al (2015) argue for the establishment of effective IT infrastructure, alignment of procedural protocols and information flow control during the R&D process. Manzini and Lazarotti (2016) and Hemphill (2004) underline the need for labelling sensitive documentation with 'confidential' or 'non-disclosure' specifications.

Finally, financial policy instruments are a prerequisite for application of formal and informal IP protection methods (Collombelli, 2020). Often, firms struggle with identifying the correct amount of finance required for trade secrecy protection (Basuchoudhary and Searle, 2019), another approach against trade secrecy exploitation by rivals, being the *maintenance of unused debt capacity* (insurance pot) (Klasa et al, 2018; Macconahie, 1997).

4.2.2. Approaches based on intangible resources

RBV stipulates that intangible resources are another of the key elements that provide the basis for strategic planning to sustain competitive advantage (Porter 1981, 1996; Hussain & Terziovski, 2016). Specific application of intangible capabilities by an organization to protect its trade secrets or other IP rights, however, also constitutes a trade secrecy protection mechanism. Approaches derived from intangible capabilities have been identified in innovation-specific processes and HR mechanisms (see Table 3).

Innovation-based approaches:

Innovation-related approaches of trade secrecy protection identified in academic literature are related to those activities carried out by an organization with a trade secret as its most valuable asset. Trade secrecy has been identified as an effective protection mechanism for both *service and product innovation* (Amara, 2018), Amara (2018) identifying four approaches, one of which combines secrecy, lead-time advantages and customer relationship management to protect the innovation of service firms. Hussinger (2006) and Amara (2018) also confirms companies tend to bundle different IP mechanisms based on size of firm and R&D innovation. In this instance companies with shorter product life cycles chose a combination of lead time and trade secrets (Thoma and Bizer, 2013).

Trade secrecy appears to be more effective in *process innovations* (Crass, 2019; Gallie, 2012; Hussinger, 2006; Leiponen ad Byma, 2009). In Keupp (2010) the studied company refrains from revealing packaging technology and specifications. The way to maintain this was keeping

the valuable information localized to the mother company and training subsidiary staff in the main facility (Quan and Chesbrough, 2009).

To continue, *development stages of innovation* also often impact the choice of IP protection mechanisms. In the pre-market innovation development stage firms often chose to rely on trade secrecy to avoid early disclosure of information (Hemphill, 2004; Gallie, 2012; Delerue ,2010; Collombelli, 2020; Thoma and Bizer, 2013; Arundel, 2001; Seo et al, 2015). Movement of the innovation to the *commercialization stage*, conversely, is usually associated with implementation of a patent or another, informal, IP mechanism (Arundel, 2004; Thoma and Bizer, 2013), such as a non-disclosure agreement (NDA) (Manzini and Lazarotti,2016), the form and stage of innovation market development a factor weighing on whether or not the company proceeds with trade secrecy (Arundel, 2004; Thoma and Bizer, 2013).

Another identified category of approaches in this section is focused around *collaboration,* de Faria and Sofka (2010) arguing reciprocity as an effective approach establishing trust between partners easing information flow. When collaborating with such business partners firms tend to follow strategic openness (Crass et al, 2019). Contrary to reciprocity and openness, however, Nelson (2016) argues for strategic withholding by academia in the early stages of commercial dealings. McAdam and Marlow (2007) also identify hostility and guarded atmosphere in collaboration between entrepreneurs. Finding the right balance of information sharing can also therefore contribute to the success of a collaboration project (Nelson, 2016).

HR approaches:

According to the systematic literature analysis, HR mechanisms constitute a major part of overall available trade secrecy protection mechanisms. Among the subcategories are trust building, managerial, training and recruitment, approaches concerning incentives and defensive legal approaches.

Implementation of trade secrecy protection within an organization, for example, requires significant *employee loyalty and trust building* (Gallié & Legros, 2012). Hannah (2007) argues employees are more likely to safeguard confidential information if put into positions of trust, Elliot et al (2019) extending into the importance of 'relational contracts', whilst Du Zubielqui et al (2016) find building trust complementary to legal contracting. Therefore, establishment of effective HR strategies for employee retention and maintenance of organizational justice can significantly increase trustworthy security practices within the organization (Flammer & Kacperczyk, 2019; Gallié & Legros, 2012), Such trust building also extends beyond employees of the company, to partners, suppliers and consumers, negating the need for legal IP protection mechanisms (Kitching & Blackburn, 1998).

For this reason, incentives have been identified as a vital category of HR approaches. *Incentive approaches* can be divided into pecuniary and non-pecuniary approaches, performance and equity-based compensation providing a sense of belonging to the company (Teece, 2000). Elliot et al (2019) and Olander and Hurmelinna- Laukkanen (2015) argue shared ownership, employee participation, schemes, deferred rewards and long-term compensation packages are very effective in confidential information safeguarding. Non-pecuniary incentives have also been effective with knowledge workers. According to Flammer and Kacperczyk (2019) providing a sense of autonomy in the choice of the next project can outweigh financial incentives for a knowledge worker. Additionally, delegation of decision-making, ongoing training and involvement of employees in social projects are also a part of IP protection approaches (Gallié & Legros, 2012). *On-the job training* the increases use of trade secrecy and establishes social norms of behaviour with regards to organizational security (Elliot et al, 2019; Gallie&Legros, 2012; Olander & Hurmelinna-Laukkanen, 2015), consequently supporting IP rights.

Culture is another defining factor of trade secrecy safeguarding under HR approaches. In his study, Liebeskind (1997) noted cultural conditions of collectivism and individualism possess the capacity to influence norms of behaviour and attitude towards information seeking and disclosure. Both masculine and assertive cultures are examples of lower levels of cooperation and knowledge sharing. Therefore, Delerue and Lejeune (2011) argue assertive cultures with individualist societies are more efficient in trade secrecy management and protection. Depending on the cultural belonging of the employee it might be necessary to limit social interaction of certain employees to avoid trade secrecy disclosure (Delerue, H.& Lejeune, 2011).

Finally, defensive, legal approaches, include NDA's, confidentiality clauses, assignment and non-compete agreements (NCAs) limit the employee from interacting with the company's trade secret unless it is required for their employment (Hannah, 2007; Lu, 2007); Marx, 2011). This restricts mobility of key employees, representing an essential mechanism of trade secrecy protection (Gallié & Legros, 2012) enacted via compensation and high pay (Delerue & Lejeune, 2010).

4.3. Dynamic capability-based trade secrecy approaches

The identified DC based approaches to trade secrecy (see Table 4) align with the three stages of DC: sensing, seizing and reconfiguring. The sensing section of the study is focused on identifying trade secrecy approaches in the literature demonstrating company awareness of environmental changes or threats to trade secrecy, the actions following relatable to seizing opportunities, implementing measures resulting from environmental changes (Teece, 1997) Finally, the reconfiguration section reveals approaches taken by companies as a final step after the threat to trade secrecy or an actual trade secrecy breach.

Informed by our conceptual framework, our analysis revealed that the lower number of trade secrecy measures as compared to the RBV approaches is explained by a smaller number of

studies available that pursue the subject of trade secret misappropriation in innovating companies; and the more limited number of identified measures that are present in the literature to react to the changes in the business environment. The most prominent of DC categories is a reconfiguration stage where companies respond to theft or misappropriation of a trade secret post factum. This, in turn, emphasizes the lack of organisational monitoring of potential threats to trade secrecy theft/misappropriation and poor selection of preventive strategies.

Table 4. DC approaches

Main DC category	Description	Sub-category	Identified approaches	Referenced studies
Sense-based approaches	The sense-based trade secrecy approaches are concentrated on organizational capacity to monitoring of environmental changes. This process constitutes a continuous evaluation of threats and opportunities to company's IP and/or trade secret.		*Investment in R&D; collaborative activities; interfirm secrecy; auditing of intellectual property assets; evaluation of operation costs against trade secrecy protection costs; binding legal contracts with customers, suppliers, etc (definition of jurisdiction).*	Klasa et al (2018); Flammer and Kacperczyk (2019); Contigiani et al (2018); Hussain and Terziovski (2016); Keisner et al (2016); Miric et al (2019); Kitching and Blackburn (1998) Elliot et al (2019); Hemphill (2004); McConnahie (1997); Castellaneta and Conti (2017); Olander and Hurmelina-Laukkanen (2015); Hussain and Terziovski (2016); Fredendall et al (2016); Nelson (2016); Soli-Saether et al (2015); Gama (2019);
Seize-based approaches	The seize-based trade secrecy approaches are concerned with functioning company measures to respond to trade secrecy threats or opportunities. These include continuous R&D and awareness training.		*R&D with continuous IP monitoring; continuation of IP auditing; use of complementary assets (lead time, complexity of design, technical actions etc.); exclusivity; continuous monitoring of HR practices.*	Amara et al (2008); Delerue (2010); Hentonnen et al (2015); Soli-Saether et al (2015); Sternitzke (2017); Nelson (2016); de Faria and Sofka (2010); Elliot et al (2019); Zobel et al (2017) Hannah (2007); Keupp et al (2010); McConnahie, 1997; McAdam and Marlow, 2007; Manzini and Lazzarotti (2015); Basuchoudhary and Searle (2020);

Reconfiguration -based approaches	The reconfiguration trade secrecy approaches are the measures of the company in response to trade secrecy breach or misappropriation. They possess an offensive and proactive character due to the urgency of the company's response.	Offensive organizational approaches Proactive HR mechanisms Offensive legal approaches Business approaches	*Strengthening of security measures; re-evaluation of access to key company premises and resources; increase of organizational corporate social responsibility engagement; severe misconduct policies; disciplinary action; HR monitoring system; cease-and desist legal mechanisms; litigation (injunction, compensation); proactive poaching; social sanctions; reconfiguration of business operations (increased advertising, new R&D, hiring, increase of capital investment); etc.*	Sofka et al (2018); Neuhausler (2012); Olander and Hurmelinna-Laukkanen (2015); Flammer and Kacperczyk (2019); Elliot et al (2019); Hemphill (2004); Hannah (2007); Marx (2011); Keupp et al (2010); Naqshbandi and Kaur (2015); Thoma and Bizer (2013); Zhao (2019); Gallie and Legros (2012); Delerue and Lejeune (2010); Neuhausler (2012); Contigiani et al (2017); Hannah (2007); Castellaneta et al (2017); Kitching and Blackburn (1998); Klasa et al (2018); Hentonnen et al (2016);

4.3.1. Sense-based approaches

According to Teece (2007), to recognize emerging opportunities, companies must invest in research activities to continuously search for new customer needs, technological opportunities or changes in demand or competitor's behaviour (Teece, 2007). In the case of trade secrecy, the identified approaches are in response to environmental changes and possibilities that can potentially endanger trade secrecy protection.

The main difference between the innovation-related mechanisms in RBV and sense approaches in the DC section lies in the overall approach to innovation. Sensing potential changes in the environment that may create a new business opportunity or threat to their trade secret may affect a company's choice of trade secrecy protection. Of course, the accepted innovation-related mechanisms of RBV are still applicable, such as limiting information flows between client and organization (Elliot et al, 2019), strategic withholding and delayed sharing (Nelson, 2016; Soli-Saether et al; 2015). However, Gama (2019) also argues that when there is a threat of undefined IP strategies between collaborating parties' interfirm secrecy is an applied

concept. In this instance, proprietary knowledge remains confidential between collaborating partners and is stipulated to the external market when it is convenient to them (Gama, 2019).

Going back to the original step of "sense" as part of the DC view, continuous auditing of new and existing intellectual assets defines the future line and direction of the company's research and development (McConnahie, 1997). A company looking to protect its current trade secrets from potential infringement or profit from new opportunities must stay on top of internal processes and continuously evaluate the cost of operations against maintenance of trade secrecy protection (Hemphill, 2004). With that in mind, organizations focused on trade secrecy may choose to define their legal rights under their relevant jurisdiction following initial limitation of information flows (Keisner et al., 2016; Miric et al., 2019), NCAs and NDAs also supporting trade secrecy protection in new opportunity discovery (Contigiani et al., 2018; Kitching & Blackburn, 1998; Hussain & Terziovski, 2016).

4.3.2. Seize-based approaches

There are few trade secrecy mechanisms identified in the literature that constitute a seize approach according to DC theory. Instead complementing continuous auditing of current and new IP assets in the 'sense' stage (McConnahie, 1997), are lead-time advantages and complexity of design (Amara et al., 2008; Sternitzke, 2017) to provides enough time for trade secrecy holders to appropriate R&D outcomes (Keupp et al, 2010; Naqshbandi and Kaur, 2015; Thoma and Bizer, 2013; Zhao, 2019).

That being said, continuous organizational R&D requires a certain level of technological competence. According to de Faria and Sofka (2010) the technological level of the collaborating organization sets the standard for knowledge protection strategies. If the environment is low-technology, broader strategies are applied, but if the environment presents high-tech aspects a more precise and narrower approach is applied to trade secrecy and other

IP assets, exclusivity being one of the narrower strategies for effective knowledge assets control applied during the R&D process (Hentonnen et al, 2015)

In addition to continuous monitoring of R&D processes, Delerue (2010) and Elliot et al (2019) argue for the continuous monitoring of organizational human resource practices. Awareness training is one of the approaches identified for trade secrecy safeguarding during R&D processes (Teece, 2007). In this instance, Hannah (2007) argues that training provides employees with an understanding of what exactly constitutes a trade secret and a capacity to maintain its safety when the need arises during the innovation process (Hannah, 2007). Damij et al (2022) have also uncovered that identification of the most relevant skill sets in employees through continuous evaluation and training stimulates more informed HR decisions and better exploitation of IP.

4.3.3. Reconfiguration-based approaches

In this study, trade secrets are key organizational assets or are affected by other key organizational resources requiring reconfiguration. The review of the selected literature identified approaches as offensive organizational, offensive legal, proactive HR and business.

Offensive organizational approaches:

Organizational approaches to trade secrecy endangering or misappropriation are focused on strengthening of routine security measures. One key organizational approach to the threat of trade secrecy misappropriation is re-evaluation of access to key company premises and resources (personnel, databases and laboratories) (Sofka et al., 2018; Maurer and Zugelder, 2000). Such continuous assessment is a necessity for an innovative organization where knowledge is dynamically changing (Neuhäusler, 2012).

Some firms choose to tackle the threat of trade secret misappropriation through increasing organizational corporate social responsibility (CSR) engagement. According to Flammer and

Kacperczyk (2019), increased organizational focus on CSR mitigates employee mobility and improves employees' propensity to disclose information if they do decide to join the rival firm. However, if the security breach does occur the responsible individual is likely to compromise both their terms of existing employment and future opportunities of employment in similar organizations (Elliot et al, 2019).

Proactive HR approaches:

Proactive HR policies mitigating knowledge misappropriation reinforce organizational efforts of trade secrecy and confidential knowledge safeguarding. According to Elliot et al (2019), when Google experiences information leaks it tracks down the source of the leak. If the source of the leak is Google's own employee, Google applies its own severe misconduct penalties and the employee is usually fired (Elliot et al, 2019). Hemphill (2004) agrees abuse of trade secret information by an employee must be met with severe disciplinary action and if the employee is let go, reminded of their continuing responsibility to not disclose such confidential information. However, despite cease-and-desist legal mechanisms, some former employees will choose to ignore threats of litigation and joined the competitor company regardless (Marx, 2011), continuous monitoring of employee behaviour, assessment of trustworthiness and reward systems for trustworthy conduct diminishing this threat of trade secret misappropriation (Olander and Hurmelinna – Laukkanen, 2015).

In instances when the employee is let go for a different reason, Hannah (2007) argues for exercising caution. According to Hannah (2007) the organization with a trade secret needs to reassure the employee with previous access to confidential information that they are not let go abruptly on unfavourable terms. Maurer and Zugelder (2000) also recommend conducting exit interviews.

A more aggressive approach to maintain competitive advantage is “proactive poaching” (Klasa et al, 2018). Stronger and financially stable companies poach rival’s employees in order to disclose their trade secrets and weaken the rival’s market position (Castellaneta and Conti, 2017). Finally, in cultures where personal networks are highly valued (e.g.China) social sanctions are another trade secrecy breach mitigation approach, fear of loss of personal relationships pushing employees to abstain from untrustworthy behaviour with regards to confidential information (Keupp et al, 2010).

Offensive legal approaches:

Kitching and Blackburn (1998) argue adoption of informal IP rights, such as trade secrecy entails a restriction of possibility to resort to law in the case of breach. However, in instances where trade secrecy breach is inevitable or has already occurred there are legal mechanisms potentially providing a company with compensation for losses incurred following information disclosure (Castellaneta et al; 2017). Among remedies available to the injured party are injunctive relief (obligation to avoid or conduct a certain behaviour), monetary penalties and occasionally imprisonment (Castellaneta et al, 2017; Elliot et al 2019; Hemphill, 2004; Contigiani et al; 2017). Legal approaches available to mitigate trade secrecy breach or a threat of breach are, however, often limited, mitigating the possibility of breaches of trade secrets ending up in court, requiring the company to demonstrate the presence of such a trade secret (Klasa et al., 2018) and high risk of trade secrecy disclosure when trying to pursue breach litigation (Delerue and Lejeune, 2010).

In instances when legal protection of trade secrecy is no longer possible, some companies choose to pursue patenting. Gallie and Legros (2012) argue if there is a high turnover of key personnel, patenting of the most essential innovations is key to avoiding dissemination of valuable knowledge. Neuhausler (2012) expands further and argues, in addition to a new

patenting strategy after trade secrecy, a company can engage in offensive blockage of competitors from using technology in the same or adjacent areas.

Business approaches:

A change in environment affecting organization's trade secrets and other forms of sensitive information forces the business to not only re-evaluate safeguarding and mitigation mechanisms, but also reconfigure business operations (Teece, 2007; Hemphill, 2004), continuous monitoring and observation of the market key to sustaining competitive advantage (Teece, 2007). According to Klasa et al (2018) companies need to engage in increased advertising, unused debt capacity additional R&D activities, active hiring of personnel, litigation (if inevitable) and increased capital investment (Klasa et al, 2018).

Needless to say, approaches to reconfiguration of business activities vary depending on the types of parties involved, business to business (B2B) activities requiring ongoing monitoring of activities of all business parties (Hemphill, 2004). In collaborating with supplier's contractual protection and trade secrecy measures both need to remain stringent (Henttonen et al., 2016). According to Hentonnen et al (2016), if secrecy protection cannot be reinforced, a company can either continue the collaboration, providing lead time and contractual drafting are sufficient; or consider other forms of cooperation. Conversely, when businesses are cooperating with government (B2G), limited knowledge sharing is the established norm (Keupp et al, 2010)

To conclude, an overview of the identified trade secrecy measures within the DC view umbrella have demonstrated an additional layer of the potential measures that can be utilized by organizations to protect and gain from their trade secrets. Despite the overlapping nature of some of the categories with the RBV view, we have been able to investigate them through the

lens of potential environmental changes and identify additional measures of trade secrecy protection and mitigation of trade secret misappropriation.

5. Conclusions

5.1 Discussion

Our study indicates that there is a range of approaches a company can pursue to protect its trade secrets that together form a system. It is evident the RBV and DC approaches require each other to make the system coherent. RBV approaches are a prerequisite to dynamic trade secrecy management approaches. The consequent navigation of this loop of approaches increases the company's chances of sustaining its trade secrets and, consequently, competitive advantage. The results of this study have also demonstrated that there are common approaches that can be applied under both the RBV and DC umbrella. Among these identified common approaches are:

1. Approaches derived from collaboration and cooperation with different business parties, such as:
    a. Approaches based on trust, such as strategic withholding, delayed sharing (Nelson, 2016) or contractual drafting prior and during the collaborative process (Hentonnen et al, 2016);
2. Approaches derived from HR awareness training (Delerue, 2010; Elliot et al, 2019);
3. Approaches based on organizational security measures and its consequent strengthening (Sofka et al, 2018);
4. Approaches based on financial capabilities and building of unused debt capacity to be able to react to environmental changes swiftly and efficiently (Klase et al, 2018);

5. Legal approaches that are centred around the non-disclosure agreements, the availability of the latter a prerequisite for effective litigation outcomes (Hemphill, 2004; Hannah, 2007).

It is worth noting that the richness of trade secrecy approaches in the proposed theoretical framework does not guarantee the maintenance of trade secret protection. The availability of such a theoretical framework can become a useful tool only if the management of organizations seeking to maintain their trade secrecy protection has the understanding and the capacity to pursue such protection approaches.

5.2 Contributions

This study therefore contributes to the academic literature in several ways. First, we contribute to the studies of Bos et al (2015) and Hannah et al (2019) who identified the trade secrecy management lifecycle but also the need for further research into its latter stages. Specifically, our study goes beyond the premise of a management lifecycle by introducing a categorized framework for trade secrecy management supported by theory (both RBV and DC).

Second, we offer additional insights into the approaches companies undertake to react to leakages and develop further secrets based on the studies of James et al (2013) and Kang and Lee (2022). We also elaborate Liebeskind's (1997) ideas on the introduction of rules, compensation and structural isolation, and set them in a categorized scheme of mechanisms for management of sensitive information by organizations aiming to protect trade secrets. The categories are clustered around organizational, legal and HR capabilities (see Figure 5 and 6), the differences in these approaches underlined by organizational goals and environmental conditions.

Third, we contribute to the broadening of the theoretical underpinnings in the subject area. Our study has demonstrated the limitations of isolated application of only one of the theoretical

foundations. It has been identified that trade secrecy safeguarding approaches can benefit from both RBV and DC theories, which are effective, and can be applied simultaneously as well as sequentially, being both overlapping and complementary with each other.

5.3 Managerial and Policy Implications

This study also suggests important practical implications. For managers, there is a vast amount of choice for managers, with regards to safeguarding their organisation's' existing or new trade secrets throughout the trade secret lifecycle. The research identifies their practical application in various stages, including misappropriation, as indicated in the table below.

Table 5. Trade secrecy approaches and managerial implications

Framework	*Category*	*Key references*	*Managerial Implications*
RBV	Defensive organizational approaches	Solli-Saether et al (2015); Elliot et al (2019); Manzini and Lazarotti (2016);	1. Introduction of internal trade secrecy protection policies. 2. Information flow control and alignment of procedural protocols. 3. Labelling of documentation as "confidential" or "non-disclosure".
	Financial approaches	Basuchoudhary et Searle (2019); Klasa et al (2018);	1. Establishment of financial policy instruments. 2. Maintenance of unused debt capacity for trade secrecy leakage mitigation.
	Physical and electronic access	Gama (2019); Hannah (2007); Sofka (2019); Keupp (2010)	1. Introduction of secure check points in facilities. 2. Access to key personnel only. 3. Encrypted cyber security protocols and avoidance of written documentation.
	Innovation-based approaches	Amara (2018); Hussinger (2016); Thoma and Bizer (2013);	1. Bundle different IP mechanisms for innovative products with shorter life cycles and service industries. 2. Localisation of valuable information to head office only. 3. Use of trade secrecy in pre-market innovation development and strategic withholding in collaboration.
	HR and legal approaches	Elliot et al (2019); du Zubielque et al (2016) Hannah (2007); Maurer and Zugelder (2000)	1. Build employee loyalty and trust. 2. Use of equity-based compensation. 3. On-the job training. 4. Assertive organizational cultures efficient in trade secrecy management. 5. Use explicit non-disclosure and non-compete agreements.
DC	Sense-based approaches	Hemphill (2004); Gama (2019); Klasa et al (2018); Elliot et al (2019).	1. Continuously monitor changes in the environment. 2. Limit information flows (strategic withholding, delayed sharing). 3. Auditing new and existing intellectual assets. 4. Use of confidentiality agreements in the discovery phase of new opportunities.
	Seize-based approaches	Amara et al (2008); Galiie and Legros	1. Continuous R&D activities. 2. Continuous awareness training.

	(2012); Hentonnen et al (2015)	3. Use of complementary approaches such as lead time advantages and complexity of design to safeguard initial stages of trade secrecy development.
Reconfiguration-based approaches	Neuhausler (2012); Olander and Hurmelinna – Laukkanen (2015); Klasa et al (2018);	1. Strengthening routine security measures. 2. Re-evaluation of access to key premises. 3. Continuous employee behaviour monitoring, assessment of trustworthiness and introduction of reward systems for trustworthiness. 4. Start litigation. 5. Increased advertising, active hiring, increased capital investment, etc.

Policy implications, by way of contrast, are focused around three areas:

1. Development of policy guidance in trade secrecy implementation and overall trade secrecy management for innovating organizations, especially SMEs.
2. Increasing awareness in trade secrecy as a robust mechanism of IP protection. Trade secrecy awareness is generally limited to limitations of confidential information access.
3. Understanding that trade secrecy is a complex process of IP management. It is, therefore, essential to consider trade secrets in their scope of applicability that is independent of the patenting system.

5.4 Limitations and Future Research

Based on our results following the SLR approach, we identified limitations in the trade secrecy literature which suggest future focus for such empirical research. First, the establishment of the categorized approaches to trade secrecy protection in this study allows room for future research on the development of a unified framework of approaches to trade secrecy protection that includes both theoretical and practical approaches and the establishment of a comprehensive process of trade secrecy management. The latter would possess practical implications for companies that are looking for guidance on how to navigate the protection of their trade secrets. Hence, scholars can focus on studies to provide a comprehensive process of trade secrecy management.

Secondly, the presence and richness of literature in the RBV results section demonstrates that more research is needed in exploring ways of mitigating the consequences of trade secret misappropriation. The categorization of approaches under the DC section has demonstrated that there is limited research in understanding the approaches the companies can apply after the breach of a trade secret, recovering of losses from it or reconfiguring business operations as a result of trade secrecy misappropriation. Accordingly, future studies can focus on investigating mitigation approaches organizations pursue post trade secrecy misappropriation.

Third, there is a gap with regards to the identified approaches and their impact on strategy building and innovation and vice versa. More precisely, how can a company utilise the identified trade secrecy approaches in the most efficient manner? More research is also needed in identifying and developing trade secrecy protection approaches under different contextual variables: industries, countries, cultures, organization sizes, etc. Hence, future studies can focus on the efficiency of trade secrecy protection approaches and their implementation in various settings (contexts and sectors).

Fourth, we have been able to pinpoint that there is a lack of synergy between HR departments of innovating companies and trade secrecy protection approaches. Some of the discussed approaches in the literature (Gallié and Legros, 2012; Delerue and Lejeune, 2011; Hannah, 2007, etc) are usually independent of other business processes. The overall understanding and acknowledgement of all these strategic synergies proves to be paramount for innovating companies working with trade secrecy. Also, there is a lack of attention to practical approaches of physical limitations and unused debt capacity for innovating companies that want to protect their trade secrets. Accordingly, it would be beneficial to explore alignment of trade secrecy approaches and business processes in the organizational context. As well as, investigation of the reasons behind the lack of awareness around practical trade secrecy approaches.

Fifth, we have identified that trade secrecy protection in collaborative processes can potentially have a negative impact on further innovative activities. Finally, no research has been done in investigating the trigger point of trade secrecy strategy change as a result of loss or spill-over of confidential information. The latter would allow the understanding of the trigger point and the necessity to consider trade secrecy management as a dynamic knowledge management process that needs to be constantly reviewed. Therefore, more research is needed on the investigation of the effects of trade secrecy on collaboration and trigger points of trade secrecy strategy change.

References

Abdul Molok, N. N., Ahmad, A., & Chang, S. (2018). A case analysis of securing organisations against information leakage through online social networking. International Journal of Information Management, 43(September), 351–356.

Almeling, D. S., Snyder, D. W., Sapoznikow, M., & McCollum, W. E. (2010). Statistical Analysis of Trade Secret Litigation in State Courts. Gonz. L. Rev., 46(2009), 57.

Amara, N., Landry, R., & Traoré, N. (2008). Managing the protection of innovations in knowledge-intensive business services. Research Policy, 37(9), 1530–1547.

Arora, A. (1997). Patents, licensing, and market structure in the chemical industry. Research Policy, 26(4–5), 391–403.

Arora, A., Ceccagnoli, M., & Cohen, W. (2000). Intellectual property strategies and the returns to R&D. In PA: The H. John Heinz III School of Public Policy and Management Working Papers Series.

Arundel, A. (2001). The relative effectiveness of patents and secrecy for appropriation. Research Policy, 30(4), 611–624.

Arundel, A., & Kabla, I. (1998). What percentage of innovations are patented? Empirical estimates for European firms. Research Policy, 27(2), 127–141.

Barros, H. M. (2021). Neither at the cutting edge nor in a patent-friendly environment: Appropriating the returns from innovation in a less developed economy. Research Policy, 50(1), 104097.

Basuchoudhary, A., & Searle, N. (2019). Computers & Security Snatched secrets: Cybercrime and trade secrets modelling a firm' s decision to report a theft of trade secrets. Computers & Security, 87.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101.

Bos, B., Broekhuizen, T. L. J., & de Faria, P. (2015). A dynamic view on secrecy management. Journal of Business Research, 68(12), 2619–2627.

Buss, P., & Peukert, C. (2015). R&D outsourcing and intellectual property infringement. Research Policy, 44(4), 977–989.

Capponi, G., Criscuolo, P., Martinelli, A., & Nuvolari, A. (2019). Profiting from innovation: Evidence from a survey of Queen's Awards winners. Structural Change and Economic Dynamics, 49, 155–169.

Castallaneta, F., Conti, R., & Kacperczyk, A. (2017). Money Secrets: How does trade secret legal protection affect firm market value? Evidence from the Uniform Trade Secret Act. Strategic Management Journal, 38, 834–853.

Chen, C., Gu, J., & Luo, R. (2022). Corporate innovation and R&D expenditure disclosures. Technological Forecasting and Social Change, 174, 121230.

Cho, I., Park, H., & Kim, J. K. (2012). The moderating effect of innovation protection mechanisms on the competitiveness of service firms. Service Business, 6(3), 369–386.

Choi, Y., Barden, J. Q., Cho, S. Y., & Arthurs, J. (2019). The Effectiveness of Secrecy As An Appropriation Mechanism Evidence From The Uniform Trade Secrets Act. SSRN Electronic Journal.

Cohen, W. M., Goto, A., Nagata, A., Nelson, R. R., & Walsh, J. P. (2002). R&D spill-overs, patents and the incentives to innovate in Japan and the United States. Research Policy, 31(8–9), 1349–1367.

Cohen, W. M., Nelson, R. R., & Walsh, J. P. (2000). Protecting their intellectual assets: Appropriability conditions and why U.S. manufacturing firms patent (or not). (No. 7552).

Colombelli, A., Grilli, L., Minola, T., & Mrkajic, B. (2020). To what extent do young innovative companies take advantage of policy support to enact innovation appropriation mechanisms? Research Policy, 49(10), 103797.

Contigiani, A., Hsu, D. H., & Barankay, I. (2018). Trade secrets and innovation: Evidence from the "inevitable disclosure" doctrine. Strategic Management Journal, 39(11), 2921–2942.

Contractor, F. J. (2019). Can a firm find the balance between openness and secrecy? Towards a theory of an optimum level of disclosure. Journal of International Business Studies, 50(2), 261–274.

Crittenden, W. F., Crittenden, V. L., & Pierpont, A. (2015). Trade secrets: Managerial guidance for competitive advantage. Business Horizons, 58(6), 607-613.

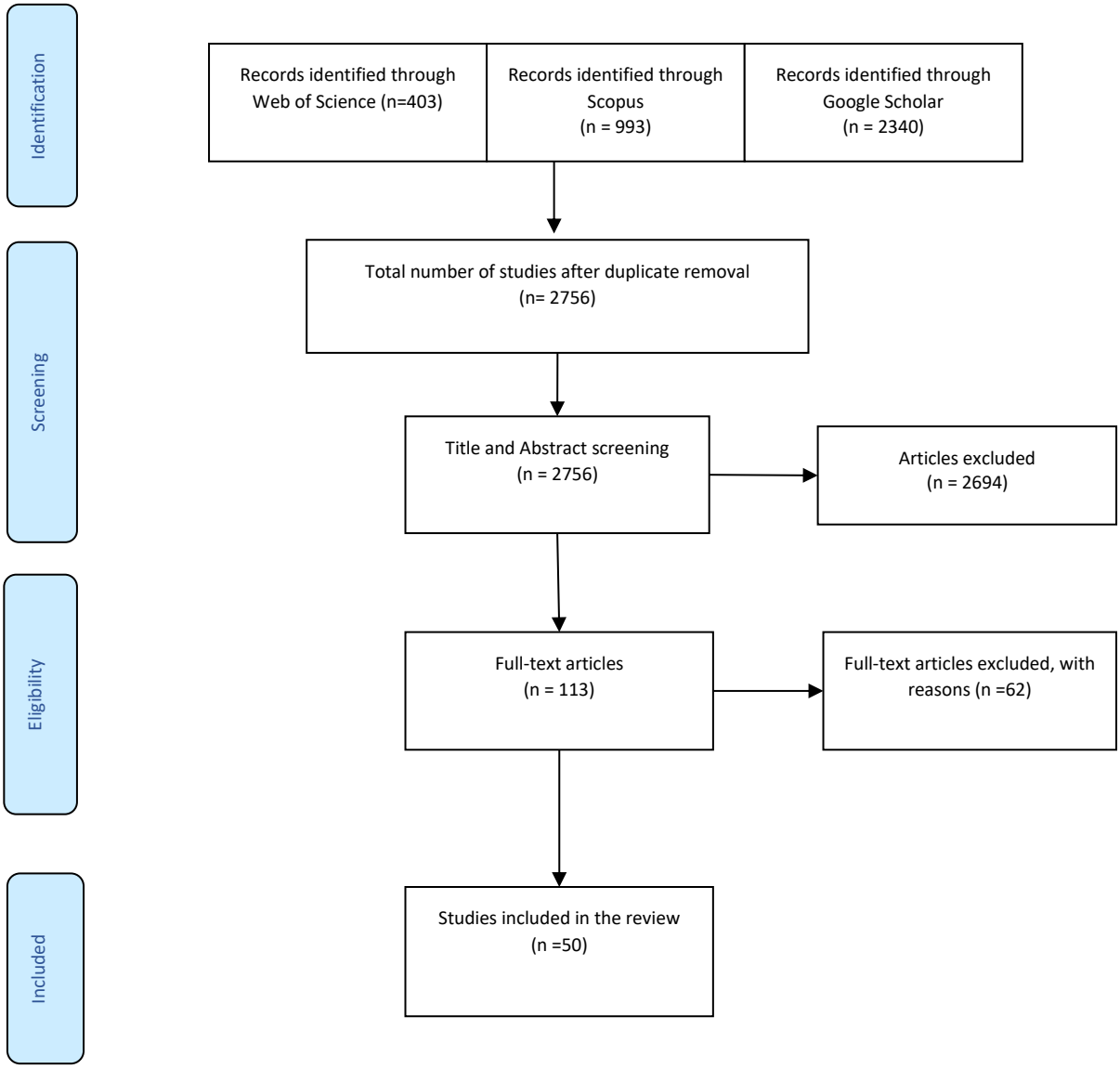
Damij, N., Hafner, A., & Modic, D. (2022). Activity-to-Skills Framework in the Intellectual Property Big Data Era. IEEE Transactions on Engineering Management.
Dass, N., Nanda, V. K., & Xiao, S. C. (2020). Intellectual Property Protection and Financial Markets: Patenting vs. Secrecy. SSRN Electronic Journal 2517838.
de Faria, P., & Sofka, W. (2010). Knowledge protection strategies of multinational firms-A cross-country comparison. Research Policy, 39(7), 956–968.
Delerue, H., & Lejeune, A. (2010). Job mobility restriction mechanisms and appropriability in organizations: The mediating role of secrecy and lead time. Technovation, 30(5–6), 359–366.
Delerue, H., & Lejeune, A. (2011). Managerial secrecy and intellectual asset protection in SMEs: The role of institutional environment. Journal of International Management, 17(2), 130–142.
de Zubielqui, G. C., Jones, J., & Statsenko, L. (2016). Managing innovation networks for knowledge mobility and appropriability: A complexity perspective. Entrepreneurship Research Journal, 6(1), 75-109.
Faria, P. De, & Sofka, W. (2010). Knowledge protection strategies of multinational firms — A cross-country comparison. Research Policy, 39(7), 956–968.
Flammer, C., & Kacperczyk, A. (2019). Corporate social responsibility as a defence against knowledge spill-overs : Evidence from the inevitable disclosure doctrine. Strategic Management Journal, 40(8), 1243–1267.
Fredendall, L. D., Letmathe, P., & Uebe-Emden, N. (2016). Supply chain management practices and intellectual property protection in China: Perceptions of Mittelstand managers. International Journal of Operations and Production Management, 36(2), 135–163.
Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking qualitative rigor in inductive research: Notes on the Gioia methodology. Organizational research methods, 16(1), 15-31.
Gallié, E. P., & Legros, D. (2012). French firms' strategies for protecting their intellectual property. Research Policy, 41(4), 780–794.
Gama, F. (2019). Managing collaborative ideation: the role of formal and informal appropriability mechanisms. International Entrepreneurship and Management Journal, 15(1), 97–118.
Gans, J. S., Murray, F. E., & Stern, S. (2017). Contracting over the disclosure of scientific knowledge: Intellectual property and academic publication. Research Policy, 46(4), 820–835.
Gennari, U. (2013). IPR training and tools for better handling of IPR topics by SMEs. World Patent Information, 35(3), 214–223.
Gimenez-Fernandez, E. M., Ferraris, A., Troise, C., & Sandulli, F. D. (2022). Openness strategies and the success of international entrepreneurship. International Journal of Entrepreneurial Behavior & Research.
Glaeser, S. (2018). The effects of proprietary information on corporate disclosure and transparency: Evidence from trade secrets. Journal of Accounting and Economics, 66(1), 163–193.
Gonzalez-Alvarez, N., & Nieto-antolı, M. (2007). Appropriability of innovation results: An empirical study in Spanish manufacturing firms. Technovation, 27, 280–295.
Graham, S. J. H. (2004). Hiding in the patent's shadow: firms' uses of secrecy to capture value from new discoveries. In GaTech TI: GER Working Paper Series (Issue 6210).
Gross, D. P. (2019). The Consequences of Invention Secrecy: Evidence from the UPSTO Patent Secrecy Program in World War II. In NBER Working Paper Series (No. 25545).
HanGyeol, S., Yanghon, C., Dongphil, C., & Chungwon, W. (2015). Value capture mechanism: R&D productivity comparison of SMEs. Management Decision, 53(2), 318–337.
Hannah, D. R. (2007). An examination of the factors that influence whether newcomers protect or share secrets of their former employers. Journal of Management Studies, 44(4), 465–487.
Hannah, D., Parent, M., Pitt, L., & Berthon, P. (2014). It' s a secret: Marketing value and the denial of availability. Business Horizons, 57(1), 49–59.
Hannah, D., Parent, M., Pitt, L., & Berthon, P. (2019). Secrets and knowledge management strategy: the role of secrecy appropriation mechanisms in realizing value from firm innovations. Journal of Knowledge Management, 23(2), 297-312.
Hemphill, T. (2004). The strategic management of trade secrets in technology-based firms. Technology Analysis & Strategic Management, 16(4), 479-494.
Henttonen, K., Hurmelinna-Laukkanen, P., & Ritala, P. (2016). Managing the appropriability of R&D collaboration. R and D Management, 46, 145–158.
Holgersson, M., & Aaboen, L. (2019). Technology in Society A literature review of intellectual property management in technology transfer offices: From appropriation to utilization. Technology in Society, 59.
Holgersson, M., & Wallin, M. W. (2017). The patent management trichotomy: patenting, publishing, and secrecy. Management Decision, 55(6), 1087–1099.
Hrdy, C. A., & Lemley, M. A. (2021). Abandoning trade secrets. Stan. L. Rev., 73, 1.
Huang, F., Rice, J., Galvin, P., & Martin, N. (2014). Openness and appropriation: Empirical evidence from Australian businesses. IEEE Transactions on Engineering Management, 61(3), 488-498.
Hughes, A., & Mina, A. (2010). The Impact of the Patent System on SMEs. In CBR Research Program on Enterpise and Innovation (No. 411).
Hussain, S., & Terziovski, M. (2016). Intellectual Property Appropriation Strategy and Its Impact on Innovation Performance. International Journal of Innovation Management, 20(2).
Hussinger, K. (2006). Is silence golden? Patents versus secrecy at the firm level. Economics of Innovation and New Technology, 15(8), 735–752.
James, S. D., Leiblein, M. J., & Lu, S. (2013). How Firms Capture Value From Their Innovations. In Journal of Management (Vol. 39, Issue 5).

Kang, H., & Lee, W. (2022). How innovating firms manage knowledge leakage: A natural experiment on the threat of worker departure. Strategic Management Journal, 43(10), 1961-1982.
Keisner, A., Raffo, J., & Wunsch-Vincent, S. (2016). Robotics: Breakthrough technologies, innovation, intellectual property. Foresight and STI Governance, 10(2), 7–27.
Keupp, M. M., Beckenbauer, A., & Gassmann, O. (2009). How managers protect intellectual property rights in China using de facto strategies. R and D Management, 39(2), 211–224.
Keupp, M. M., Beckenbauer, A., & Gassmann, O. (2010). Enforcing intellectual property rights in weak appropriability regimes: The case of de facto protection strategies in China. Management International Review, 50(1), 109–130.
Kitching, J., & Blackburn, R. (1998). Intellectual property management in the small and medium enterprise (SME). Journal of Small Business and Enterprise Development, 5(4), 327–335.
Klasa, S., Ortiz-molina, H., Serfling, M., & Srinivasan, S. (2018). Protection of trade secrets and capital structure decisions. Journal of Financial Economics, 128(2), 266–286.
Kunisch, S., Denyer, D., Bartunek, J. M., Menz, M., & Cardinal, L. B. (2023). Review Research as Scientific Inquiry. Organizational Research Methods, 26(1), 3-45.
Leiponen, A., & Byma, J. (2009). If you cannot block, you better run: Small firms, cooperative innovation, and appropriation strategies. Research Policy, 38(9), 1478–1488.
Lemper, T. A. (2012). The critical role of timing in managing intellectual property. Business Horizons, 55, 339–347.
Levin, R. C., Klevorick, A. K., Nelson, R. R., Winter, S. G., Gilbert, R., Griliches, Z., Levin, R. C., & Nelson, R. R. (1987). Linked references are available on JSTOR for this article: Appropriating the Returns from Industrial Research and Development. Brookings Papers on Economic Activity, 1987(3), 783–831.
Liebeskind, J. P. (1997). Knowledge, Strategy, and the Theory of the Firm. Strategic Management Journal, 17(Winter Special Issue).
Lichtenthaler, U. (2008). Open innovation in practice: an analysis of strategic approaches to technology transactions. IEEE transactions on engineering management, 55(1), 148-157.
Lliott, K. A. E., Atacconi, A. N. P., Wierzbinski, J. O. S., & Illiams, J. U. W. (2019). Knowledge Protection in Firms: A Conceptual Framework and Evidence from HP Labs. European Management Review, 16(1), 179–193.
Lu, L. Y. Y. (2007). Protecting intellectual property rights. Research Technology Management, 50(2), 51–56.
Manzini, R., & Lazzarotti, V. (2016). Intellectual property protection mechanisms in collaborative new product development. R and D Management, 46.
Manzini, R., Lazzarotti, V., & Pellegrini, L. (2012). IP and open innovation: Theory and practice. International Journal of Technology Marketing, 7(2), 119–134.
Marx, M. (2011). The Firm Strikes Back: Non-compete Agreements and the Mobility of Technical Professionals. American Sociological Review, 76(5), 695–712.
McAdam, B. & Marlow, S. (2007). Building futures or Stealing Secrets? Entrepreneurial Cooperation and Conflict within Business Icubators. International Small Business Journal, 25(4), 361–382.
Milesi, D., Petelski, N., & Verre, V. (2013). Innovation and appropriation mechanisms: Evidence from Argentine microdata. Technovation, 33, 78–87.
Miric, M., Boudreau, K. J., & Jeppesen, L. B. (2019). Protecting their digital assets: The use of formal & informal appropriability strategies by App developers. Research Policy, 48(8), 103738.
Moerchel, A., Tietze, F., Aristodemou, L., & Vimalnath, P. (2022). A Novel Method for Visually Mapping Intellectual Property Risks and Uncertainties in Evolving Innovation Ecosystems: A Design Science Research Approach for the COVID-19 Pandemic. IEEE Transactions on Engineering Management.
Monteiro, F., Mol, M., & Birkinshaw, J. (2017). Ready to be Open? Explaining the Firm Level Barriers to Benefiting From Openness to External Knowledge. Long Range Planning, 50(2), 282–295.
Naqshbandi, M. M., & Kaur, S. (2015). Effectiveness of innovation protection mechanisms in Malaysian high-tech sector. Management Research Review, 38(9), 952–969.
Neuhäusler, P. (2012). The use of patents and informal appropriation mechanisms - Differences between sectors and among companies. Technovation, 32(12), 681–693.
Olander, H., & Hurmelinna-Laukkanen, P. (2015). Proactive HRM for reducing knowledge risks-evaluating commitment and trustworthiness. International Journal of Innovation Management, 19(6), 1–20.
Png, I. P. L. (2017). Secrecy and Patents: Evidence from the Uniform Trade Secrets Act. Strategy Science, 2(3), 176–193.
Quan, X., & Chesbrough, H. (2009). Hierarchical segmentation of R&D process and intellectual property protection: Evidence from multinational R&D laboratories in China. IEEE Transactions on Engineering Management, 57(1), 9-21.
Reitzig, M. (2004). Strategic Management of Intellectual Property: An Integrated Approach. MIT Sloan Management Review, 55(4), 157–184.
Reitzig, M., & Puranam, P. (2009). Value appropriation as an organizational capability: The case of IP protection through patents. Strategic Management Journal, 30(7), 765-789.
Ritala, P., Olander, H., Michailova, S., & Husted, K. (2015). Knowledge sharing, knowledge leaking and relative innovation performance: An empirical study. Technovation, 35, 22–31.
Rojon, C., Okupe, A., & McDowall, A. (2021). Utilization and development of systematic reviews in management research: What do we know and where do we go from here?. International Journal of Management Reviews, 23(2), 191-223.
Salzberg, S., Birney, E., Eddy, S., & White, O. (2003). Unrestricted free access works and must continue. Nature, 422(6934), 801–801.
Searle, N. (2021). The Economic and Innovation Impacts of Trade Secrets. UK Intellectual Property Office Research Paper, (2021/01).
Sofka, W., de Faria, P., & Shehu, E. (2018). Protecting knowledge: How legal requirements to reveal information affect the importance of secrecy. Research Policy, 47(3), 558–572.

Solli-Saether, H., Karlsen, J. T., & Oorschot, K. Van. (2015). Strategic and Cultural Misalignment: Knowledge Sharing Barriers in Project Networks. Project Management Journal, 46(3), 49–60.
Sternitzke, C. (2017). Interlocking patent rights and value appropriation: Insights from the Razor Industry. IEEE Transactions on Engineering Management, 64(2), 249-265.
Suzuki, K. (2015). Economic growth under two forms of intellectual property rights protection: patents and trade secrets. Journal of Economics, 115(1), 49-71.
Teece, D. J. (2000). Strategies for Managing Knowledge Assets: The Role of Firm Structure and Industrial Context. Long Range Planning, 33(1), 35–54.
Teixeira, A. A. C., & Ferreira, C. (2019). Intellectual property rights and the competitiveness of academic spin-offs. Journal of Innovation and Knowledge, 4(3), 154–161.
Thomä, J., & Bizer, K. (2013). To protect or not to protect? Modes of appropriability in the small enterprise sector. Research Policy, 42(1), 35–49.
Thumm, N. (2001). Management of Intellectual Property Rights in European Biotechnology Firms. Technological Forecasting and Social Change, 67(2–3), 259–272.
Tietze, F., Vimalnath, P., Aristodemou, L., & Molloy, J. (2020). Crisis-critical intellectual property: findings from the COVID-19 pandemic. IEEE Transactions on Engineering Management.
Toma, A., Secundo, G., & Passiante, G. (2018). Open innovation and intellectual property strategies: Empirical evidence from a bio-pharmaceutical case study. Business Process Management Journal, 24(2), 501–516.
Wajsman, N., & García-Valero, F. (2017). Protecting Innovation through Trade Secrets and Patents: Determinants for European Union Firms. European Union Intellectual Property Office. European Observatory on Infringements of Intellectual Property Rights.
Walsh, J. P., & Huang, H. (2014). Local context, academic entrepreneurship and open science: Publication secrecy and commercial activity among Japanese and US scientists. Research Policy, 43(2), 245–260.
WIPO (2021). WIPO Symposium on Trade Secrets and Innovation. https://www.wipo.int/meetings/en/details.jsp?meeting_id=68890
Zhao, M. (2006). Conducting R&D in countries with weak intellectual property rights protection. Management Science, 52(8), 1185–1199.
Zhao, X. (2019). Patenting or Secret? The Interaction between Leading Firms and Following Firms Based on Evolutionary Game Theory and Multi-Agent Simulation. International Journal of Innovation Management, 23(7), 1–22.
Zobel, A. K., Lokshin, B., & Hagedoorn, J. (2017). Formal and informal appropriation mechanisms: The role of openness and innovativeness. Technovation, 59, 44–54.

Appendices

Appendix 1. Prisma flowchart



Appendix 2. List of selected studies and the inclusion and exclusion criteria

Articles	Year	Impact Factor	Citations	CABS Ranks
Barros, H. M. (2021). Neither at the cutting edge nor in a patent-friendly environment: Appropriating the returns from innovation in a less developed economy. Research Policy, 50(1), 104097.	2021	5.3	1	4
Colombelli, A., Grilli, L., Minola, T., & Mrkajic, B. (2020). To what extent do young innovative companies take advantage of policy support to enact innovation appropriation mechanisms? Research Policy, 49(10), 103797.	2020	5.3	9	4
Basuchoudhary, A., & Searle, N. (2019). Snatched secrets: Cybercrime and trade secrets modelling a firm's decision to report a theft of trade secrets. Computers & Security, 87, 101591.	2019	7.9	5	**0**
Capponi, G., Criscuolo, P., Martinelli, A., & Nuvolari, A. (2019). Profiting from innovation: Evidence from a survey of Queen's Awards winners. Structural Change and Economic Dynamics, 49, 155-169.	2019	2	5	2

Elliott, K., Patacconi, A., Swierzbinski, J., & Williams, J. (2019). Knowledge protection in firms: A Conceptual framework and evidence from HP labs. European Management Review, 16(1), 179-193.	2019	2.2	5	3
Flammer, C., & Kacperczyk, A. (2019). Corporate social responsibility as a defense against knowledge spillovers: Evidence from the inevitable disclosure doctrine. Strategic Management Journal, 40(8), 1243-1267.	2019	5.4	43	4
Gama, F. (2019). Managing collaborative ideation: the role of formal and informal appropriability mechanisms. International Entrepreneurship and Management Journal, 15(1), 97-118.	2019	3.8	9	1
Hannah, D., Parent, M., Pitt, L., & Berthon, P. (2019). Secrets and knowledge management strategy: the role of secrecy appropriation mechanisms in realizing value from firm innovations. Journal of Knowledge Management.	2019	8.6	6	2
Miric, M., Boudreau, K. J., & Jeppesen, L. B. (2019). Protecting their digital assets: The use of formal & informal appropriability strategies by App developers. Research Policy, 48(8), 103738.	2019	5.3	21	4
Contigiani, A., Hsu, D. H., & Barankay, I. (2018). Trade secrets and innovation: Evidence from the "inevitable disclosure" doctrine. Strategic Management Journal, 39(11), 2921-2942.	2018	5.4	34	4
Glaeser, S. (2018). The effects of proprietary information on corporate disclosure and transparency: Evidence from trade secrets. Journal of Accounting and Economics, 66(1), 163-193.	2018	7.1	89	4
Klasa, S., Ortiz-Molina, H., Serfling, M., & Srinivasan, S. (2018). Protection of trade secrets and capital structure decisions. Journal of Financial Economics, 128(2), 266-286.	2018	8.7	154	4
Molok, N. N. A., Ahmad, A., & Chang, S. (2018). A case analysis of securing organisations against information leakage through online social networking. International Journal of Information Management, 43, 351-356.	2018	18.9	6	2
Sofka, W., de Faria, P., & Shehu, E. (2018). Protecting knowledge: How legal requirements to reveal information affect the importance of secrecy. Research Policy, 47(3), 558-572.	2018	5.3	19	4
Castellaneta, F., Conti, R., & Kacperczyk, A. (2017). Money secrets: How does trade secret legal protection affect firm market value? Evidence from the uniform trade secret act. Strategic Management Journal, 38(4), 834-853.	2017	5.4	28	4
Png, I. P. (2017). Law and innovation: evidence from state trade secrets laws. Review of Economics and statistics, 99(1), 167-179.	2017	7.1	129	4
Zobel, A. K., Lokshin, B., & Hagedoorn, J. (2017). Formal and informal appropriation mechanisms: The role of openness and innovativeness. Technovation, 59, 44-54.	2017	5.7	77	3
de Zubielqui, G. C., Jones, J., & Statsenko, L. (2016). Managing innovation networks for knowledge mobility and appropriability: A complexity perspective. Entrepreneurship Research Journal, 6(1), 75-109.	2016	2.1	30	2
Fredendall, L. D., Letmathe, P., & Uebe-Emden, N. (2016). Supply chain management practices and intellectual property protection in China: Perceptions of Mittelstand managers. International Journal of Operations & Production Management.	2016	5.6	18	4
Henttonen, K., Hurmelinna-Laukkanen, P., & Ritala, P. (2016). Managing the appropriability of R&D collaboration. R&d Management, 46(S1), 145-158.	2016	2.9	46	3
Manzini, R., & Lazzarotti, V. (2016). Intellectual property protection mechanisms in collaborative new product development. R&D Management, 46(S2), 579-595.	2016	2.9	63	3
Nelson, A. J. (2016). How to share "a really good secret": Managing sharing/secrecy tensions around scientific knowledge disclosure. Organization Science, 27(2), 265-285.	2016	6.6	31	4
Olander, H., & Hurmelinna-Laukkanen, P. (2015). Proactive HRM for reducing knowledge risks—evaluating commitment and trustworthiness. International Journal of Innovation Management, 19(06), 1540011.	2015	1.3	7	2
Solli-Sæther, H., Karlsen, J. T., & van Oorschot, K. (2015). Strategic and cultural misalignment: Knowledge sharing barriers in project networks. Project Management Journal, 46(3), 49-60.	2015	4.6	44	1
Milesi, D., Petelski, N., & Verre, V. (2013). Innovation and appropriation mechanisms: Evidence from Argentine microdata. Technovation, 33(2-3), 78-87.	2013	5.7	55	3
Thomä, J., & Bizer, K. (2013). To protect or not to protect? Modes of appropriability in the small enterprise sector. Research Policy, 42(1), 35-49.	2013	5.3	156	4
De Faria, P., & Sofka, W. (2010). Knowledge protection strategies of multinational firms—A cross-country comparison. Research Policy, 39(7), 956-968.	2012	5.3	135	4
Gallié, E. P., & Legros, D. (2012). French firms' strategies for protecting their intellectual property. Research Policy, 41(4), 780-794.	2012	5.3	116	5
Delerue, H., & Lejeune, A. (2011). Managerial secrecy and intellectual asset protection in SMEs: The role of institutional environment. Journal of International Management, 17(2), 130-142.	2011	3.8	41	3
Marx, M. (2011). The firm strikes back: non-compete agreements and the mobility of technical professionals. American Sociological Review, 76(5), 695-712.	2011	10.9	220	4
Delerue, H., & Lejeune, A. (2010). Job mobility restriction mechanisms and appropriability in organizations: The mediating role of secrecy and lead time. Technovation, 30(5-6), 359-366.	2010	5.7	60	3
Keupp, M. M., Beckenbauer, A., & Gassmann, O. (2010). Enforcing intellectual property rights in weak appropriability regimes. Management International Review, 50(1), 109-130.	2010	3.2	96	3
1. Amara, N., Landry, R., & Traoré, N. (2008). Managing the protection of innovations in knowledge-intensive business services. Research policy, 37(9), 1530-1547.	2008	5.3	319	4
González-Álvarez, N., & Nieto-Antolín, M. (2007). Appropriability of innovation results: An empirical study in Spanish manufacturing firms. Technovation, 27(5), 280-295.	2007	5.7	124	3
Hannah, D. R. (2007). An examination of the factors that influence whether newcomers protect or share secrets of their former employers. Journal of Management Studies, 44(4), 465-487.	2007	9.4	45	4

Hurmelinna-Laukkanen, P., & Puumalainen, K. (2007). Nature and dynamics of appropriability: strategies for appropriating returns on innovation. R&d Management, 37(2), 95-112.	2007	2.9	257	3
Louis Y. Y. Lu (2007) Protecting Intellectual Property Rights, ResearchTechnology Management, 50:2, 51-56, DOI: 10.1080/08956308.2007.11657430	2007	2.4	23	2
McAdam, M., & Marlow, S. (2007). Building futures or stealing secrets? Entrepreneurial cooperation and conflict within business incubators. International Small Business Journal, 25(4), 361-382.	2007	8.9	234	3
Hussinger, K. (2006). Is silence golden? Patents versus secrecy at the firm level. Economics of Innovation and New Technology, 15(8), 735-752.	2006	3	132	2
Hemphill, T. (2004). The strategic management of trade secrets in technology-based firms. Technology Analysis & Strategic Management, 16(4), 479-494.	2004	1.8	20	2
Cohen, W. M., Goto, A., Nagata, A., Nelson, R. R., & Walsh, J. P. (2002). R&D spillovers, patents and the incentives to innovate in Japan and the United States. Research policy, 31(8-9), 1349-1367.	2002	5.3	`1067	4
Arundel, A. (2001). The relative effectiveness of patents and secrecy for appropriation. Research policy, 30(4), 611-624.	2001	5.3	1069	4
Maurer, S. D., & Zugelder, M. T. (2000). Trade secret management in high technology: a legal review and research agenda. The Journal of High Technology Management Research, 11(2), 155-174.	2000	3.4	41	2
Teece, D. J. (2000). Strategies for managing knowledge assets: the role of firm structure and industrial context. Long range planning, 33(1), 35-54.	2000	4	1831	3
Arundel, A., & Kabla, I. (1998). What percentage of innovations are patented? Empirical estimates for European firms. Research policy, 27(2), 127-141.	1998	5.3	1328	4
Kitching, J., & Blackburn, R. (1998). Intellectual property management in the small and medium enterprise (SME). Journal of small business and enterprise development.	1998	3.8	178	2
Liebeskind, J. P. (1997). Keeping organizational secrets: Protective institutional mechanisms and their costs. Industrial and Corporate Change, 6(3), 623-663.	1997	2.8	300	3
McConnachie, G. (1997). The management of intellectual assets: delivering value to the business. Journal of Knowledge Management.	1997	8.6	59	2
Harabi, N. (1995). Appropriability of technical innovations an empirical analysis. Research policy, 24(6), 981-992.	1995	5.3	564	4
Levin, R. C., Klevorick, A. K., Nelson, R. R., Winter, S. G., Gilbert, R., & Griliches, Z. (1987). Appropriating the returns from industrial research and development. Brookings papers on economic activity, 1987(3), 783-831.	1987	3.7	5260	3