CHALMERS
UNIVERSITY OF TECHNOLOGY

Think it, Build it, *Shhhh*...ip it!

Managing trade secrets in the context of agile technology development

Master's thesis in the Master's Program
Entrepreneurship and Business Design

ELLENOR HAYES

DEPARTMENT OF TECHNOLOGY MANAGEMENT AND ECONOMICS
Division of Entrepreneurship and Strategy

CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden 2020
www.chalmers.se

Report No. E2020:037

Think it, Build it, *Shhhh*...ip it! Managing trade secrets in the context of agile technology development

ELLENOR HAYES

MASTER THESIS E2020:037

Department of Technology Management and Economics
Division of Entrepreneurship and Strategy
Chalmers University of Technology
SE-412 96 Gothenburg, Sweden
Telephone: +46 (0) 31-772 1000

Abstract

Over the past two decades, agile methodologies have become a mainstay of software development practices at companies large and small. With their focus on short development cycles and autonomous, self organizing teams, agile technology development presents a significant challenge for the effective management of trade secrets. At the same time, many of the intellectual assets of highest strategic importance to agile technology companies — e.g. proprietary algorithms, machine learning models, unique datasets, and valuable data derived insights — cannot be registered as patents, trademarks or designs. (Nor can they be effectively claimed and protected via copyright.) Rather, if the company is to retain any intellectual property based control position in relation to these assets, they must be managed and protected as trade secrets.

Via a systematic literature review and multiple case study research design, this study examines this tension and seeks to contribute to the field by providing research based guidance on how agile technology companies may incorporate trade secret protection procedures without undermining the speed and autonomy of their product development practices.

The findings demonstrate that, by relying on the inherent flexibility of the laws governing trade secrets (specifically the contextual requirement of “reasonable steps”), it is possible to manage the tension between agility and robust trade secret protection. In doing so, agile technology companies should take a measured approach that focuses on building awareness and trust among individual employees so as to frame trade secret management as a cross functional task and enable positive behaviors.

The findings of the study can be used to inform the development of trade secret protection procedures that enable technology companies to continue to develop products with agility while using trade secrets to secure practically effective and legally defensible intellectual property based control positions for their most strategically important assets.

Acknowledgments

Interviews have been central to the empirical research that underpins this study. Therefore, although I have assured their anonymity, I would first like to thank each and every one of the individuals and companies that agreed to participate in my research. I am hopeful that this thesis will help to unravel some of the mystery that shrouds trade secrets and shape the way we use them to protect the valuable assets generated in the context of agile technology development.

Thank you to Bowman Heiden, Ulf Petrusson, Karla Soler Riba, and everyone at the Center for Intellectual Property (CiP). The CiP education has undoubtedly been a turning point in my professional development for which I will be forever grateful.

Thanks also to my faculty supervisor at Chalmers University of Technology, Sarah van Santen, for her invaluable guidance and feedback, and without whom this thesis would not have come together in the way it did.

I would also like to acknowledge and thank the esteemed IP practitioners — particularly Ruud Peters, Donal O'Connell, Haakon Thue Lie, Nigel Wong and Per Wendin — who were generous enough to share their time and perspectives and helped shape my research in its early stages. It is my intention that Ruud's catch cry "IP Strategy *is* Business Strategy" echoes clearly through the pages of this thesis, as it will throughout the rest of my career.

Finally, I would like to thank my friends and family whose love and support is the foundation of everything I do and has kept me sane while writing a thesis in the midst of global pandemic.

Ellenor Hayes, Gothenburg, June 2020

Contents

Abbreviations

EU	European Union
EU TSD	European Trade Secret Directive
IA	Intellectual Asset
IC	Immaterial, Intangible or Intellectual Capital
IP	Intellectual Property
IPR	Intellectual Property Right
SaaS	Software as a Service
TRIPS	Trade Related Aspects of Intellectual Property
TSPM	Trade Secret Protection Measure
US	United States of America
US DTSA	United States Defend Trade Secrets Act
US UTSA	United Stated Uniform Trade Secrets Act
WIPO	World Intellectual Property Organization

List of Figures

List of Tables

1. Introduction

1.1. Background and Purpose

The term *agile development* was originally conceived in 2001 and articulated in the 12 principles laid down in the original Manifesto for Agile Software Development published by the nonprofit Agile Alliance (Beck et al., 2001). It has become a buzz word across multiple industries, a darling of the technology press, and a catch cry of employer branding (Meyer, 2014). Over the past two decades, it has also become a mainstay of software development practices at companies large and small (HBR Analytic Services, 2015). Today, there is no one, fixed process which solely encapsulates agile development. However, all more or less reflect the original manifesto's objective of achieving higher quality software in a shorter period of time via self organizing teams collaborating with customers with less documentation and reduced time to market. Out of this, many frameworks (and catchy slogans, including the one adapted in the title of this study) have been developed. Though not without critics (see for example Denning, 2012), agile development is generally accepted to be an efficient and effective approach to software development. It has even been adopted beyond the software industry (Ciric et al., 2018).

If successful, agile development practices will lead to the creation of products that meet user needs and deliver some sort of value. Often, and especially in the case of agile software development, these products will be intangible. Rather than being made up of physical parts or ingredients, they consist of a range of intellectual assets (IAs). IAs, unlike physical goods, are ubiquitous, inexhaustible, and nondepletable (Reichman & Samuelson, 1997). As such they are inherently difficult to control. Intellectual property (IP) is one important means of securing control positions around the IAs. However, knowing and deciding which type of IP should be applied is not always straightforward. When the requirements of novelty, non obviousness/inventiveness and usefulness are met, patents may offer some protection for technical solutions. Though the pendulum seems to have swung back in favor of software patentability in the US recently (Klemens, 2019), in a 'post Alice' world, the patentability of software based inventions is significantly reduced (Stern, 2014). Meanwhile, copyright theoretically prevents direct duplication of original works created during agile product development (including, for example, source code, product specifications and databases). However, due to the limitations of copyright protection to the "fixed expression" of an original work, it cannot protect against the reproduction of ideas or concepts or prevent others from independently creating something similar or identical or having the same technical effect. Indeed, many of the IAs of highest strategic importance to agile

technology companies — for example, proprietary algorithms, machine learning models, unique datasets, and valuable data derived insights — cannot be registered as patents (or trademarks or designs). Nor can they be effectively claimed and protected by copyright. Hence, the only remaining candidate for an IP based control position is trade secrets.

In the knowledge economy, trade secrets remain one of the most important categories of IP according to industry. In 2017, international law firm, Baker McKenzie, commissioned a global survey and report to examine the role trade secrets play in today's digital age wherein 82% of the over 400 senior executives surveyed, said that they believed “trade secrets are an important, if not essential, part of their businesses” (Baker McKenzie, 2017, p. 3). This is unsurprising given that trade secret protection can extend to an extremely broad range of IAs and there is no requirement for originality or stringent and costly registration process. What is more surprising is the fact that the same report highlighted that a mere third of the companies surveyed had procedures in place to respond to the threat of or actual theft of trade secrets (Baker McKenzie, 2017, p. 4). There is a clear disconnect here because trade secrets do not meaningfully exist unless they are actively managed. Unlike patents, trademarks, or designs which can be registered and are protected by way of government granted monopoly, trade secret law exists only as a backstop — the first and only practical source of protection for trade secrets is the owner's own diligence (Pooley, 2015). This is particularly challenging in the context of agile technology companies, where the core challenge is developing and implementing trade secret protection procedures that do not undermine or hinder other operational imperatives.

Looking at IP management more broadly, there are inherent rigidities in traditional approaches and inconsistencies with the speed and flexibility of technology development in the digital age. Traditionally, many IP managers have worked reactively — for example, by relying on invention disclosures to know when and what to patent (Millien & George, 2016). Agile methodologies disrupt this and generally leave very little (if any) thought to the management of IAs and controlling them via IP. Looking at trade secret management in particular, traditional approaches (developed in the industrial economy) have involved a combination of systems and processes that are in direct conflict with the agile development philosophy. For example, carefully curated internal “Trade Secret Registries” (such as those advocated by Pooley (2015a) and O’Connell (2017)) are at odds with the Agile Manifesto’s call for reduced reliance on written documentation. Further, physical or digital measures which restrict access to important IAs on a strictly need to know basis

have the potential to stymie developers' ability to work with autonomy and may fatally undermine feelings of trust in agile teams.

While some thought has been given to how IP practitioners can update their practices to better align with the agile development teams they support (Lersten et al., 2020; Millien & George, 2016), this work has focused on securing patents for technical inventions. To date, research in the field of trade secret management has been very limited. The extant literature generally acknowledges challenges of maintaining and managing trade secrets (Hannah, 2005; Hannah & Robertson, 2015; Hemphill, 2004; Robertson et al., 2015; Stead & Cross, 2009) and their importance in protecting a range of IAs that cannot be adequately protected via any other form of intellectual property right (IPR) (Bos et al., 2015; Crittenden et al., 2015; Hannah et al., 2019). However, to date, no research has examined the inherent tension between agile product development and trade secret protection.

This study takes up this challenge and seeks to provide insight and develop the literature on the ways in which technology companies experience and can manage the tension between agile product development practices and trade secret protection procedures. The purpose of the study is to inform the development and implementation of practical trade secret protection procedures that enable technology companies to continue to develop products with agility while using trade secrets to secure practically effective and legally defensible IP based control positions for their most strategically important IAs.

1.2. Research Question

The specific issue under investigation in this study is how agile technology companies can manage the tension between trade secret protection procedures and the speed and autonomy with which their teams develop new products.

The research question is thus framed as follows:

> How can agile technology companies incorporate trade secret protection procedures without undermining the speed and autonomy of their product development practices?

1.3. Scope & Delimitations

Given the proliferation of different approaches to agile development mentioned above, and the expansive meaning of the term *technology*, the scope of what could be considered an *agile technology company* is extremely broad. For the purposes of this study, and as discussed in greater detail below, the characterization of technology companies as *agile* will be based on the core attributes of agile development set out in the original Manifesto for Agile Software Development (Beck et al., 2001). That is to say, any company that develops any kind of technology based product and/or service and professes to optimize its development processes for Speed, Autonomy, User Centricity and Quality, is within the scope of this study. Noting that this is still extremely broad, it is the first two attributes — Speed and Autonomy — which form the metrics against which the impact of trade secret protection measures (TSPMs) will be specifically investigated. Beyond simply limiting the scope of the study, these two attributes are where the most explicit tension between trade secret management and agile development is likely to manifest.

Trade secrets can be examined from multiple perspectives — including legal, economic, marketing/public relations, organizational psychology, sociology, and innovation science. This study is cross disciplinary but the primary perspective is management science. Specifically, the research focuses on how the process of managing and maintaining trade secrets (as a control position for strategically important IAs) can be incorporated into the practices of product development teams working at agile technology companies.

2. Theoretical Foundation

This chapter unpacks the key concepts and theories underpinning the study. First, Intellectual Asset Mapping is introduced as a means of bringing the resource base of knowledge based organizations (including agile technology companies) into higher resolution. Only once it is clear which IAs are present and how the company derives value from them, is it possible to adopt a structured and systematic approach to controlling them to maximize their value. To theoretically frame this process, the concept of Appropriability is introduced together with a framework of Structural Control Positions. The latter provides an overview of the options available to knowledge based organizations (again, including agile technology companies) to control their intangible resource base and positions secrecy (and it's legal manifestation as trade secrets) within a broader context of potential appropriability mechanisms. From there, the discussion hones in on the specific control position, Trade Secrets, and context, Agile Development, at the center of the study. It ends with an examination of the apparent tension between these two concepts — i.e. the core phenomenon under examination.

2.1. Intellectual Asset Mapping

In order to identify what could be protected as a trade secret by any organization, it is necessary to identify the underlying resources that are at the core of the current (or anticipated) value that the organization delivers to the market. One very effective way to do this is the process of IA mapping.

The theory of IA mapping is based on the idea that knowledge based organizations or projects can be broken down into discrete intellectual components – i.e. IAs – and that doing so provides a useful starting point for capturing, managing, protecting and leveraging the organization or project's core resource base (Petrusson, 2016). By identifying and examining the underlying IAs, rather than focusing purely on the IPRs or other measures that can be used to control them, it becomes possible to understand the intangible resources which form the basis of and drive value creation. This process of identifying and mapping IAs can be used by any business in any industry, but it is particularly useful for knowledge based organizations where the core resource base is intangible — a description which applies to almost all agile technology companies, especially those which trade primarily in software products.

As discussed below, one (but by no means the only) way of securing control over IAs is via IPRs. In doing so, it is necessary to distinguish between the underlying IA and the IPR which is invoked to protect it. The IA mapping process is also helpful in that it addresses the layer below any available IPRs and thereby enables strategic decision making about how to protect them in a way that is compatible with and, ideally, maximizes the organization's ability to utilize and create business value from them. For example, if a technical solution (the underlying IA) fulfills certain legally defined criteria, it may be registered and protected as a patent (the potential IPR). However, as discussed in the next section, IPRs (or “Rights Based” control positions) are by no means the only means of controlling valuable IAs. While the said technical solution may indeed fill the legally defined criteria to be registered as a patent, patenting is not necessarily the most effective means of control. For example, after assessing that third party infringement could not be easily detected (for example in certain so called “under the hood” technologies) or the patented technology could easily be invented around, the organization may be wise to decide to maintain the same technical solution as a trade secret (a “Secrecy Based” control position) as a strategic alternative to patent protection.

The theory of IA mapping is closely related to the theory of the technology based firm developed by Granstrand (1998). Granstrand draws a distinction between the material (tangible) and immaterial (intangible) resource categories available to any given firm. The latter category, he says, makes up the firm’s immaterial (or intangible or intellectual) capital (IC). This includes registrable IPRs (such as patents and trademarks) and unregistered IPRs (including trade secrets) but is critically much broader and also encompasses know-how, goodwill, and power in internal and external relations and human competence that lies within the firm. By using IA mapping it is possible to gain an even clearer understanding of the assets which form the IC of any given firm.

2.2. Appropriability and Structural Control Positions

Once the core intangible value drivers of an organization have been identified via the IA mapping process, the next step is to ensure that the firm has the capacity to retain and leverage their value of the IAs by securing effective control positions around them. A key challenge in this pursuit is that, due to their inherent nature as non rivalrous and non exclusive, IAs may be spread instantaneously as soon as they become known (Wagner, 2003). Without some type of control mechanism, it is impossible to meaningfully transact IAs as economic goods.

The concept of appropriability is well established in the fields of economics and innovation management (see, inter alia, the work of Arrow, 1962; Lavie, 2006; Teece, 1986; Teece et al., 1997; Von Hippel, 1982). Put simply, appropriability refers to the capacity of the firm to retain the value it creates for its own benefit (Kay, 1995). There are many potential appropriation mechanisms available to firms seeking to control IAs — including IPRs, secrecy, lead time advantage, complexity, and speed. Teece (1986) explains that appropriation regimes can be characterized as "tight" or "loose" depending on how easy or difficult it is for competitors to imitate the innovation in question. Due to the "generally weak" legal protection of secrets in most jurisdictions, secrecy may be characterized as a "loose" appropriation mechanism (especially when compared to patents) (see Granstrand, 1999, p. 237). Despite this, extant academic research has found that secrecy is in practice perceived as one of the most important and effective appropriability mechanisms for many firms across industries (see, for example, Cohen et al., 2000; and more recently, Choi et al., 2019).

Conceptually, appropriability is closely related to the Model of Structural Control Positions introduced by Petrusson (2004, p. 136) (Petrusson's Model). Though it is less established in the academic literature, Petrusson's Model provides a helpful and holistic overview of the appropriability mechanisms which are available to firms to build robust structural control positions around strategically important IAs.

According to Petrusson's Model, the available control positions can be sorted into three categories: legal, business, and technical. Legal control incorporates secrecy (the primary control/appropriability mechanism investigated in this study) but also includes rights based property (i.e. IPRs) and contractual control. Business control is based on market power and technical control includes any technical means by which IAs can be controlled. An adapted version of Petrusson's Model is set out below:

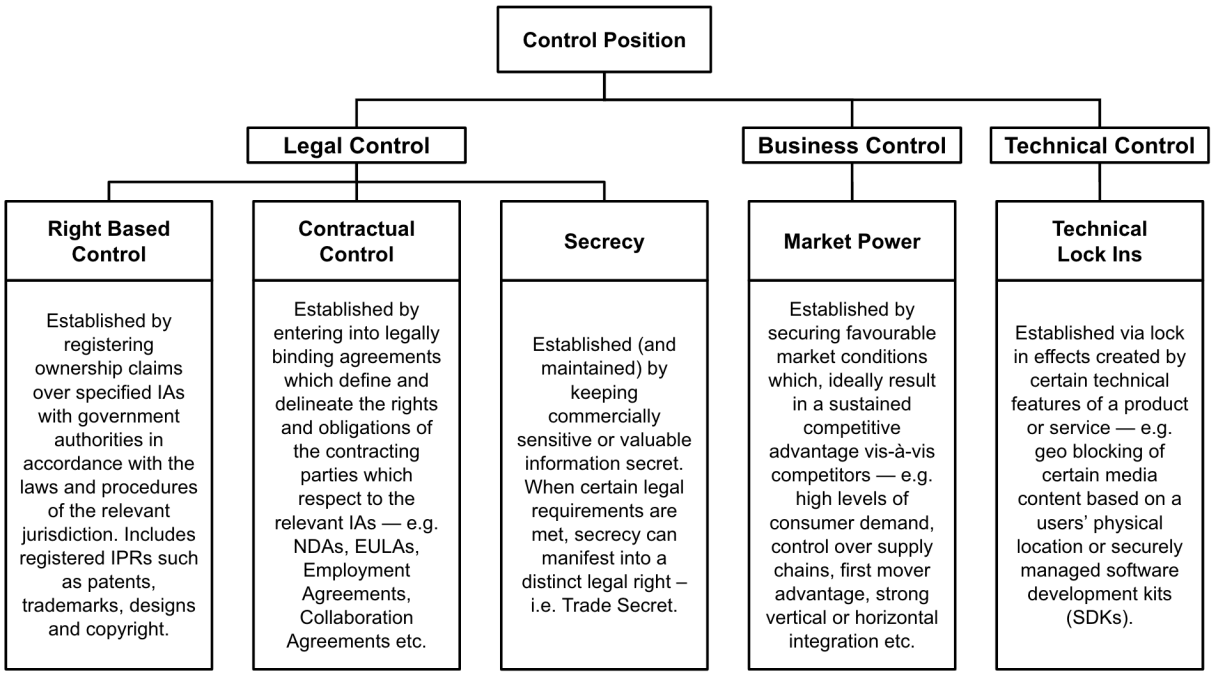


Figure 1. Adapted version of Petrusson's Model of Structural Control Positions

Petrusson's Model places secrecy (and its legal manifestation as trade secrets) within the broader context of other control positions which can be secured around IAs. This is critical for the current study because it demonstrates that secrecy (and its legal manifestation as "trade secrets") can be viewed as part of a broader set of tools that can be used to protect valuable IAs and not as a rigid set of rules that must be followed in order to comply with a strict legal standard.

Petrusson's Model also demonstrates how trade secrets, while commonly considered a type of IP (alongside patents, trademarks, copyright, and design), are separate and distinct from these rights based IPR control positions and must, therefore, be maintained and managed via distinct processes. The separation of secrecy from rights based control in Petrusson's Model is consistent with the position taken by Hurmelinna-Laukkanen and Puumalainen (2007, p. 97) who, when examining the closely related concept of appropriability, argue that "practical" secrecy ("in the sense that the knowledge is restricted to a limited group of people") can be considered independent and distinct from IPRs.

Finally, and importantly Petrusson's Model highlights how contracts can be used to construct a separate legal control position around IAs. There is a particular synergy between secrecy and contract based control positions because in the context of an organization with multiple

stakeholders (including employees, collaboration partners etc.) contracts are one of the key mechanisms by which trade secrets can be managed and maintained.

2.3. Trade Secrets

Trade secrets can be defined broadly as “any confidential business information which provides an enterprise a competitive edge” (WIPO, n.d.). They have been deemed by some as “the ‘ugly duckling’, ‘Cinderella’ or ‘stepchild’ of intellectual property” (Sousa e Silva, 2016, p. 310). While others have heralded them as the “future of intellectual property” (Bambauer, 2016, p. 833). They are unique in the sense that the disclosure of a trade secret results in a complete loss of protection. As such, trade secret laws exist only as a backstop against theft or misappropriation (Pooley, 2015a).

Nonetheless, trade secrets remain one of the most important categories of IP. As mentioned above, the 2017 global survey and report commissioned by Baker McKenzie examined the role trade secrets play in today's digital age. There, 82% of the over 400 senior executives surveyed, said that they believed “trade secrets are an important, if not essential, part of their businesses” (Baker McKenzie, 2017, p. 3).

The following sections canvas the legal definition of trade secrets under international law (the TRIPS Agreement) and in two significant jurisdictions (the US and the EU), as well as the relationship between trade secrets and the two closely related concepts of secrecy and appropriability.

Legal Definition

Fundamentally, trade secrets are secrets that exist and can be traded independently of any legislative frameworks. In this sense, it can be said that the laws on trade secrets are regulative and not constitutive (Lie, 2020). This is one of the fundamental differences between trade secrets and other types of IP discussed in further detail below. Nonetheless, legislation with respect to trade secrets exists in most developed jurisdictions. Together with judicial discourse in the form of case law where relevant, these laws define the contours and determine the enforceability of a trade secret in any given context. Helpfully, a level of international harmonization has developed around trade secret law with most developed nations adopting similar legal definitions of trade secrets and minimum standards for their protection (Hallenborg et al., 2008).

TRIPS Agreement

The Agreement on Trade Related Aspects of Intellectual Property (TRIPS) is a multilateral agreement on IP. It came into effect on 1 January 1995 and is considered the most comprehensive multilateral agreement on IP to date (World Trade Organization, n.d.). The TRIPS Agreement sets out minimum standards of protection to be provided in each of the main areas of intellectual property — including trade secrets — by each of the member states (all 164 member nations of the World Trade Organization since 29 July 2016).

Article 39.2 of the TRIPS Agreement provides for the protection of trade secrets (referred to as "undisclosed information") provided that the information:

- is secret;
- has commercial value because it is secret; and
- has been subject to reasonable steps under the circumstance to keep it secret.

Before unpacking each of these requirements, it is helpful to briefly touch on how they have been interpreted by and implemented into the legal system of two important signatories of the TRIPS Agreement — the US and the EU.

US Legislative Framework

In recent years, protections for trade secrets under US Law have become significantly more robust. The most recent legislation is the *Defend Trade Secrets Act of 2016* (US DTSA). Most notably, the US DTSA establishes a federal civil cause of action for trade secret misappropriation relating to any product or service used in or intended for use in, interstate or foreign commerce. Prior to this, trade secrets in the US were governed by state law which had achieved a certain level of harmonization via the *Uniform Trade Secrets Act* (US UTSA) — various versions having been adopted by 48 of the 50 states. The third relevant piece of the US regulatory framework is the *Economic Espionage Act of 1996* (US EEA) which allows for the criminal prosecution of those who engage in "economic espionage" or the "theft of trade secrets." The US EEA also allows for the Attorney General to bring a civil action to obtain injunctive relief against any violation of the US EEA.

EU Legislative Framework

Prior to 2016, the EU did not have any specific legal provisions to protect trade secrets or undisclosed information. Rather, they were governed by the national laws of each member state with no regional harmonization. This changed with the introduction of the European Commission's Directive on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use, and disclosure (EU TSD). The purpose of the EU TSD was to promote the establishment of an "Innovation Union" (European Commission, n.d.) by supporting the process of trust building between different parties and encouraging cross border collaborations and transactions involving trade secrets. The introduction of the EU TSD had the effect of requiring each member state to enact laws and administrative provisions to comply with the Directive by 9 June 2018.

Three Common Requirements

Though there are some nuanced differences across jurisdictions, the effect of the TRIPS Agreement was the adoption of a consistent international legal definition of trade secrets involving three common requirements. Each of these is discussed in further detail below.

Secret

First, for an IA to fall within the legal definition of a trade secret it must indeed be secret — i.e. not generally known or easily ascertainable. To promote the free movement of employees in the knowledge economy, it must also not consist of an employee's individual skill or tacit knowledge. While this requirement may seem obvious and straightforward, the actual distinction between what is and is not a protectable trade secret can be very blurred and highly contentious. Pooley (2015a, p. 34) provides the following helpful visualization to understand this requirement, noting that "for the most valuable trade secrets, lawsuits can go on for years over whether information lies inside or outside the line."

Figure 2. Adapted version of Pooley's Trade Secret Model

Commercial Value

Second, the secret must be commercially valuable *because* it is secret — i.e. the economic benefit accrued to the owner of the trade secret must derive specifically from the fact that it is not generally known and not just from the value of the information itself. This is an important distinction because, for example, personal information about customers or employees which is kept secret to maintain their legal right to privacy will not normally constitute a trade secret. Also, independent creation or discovery of the secret by a third party can eliminate a secret's commercial value and hence extinguish the owner's right to claim protection in the event of theft or misappropriation.

Reasonable Steps

Finally, in order to be able to enforce any rights to a trade secret in the event of theft or misappropriation, the owner must demonstrate that it has taken "reasonable steps" to actively protect and maintain the secret. What is reasonable depends on the specific circumstances — including the size and sophistication of the entity claiming trade secret protection, the nature of the IA in dispute, and a range of other factors. Thus, the specific steps and mechanisms used to protect a trade secret are of core importance to not only the maintenance of the secret but also the owner's ability to seek legal recourse in the event of theft or misappropriation.

Relationship between Trade Secrets and Secrecy

The foregoing discussion highlights that, while the scope of what may qualify as a trade secret is very broad, a trade secret only exists as a legal right in a fairly narrowly defined set of circumstances. However, it is possible, indeed common, for firms to keep business related information somewhat clandestine without actively managing it as a trade secret. There are many instances in which an IA could be treated with a degree of secrecy or confidentiality without rising to the status of a legally enforceable trade secret. Whether or not it does will only become known in the event of a court decision confirming its theft or misappropriation. It is therefore important to make a distinction between the concept of secrecy and the existence of trade secrets.

Secrecy can be defined as the deliberate concealment of information from others (Bok, 1989; Kelly, 2002). The concept has long been studied within the field of social science. Writing in the early twentieth century, Simmel (1906) argued that, alongside some level of knowledge about the other person, a degree of secrecy is a prerequisite for every social interaction. In discussing the social currency conveyed by keeping things secret he cites the timeless example of a child proudly declaring “I know something you don't know" — a phrase which conveys a sense of pride and self aggrandizement even if it is entirely baseless (Simmel, 1906, p. 464).

The power of secrecy in a more commercial context is explored by Mills (2015). In discussing the strategic value of secrets in marketing campaigns, Mills delineates between the three roles an individual may inhabit in relation to a secret: (i) the Insider (who knows the secret); (ii) the Aspirant (who is aware of the secret but does not know it); and (iii) the Outsider (who is unaware of the secret). Secrecy as a strategic brand activity is deployed to great effect by some companies — for example, Apple, which zealously guards details about what products will be released and what new models and features each will have (Dickey, 2013) and at the same time invests in marketing campaigns that tantalize Apple devotees with taglines such as “Hey Siri, give us a hint” (for details on that campaign see Dillet, 2015).

It is clear that the concept of secrecy is much broader than the legal definition of a trade secret. To further illustrate the distinction between them, it is possible to articulate several scenarios in which secret information, while important or even valuable to the holder, would be unlikely to legally constitute a trade secret (Regnér, 2017 citing Thue Lie, 2017). For example:

- A list of suppliers or customers which is saved on a shared hard drive without any access restrictions or password protection — it would be difficult to demonstrate that the holder of this information had taken “reasonable steps” to keep it secret.
- Personal information about customers or employees which is kept secret purely to maintain their legal right to privacy — assuming that the information is kept secret only to comply with privacy legislation, it may be difficult to argue that keeping this information secret provides the holder with a competitive advantage.
- A sauce recipe that is used but not disclosed by a restaurant, but is also published in a book which is available at the local library — since the recipe is in the public domain, it is generally known and easily accessible.
- Information about a competitor's tax evasion — it is difficult to argue that this information provides the holder a competitive advantage while it remains secret (indeed, it would likely be more advantageous if the information about the competitor's tax evasion came under public scrutiny).

Trade Secrets vs Other Forms of IP

As mentioned above, trade secrets are sometimes considered to be (inter alia) the “ugly duckling” of IP (Sousa e Silva, 2016, p. 310). One reason this discourse persists is that, in the absence of a right to exclude, it is possible to argue that trade secrets are not a form of property at all (discussed at length by Graves, 2007) or that they are, at most, “odd aspirants to the status of property” (Bok, 1989, p. 144). Indeed, other types of IP (patents, copyright, trademarks, designs) all provide exclusivity for varying lengths of time — typically 20 years for patents, the life of the author plus 70 years for copyright, during commercial use for trademarks and between a maximum of 14 and 25 years for designs. Trade secrets, on the other hand, convey no such exclusivity. It is not possible to prevent others from independently developing or reverse engineering the IAs which are held as trade secrets. Indeed, a claim of trade secret status will typically be eroded if this is the case. Instead of a right to exclude, trade secret law (“merely”) provides a legal remedy in the event of unlawful misappropriation.

Another fundamental and fascinating difference between trade secrets is put forward by Thue Lie (2020) who sharply observes that trade secret rights vest on different principles to other IPRs in that law merely regulates trade secrets, but is not constitutive. For example, where patents only

exist because of patent law, secrecy exists and is used as a control position in trade relationships irrespective of trade secret law, which is merely there to regulate and provide legal recourse when secrecy is breached.

The fundamental differences between trade secrets and the other types of IP even led one prominent legal scholar to question whether trade secret jurisprudence has a footing in any coherent body of legal theory at all (Bone, 1998). As Pooley (2020) notes, the discussion is further exacerbated by the inconsistent characterization of trade secrets as a category of IP under US law (and the TRIPS Agreements) and the specific exclusion of trade secrets as a type of IP under the EU TSD. This debate is deeply rooted in legal jurisprudence and the doctrinal underpinnings of trade secrets. However, in the context of this study (which takes a practical approach to trade secret management), it is not necessary to unpick any further. Rather, it is sufficient to acknowledge the subtle peculiarity of trade secrets as a type of IP, while focusing on their role in creating legally defensible control positions around strategically important IAs — specifically in the context of agile technology companies.

2.4. Agile Development

The concept and process of agile development was originally conceived in 2001 and articulated in the 12 principles laid down in the original *Manifesto for Agile Software Development* (Beck et al., 2001). To understand the concept and practice of agile development, it is helpful to compare it to the more traditional waterfall approach which was first formally described in the context of software development by Royce (1970). Waterfall software development typically involves a sequential, flow down process. This was depicted by Millien and George (2016) in the figure below:

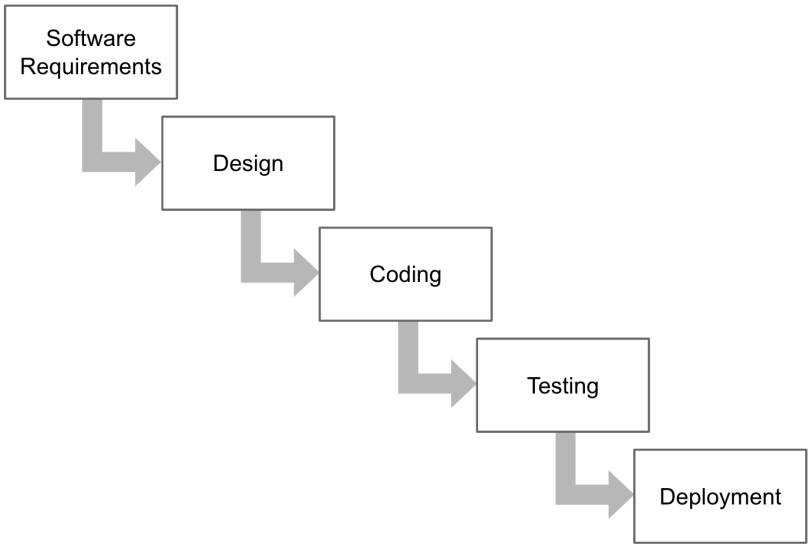


Figure 3. Typical Waterfall Software Development Process

In contrast, agile software development generally involves small, cross functional teams of designers, coders, and testers that work through multiple short iterations (commonly called “sprints”) with a view to building imperfect but functional products that can be continuously deployed for internal and external testing and user feedback. The aim is to develop and ship products with increasing functionality after each iteration, maximum responsiveness to proven user needs/demands, and minimal wasted time and resources (Meyer, 2014). A simple figure showing a typical agile development process also depicted by Millien and George (2016) is set out below:

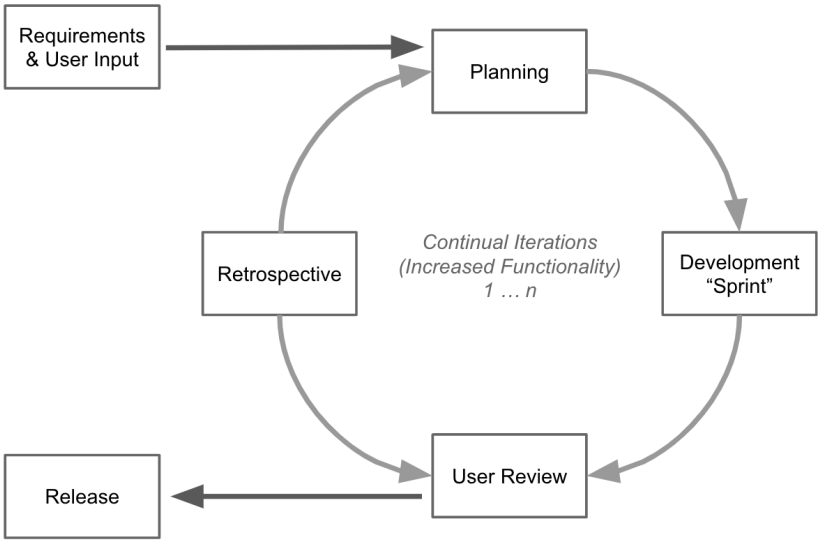


Figure 4. Example Agile Software Development Process

Today, there is no one, fixed process which solely encapsulates agile development. Rather, various approaches have been developed, including Scrum, Kanban, Lean, and DevOps (Komus & Kuberg, 2017). However, all more or less reflect the original manifesto's objectives, which can be summarized in the following four core attributes:

- Speed: Short development cycles resulting in reduced time to market;
- Autonomy: Self organizing teams, reliant on and generating minimal documentation;
- User centricity: Iterative development based on continuous user testing; and
- Quality: Resulting in software that is fully functional for the end users.

In the context of this study, it is the first two attributes — Speed and Autonomy — which will be the metrics against which the impact of TSPMs will be investigated/measured. This is because the most explicit tension between trade secret management and agile development manifests in terms of its impact on the speed and individual or team autonomy. For example, the imposition of digital access controls for trade secret IAs will almost inevitably result in some additional friction in development cycles, ultimately slowing them down. Similarly, reducing the visibility or communication of strategic insights or business plans across a company means that teams must be organized with a greater degree of centralized control, hence reducing autonomy. This tension is discussed further below.

2.5. Tension between Trade Secrets and Agility

A key assumption underpinning this study is that, in the context of agile technology companies, reliance on trade secrets as a structural control position can reduce the speed and/or inhibit the autonomy of product development teams. However, this assumption is not necessarily incontestable.

On one hand, trade secrets (unlike other IPRs) do not require any formal registration process. As long as the IA remains secret and retains its resultant commercial value, trade secret protection will endure and extend to new iterations, improvements or additions (Lie et al., 2020). This is in stark contrast to patents, trade marks, designs and copyright, all of which protect an IA at a fixed

moment in time (i.e. at the time the patent, design or trade mark application was filed or, in the case of copyright, the fixed expression of the work was created). In this sense, it could be said that trade secrets are highly flexible and dynamic, and therefore may be well adapted for use as a structural control position in agile contexts.

On the other hand, the potential for IP management strategies that incorporate trade secrecy to have a negative impact on R&D productivity and innovativeness in any company is well recognized. Charles Kettering, vice-president of General Motors Research Corporation from 1920 to 1947, is quoted in Granstrand (1999, p. 254), as having said: "When you lock the doors of the laboratory you lock more out than you lock in." If the negative impacts of trade secret protection were felt so acutely by one of the titans of 20th century industry, their potential incompatibility with modern day agile technology companies is almost self explanatory.

Trade secrets also have some significant limitations with respect to their use as control positions for technical solutions (a specific but important category of IAs, particularly in the context of agile *technology* companies). For example, Holgersson and Wallin (2017, p. 1091) highlight the limitations of trade secrets in securing freedom to operate (FTO) for technical solutions noting that *"[a] secrecy strategy … runs the risk of having the invention patented by someone else, inhibiting the commercial opportunities [or FTO] for the firm."*

Another significant limitation of trade secrets is their transactability on markets. In the absence of an officially registered/government granted monopoly and written claims to clearly articulate the metes and bounds of the underlying IA, trade secrets are relatively amorphous, especially when compared to patents. Therefore, while it is *possible* to contract for the sale or license of trade secrets they are relatively difficult to transact. In the context of agile technology companies, which stand to gain a lot by engaging in open innovation (Conboy & Morgan, 2010), a process that necessitates the transaction of IAs and IP between firms (Granstrand & Holgersson, 2014), this limitation is amplified.

Of course, the above two points are only relevant insofar as the firm is deciding how to protect its patentable technical solutions. As discussed in the introduction, these are only a narrow subset of the IAs of potential value and strategic importance to agile technology companies. For many others, including "under-the-hood" technical solutions, proprietary algorithms, machine

learning models, research results, raw data, refined datasets, business plans and strategies, which can or should not be patented, these considerations are plainly not relevant.

Looking at the tension between trade secrets and agility more broadly, it is helpful to return to the core values of agile development practices as articulated in the Agile Manifesto (Beck et al., 2001). They are:

- "**Individuals and interactions** over processes and tools"
- "**Working software** over comprehensive documentation"
- **"Customer collaboration** over contract negotiation"
- **"Responding to change** over following a plan"

Taking each of these in turn, it is possible to articulate several instances where trade secret protection procedures (at least how they have traditionally been conceived and implemented in more industrial settings) could be in conflict with the agile development philosophy.

First, valuing individuals and interactions over processes and tools indicates that TSPMs which call for the imposition of access controls around or otherwise hinder open and transparent internal communication channels are likely to cause friction.

Second, prioritizing working software over comprehensive documentation makes the task of identifying the underlying IAs could be protected as a trade secret (or another form of IP) particularly challenging, especially in organizations where the IP function relies upon product development roadmaps and other documentation to preempt and act on IP opportunities and risks.

The third, customer collaboration over contract negotiation, is perhaps the most obvious friction point. Not only does it involve releasing products to third parties — potentially exposing valuable trade secrets — it advocates doing so with limited regard to first negotiating and entering into non disclosure or confidentiality agreements to ensure these assets remain safeguarded during testing.

Finally, responding to change over following a plan, while not directly at odds with trade secret management, signals a general level of flexibility and disregard for rigid rules or procedures which may increase the likelihood of trade secret leakage.

Of course, these observations are very high level and the founding members of the Agile Alliance did not advocate dispensing with processes, tools, documentation, contracts, and plans entirely. But it is clear that a company which sees such aspects of organizational life as secondary may be a particularly difficult place to protect trade secrets.

3. Methodology

This chapter describes the methodology employed during the study. It includes an outline of the research strategy, design and methods and concludes with a discussion on the quality of the research with reference to the key metrics or reliability and validity.

3.1. Research Strategy

The research strategy of this study is grounded in the purpose — i.e. to understand how agile technology companies can manage the tension between trade secret protection procedures and the speed and autonomy with which their teams develop new products. The research strategy has been shaped by the interplay between this purpose and the relevant concepts and theories outlined in Chapter 2.

Relationship between Research and Theory

A predominantly iterative inductive approach has been taken to this study — i.e. observations have been used to inform the development of a theory (or set of generalizable inferences) in response to the research question.

Qualitative and Quantitative Research Considerations

Qualitative and quantitative research have distinct epistemological and ontological positions and as such can be viewed as two separate clusters of research strategies (Bryman & Bell, 2011). Given the relationship between research and theory and the epistemological and ontological considerations set out above, qualitative research methods were found to be the most appropriate for this study.

3.2. Research Design

The research design employed in the current study is that of a systematic literature review together with a comparative/multiple case study.

Literature reviews are a useful means of obtaining a foundational understanding of the topic of trade secret management and the themes, theories, and recommendations that scholars and practitioners have developed in the field. Taking a systematic approach has helped to ensure that the review is thorough and free from personal bias on the part of the author. Systematic

literature reviews are also acknowledged as particularly valuable when researching management and business topics where there is conflicting evidence concerning best practice approaches (Bryman & Bell, 2011) — a benefit which is highly relevant to the current study. It also provides a robust foundation to a study where, given the high sensitivity of the topic, the ability to access candid insights via case studies was (at the outset) uncertain. Finally, and importantly, given the relatively nascent nature of this research area and the small volume of formal academic publications, it was also feasible to conduct a systematic literature review within the constrained time frame of this study.

Case study research is focused on understanding the complexity and particular nature of the case in question and is very popular and widely used in business research (Bryman & Bell, 2011). This study seeks to understand how agile technology companies can manage the tension between trade secret protection procedures and the speed and autonomy with which their teams develop new products. Given the vast array of potential TSPMs and variability in the ways agile tech teams can and do work, this is a complex equation with no linear, observable causes and effects. To expand the breadth of the insights gleaned beyond the experience of a single case, the research design has not been confined to a single case. Rather, with a view to detecting themes and trends and developing theories in response to the research question, multiple cases have been investigated. The comparative aspect of the research design has also allowed for the findings to be presented at a higher level of abstraction — appropriate given the highly sensitive nature of the core issue under investigation.

The interplay between these two methods is at the core of the research design. The systematic literature review provides information about the range of TSPMs that are available for agile technology companies to secure and maintain trade secret status for key IAs and the conditions for effective trade secret management according to earlier studies. Meanwhile, the multiple case studies shed light on the perceived impact of these measures on speed and autonomy and unlock insight into how they can be implemented in a way that is compatible with agile technology development.

3.3. Research Methods

Systematic Literature Review

The systematic literature review covers two distinct categories of literature on the topic of trade secret management — non academic articles published online by service providers (Category 1 Literature) and academic/peer reviewed journal articles (Category 2 Literature).

The Category 1 Literature consists of non academic articles published online by service providers (including law firms, consultancies, software and SaaS providers, insurers etc.) on the subject of trade secret management. Though they typically lack academic rigor, these articles are often the first port of call when a company or individual is seeking to implement some kind of trade secret protection procedures or is confronted with trade secret theft or misappropriation. Many profess to offer practical tips and insights on best practice trade secret management. They are therefore highly relevant to the current study and serve to supplement the limited academic literature also under review. The review of this category thus provided information on the nature and range of specific TSPMs that are available and commonly recommended to companies (including agile tech companies) in order to secure and maintain trade secret status for their key IAs.

The Category 1 Literature was identified with two separate queries on Google Web Search using the terms [Trade Secret Management] and [Trade Secret Protection]. The 250 first results from each search were reviewed in brief and refined into a preliminary set of approximately 50 articles which seemed relevant to the study. That set was reviewed in detail pursuant to the following criteria:

- Authored by or on behalf of a law firm or other service provider
- Published on the law firm/service providers' own website or via an industry publication
- Content included practical advice on management of trade secrets — i.e. at least one recommendation to implement one or more TSPM — and was not exclusively focused on the legal construction of trade secrets by reference to specific case law or legislation
- Content was jurisdictionally neutral or written either from a European or US perspective (both of which are fairly harmonious and represent a quasi global standard with under the TRIPS Agreement)

- Published within last 10 years (i.e. since 2010)

Based on these parameters, this category was narrowed down to 30 relevant non academic articles which formed part of the review.

Data collected via the systematic literature review in Category 1 was analyzed by reviewing each article and recording which TSPMs were recommended in each. Based on this data, a catalog of over 120 distinct TSPMs was developed, coded, and labeled inductively to reflect the seven different categories of TSPMs (in turn divided to a further 31 subcategories). The full TSPM catalog is included as Appendix A. The seven categories of TSPMs are set out and discussed in further detail in Chapter 4 below.

The Category 2 Literature consists of academic/peer reviewed journal articles published in the field of IP management research, with a specific focus on secrecy and/or trade secrets. Though it appears to be gaining momentum as a discrete research field, Category 2 Literature is still fairly limited. The majority of IP management research either retains a broad scope (covering a range of IPRs) or is focused specifically on patents (Holgersson & van Santen, 2018). Nonetheless, the review of this category helped to shape an understanding of the practical conditions that the available empirical evidence has so far found to be ideal for effective trade secret management. It also provided a foundational understanding of the prior research conducted and the themes and theories that have started to emerge from this relatively under researched sub area of IP management.

The Category 2 Literature was identified with searches of the Clarivate Web of Science, Google Scholar and peer reviewed full text articles in the catalog of the Chalmers University of Technology Library. The search parameters used were ["Trade Secret*"] AND [Manage* OR Protect*] with results limited to the most recent twenty years (i.e. since 2000). The abstract of the 100 first results on each database were studied, leading to the identification of 21 relevant articles which formed part of the review.

Data collected via the systematic literature review in Category 2 was analyzed by reviewing each article and creating a table summarizing the nature of each study, the sample and method used, the key issue(s) examined, and the key themes of the results/conclusions drawn. The table is included as Appendix B. The key themes and main takeaways from the Category 2 Literature are discussed in further detail in Chapter 4 below.

Semi Structured Interviews

Phase 1 Interviews

To understand the perceived impact of available TSPMs on agile technology development practices, data was collected via semi structured interviews with 12 employees at a software based audio streaming technology company which has been recognized as having been extremely successful in incorporating agile methodologies into its product development practice. Participants were recruited across all levels of the organization based on their availability, willingness to participate and with a view to gaining perspectives from a broad cross section of the company. The sample of interviewees was comprised of:

- Senior/Group Level Engineers and Product Managers with strong experience in managing agile development teams and high level oversight as to the impact of TSPMs on their teams' ways of working.
- Engineers, Product Managers, and Agile Coaches with experience working in (but not necessarily leading) agile development teams and more detailed insight into the impact of TSPMs on their own and their teams' ways of working.
- IP Counsel and Patent Engineers with knowledge of IP law (including trade secrets) and experience in advising on/managing IP issues in the context of an agile technology company.

A copy of the interview templated used to guide the semi structured interviews in Phase 1 is included as Appendix C.

Phase 2 Interviews

To broaden the practical insights beyond just one company and add a comparative element to the study, data was also collected via semi structured interviews with representatives from three additional technology companies that also incorporate agile methodologies into their product development practices. Participants represented a range of technology sectors namely ride sharing/delivery, media streaming, and cloud computing services. Each individual participant was selected because of their central role in managing IAs and protecting IP in the context of an agile

technology company. A copy of the interview templated used to guide the semi structured interviews in Phase 2 is included as Appendix D.

Given the sensitivity of the topic and to encourage candid responses, no transcripts of the interviews were created. Instead, to encourage candidness, all interview participants were assured that data collected during the interview would be presented with a high level of abstraction and there would be no attribution of specific views to any particular individual or company. An anonymized list of interviewees is included as Appendix E.

Data collected via the semi structured interviews (both Phase 1 and 2) was analyzed reviewing detailed interview notes and coding them to extract common responses and identify core themes. The Gioia Method (as discussed by Gioia et al., 2012) was adapted in the coding process as a means of grounding theories developed in the study and maximizing the qualitative rigor of the analysis. Specifically, the analysis first involved the identification of common responses across two or more of the interviewees to extract 40 First Order Concepts. These concepts were then analyzed and arranged in terms of the structural relationships and thematic commonalities into eight Second Order Observations — which provide the structure of the interview results in Chapter 4. Finally, the emergent data, First Order Concepts and Second Order Observations, together with the insights and understanding developed via the systematic literature review, were collated into three overarching Aggregated Dimensions which provide the structure of the discussion on the major findings on the study in Chapter 5. A visualization of the interview data analysis process is included as Appendix F.

3.4. Quality of Research

There are numerous ways one can assess the quality of qualitative research (Bryman & Bell, 2011). In assessing the quality of the current study, the two key criteria of reliability and validity are examined.

Reliability

Research reliability can be divided into two parts. External reliability refers to the degree to which a study can be replicated. Internal reliability refers to whether or not one or more observers can agree upon what they see and hear.

Given the unique social setting in which all qualitative research is conducted, it is impossible to replicate any study exactly. This is particularly true in the current study. Due to the highly sensitive nature of the research topic — i.e. how the companies studied manage some of their most valuable and strategically important IAs — a significant portion of the data (i.e. the interview responses) have been kept confidential. Indeed, all interviewees were assured that their personal identities would not be attributed to any responses given and, in the case of the external interviews, it was agreed that the identity of the three companies represented would also remain anonymous. Despite the limitations this places on the precise replicability of the research, these measures were implemented to encourage a greater degree of transparency and candidness on the part of the interviewees. On the whole, this contributes to the quality of the data used in the study. Furthermore, notwithstanding the confidentiality requirements, all available steps have been taken to enable future researchers to replicate the study with similar results. For example, the research design has been documented meticulously, including details of search queries and interview templates used.

Similarly, it is impossible to completely exclude the personal bias of researchers in any qualitative study. However, the inclusion of a detailed articulation of the relevant theoretical concepts and frameworks should help to facilitate consistent observations by future researchers in the field.

Validity

Research validity can also be viewed as external and internal. External validity refers to the degree to which findings can be generalized across social settings. Internal validity refers to whether or not there is a good match between researcher's observations and the theoretical ideas they develop.

In the current study, data was collected from various sources, including a wide range of literature and four different technology companies which incorporate some kind of agile methodology into their product development practices. This adds strength to the external validity such that the results provide a useful insight into the phenomena under examination. As a result, the study's conclusions are reasonably transferable and may be used as guidance for the development and implementation of trade secret management practices at other agile technology companies. They may also serve as guidance for future research. However, the results are not suitable as a means of drawing conclusions for a larger group or field.

Internal validity tends to be a strength of qualitative research. In the current study, despite the constrained time frame, the researcher has had a deep level of engagement with the results. This coupled with the predominantly iterative inductive approach taken, means that there is a high level of conformity between concepts developed and observations made based on the available data.

4. Results

This chapter sets out the results of the study. First, it sets out the results of the structured literature review. Then, it presents the data collected during the two phases of interviews.

4.1. Systematic Literature Review

This section is structured according to the two categories of literature reviewed as part of this method. It ends with concluding observations made in relation to the literature review as a whole.

Category 1 Literature: Non Academic Articles

The Category 1 Literature was comprised of 30 non academic articles published online by service providers on the subject of trade secret management. Despite the fact that they are not generally research based or subject to academic rigor, they are based on the professional experience of practitioners who stand at the front line of trade secret management and are representative of the available practical advice on the day to day management of trade secrets. An overview of the Category 1 Literature is set out below in Table 1.

Title		Author Name/s (Firm/Company)	Date
1	Implementing a Trade Secrets Protection Program	Michael Greco (Fisher Phillips)	2 November 2013
2	11 strategies for protecting trade secrets	David G. Bates (Gunster)	15 May 2015
3	How to Mitigate Risks Associated with Trade Secret Theft	Pamela Passman (Marsh & McLennan Insurance)	23 July 2015
4	Trade Secret Protection: What are Reasonable Steps?	Pamela Passman (Seyfarth)	31 July 2015
5	Back in fashion – trade secrets in the modern enterprise	James Pooley (James Pooley, PLC)	1 October 2015
6	Trade Secrets	Donal O'Connell (IPEG Consultancy)	14 January 2016
7	Leading Practices to Protect Trade Secrets	Allen Dixon (Wolters Kluwer)	1 November 2016
8	Undiscovered country – building a trade secret culture	Tom Ewing (Avancept LLC) & Donal O'Connell (IPEG Consultancy)	31 March 2017
9	Ways to proactively protect your intellectual property and trade secrets	(Hendershot, Cowart & Hisey, P.C.)	15 August 2017

10	Harmonize Your Trade Secret Protection To Protect You Assets	Elizabeth E. Atlee (CBRE), Devon C. Beane & Christina N Goodrich (K&L Gates LLP)	December 2017
11	Five Strategies for Protecting Trade Secrets	Emma R. Schuering & Eric E. Packel (Polsinelli PC)	4 December 2017
12	Top 5 tips for protecting trade secrets	(Lewis Silkin)	8 December 2017
13	IP Law 101: 3 Ways to Protect Your Trade Secrets	Noah Webster & Brian Bianco (Akerman LLP)	23 March 2018
14	Trade Secret Governance: Aligning Policy & Procedure	Eyal Iffergan (Hyperion Global Partners)	5 June 2018
15	All About Trade Secret Management	Peter Ackerman (Decipher)	12 June 2018
16	Trade Secrets – What They Are And How To Protect Them	(JA Kemp)	15 June 2018
17	Protecting and Exploiting your Trade Secrets in 2018	Ash von Schwan (Bryan Cave Leighton Paisner)	19 July 2018
18	The Process for Managing Trade Secrets	Donal O'Connell (IPEG Consultancy)	27 September 2018
19	Trade Secrets Directive: practical steps to protecting trade secrets	(Simmons + Simmons)	29 October 2018
20	Protecting trade secrets during corporate transactions	Christopher K. Larus & Rajin Singh Olson (Robins Kaplan, LLP)	January 2019
21	Step Plan Trade Secrets Directive: Steps companies should take in order to protect their know-how	(Taylor Wessing)	16 April 2019
22	10 Best Practices for Trade Secrets Protection	(Baker McKenzie LLC)	19 April 2019
23	Sworn to Secrecy: Protecting Trade Secrets and Intellectual Property	Rachael L. Rodman (Ulmer & Berne LLP) & Peter A. Halprin (Pasich LLP)	1 June 2019
24	Trade Secret Protection for Customer Lists: A Checklist	Ann Motl (Fish & Richardson)	26 June 2019
25	The Increasing Importance of Trade Secrets and Trade Secret Asset Management Explained	Donal O'Connell (Chawton Innovation Services Ltd.)	20 July 2019
26	The Secret to Protecting Trade Secrets	(Winston Strawn LLC)	23 August 2019
27	Securing Against Trade Secret Pitfalls and Dangers Arising From Employee Mobility Situations	Eugene Mar (Farella Braun + Martel LLP) & Walton Norfleet (Smiths Group PLC)	8 October 2019

28	Developing a trade secret protection program to reduce risk and increase court enforcement	Mark Terman (Drinker Biddle & Reath LLP)	9 October 2019
29	What are Trade Secrets and How Can you Protect Them?	(Aeton Law Partners)	24 October 2019
30	How And When To Protect Trade Secrets	Todd Zimmerman & Abigale Griffin (Fredrikson & Byron)	18 February 2020

Table 1. Category 1 Literature: Non Academic Articles

The articles comprising the Category 1 Literature collectively recommended over 120 potential TSPMs. Having systematically reviewed and cataloged the TSPMs recommended in each article, it was possible to iteratively categorize them into the following seven categories, and 31 subcategories.

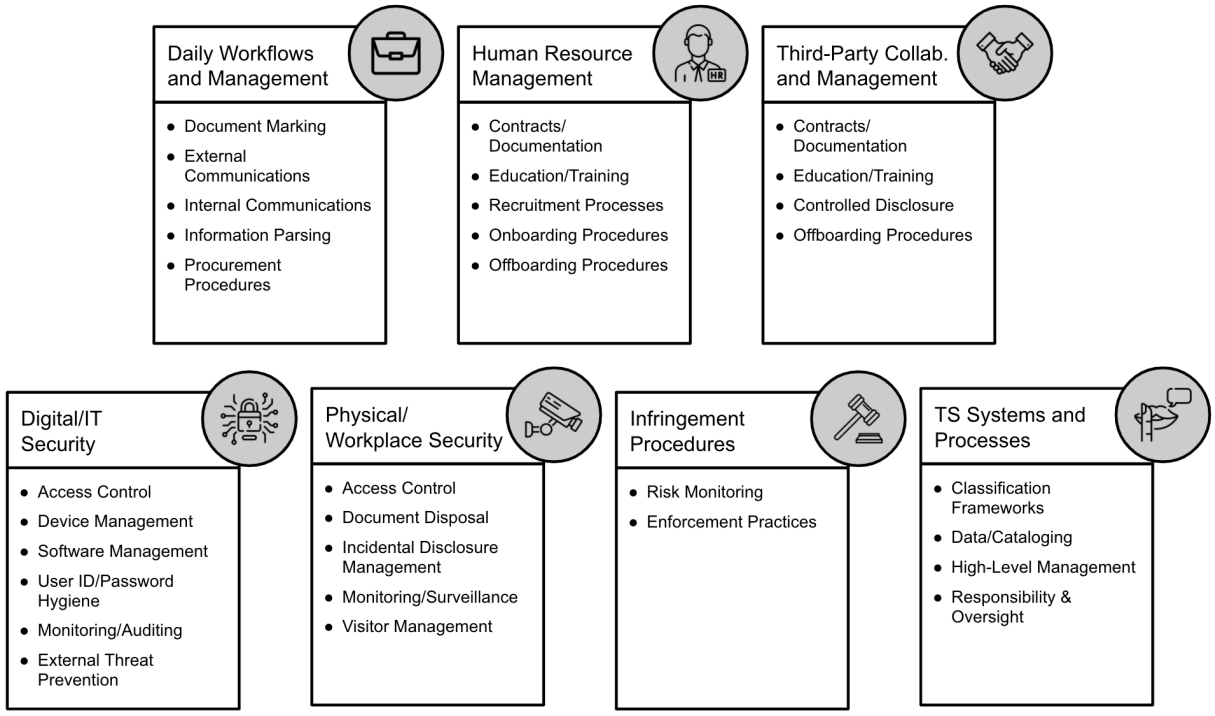


Figure 5. TSPM Categories derived from Category 1 Literature

Each of the seven categories is discussed below, while the full catalog is included as Appendix A.

TSPM Category 1: Daily Workflows and Management

This category can be broadly described as measures which can be incorporated into the day to day workflows and where the action required to implement them falls at the individual employee level. It includes general processes such as marking documents or files that contain trade secret IAs, as well as more detailed “best practice” recommendations about how such marking should be done — i.e. differentiating marking between different levels of sensitivity and confidentiality and ensuring that marking accurately and consistently reflects the contents (to avoid diluting the meaning). It also covers the measures which impact both internal and external communications, such as limits on meeting attendees and the recipients of information via group communication channels internally, and implementing external publication review procedures. Information parsing (the process of dividing trade secret IAs into pieces such that no single individual or team has access to/ability to reveal the whole thing) is also included in this category.

TSPM Category 2: Human Resource Management

It is widely acknowledged that a company's own employees pose one of the most significant risks of trade secret leakage (see for example discussion by Pooley, 2015). It also highlighted that, despite trade secrets being a legally enforceable category of IP (if protected with “reasonable steps”), trade secrets are largely predicated on managing human behaviors. Consistent with this, the Category 1 Literature included an extensive range of TSPMs focused on human resource management. Given that much of the Category 1 Literature was authored by lawyers/law firms it is also unsurprising that many of the recommendations in this area were focused on contractual obligations, including employee confidentiality, non disclosure, non solicitation and non compete. Encouragingly in light of the results of the empirical studies in the Category 2 Literature (discussed below), there were also a number of measures focused on education and training of employees, and building awareness during both onboarding and offboarding procedures.

TSPM Category 3: Third Party Collaboration and Management

This category covers the precautions that a trade secret holder can take when collaborating with third parties or licensing out trade secret IAs. Similar to the measures recommended in the area of human resource management, many of the recommendations in this area were focused on contractual obligations, most notably non disclosure agreements. It also included more detailed recommendations about the collaborations with third parties can be structured, including advice

on staged disclosure and recommendations on the precise clauses that should be included in licensing agreements which cover trade secrets. Beyond contracts and documentation, this category also included recommendations on education and awareness building and offboarding procedures at the end of third party engagements.

TSPM Category 4: Digital/IT Security

This category covers measures which relate to the digital and IT infrastructure that can be used as a means of protecting trade secrets. It includes some of the measures which are arguably the most impactful and controversial (especially in the context of agile development practices). In particular, many articles in the Category 2 literature advocate implementing digital access control measures on trade secret IAs on a “need to have” basis and/or restricting remote access to files containing trade secret IAs.

Perhaps a reflection of the fact that technology changes at such a fast pace, many of the measures in this category are very fundamental and (far from being controversial) are part of the basic hygiene of running a business in the modern world. For example, it is unlikely that any reasonably established or sophisticated company would need to be reminded of the importance of password protecting devices or setting up personalized User IDs for devices and accounts. Other recommendations in this category are already on the verge of obsolescence — e.g. prohibiting or restricting the use of USB flash drives may have been effective five years ago, but as we increasingly move IT systems to the cloud, the impact of this recommendation is limited. To avoid obsolescence of specific measures and avoid the complexity of IT systems, a significant number of articles deferred to making a general recommendation to develop, implement and maintain comprehensive information security systems to minimize the risk of cybersecurity infringements.

One of the points that this category of TSPMs highlights (and a point which was also raised during the interviews) is that there is an opportunity for trade secret management to piggyback on other business critical systems and processes.

TSPM Category 5: Physical/Workplace Security

This category covers the measures recommended in the Category 1 Literature to prevent the theft or leakage of trade secret IAs using physical means or by securing physical environments. Analogous to the digital access restrictions in TSPM Category 4, this includes the

recommendation to implement physical access control measures on trade secret IAs on a need to have basis. This measure, along with others focused on physical access control in this category, has clear relevance to industrial companies that are seeking to protect the know-how behind tangible processes — for example manufacturing methods, foodstuff ingredients, or the precise composition of chemical compounds.

Other measures in this category include carefully managing document disposal, conducting surveillance, limiting and/or managing visitor access to the workplace. One particularly interesting recommendation to avoid incidental disclosure is to limit or avoid the physical expression of confidential information within the workspace — e.g. via signage laying out strategic plans or insights or by erasing whiteboards after team discussions.

It is difficult to see the relevance of many of the measures in this category to agile technology companies — especially those which are focused on developing intangible software based products or services. However, in drawing any conclusions on this, it is necessary to distinguish between the technology type (e.g. intangible vs tangible) and the operational model or production practices (e.g. agile vs waterfall). While there is an interaction effect here — i.e. intangible products and services by their very nature have higher flexibility and speed of development than tangible products or services — it is not necessarily the case that companies which produce them have adopted agile development processes.

TSPM Category 6: Infringement Procedures

This category of TSPMs focuses on how to handle or specifically monitor/investigate instances where there is an actual or high likelihood of trade secret leakage, theft or misappropriation. It includes more high level recommendations to develop an action plan to react to such events, as well as more targeted and proactive measures — for example, identifying and monitoring the business/R&D activities of the new employers of recently departed employees (particularly those who have been exposed to trade secret IAs). Given the focus on how to effectively manage trade secrets to prevent or minimize the risk of infringement (with a view to maintaining a secrecy based control position), this category is less relevant to the current study.

TSPM Category 7: Trade Secret Specific Systems and Processes

The final category of TSPMs are those that focus specifically on the trade secret specific systems and processes that can be implemented with a view to increasing the strength of

protection/minimize the risk of leakage. These include developing systems/frameworks to classify trade secret types or assist the business in identifying which of its assets qualify for trade secret protection. It also includes a range of detailed measures related to trade secret data (and metadata) collection and cataloging, together with high level management goals and recommendations on who, within an organization, should bear responsibility for/oversee trade secret management.

Category 2 Literature: Academic Articles

The Category 2 Literature consists of 21 academic/peer reviewed journal articles on the topic of trade secret management. As mentioned above, within the broader field of IP management research, trade secret management is a relatively nascent subfield. Nonetheless, the Category 2 Literature covered a broad spectrum of studies — including several theoretical model based studies, some conceptual discussions/essays, and some empirical evidence based studies. Thus, despite the small sample size, the Category 2 Literature presents a (reasonably) holistic view of the available research on the general conditions required for effective trade secret management. An overview of the Category 2 Literature is set out below in Table 2.

	Title	Author/s	Journal	Year
1	Trade secrets and information sharing	Ronde, T	Journal of Economics & Management Strategy	2001
2	A theory of trade secrets in firms	Zabojnik, J	International Economic Review	2002
3	Little patents and big secrets: managing intellectual property	Anton, JJ; Yao, DA	RAND Journal of Economics	2004
4	The strategic management of trade secrets in technology-based firms	Hemphill, TA	Technology Analysis & Strategic Management	2004
5	Should I keep a secret? The effects of trade secret protection procedures on employees' obligations to protect trade secrets	Hannah, DR	Organization Science	2005
6	Preserving trade secrets between competitors in B2B interactions	Malik, Z; Bouguettaya, A	International Journal of Cooperative Information Systems	2005

7	Protecting know-how and trade secrets in collaborative R&D relationships	Slowinski, G; Hummel, E; Kumpf, RJ	Research-Technology Management	2006
8	An examination of the factors that influence whether newcomers protect or share secrets of their former employers	Hannah, DR	Journal of Management Studies	2007
9	On the Virtues of Secrecy in Organizations	Dufresne, RL; Offstein, EH	Journal of Management Inquiry	2008
10	The management and security of trade secrets: an exploratory study	Stead, DR; Cross, AR	International Journal of Intellectual Property Management	2009
11	Cui Bono? The Selective Revealing of Knowledge and Its Implications for Innovative Activity	Alexy, O; George, G; Salter, AJ	Academy of Management Review	2013
12	Bringing Secrecy into the Open: Towards a Theorization of the Social Processes of Organizational Secrecy	Costas, J; Grey, C	Organization Studies	2014
13	Why and How Do Employees Break and Bend Confidential Information Protection Rules?	Hannah, DR; Robertson, KM	Journal of Management Studies	2015
14	A dynamic view on secrecy management	Bos, B; Broekhuizen, TLJ; De Faria, P	Journal of Business Research	2015
15	We're leaking, and everything's fine: How and why companies deliberately leak secrets	Hannah, DR; McCarthy, IP; Kietzmann, J	Business Horizons	2015
16	The secret to protecting trade secrets: How to create positive secrecy climates in organizations	Robertson, KM; Hannah, DR; Lautsch, BA	Business Horizons	2015
17	Trade secrets: Managerial guidance for competitive advantage	Crittenden, WF; Crittenden, VL; Pierpont, A	Business Horizons	2015
18	How to Share “a Really Good Secret”: Managing Sharing/Secrecy Tensions around Scientific Knowledge Disclosure	Nelson, AJ	Organization Science	2016
19	Spill Your (Trade) Secrets: Knowledge Networks as Innovation Drivers	Pedraza-Farina, LG	Notre Dame Law Review	2017

20	Protecting knowledge: How legal requirements to reveal information affect the importance of secrecy	Sofka, W; de Faria, P; Shehu, E	Research Policy	2018
21	Secrets and Knowledge Management Strategy: The Role of Secrecy Appropriation Mechanisms in Realizing Value from Firm Innovations	Hannah, DR; Parent, M; Pitt, L; Berthon, P	Journal of Knowledge Management	2019

Table 2. Category 2 Literature: Academic Articles

A table presenting details of the type, sample and method, key issues examined, results/conclusions and relevant themes that emerged from the research presented in the Category 2 Literature is included as Appendix B. A discussion of the key themes that emerged from a systematic review of the Category 2 Literature are set out below.

Secrecy's Impact on Productivity

A key assumption underpinning this study is that, in the context of agile technology companies, reliance on trade secrets as a structural control position will inevitably reduce the speed and/or inhibit the autonomy of product development teams. The Category 2 Literature broadly acknowledged that the trade off between secrecy and productivity exists to some extent irrespective of the operating model of the firm. Indeed, the earliest study by Rønde (2001) models the impact of one TSPM (information parsing) on firm productivity and employee retention. The models are based on industrial processes (one example given is the production of Michelin tires), where different aspects of the physical production process can be parsed between different teams/individuals. The key finding being that it may be optimal to limit the number of employees who have access to trade secret information, even if it reduces the firm's productive efficiency. It is not clear how/if this approach could be adapted to effectively protect trade secrets in the context of agile software development.

A more contemporary study by Robertson et al. (2015) purports to provide the "secret to protecting trade secrets" by creating positive secrecy climates — i.e. "places where organizational secrets are strongly valued by employees and seen as a part of their formal role responsibilities" (p. 671). While the cultivation of a positive secrecy climate model may be an effective and worthwhile way to protect trade secrets, the model also highlights significant negative of such a culture — i.e. that knowledge sharing at an organizational level is likely to be reduced, including the possibility that

even information that needn't be kept secret will circulate less freely. The literature review by Hannah et al. (2019) focused on the nature of "secrecy appropriation mechanisms" and their role in supporting innovation also acknowledges the negative effects such measures can have on a number of organizational dynamics, including productivity.

Secrecy as a Structural Imperative

Another theme that emerges from a review of the Category 2 Literature is that secrecy is a positive (or at least necessary) component of most organizations (if not all human relationships). The virtues of secrecy in organizations are discussed directly by Dufresne and Offstein (2008) who highlight that secrecy is a positive and necessary component of business strategy, most notably for its powerful role in maintaining control over valuable resources. This resonates with the central hypothesis of Anton and Yao (2004) and Bos et al. (2015) on the role of secrecy as a mechanism for appropriating value from innovation. The emergence of this theme from the Category 2 Literature also aligns with the broader academic discussion (mentioned above) around secrecy being a very important and effective appropriation mechanism (Choi et al., 2019; Cohen et al., 2000).

Costas and Grey's (2014) conceptual work on the role of both formal and informal secrecy in organizations, also resonates with this theme. They highlight that the role of secrecy goes beyond its function in protecting valuable information, but also "about social aspects of organizational life, such as the cementing of group identity" (p. 1424). Meaning that beyond being an important and effective appropriability mechanism or structural control position, secrecy can be a means of creating feelings of cohesion and belonging between colleagues and teams.

In terms of secrecy's role in IP strategy, Stead and Cross' (2009) empirical research found that, among experienced IP professionals, patents and trade secrets are viewed as compliments (not substitutes). The histographic review by Crittenden et al. (2015, p. 6) provides a nuanced view of the strategy that can underpin the decision to protect an IA as a trade secret and their important role in creating "deep and wide economic moats" for all types IAs at all types of companies. This highlights that, alongside other IPRs, trade secrets are a useful and necessary tool for capturing and controlling IAs.

Disclosure as a Strategic Decision

Another theme that emerges from the Category 2 Literature is that the opposite of secrecy — disclosure — can also be strategically advantageous. This is obviously the case when a firm chooses to collaborate with third parties — a scenario examined by Slowinski et al. (2006) who authored a paper similar in style to much of the Category 1 Literature but with recommendations grounded in empirical research. Alexy et al. (2013) discuss four instances when the decision not to protect information as a trade secret, but rather take the opposite approach by "selective revealing" can be a powerful mechanism to reshape collaborative behaviors and gain competitive advantages. Similarly, Hannah et al. (2015) highlight that “deliberately leaking” information can be a means of creating value and gaining a competitive advantage. Framed in the context of a research setting, the paper by Nelson (2016) also includes disclosure (either strategically parsed, delayed, or via a patent filing) as a means of balancing the benefits and detriments of sharing scientific research results.

Holistic and Dynamic Trade Secret Management

Perhaps the strongest theme that emerged from the Category 2 Literature is that, in order to be effective, trade secret management must be multifaceted and cannot be viewed as a one time decision or static configuration of strategic measures. Slowinski et al. (2006) describe the challenge of managing trade secrets in the context of joint technology development projects as two fold, involving (i) well crafted legal agreements entered into in timely phases as the project evolves and (ii) managing human behaviors (i.e. training and communication). However, the wider body of research in the Category 2 Literature suggests that it is even broader than this. For example, in describing the strategic management of trade secrets as influenced by the legal, organizational and market environments, Hemphill (2004) provides a framework to guide a logical approach to reaching a managerial choice of trade secrecy over other forms of IP protection. Importantly, Hemphill’s approach highlights that trade secret management does not happen in a vacuum. In order to be effective, it must be guided by the push and pull of multiple factors and balance competing interests, both internal and external.

Research by Stead and Cross (2009) seeks to illuminate some basic questions about trade secrets — what are they, who typically knows them, and how secrecy is maintained in a typical business? They conclude that trade secrets (specifically valuable confidential information) can exist at all levels of an organization, but the level of specificity known and incentives that promote

the maintenance of trade secrets at different levels of the hierarchy varies significantly. They also find that trade secrets tend to have a life cycle. Though, in law, they are immortal, they do not typically last forever meaning that decisions about investing in their protection should be iterative and ongoing.

The model developed by Zabojnik (2002) examines the implications of wage structures and employee remuneration on trade secret management. Though the scope of the study is narrow, a key conclusion is that simply paying higher salaries will not efficiently negate the risk of trade secret leakage via employee attrition. There is no silver bullet solution. Rather, it is necessary to take a holistic approach to trade secret management which pulls on various levers — including, but certainly not limited to, competitive salaries and benefits — to encourage and incentivize the protection of trade secrets.

The work by Alexy et al. (2013), Hannah et al. (2015) and Nelson (2016) which all examine the strategic advantages that can be gained by controlled disclosure, supports the notion that trade secret management should not be viewed as an absolute or finite decision. But rather, it is necessary to weigh the various pros and cons of maintaining the trade secret and taking into account the multifarious factors which impact a decision to conceal or share it. A similar point is made by Bos et al. (2015) who present trade secret management as a lifecycle process rather than a one time decision and provide a helpful dynamic framework through which to view this.

Balanced Trade Secret Management

In addition to being holistic and dynamic, a key theme emanating from the Category 2 Literature is that trade secret protection procedures should be in balance and implemented in moderation — a.k.a. there is such a thing as too much trade secret protection and if TSPMs are too numerous or too onerous they could undermine their original purpose. Hannah and Robertson's (2015) research on the questions of why employees bend or break rules intended to protect confidential information indicates that there is such a thing as "overkill" when it comes to trade secret management. Their empirical findings show that *more* TSPMs does not necessarily mean more effective protection. Rather, their work underscores that the goal of any trade secret protection program is to have enough protection, not as much as possible. A specific example of the potentially destructive effects of too much trade secret protection is an interesting finding by Hannah (2007). His research found that non compete agreements (a frequently recommended

Human Resource Management TSPM in the Category 1 Literature) actually have a negative impact on employees' perceived obligation to maintain their former employers' trade secrets.

According to the Category 2 Literature, the need for a balanced (or even restrained) approach to trade secret management is also true at a purely economic level — as Zabojnik's (2002) model indicates, managers may have an incentive to protect their firms' trade secrets more than is optimal. A key message from the work by Hannah et al. (2019) is that not all of the measures that exist to protect trade secrets (i.e. the 120+ identified in the Category 1 Literature) will actually be meaningful in protecting trade secrets in any given context. Rather the objective is to identify which IAs are worth protecting and selecting sufficiently robust TSPMs that are most likely to be followed and have a minimal downside for the competing operational and strategic objectives of the firm.

Employer/Employee Trust

One of the most active scholars in the field of trade secret management is David Hannah. One of the core tenets within his work is that trade secret management is closely linked to the relationship of trust that (ideally) exists between employers and employees.

The earliest of Hannah's papers within the Category 2 Literature (Hannah, 2005) examines the impact of organizations' formal efforts to protect trade secrets (via either "access restrictions" or "handling procedures") on employees' beliefs about their obligations to protect those secrets. The empirically based findings were that employees' levels of familiarity with access restrictions were negatively related to their feelings of obligation to protect trade secrets. Meanwhile, familiarity with handling procedures was positively related to the obligations employees felt to protect trade secrets. The implication being that trade secret management (at least as it pertains to managing employee behaviors) is closely linked to building a level of reciprocal trust. Practically, Hannah's findings indicate that a good approach may be to limit the number and extent of any access restrictions and instead focus on developing and implementing handling procedures, together with robust education/awareness building campaigns (discussed in further detail below). Also, if or when access restrictions are necessary, it is important to message that the existence of the access restrictions does not mean that the employee is not trusted.

Building on this, Hannah (2007) explores the influence of psychological contracts and the expectations of reciprocity therein. He concludes that a perceived violation of the psychological

contract by the employer (in the mind of the employee) leads to reduced feelings of obligation to maintain trade secrets. Hannah and Robertson (2015) found that employees are more likely to comply with rules on the protection of confidential information that they perceive as justified. This highlights that the feelings of trust must be reciprocal in order to be effective. The work by Robertson et al. (2015) (to which Hannah was also a contributing author) also highlights that building loyalty and trust among employees is a key factor in the creation of positive secrecy climates.) Their advice on the creation of positive secrecy climates is based on the key premise that “if managers want to protect their organizations’ trade secrets, they cannot simply implement strict rules. Instead, they must convince employees about the importance of trade secret protection” (p. 671). This speaks to the fact that effective trade secret management is not as simple as developing and enforcing policies and guidelines.

This theme was also discerned across two other studies within the Category 2 Literature. While expounding the virtues of secrecy, Dufresne and Offstein (2008) acknowledge the tension that exists between it and openness. Given the necessity of some degree of secrecy, it is up to managers, they say, "to strike a balance between compartmentalization on the one hand and expansive, transparent knowledge sharing on the other” (p. 104). Costas and Grey (2014) observe that in “creative organizations with flat hierarchies … secrecy is likely to be regarded as anomalous and even illegitimate” (p. 1434). They highlight the particular challenge of trying to retain a culture of trust while imposing TSPMs that inhibit the flow of information — especially in organizations which “put a premium on internal knowledge sharing” (p. 1434). (A practice which is very commonly associated with agile technology companies.)

On the other hand, Costas and Grey (2014) also posit that the social process of keeping something secret can be a tool for building trust within an organization. This aligns with one of the findings from Hannah (2007) that the outcome of protect vs. share decisions is linked to humans' innate need to develop a sense of identification and acceptance within new social groups. This tends to support the notion that an effective approach to trade secret protection may be to focus on secrecy as means of consolidating feelings of belonging by individuals within an organization while distancing outsiders (i.e. leveraging an “us vs them” mentality).

Education and Awareness Building

The final theme that emerges from the Category 2 Literature is that education and awareness building is a critical cornerstone of truly effective trade secret management. At a basic level,

Hannah (2007) found that employee's perceptions of what does or does not constitute a trade secret is not necessarily aligned with legal definitions. This is a simple and obvious indicator of the importance of education and training in any trade secret protection program. More generally, education and awareness building is required in order to achieve the level of reciprocal trust that the findings of Hannah and Robertson (2015, p. 410) show are a catalyst for compliance. If employees have the opportunity to understand the reason behind TSPMs which might otherwise impact their day to day work, they will be more willing to "tolerate the tension that they create".

Robertson et al. (2015) also highlight the importance of winning both hearts and minds in an attempt to securely safeguard trade secrets. Their advice on the creation of positive secrecy climates centers on getting employees to understand not only what trade secrets are, but also why they are important and how they are expected to behave in order to protect them. They draw attention to the fact that simply having numerous policies in place and substantial punishments prescribed for breaches of secrecy is not necessarily the hallmark of an organization with robust trade secret protection. Rather, the most effective approach is to cultivate a culture where (in addition to a level of trust in leadership) employees have a high level of familiarity with, understanding of, and respect for trade secret protection procedures.

Concluding Observations on Systematic Literature Review Results

The Category 1 Literature demonstrates that there is a wide array of practical measures available to manage trade secrets — some of which are part of the basic hygiene of running a modern business, but many which go beyond the normal day to day operations of many organizations and may be adopted with a view to protecting valuable IAs as trade secrets. The fact that the Category 1 Literature collectively contains over 120 discrete TSPMs highlights the fact that no single article written for a general audience can profess to hold the absolute solution or best practice approach for managing trade secrets in any given context.

The Category 2 Literature provides insight into the role of secrecy (and disclosure) in business. It highlights that while secrecy can negatively impact productivity, it is also a strategically important and necessary component to all organizations. That is not to say that everything should be kept from public view. Indeed, disclosure of certain information and IAs can be a powerful tool — especially when used mindfully and strategically in pursuit of a recognized competitive advantage. The Category 2 Literature also provides useful guidance on the general shape and objectives of effective trade secret protection efforts. First they should be holistic, dynamic, and balanced. Also,

they should be closely linked to and focused on establishing employer/employee trust. Finally, a key means of achieving this is via education and awareness building.

When taken together, the Category 1 and 2 Literature provide a useful framework for approaching the challenge of trade secret management in general, not specific to the context of agile technology development. The Category 1 Literature serves as a sort of à la carte menu from which various TSPMs can be selected, implemented (and discarded) dynamically depending on the context. Meanwhile, the Category 2 Literature provides guidance on the overarching objectives that should be front of mind when shaping trade secret protection procedures in order to maximize their effectiveness and efficiency.

4.2. Semi Structured Interviews

The results of this method are set out below with reference to the second order observations that emerged from the interview data. This section ends with some concluding observations made in relation to the results of the data gathered via all of the semi structured interviews conducted and its relationship to the results of the systematic literature review.

"Reasonable steps" are contextual

The first theme which emerged very clearly from the interview data is the importance of the inherent flexibility within the legal standard of "reasonable steps" that a trade secret owner must take in order to obtain recompense in the event of trade secret misappropriation. By design, this legal standard is highly contextual and this should be to the advantage of agile technology companies. The way a company manages its trade secrets is inextricably linked to the way it conducts business. In this way, "reasonable steps" is at the core of trade secret management.

Therefore, an agile technology company which optimizes for speed and autonomy of its development teams by cultivating a high level of internal transparency and openness, should not be expected to take the same steps to protect its trade secrets as a company which conducts business by intentionally siloing information between departments and/or management levels. As one respondent put it "'old school' protections may have been reasonable for 'old school' companies", but that doesn't mean they should be the blueprint for all trade secret management.

This renders some of the TSPMs recommended in the Category 1 Literature obsolete. For example, the process of cataloging and estimating the value of most of the IAs developed by agile

teams included in TSPM Category 7) will usually take a disproportionate amount of time and resources — especially when (as is discussed below) many potentially trade secret IA developed in this context have a very short shelf life.

As was also discussed in relation to the TSPM Category 5 concerning physical/workplace security, the nature of the product or service under development is also highly relevant to the question of “reasonable steps”. The concept that physical location of employees is irrelevant to most modern technology companies (amplified by the highly distributed nature of the global workforce due to COVID-19 pandemic, ongoing at the time of writing) does not equally apply to a software company seeking to claim trade secret status for a proprietary dataset stored in the cloud and a hardware company developing the prototype for a new device. Rather, the notion of what is reasonable is dependent on a range of contextual factors, including but not limited to, the development methodology.

Trade secret management is dynamic

While an important advantage, the nature of reasonable steps as a moving target is also a pressing challenge for trade secret management in the context of agile technology development. Two clear concepts that emerged here were that there can be no “one size fits all” approach and general “Do Not Share” policies are unhelpful. Rather, much like the iterative nature of agile development cycles themselves, trade secret management in this context requires a constant process of adjustment and realignment. This was the second theme to emerge from the interview data and is particularly notable due to its resonance with the results of the Category 2 Literature review.

The empirical data gathered during the interviews supported the Category 2 Literature review results indicating that not all trade secrets have a long shelf life. The decision to keep something as a trade secret should be constantly revisited because something may be worth concealing now, may not warrant concealment forever. Beyond this the interview data suggests that sometimes the best "protection" for trade secrets in an agile context is to simply to continuously replace them by ensuring that any secrets that are made public or leaked to competitors (e.g. by reverse engineering or departing employees) are rendered redundant due to the sheer speed of ongoing innovation and technological development.

Internal information flows are critical

Just because agile technology companies tend to embrace transparency and openness, does not mean that they get a free pass to claim anything and everything they develop as a trade secret. The other two criteria of “secret” and “commercial value (because of secrecy)” still apply. Therefore, if trade secrets are to be relied upon as a structural control position, some degree of control over information flows is necessary. The interview data suggests that the best approach to this is to embrace internal openness while focusing on trade secret protection efforts on controlling flows of information externally/outside the company “walls”. This approach preserves the opportunities for incidental absorption of information which several interviewees valued very highly as a means of sparking creativity and giving rise to innovation. The interview data also suggested that in terms of impact on corporate culture, measures that involve distancing external people are less potentially damaging.

In this scenario, a possible approach presented in the interview data is to simply treat all potentially trade secret information as internally confidential — i.e. without distinguishing between the strategic value or level of protection for any individual IA. Alternatively, several interviewees signaled that a layered structure to internal information sharing could be useful wherein some distinction is made between information which is “nice to know”, “work adjacent” and “need to know”. In this structure, the level of detail shared decreases as the scope of sharing increases. Under this approach, the wide internal communication of so called “North Star Goals” (which is important for allowing agile autonomous teams to align their work in pursuit of particular strategic objectives) is not necessarily incompatible with trade secret management.

TSPMs can leverage other systems and processes

A further theme which emerged from the interview data was that trade secret management cannot occur in a vacuum. Rather, it can and must interact with other systems and processes. This overlaps with the concept (outlined above) that the way a company manages its trade secrets is inextricably linked to the way it conducts business.

Indeed, TSPMs can purposefully “piggyback” on, or more passively, be a positive by-product of other systems and processes — especially data governance processes and compliance (particularly privacy regulation compliance) measures. For example, despite the fact that all four companies involved in this study successfully incorporate agile methodologies into their

development processes and optimize ruthlessly for speed of execution, all of them have some degree of existing internal access controls in place. These are an essential means of achieving one or more operational imperative for their business, but not specifically for managing trade secrets. In the context of agile technology companies, where TSPMs may tend to be viewed as an unwelcome layer of bureaucracy or hindrance to operational efficiency, there is a significant opportunity here. Namely, to leverage these existing structures for the benefit of trade secret management but without adding additional burdens or blockers.

The interview data also highlighted that the biggest risk of trade secret leakage pertains to what is held within people's (i.e. employees, past and present) heads. Hence, human resource management systems and processes — particularly as they pertain to departing employees — are a key area that can be leveraged to protect trade secrets.

TSPMs can support agile development

Quite the opposite of being perceived as a hindrance to operational efficiency, the interview data also highlighted that TSPMs have the capacity to support agile development teams. Indeed, a number of interviewees identified that "good" trade secret management can aid speed and autonomy. For example, specific TSPMs such as access restrictions and document marking can make it clear that a specific asset can be utilized freely or must be handled in a specific way. On the other side of the coin, clear and widely communicated trade secret management processes can help teams to identify what is truly valuable to the organization and empower them to be more proactive and intentional about how it can be protected. Moreover, the interview data gave rise to the concept that creating a culture of sharing (even externally) can result in a clearer understanding among individuals and teams about what, when and why specific assets can or should not be shared — i.e. the opposite of the unhelpful general "Do Not Share" policies mentioned above.

Trade secret management is a shared responsibility

A premise that is supported by both the Category 1 and 2 Literature is that, in order to be effective, trade secret management must be cross functional and not the sole responsibility of one individual or team. The interview data suggests that in the context of agile technology companies (especially those with a culture of radical openness and transparency), trade secret management should be beyond cross functional. Rather, it should be viewed as everyone's shared responsibility. This is

consistent with the autonomy that is typically extended to agile teams. It also aligns with the concept that disclosure decisions are usually business decisions and that such decisions should be made at the lowest possible level within agile organizations — i.e. by the people who are closest to the information and data required to make the best decision.

This bottom up philosophy is tempered by the interview data which also supports the concept that there needs to be a level of executive buy in on the importance of some degree of control over disclosure in order for any form of trade secret management to be effective.

IP function should facilitate and enable

In light of this cross functionality, one of the most illuminating themes to emerge from the interview data is the role of the IP function (i.e. the team or person responsible for IP generally) in managing trade secrets in the context of agile technology companies. Despite the fact that trade secrets are a form of IP, it cannot be solely up to the IP function to see that they are properly protected and maintained.

Rather, the IP function should be the path of escalation for questions or issues that arise in relation to trade secret management. In that role, they should seek to facilitate conversations and support the decision making process around whether to disclose or retain strategically important IAs as trade secrets. This is fundamental because (as mentioned above) disclosure decisions are usually business decisions. While the IP function may be well placed to act as guardians of the business' best interests in these situations, the strategic value of disclosing a (potential) trade secret is not always apparent to "the lawyers" (which many IP professionals tend to be).

Autonomous teams need flexible support with trade secret management. As such rigid policies or guidelines are of limited use. It is also true that, from an enforcement perspective, there is a lot about trade secret management that should not be written into formal policies (because failure to enforce written policies, if they exist, tends to be viewed negatively by courts in the event of a litigious secret dispute.) So rather than writing up formal trade secret protection policies (and then stringently policing their compliance), the role of the IP function should be focused on empowering teams with knowledge about trade secrets and enabling positive behaviors.

Concluding Observations Semi Structured Interview Results

The results of the semi structured interviews build on both the menu of TSPMs provided by the Category 1 Literature and the research based guidance on the overall shape and objectives of effective trade secret management provided by the Category 2 Literature. In particular, the concepts and observations which emerge from the interview data provide specific insight to the most important considerations when approaching the challenge of trade secret management in the specific context of agile technology development.

Helpfully, the legal standard of “reasonable steps” is contextual. In the context of agile technology companies, where internal information flows are critical, the TSPMs required to meet this standard should be viewed differently to the old school companies where siloing information was not completely incompatible with their business and operational models.

Though at first blush, TSPMs may be viewed as added red tape or innovation blockers in agile companies, there is an opportunity for them to interact with and leverage off of other systems and processes. If implemented mindfully, certain TSPMs can even support agile development by bringing an organization's valuable IA into sharper relief and adding clarity around the behaviors required to ensure that they retain their value.

To make this work, trade secret management must be dynamic and viewed as a shared responsibility. In this context, the role of the IP function is to facilitate conversations and enable behaviors which protect and promote the best interests of the business.

5. Discussion

This chapter aims to interpret and explain the research results and their relevance. It highlights the major findings, comments on how the results answer the research question, discusses the contribution and limitations of the study and proposes recommended areas for future research.

5.1. Highlights of Major Findings

The old adage “loose lips, sink ships” originated during World War II from the US Office of War Information. It was a patriotic creed meaning that unguarded talk may give useful information to enemy spies. It is unlikely that the US Office of War Information would have endorsed the agile methodology. But, the fact is that today, many agile technology companies gain a great deal by embracing transparency and openness and leveraging the speed and autonomy it enables. Indeed, encouraging loose lips (at least internally) has allowed these companies to efficiently build some pretty great things and unlock a competitive edge that more tight lipped organizations may struggle to attain.

In light of this, it is worth seriously considering whether trade secrets can realistically be relied upon as a structural control position by companies which adhere to agile development methodologies. Perhaps companies that take the decision to optimize for speed and autonomy by embracing transparency and openness, must simply accept that trade secrets are incompatible with their business model and instead focus on managing their valuable IAs via rights based IPRs (patents, copyright, trademarks, designs) or other structural control positions. Another option is to abandon any attempt to control, and rely purely on speed of execution to continually outpace competitors. Thereby ensuring that IAs which could have been suitable for trade secret protection are regularly replaced, rather than strenuously protected.

However, as discussed in the introduction to this study, many of the IAs generated by agile technology companies — for example, proprietary algorithms, machine learning models, unique datasets, and valuable data derived insights — are not suitable for protection via rights based IPRs. At the same time, the idea that these strategically important assets would be left entirely unprotected should be enough to make even the most cavalier “techbro” lose sleep! So, the question remains, how can the management of trade secrets be effectively and harmoniously integrated into the product development practices at agile technology companies?

The results of this study indicate that there are three key components (which correspond to the Aggregate Dimensions of the interview results) to answering this question. Each will be discussed below in turn.

Walled Gardens

Much of the common rhetoric around trade secret management focuses on limiting access to trade secret IAs on a “need to know” basis. This phrase brings to mind strict information silos where different individuals or teams are set to work on a specific task or project, with predefined objectives, milestones and metrics, and limited insight or knowledge as to how this aligns with what other individuals or teams are working on or fits within the broader strategy of the organization. A famous example of this is Apple — clearly a very successful company and one that Robertson et. al. (2015, p. 671) refer to as having had a “positive secrecy climate since its inception”. As discussed above, Apple has notoriously siloed product development practices. It is rumored that Apple employees are not allowed to disclose any details of the product area they’re working on, even to colleagues within the same company (MacInnis, 2017). In such contexts “need to know” is clearly limited to very small and defined groups. But in the context of agile product development, where there is a focus on teams working autonomously to solve problems and achieve defined and widely communicated North Star Goals, this extreme practice of information siloing is simply incompatible. In this context, for people to do their job, they literally need to know a broader spectrum of information and have access to a larger body of potentially valuable IAs. So how can this be achieved without forgoing any recourse to trade secret protection for strategically important IAs?

As with any good IP strategy, the way you manage trade secrets should be inextricably linked to the way you run your business. As agile technology companies have generally made a decision to optimize for speed and autonomy by placing a high value on transparency and openness, it is not practical to implement TSPMs that mandate siloed information and stringent access controls. The alternative approach that emerged from this study is analogous to a walled garden. That is, trade secret management in the context of agile technology companies should retain the level of internal openness that is suitable for each unique business and focus on building and continually fortifying clear and strong external boundaries. This allows for information to flow freely inside the company and preserves valuable opportunities for incidental exposure to information and knowledge which, while not strictly within the purview of an individual or team, may result in new

sparks of creativity or innovation. This is analogous to the healthy growth, biodiversity, and opportunities for cross pollination that occur in a flourishing garden.

In terms of the relevant TSPMs, the focus must be on closing the gates and protecting the outer walls. This means that agile companies should focus their attention on TSPM Category 3 to ensure that their assets are robustly protected when collaborating with third parties or licensing out trade secret IAs. Of equal importance is TSPM Category 2 (Human Resource Management), especially those measures which focus on including enduring non disclosure and confidentiality obligations in employment agreements and processes for offboarding departing employees. As far as they relate to limiting trade secret theft or leakage from external threats, several measures from TSPM Categories 4 (Digital/IT Security) and 5 (Physical/Workplace Security) are also clearly relevant and appropriate.

These recommendations are consistent with the empirical finding of this study that TSPMs which involve distancing external people (rather than creating internal barriers) are likely to be less impactful to agile product development practice. Not only does this resonate with the finding (from the Category 2 Literature) that secrecy plays an imperative role within organizational life (see the discussion on Secrecy as a Structural Imperative in Part 4.1), it is also generally compatible with the operational imperatives of agile technology companies.

Embracing internal openness does not imply that all internal facing TSPMs should be avoided. Indeed, the empirical findings of this study also suggest that secrets are not (always) the enemy of speed and autonomy. Indeed, when implemented appropriately certain TSPMs in TSPM Category 1 (Daily Workflows and Management) have the capacity to aid agile product development practices. For example, some level of access restrictions can help to reduce the noise of internal documentation and/or discussions allowing individuals and teams to access information that is relevant to them more efficiently. Similarly, implementing handling procedures (e.g. document marking guidelines) can have the effect of more clearly communicating and clarifying expected behaviors. This demonstrates that, in companies where information sharing is part of successfully doing business, blanket policies that forbid any type of sharing or access can be especially unhelpful. But carefully selected TSPM can actually support the workflows of agile teams — much like careful pruning and calculated landscaping can clear the weeds and encourage new growth.

Hearts and Minds

To extend the garden analogy, employees' minds are the biggest open gate. What they disclose (either intentionally or unintentionally) is the biggest risk to the protection and maintenance of trade secrets. This is true at most organizations, not just agile technology companies. That said, the second key component to managing trade secrets in the context of agile technology development is to understand that the core task is to manage human behaviors.

A significant finding of this study (particularly from the Category 2 Literature) was that employee perceptions of trust (both in their trust in their employer and their employers' trust in them) is essential to the effectiveness of any trade secret management practices. As a result, possibly the most important aspect of trade secret management is winning people's hearts and minds. In practical terms, this means that agile technology companies should focus on TSPMs (particularly those in TSPM Category 2: Human Resource Management) which focus on educating and building awareness among new recruits and existing employees. TSPM Category 3 (Third Party Collaboration and Management) also highlights that beyond standard contracts and documentation, education and awareness building can also be a means of reducing the risk of trade secret theft or leakage during external collaborations or partnerships.

Education and awareness building also forms a critical part of the role of the IP function at agile technology companies seeking to implement effective trade secret management practices.

Bee Keeping

Finally, this study has shown that, in the context of agile technology development, the fundamental role of the IP function in managing trade secrets is to facilitate conversation and enable behaviors that are in the best interests of the company. Despite what some of the articles in the Category 1 Literature would have readers believe, there is no one size fits all solution to trade secret management. Agile teams need particularly flexible and dynamic support when it comes to trade secret management.

This is especially true in light of the fact that most trade secrets are not immortal, but rather they tend to have a life cycle and will usually expire or become obsolete. In the context of agile development, which is built around iterative cycles of continuous improvement, this is likely to be even more true. This begs some examination of the true value of several of the measures in TSPM Category 7 (Trade Secret Specific Systems and Processes) in the context of agile

technology companies — particularly those that involve diligently collecting data, cataloging and estimating the value of trade secrets. The empirical evidence collected in this research found that this is likely to require a disproportionate amount of time and resources in the context of agile technology development.

Rather, in supporting agile teams, there is an opportunity for the IP function to leverage the systems and processes already in place. For example, in many agile technology companies that have reached a certain size and level of organizational sophistication privacy compliance and data governance structures can have the additional function of helping to manage and protect trade secrets. This opportunity is also exemplified by the fact that the vast majority of the TSPMs that were cataloged from the Category 1 Literature are well outside the remit of the IP function — for example, HR, IT, Workplace Services etc. This finding is particularly relevant to TSPM Category 4 (Digital/IT Security) which includes various measures which would be considered basic hygiene for most modern companies but demonstrate how existing infrastructure can be leveraged to protect trade secrets.

Ultimately, while the IP function is an important advocate for trade secret management it must also work with and rely on various stakeholders across the organization. From this position, the core task of the IP team is to enable developers to continue to create great products while also protecting trade secrets in their day to day work. To return once more to the horticultural theme of this discussion, in this sense the role of the IP function can be conceived as that of a beekeeper, whose job it is to embrace the natural conditions that allow their swarm to thrive, let the bees venture freely collecting pollen beyond the hive, keep out of their way as they create the honey and try not to get stung!

5.2. Answer to Research Question

This study set out to answer the following research question:

> *How can agile technology companies incorporate trade secret protection procedures without undermining the speed and autonomy of their product development practices?*

The results demonstrate that the way to achieve this to first accept the organizational structures and processes. Then, incorporate TSPMs that fit this context. Hopefully, the above discussion makes clear that this is both a worthy and attainable goal.

5.3. Contribution of Research

The existing academic literature on trade secret management generally acknowledges the challenge of maintaining and managing trade secrets (Hannah, 2005; Hannah & Robertson, 2015; Hemphill, 2004; Robertson et al., 2015; Stead & Cross, 2009) and their importance in protecting a range of IAs that cannot be adequately protected via other IPRs (Bos et al., 2015; Crittenden et al., 2015; Hannah et al., 2019). This study goes beyond this by examining the apparent tension between product development and trade secret protection in the specific context of agile technology companies. It aims to contribute to the field by providing research based guidance on the development and implementation of practical TSPMs by agile technology companies.

5.4. Limitations of Research

The definition of an agile technology company is extremely broad. In light of this, a key limitation of this research is that it only reflects practical insights from four companies — one which provided a reasonably high degree of access and insights and three which, due to the sensitive nature of the topic and short timeframe of the study, were less accessible to the researcher. Ideally, the sample size for the comparative multiple case study component of the research would be larger and the level of access/insight be uniformly deep.

Secondly, a key limitation of this study is the limited impact it is likely to have on shaping future case law. This paper has focused on trade secrets from a management perspective. But the reality of any trade secret management is that you are trying to achieve dual objectives. On the one hand, you are trying to maintain control over strategically important IAs by keeping them out of the purview of competitors, and on the other, you are attempting to preemptively prove to a court of law that you took “reasonable steps” to maintain your secrets (despite the fact that you were using them every day in trade to build a competitive advantage). This is a tricky equation at the best of times, not least when your business model relies on achieving speed and autonomy but embracing openness and transparency. Although it seeks to illuminate how agile technology companies can use trade secrets as both a practical and legal tool to protect valuable IAs, this study will have little bearing on precedent to be set by future cases. However, it will be interesting to see whether the inherent flexibility of the legal requirement for “reasonable steps” can embrace the open and information sharing practices of modern agile technology companies.

5.5. Suggestions for Future Research

As mentioned several times above, trade secret management is a relatively nascent field of research. As such, the possibilities for future research are countless. One area that is closely aligned, but beyond the scope of the current study is the interplay between trade secret management and the careful curation of the corporate culture at agile technology companies. Specifically, the way in which the employer branding around being agile, a start up or contributing to open source technological development may impact or impinge upon the ability to effectively manage trade secrets.

Looking forward, and to address the limitation of this study's impact on the development of future trade secret case law, another area of interest for further research may be to review the development of jurisprudence on "reasonable steps". Specifically, to see how/if it evolves to take into account changing business practices, including the growing adoption of agile methods for product development in the software industry and beyond.

6. Conclusion

An essential characteristic of trade secrets is that they are not meant to be locked away, but rather to be used in trade. Therefore, the notion that their protection would undermine the way that any company does business is an obvious non sequitur. However, perhaps due to the industrial origins of trade secret law, the common advice on trade secret management makes it difficult to discern how this seemingly broad and flexible IP tool can be used in the context of agile technology development. This study has attempted to demystify and provide research based guidance on how this may be achieved.

The key lesson is that the ultimate aim of effective trade secret management (even beyond the context of agile technology companies) is not to do everything. It is to do enough. While many skilled and experienced practitioners may advise on particular measures that should be imposed, there is no way any single organization could feasibly do them all. Whatsmore, there is definitely such a thing as “overkill” when it comes to trade secret management, and having more and more stringent measures in place will not result in a reduced risk of leakage.

Helpfully, the law on trade secrets has flexibility built in, and “reasonable steps” is a moving target. This is good news for IP managers at agile technology companies because it means that, far from trying to implement all or as many as possible TSPMs, it will be more effective to select only those that are truly compatible with (and reasonable in light of) the context. The goal here is to minimize any trade off between agility and trade secret management. Of course, this flexibility also represents a challenge because it is necessary to continually review practices, learn and adjust, to conform to what is reasonable across time and contexts.

In rising to this challenge, the overarching focus should be on building awareness and trust among individual employees so as to frame trade secret management as a cross functional task and to enable positive behaviors. The outcome should be an approach which aligns with and supports (rather than fundamentally disrupts) the business model and practices which enable the creation of these valuable assets in the first place.

References

Ackerman, P. (2018). *All About Trade Secret Management*. Decipher. https://www.innovation-asset.com/blog/all-about-trade-secret-management-0-0

Aeton Law Partners. (2019). *Protecting Trade Secrets and Confidential Information*. Aeton Law Partners. https://www.aetonlaw.com/blog/protecting-trade-secrets-confidential-information/

Alexy, O., George, G., & Salter, A. J. (2013). Cui Bono? The Selective Revealing of Knowledge and Its Implications for Innovative Activity. *Academy of Management Review*, *38*(2), 270–291.

Anton, J. J., & Yao, D. A. (2004). Little patents and big secrets: Managing intellectual property. *RAND Journal of Economics (RAND Journal of Economics)*, *35*(1), 1–22.

Atlee, E. E., Beane, D. C., Goodrich, C. N., & Lawton, C. (2017). Harmonize Your Trade Secret Protection To Protect Your Assets. *ACC Docket*, 8.

Baker McKenzie. (n.d.). 10 Best Practices for Trade Secrets Protection. *Baker McKenzie Insight*. Retrieved May 31, 2020, from https://www.bakermckenzie.com/en/insight/publications/2019/04/10-best-practices-trade-secrets

Bambauer, D. (2016). Secrecy is dead—Long live trade secrets. *Denver University Law Review*, *93*(4), 833–853.

Bates, D. G. (2015). 11 strategies for protecting trade secrets. *The Business Journals*. https://www.bizjournals.com/bizjournals/how-to/growth-strategies/2015/05/11-strategies-for-protecting-trade-secrets.html

Beck, K., Beedle, M., Bennekum, A. van, Cockburn, A., Cunningham, W., Fowler, M., Grenning, J., Highsmith, J., Hunt, A., Jeffries, R., Kern, J., Marick, B., Martin, R. C., Mellor, S., Schwaber, K., Sutherland, J., & Thomas, D. (2001). *Manifesto for Agile Software*

Development. https://agilemanifesto.org/

Bok, S. (1989). *Secrets: On the Ethics of Concealment and Revelation*. Vintage.

Bone, R. G. (1998). *A New Look at Trade Secret Law: Doctrine in Search of Justification*. *86*(2), 241.

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

Bryman, A., & Bell, E. (2011). *Business Research Methods* (3rd ed). Oxford University Press.

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., Nelson, R., & Walsh, J. (2000). *Protecting Their Intellectual Assets: Appropriability Conditions and Why U.S. Manufacturing Firms Patent (or Not)* (No. w7552; NBER Working Paper Series, p. w7552). National Bureau of Economic Research.

Conboy, K., & Morgan, L. (2010). Future Research in Agile Systems Development: Applying Open Innovation Principles Within the Agile Organisation. *Agile Software Development: Current Research and Future Directions*.

Costas, J., & Grey, C. (2014). Bringing Secrecy into the Open: Towards a Theorization of the Social Processes of Organizational Secrecy. *Organization Studies*, *35*(10), 1423–1447.

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

Dickey, M. R. (2013). *The Most Extreme Examples Of Secrecy At Apple*. Business Insider. https://www.businessinsider.com/the-most-extreme-examples-of-secrecy-at-apple-2013-7

Dillet, R. (2015). Have You Tried Asking Siri To Give You A Hint? *TechCrunch*. http://social.techcrunch.com/2015/08/27/have-you-tried-asking-siri-to-give-you-a-hint/

Dixon, A. (2016). *Leading Practices to Protect Trade Secrets*. Kluwer Patent Blog.

http://patentblog.kluweriplaw.com/2016/11/01/leading-practices-to-protect-trade-secrets/

Dufresne, R. L., & Offstein, E. H. (2008). On the Virtues of Secrecy in Organizations. *Journal of Management Inquiry*, *17*(2), 102–106.

European Commission. (n.d.). *Innovation Union* [Text]. European Commission - European Commission. Retrieved March 9, 2020, from https://ec.europa.eu/info/research-and-innovation/strategy/goals-research-and-innovation-policy/innovation-union_en

Ewing, T., & O'Connell, D. (2017). Undiscovered country – building a trade secret culture. *IAM Magazine*. https://www.iam-media.com/patents/undiscovered-country-building-trade-secret-culture

Gioia, D., Corley, K., & Hamilton, A. (2012). Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology. *Organizational Research Methods*, *16*(1), 15–32.

Granstrand, O. (1998). Towards a theory of the technology-based firm. *Research Policy*, *27*(5), 465–489.

Granstrand, O. (1999). *The Economics and Management of Intellectual Property: Towards Intellectual Capitalism*. Edward Elgar Publishing Limited.

Granstrand, O., & Holgersson, M. (2014). The Challenge of Closing Open Innovation: The Intellectual Property Disassembly Problem. *Research-Technology Management*, *57*.

Graves, C. T. (2007). Trade Secrets as Property: Theory and Consequences. *Journal of Intellectual Property Law*, *15*(1), 39–51.

Greco, M. (2013). Implementing a Trade Secrets Protection Program. *Fisher Phillips Non-Compete and Trade Secrets Blog*. https://www.fisherphillips.com/Non-Compete-and-Trade-Secrets/Implementing-a-Trade-Secrets-Protection-Program

Hallenborg, L., Ceccagnoli, M., & Clendenin, M. (2008). Intellectual Property Protection in the Global Economy. In *Technological Innovation: Generating Economic Results*. Emerald Group Publishing.

Hannah, D. R. (2005). Should I Keep a Secret? The Effects of Trade Secret Protection

Procedures on Employees' Obligations to Protect Trade Secrets. *Organization Science*, *16*(1), 71–84.

Hannah, D. R. (2007). *An Examination of the Factors that Influence Whether Newcomers Protect or Share Secrets of their Former Employers*. *44*(4), 465–487.

Hannah, D. R., Mccarthy, I. P., & Kietzmann, J. (2015). *We're leaking, and everything's fine: How and why companies deliberately leak secrets*. *58*(6), 659–667.

Hannah, D. R., 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.

Hannah, D. R., & Robertson, K. (2015). Why and How Do Employees Break and Bend Confidential Information Protection Rules? *Journal of Management Studies*, *52*(3), 381–413.

Hemphill, T. (2004). *The Strategic Management of Trade Secrets in Technology-based Firms*. *16*(4), 479–494.

Hendershot, Cowart & Hisey, P.C. (2017). *Ways to proactively protect your intellectual property and trade secrets*. Hendershot Cowart, P.C. https://www.hchlawyers.com/blog/2017/august/ways-to-proactively-protect-your-intellectual-pr/

Holgersson, M., & van Santen, S. (2018). The Business of Intellectual Property: A Literature Review of IP Management Research. *Stockholm Intellectual Property Law Review*, *1*(1).

Holgersson, M., & Wallin, M. W. (2017). The patent management trichotomy: Patenting, publishing, and secrecy. *Management Decision*, *55*(6), 1087–1099.

Hurmelinna-Laukkanen, P., & Puumalainen, K. (2007). Nature and dynamics of appropriability: Strategies for appropriating returns on innovation. *R&D Management*, *37*(2), 95–112.

Iffergan, E. (2018). *Trade Secret Governance: Aligning Policy & procedure*. Hyperion Global Partners. https://insights.hgpresearch.com/trade-secret-governance-aligning-policy-

procedure

JA Kemp. (2018). Trade Secrets – What They Are And How To Protect Them. *JA Kemp*. https://www.jakemp.com/en/knowledge-centre/briefings-and-articles/briefing-detail

Kelly, A. E. (2002). *The psychology of secrets*. Springer Science & Business Media.

Klemens, B. (2019). Software patents poised to make a comeback under new patent office rules. *Ars Technica*. https://arstechnica.com/tech-policy/2019/01/software-patents-poised-to-make-a-comeback-under-new-patent-office-rules/

Larus, C. K., & Olson, R. S. (2019). Protecting trade secrets during corporate transactions. *Financier Worldwide*. https://www.financierworldwide.com/protecting-trade-secrets-during-corporate-transactions

Lewis Silkin. (2017). *Top 5 tips for protecting trade secrets*. Lewis Silkin. https://www.lewissilkin.com/Insights/Top-5-tips-for-protecting-trade-secrets

Lie, H. T. (2020). *Trade Secret Management in Collaborations and Open Innovation* [Doctoral Thesis]. Norwegian University of Science and Technology.

Lie, H. T., Hokstad, L. M., & O'Connell, D. (2020). *Teaching Trade Secret Management with Threshold Concepts* [Research Paper].

Malik, Z., & Bouguettaya, A. (2005). Preserving trade secrets between competitors in B2B interactions. *International Journal of Cooperative Information Systems*, *14*, 265–297.

Mar, E., & Norfleet, W. (2019). Securing Against Trade Secret Pitfalls and Dangers Arising From Employee Mobility Situations. *JD Supra*. https://www.jdsupra.com/legalnews/securing-against-trade-secret-pitfalls-17064/

Meyer, B. (2014). *Agile! The Good, the Hype and the Ugly*. Springer International Publishing.

Millien, R., & George, C. (2016). Protecting IP in an Agile Software Development Environment. *Ipls Proceedings*, *27*(1), 8–14.

Mills, A. (2015). Everyone loves a secret: Why consumers value marketing secrets. *Business Horizons*, *58*(6), 643–649.

Motl, A. (2019). Trade Secret Protection for Customer Lists: A Checklist. *JD Supra*. https://www.jdsupra.com/legalnews/trade-secret-protection-for-customer-29052/

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.

O’Connell, D. (2016). *Trade Secrets*. Intellectual Property Expert Group. https://www.ipeg.com/trade-secrets/

O’Connell, D. (2017). *Trade Secret Asset Management Systems*. https://www.linkedin.com/pulse/trade-secret-asset-management-systems-donal-o-connell/

O’Connell, D. (2018). *The process for managing trade secrets*. Intellectual Property Expert Group. https://www.ipeg.com/the-process-for-managing-trade-secrets/

O’Connell, D. (2019). The Increasing Importance of Trade Secrets and Trade Secret Asset Management Explained. *Seyfarth Shaw Trading Secrets Blog*. https://www.tradesecretslaw.com/2019/07/articles/trade-secrets/the-increasing-importance-of-trade-secrets-and-trade-secret-asset-management-explained/

Passman, P. (2015a). *How to Mitigate Risks Associated with Trade Secret Theft*. BRINK – News and Insights on Global Risk. https://www.brinknews.com/how-to-mitigate-risks-associated-with-trade-secret-theft/

Passman, P. (2015b). Trade Secret Protection: What are Reasonable Steps? *Seyfarth Shaw Trading Secrets Blog*. https://www.tradesecretslaw.com/2015/07/articles/trade-secrets/trade-secret-protection-what-are-reasonable-steps/

Petrusson, U. (2004). *Intellectual Property and Entrepreneurship: Creating Wealth in the Intellectual Value Chain*. Center for Intellectual Property.

Petrusson, U. (2016). *Research and Utilization*. Tre Böcker Förlag AB.

Pooley, J. H. A. (2015a). *Secrets: Managing Information Assets in the Age of Cyberespionage*.

Verus Press.

Pooley, J. H. A. (2015b). Back in fashion – trade secrets in the modern enterprise. *IAM Magazine*. https://www.iam-media.com/litigation/back-fashion-trade-secrets-modern-enterprise

Pooley, J. H. A. (2020). It's About Control, Not Exclusion: Why Trade Secrets Are Treated Like Property, Part 1. *IP Watchdog*. https://www.ipwatchdog.com/2020/01/21/control-not-exclusion-trade-secrets-treated-like-property-part-1/id=118071/

Regnér, S. (2017). *Trade secret management in growing technology based small businesses* [Master Thesis]. Chalmers University of Technology.

Reichman, J. H., & Samuelson, P. (1997). Intellectual Property Rights in Data? *Vanderbilt Law Review*, *50*, 51–166.

Robertson, K. M., Hannah, D. R., & Lautsch, B. A. (2015). The secret to protecting trade secrets: How to create positive secrecy climates in organizations. *Business Horizons*, *58*(6), 669–677.

Rodman, R. L., & Halprin, P. A. (2019). Sworn to Secrecy: Protecting Trade Secrets and Intellectual Property. *Risk Management*. http://www.rmmagazine.com/2019/06/01/sworn-to-secrecy/

Rønde, T. (2001). Trade Secrets and Information Sharing. *Journal of Economics & Management Strategy*, *10*(3), 391–417.

Royce, D. W. W. (1970). Managing the Development of Large Software Systems. *IEEE WESCON*, 11.

Schuering, E. R., & Packel, E. E. (2017). *Five Strategies for Protecting Trade Secrets*. The National Law Review. https://www.natlawreview.com/article/five-strategies-protecting-trade-secrets

Simmel, G. (1906). The Sociology of Secrecy and of Secret Societies. *American Journal of Sociology*, *11*(4), 441–498. JSTOR.

Simmons & Simmons. (2018). *Trade Secrets Directive: Practical steps to protecting trade secrets*. Simmons & Simmons. https://www.simmons-simmons.com/en/publications/ck0dbizk5mqkc0b597w7tppet/261018-trade-secrets-directive-practical-steps-to-protecting-trade-secrets

Slowinski, G., Hummel, E., & Kumpf, R. J. (2006). Protecting Know-How And Trade Secrets In Collaborative R&D Relationships. *Research-Technology Management*, *49*(4), 30–38.

Sousa e Silva, N. (2016). A practical guide to a fast-changing and increasingly popular subject. *Journal of Intellectual Property Law & Practice*, *11*(4), 310–311.

Stead, D. R., & Cross, A. R. (2009). The management and security of trade secrets: An exploratory study. *International Journal of Intellectual Property Management*, *3*(3), 256.

Stern, R. H. (2014). Alice v CLS Bank: US Business Method and Software Patents Marching towards Oblivion? *European Intellectual Property Review*, *10*, 619–629.

Taylor Wessing. (2019). *Step Plan Trade Secrets Directive: Steps companies should take in order to protect their know-how*. TaylorWessing.com. https://deutschland.taylorwessing.com/en/step-plan-trade-secrets-directive

Teece, D. J. (1986). Profiting from technological innovation: Implications for integration, collaboration, licensing and public policy. *Research Policy*, *15*, 285–305.

Terman, M. (2019). Developing a trade secret protection program to reduce risk and increase court enforcement. *Los Angeles & San Francisco Daily Journal*, 2.

von Schwan, A. (2018). *Protecting and Exploiting your Trade Secrets in 2018*. Bryan Cave Leighton Paisner. https://www.bclplaw.com/en-US/insights/protecting-and-exploiting-your-trade-secrets-in-2018.html

Wagner, R. P. (2003). Information Wants to Be Free: Intellectual Property and the Mythologies of Control. *Columbia Law Review*, *103*, 995–1034.

Webster, N., & Bianco, B. (2018). IP Law 101: 3 Ways to Protect Your Trade Secrets. *ACC Docket*. https://www.accdocket.com/articles/ip-law-3-ways-to-protect-your-trade-

secrets.cfm

Winston & Strawn LLP. (2019). The Secret to Protecting Trade Secrets. *True Office Learning*. https://www.trueofficelearning.com/blog/the-secret-to-protecting-trade-secrets

WIPO. (n.d.). *Types of intellectual property*. World Intellectual Property Organization: About IP. Retrieved March 6, 2020, from https://www.wipo.int/about-ip/en/index.html

World Trade Organization. (n.d.). *Overview: TRIPS Agreement*. World Trade Organization. Retrieved March 2, 2020, from https://www.wto.org/english/tratop_e/trips_e/intel2_e.htm

Zabojnik, J. (2002). A Theory of Trade Secrets in Firms. *International Economic Review*, *43*(3), 831–855.

Zimmerman, T., & Griffin, A. (2020). How And When To Protect Trade Secrets. *Fargo INC! Magazine*. https://www.fargoinc.com/how-and-when-to-protect-trade-secrets/

Appendix A: TSPM Catalogue

TSPM Category 1: Daily Workflows and Management	
Sub-Category	**Measure**
Document Marking	Identify and mark documents/files which contain trade secret IAs
Document Marking	Differentiate marking between different levels (e.g. what is claimed as 'trade secret' vs what is merely 'commercially sensitive' or 'confidential')
Document Marking	Avoid labelling documents/files that are not really 'trade secret'/'confidential'/'commercially sensitive' as such (to avoid diluting the meaning of labels)
External Communications	Review materials before publication to ensure there are no inadvertent disclosure trade secret IAs
Internal Communications	Limit recipients of information via email distribution lists and other group communication channels
Internal Communications	Limit attendees at meetings concerning (potential) trade secret IAs on a need to know basis
Information Parsing	Divide trade secret IA into pieces such that no individual has access to/ability to reveal the whole thing
Procurement Procedures	Use external consultant or separate individuals/team that inspect, analyse or trial acquisition opportunities from individuals/team who will work on the internal project (to avoid third party trade secret tainting)
TSPM Category 2: Human Resource Management	
Sub-Category	**Measure**
Contracts/Documentation	Put confidentiality agreements in place with employees
Contracts/Documentation	Put non-disclosure agreements in place with employees
Contracts/Documentation	Obtain written acknowledgement from departing employees of continuing secrecy obligations, return of all company property etc. (i.e. "Termination Certification")
Contracts/Documentation	Put additional/targeted agreements (acknowledgments, warranties etc.) in place with specific employees to prevent/reduce risk of third party trade secret tainting
Contracts/Documentation	Put non-solicitation agreements in place with employees
Contracts/Documentation	Put non-compete agreements in place with employees
Contracts/Documentation	Include secrecy obligations in employee handbooks
Contracts/Documentation	Put IP/invention assignment agreements in place with employees
Contracts/Documentation	Provide written reminder of continuing secrecy obligations to departing employees
Contracts/Documentation	Obtain employee consent to device monitoring as a condition to access of company systems and information
Contracts/Documentation	Notify the new employer of departing employees of individuals ongoing secrecy obligations
Contracts/Documentation	Put additional/targeted agreements (NDAs, non-competes etc.) in place with specific employees to safeguard company trade secrets
Contracts/Documentation	Keep records of training each employee has received in relation to trade secret policies and protections on personnel files
Contracts/Documentation	Obtain periodic written acknowledgement of employee's secrecy obligations (e.g. as part of annual performance reviews, upon promotion decisions etc.)
Education/Training	Develop and conduct an general employee trade secret awareness/education programme
Education/Training	Continually remind employees of secrecy obligations (e.g. via annual training or computer login messaging)
Education/Training	Develop and conduct an employee IT security awareness/education programme
Education/Training	Develop and conduct a board/senior management level trade secret awareness/education programme
Education/Training	Train managers to monitor contributions of new employees (or contractors and consultants) that may be at risk of third party trade secret tainting
Recruitment Processes	Conduct background checks and avoid hiring individuals at risk of third party trade secret tainting
Recruitment Processes	Train interviewers (i.e. hiring managers, talent acquisition teams etc.) on trade secret tainting risks (to avoid asking questions that could be perceived as inquiring about third party/previous employer trade secrets)
Recruitment Processes	Exclude lead engineers from active recruitment or background checks of new employees at risk of third party trade secret tainting
Onboarding Procedures	Conduct entry interviews with new employees that will have access to trade secrets to explain secrecy obligations
Onboarding Procedures	Conduct entry interviews with new employees that may be at risk of third party trade secret tainting
Onboarding Procedures	Conduct or commission forensic reviews of new employees that may be at risk of third party trade secret tainting (e.g. audit documentation and scan devices)
Onboarding Procedures	Assist new employees with third party trade secret tainting risks (e.g. from previous employers) to comply with ongoing secrecy obligations
Offboarding Procedures	Conduct exit interviews with all departing employees including reminder of ongoing secrecy obligations
Offboarding Procedures	Develop and use a checklist for the return of company equipment by departing employees
Offboarding Procedures	Conduct specific/targeted exit interviews with departing employees that pose a high risk of trade secret theft or leakage (e.g. new employer is close competitor, departing on bad terms etc.)

Offboarding Procedures	Ensure the prompt return of all company property (including devices and documents) by departing employees
Offboarding Procedures	Ensure any devices not returned by departing employees are remotely deactivated and purged
TSPM Category 3: Third Party Collaboration and Management	
Sub-Category	**Measure**
Contracts/Documentation	Put non-disclosure agreements and/or confidentiality agreements in place with third-parties
Contracts/Documentation	Put targeted agreements (NDAs, confidentiality agreements etc.) in place with third parties - negotiated with a view to strategic business objectives and specific IAs to be shared
Contracts/Documentation	Include express prohibition on reverse engineering in third party agreements
Contracts/Documentation	When licensing out trade secret IAs, include obligation for third party to take equivalent steps to prevent disclosure
Contracts/Documentation	When licensing out trade secret IAs, include right to conduct spot checks on compliance with secrecy obligations
Contracts/Documentation	When licensing out trade secret IAs, include obligation for third party to immediately report full details of any suspected leaks
Contracts/Documentation	Include express prohibition on disclosure during risky business activities by third parties (e.g. contract bidding or marketing activities)
Education/Training	Develop and conduct an trade secret awareness/education programme for third parties (e.g. suppliers or other business partners)
Education/Training	Continually remind third parties of secrecy obligations (e.g. upon contract renewal or project milestones)
Controlled Disclosure	Implement technical controls on files shared with third parties to limit ability to further disseminate or indefinitely download
Controlled Disclosure	Share trade secret IAs with third parties only on a "need to know" basis
Controlled Disclosure	Provide only hard copies of documents containing trade secret IAs and collect them back once meeting/project/collaboration is completed
Controlled Disclosure	Limit/scrub document/file metadata before sharing with third parties
Controlled Disclosure	Disclose information in a staggered manner during third party negotiations (so that not all information is disclosed before the more advanced stages of negotiation)
Offboarding Procedures	Develop and use a checklist for the return of company equipment at end of third party engagements
Offboarding Procedures	Ensure the return or destruction of all documents (physical and electronic) containing trade secret IAs at the conclusion of third party collaborations
Offboarding Procedures	Remind third parties of continuing secrecy obligations when contracts are terminated
TSPM Category 4: Digital/IT Security	
Sub-Category	**Measure**
Access Control	Implement digital access control measures on trade secret IAs on a need to have basis
Access Control	Password protect devices
Access Control	Password protect files containing trade secret IAs
Access Control	Restrict ability to print, copy or download files containing trade secret IAs
Access Control	Restrict remote access to files containing trade secret IAs
Device Management	Enable remote locking, deactivation and purging of company owned devices (e.g. if lost, an employee is suspected of wrongdoing or is departing the company)
Device Management	Prohibit or restrict use of USB flash drives (or other personal storage devices)
Device Management	Issue company owned devices to employees (no BYOD)
Device Management	Format hard drives (to delete data) before disposing of devices
Device Management	Implement automatic lock screen/log-out functions for inactive devices
Device Management	Prohibit personal use of company owned devices
Device Management	Enable access to company owned devices (e.g. for in person or remote searching in the event of suspected trade secret leakage)
Software Management	Prohibit use of non-approved apps or access to specific websites on company issued devices
Software Management	Use “sandboxing” software to segregate business & personal information on employee personal devices
User ID/Password Hygiene	Mandate periodic password updates (e.g. every 60 days)
User ID/Password Hygiene	Ensure passwords are robust (e.g. multiple characters, letters, numbers symbols)
User ID/Password Hygiene	Use personalized User IDs for devices/accounts
User ID/Password Hygiene	Mandate unique passwords for different systems/each update cycle
User ID/Password Hygiene	Implement two-factor authentication (not just password control)
Monitoring/Auditing	Monitor digital access to trade secret IAs
Monitoring/Auditing	Monitor and keep records/logs of all requests to access, transfer, download or use files that contain trade secret IAs

Monitoring/Auditing	Monitor employee devices (e.g. internet actions)
External Threat Prevention	Develop, implement and maintain comprehensive information security systems to minimise the risk of cybersecurity infringements
External Threat Prevention	Encrypt files that contain trade secret IAs
External Threat Prevention	Implement differentiated/extra cybersecurity protections for files that contain trade secret IAs
TSPM Category 5: Physical/Workplace Security	
Sub-Category	**Measure**
Access Control	Implement physical access control measures on trade secret IAs on a need to have basis
Access Control	Make use of physical barriers (e.g. gates, locks, safety deposit boxes)
Access Control	Require identity and access badges for workplaces or specific location relevant to trade secret IAs
Access Control	Prohibit cameras/phones from workplaces or specific location relevant to trade secret IAs
Access Control	Implement physical access control measures on servers/critical IT infrastructure
Document Disposal	Shred paper documents containing trade secret IAs before discarding
Document Disposal	Secure physical rubbish removal sites (including posting "NO TRESPASSING" signage)
Document Disposal	Regulate destruction of confidential materials (e.g. to be carried out by a designated teams or authorised third parties)
Incidental Disclosure Management	Keep shared physical spaces clear of confidential information (e.g. minimize signage laying out strategic plans or insights, erase whiteboards after team discussions etc.)
Incidental Disclosure Management	Prohibit employees from working on confidential documents in public spaces (e.g. cafes, public transport)
Monitoring/Surveillance	Monitor physical access to trade secret IAs
Monitoring/Surveillance	Monitor access to servers/critical IT infrastructure
Visitor Management	Avoid or narrow workplace tours and other onsite events
Visitor Management	Require visitors to sign in
Visitor Management	Require visitors to wear visitor tags
Visitor Management	Require visitors to be escorted at all times
Visitor Management	Confirm the identity and authority of service providers (e.g. IT/hardware repairs) before granting access to critical infrastructure
TSPM Category 6: Infringement Procedures	
Sub-Category	**Measure**
Risk Monitoring	Identify and monitor the business/R&D activities of the new employers of recently departed employees who have been exposed to trade secret IAs
Risk Monitoring	Investigate departing employees if behaviour is suspicious or risk of trade secret theft is high
Risk Monitoring	Monitor the business/R&D activities of external parties who have been exposed to trade secret IAs
Enforcement Practices	Enforce rights in the event of trade secret theft/misappropriation (e.g. via litigation or C&D letters or employee disciplinary procedures)
Enforcement Practices	Develop an action plan for dealing with trade secret leakage, theft or misappropriation
TSPM Category 7: Trade Secret Specific Systems and Processes	
Sub-Category	**Measure**
Classification Frameworks	Develop a system for classifying trade secrets types (e.g. based on nature, date of creation, responsible person/s etc.)
Classification Frameworks	Develop a set of qualifying criteria for an IA to be considered a trade secret
Data/Cataloging	Create/use a 'Trade Secret Register' to catalogue company's trade secret IAs
Data/Cataloging	Use a trade secret management system (e.g. "Aon TSR" or "Hazel TSAM" Systems)
Data/Cataloging	Collect and track trade secret metadata (i.e. information about the trade secret (e.g. name, date of creation, creator/s, physical or digital location, ownership, type, who has access, relevant TSPMs)
Data/Cataloging	Determine and record the economic value of each trade secret IA (e.g. how much time and money has or will be spent to develop)
Data/Cataloging	Catalogue IAs that have been received from/revealed by third parties that may have risk of trade secret tainting
Data/Cataloging	Record how company trade secret IAs are protected (i.e. relevant TSPMs at a company wide or individual IA level)
Data/Cataloging	Record how third party trade secret IAs are managed/protected (i.e. relevant TSPMs at company or individual IA level)
Data/Cataloging	Catalogue which company trade secret IAs have been shared/disclosed to third parties
Data/Cataloging	Ensure that each trade secret IA is maintained in a defined form to ensure its existence can be proven (e.g. a customer list must be maintained in written form)
High-Level Management	Cultivate/establish a 'trade secret culture'

High-Level Management	Conduct regular trade secret audits
High-Level Management	Develop incentives for compliance with trade secret policies
Responsibility & Oversight	Appoint a dedicated person responsible for day-to-day management of trade secrets
Responsibility & Oversight	Appoint a cross-functional team headed by someone with overall control to oversee trade secret management
Responsibility & Oversight	Engage board or C-Suite level executives in the management of trade secrets

Appendix B: Overview of Category 2 Literature Review Results

Author/s (Year)	Type of Study	Sample & Method	Key Issue/s Examined	Results & Conclusions	Theme of Results/Conclusions
Rønde (2001)	Theoretical (model-based)	Theoretical model of two employees at an industrial firm with variations on organization of production	The impact of information parsing (as a measure for trade secret protection) on firm productivity and employee retention, where information about the full production process is (i) shared fully with all employees; (ii) divided between employees on a, need-to-know but non-hierarchical basis; or (iii) divided between employees on a hierarchical basis (i.e. centralized control with upper management)	Key finding: It may be optimal to limit the number of employees who have access to trade secret information, even if it reduces the firm's productive efficiency. Secondary finding: If the efficiency cost is the same, it is more profitable to divide information between employees on a, need-to-know but non-hierarchical basis, rather than to divide information between employees on a hierarchical basis (i.e. centralized control with upper management)	- Secrecy's Impact on Productivity
Zabojnik (2002)	Theoretical (model-based)	Theoretical model of trade secrets in hierarchical firms	The implications of wage structures and employee remuneration on trade secret management. Based on the assumptions that (i) increased employee retention will result in decreased trade secret leakage; and (ii) managers have access to all trade secrets that pertain to their hierarchical level as well as to all lower levels in a firm.	Managers may have an incentive to overpay their subordinates and protect their firms' trade secrets more than is optimal.	- Holistic and Dynamic Trade Secret Management - Balanced Trade Secret Management
Anton And Yao (2004)	Theoretical (model-based)	Theoretical model of two firms (an "innovator" and a "follower") across three stages of market interactions	The implications of the innovators decisions to protect IP (via patent or trade secret) or disclose innovation information without protection	Three categories of innovation which are optimally protected/disclosed in different ways: (i) Small inventions are not likely to be imitated (and can be disclosed freely) (ii) Medium inventions involve a	- Secrecy as a Structural Imperative

Author/s (Year)	Type of Study	Sample & Method	Key Issue/s Examined	Results & Conclusions	Theme of Results/Conclusions
				form of “implicit licensing” (iii) Large inventions are best protected primarily through secrecy when property rights (i.e. patents) are weak or unavailable	
Hemphill (2004)	Conceptual	N/A	Describes the strategic management of trade secrets as influenced by the legal, organizational and market environments	Provides a framework to guide managerial choice of trade secrecy over other forms of IP protection and sets out a list of sequential questions for management to answer in formulating a TS strategy	- Holistic and Dynamic Trade Secret Management
Hannah (2005)	Empirical	Survey interviews with 111 employees of two high-tech organizations	The impact of organizations' formal efforts to protect trade secrets (i.e. either "access restrictions" (ARs) or "handling procedures" (HPs)) on employees’ beliefs about their obligations to protect those secrets	Trade secret management in an organization is closely linked to the concept of trust. - Employees’ levels of familiarity with ARs were negatively related to their felt obligations to protect trade secrets. - Employees’ levels of familiarity with HPs were positively related to the obligations they felt to protect trade secrets.	- Employer/Employee Trust - Central Role of Education and Awareness Building
Malik And Bouguettaya (2005)	Technical (model-based)	N/A	Proposes an approach for preserving trade secrets in B2B interactions among competitors, specifically focused on digital transfer of customer information in e-commerce environments	A technique of artificially doctoring addresses to make it computationally difficult for competitors to gain useful marketing advantage mining the competitor’s customer data.	N/A
Slowinski, Hummel And Kumpf (2006)	Empirical	Interviews with representatives of 30 member companies of the Industrial Research Institute - a US based organization that "brings leaders of R&D together to discover and share	Starting from the proposition that sharing proprietary intellectual assets is essential to meeting the objectives of the collaboration, discusses best practices for managing trade secrets in the context of joint technology development projects	Managing trade secrets in the context of joint technology development projects is a two-fold challenge involving (i) well crafted legal agreements entered into in timely phases as the project evolves and (ii) managing human behaviours (i.e. training and	- Holistic and Dynamic Trade Secret Management - Disclosure as a Strategic Decision

Author/s (Year)	Type of Study	Sample & Method	Key Issue/s Examined	Results & Conclusions	Theme of Results/Conclusions
		best practices in the management of technological innovation."		communication). Means of effectively of sharing proprietary information during collaborations, categorized into four areas: - Sets of Agreements in general - NDAs specifically - Joint Development Agreement specifically - Organizational issues	
Hannah (2007)	Empirical	Survey interviews with 111 employees of two high-tech organizations to gather qualitative and quantitative data	Factors which influence individuals' decisions about whether to protect or share secrets following a transition from one organization to another (so called "protect vs. share decisions")	The outcome of protect vs. share decisions is linked to humans innate need to develop a sense of identification and acceptance within new social groups. People's perceptions of what does or does not constitute a trade secret is not necessarily aligned with legal definitions. Key considerations are: - Whether the information is publicly available - if yes, not considered TS (but there is little nuance around the question of "easily ascertainable") - Whether it is general or specific - if specific, more likely considered TS (participants believed that "general information was less likely to be sensitive") - Whether is it positive of negative - if negative (i.e. knowledge of what does not work), less likely to be considered TS	- Employer/Employee Trust - Central Role of Education and Awareness Building - Holistic and Dynamic Trade Secret Management - Balanced Trade Secret Management
Dufresne And Offstein (2008)	Conceptual	N/A	Examination of the instances where secrecy is a positive and necessary component of business strategy, as well as the inherent	Given the virtues and necessity of some degree of secrecy discussed, it is up to managers "to strike a balance between	- Secrecy as a Structural Imperative - Employer/Employee Trust

Author/s (Year)	Type of Study	Sample & Method	Key Issue/s Examined	Results & Conclusions	Theme of Results/Conclusions
			tension between secrecy and openness in any organization	compartmentalization on the one hand and expansive, transparent knowledge sharing on the other."	
Stead And Cross (2009)	Empirical	Interviews with 22 practitioners in the field of IP management	Exploratory research to provide a foundation for a general understanding of the nature and governance of trade secrets and their role in management practice	Due to the exploratory nature of the research findings were broad and numerous. Some of the most illuminating are: - Trade secrets tend to have a life cycle - though, in law, they are immortal, they do not typically last forever - Trade secrets tend to be held collectively, not by individual employees or directors - Large firms, which are likely to have multiple trade secrets, are likely to withstand damage inflicted by TS leakage relatively easily, compared to small firms with fewer trade secrets. - In large firms, knowledge is distributed throughout the structure; at lower levels, it is more detailed but more partial while at higher levels, it is less detailed but covers a wider span of functions including finance, procurement, technology and sales. - In larger firms, the most reported mechanism for TS management was a policy of 'need to know', whereby sensitive items of information are made known only to those who need them for the performance of their work. - By experienced IP professionals, patents and trade secrets are	- Secrecy as a Structural Imperative - Holistic and Dynamic Trade Secret Management

Author/s (Year)	Type of Study	Sample & Method	Key Issue/s Examined	Results & Conclusions	Theme of Results/Conclusions
				viewed as compliments, not substitutes.	
Alexy, George And Salter (2013)	Conceptual	N/A	The strategic considerations that impact a firm's decision to "selectively reveal" information in order to initiate collaborative relationships, shape competitive landscapes and/or improve access to new technologies and markets	By selectively revealing information a firm can achieve one of four strategic outcomes: (i) Issues spreading: Encourage others to participate in shared problem solving and/or to make complementary investments (ii) Agenda shaping: Highlight focal firm's future demands so others can privately invest in and/or actively assist firm in developing solutions and complementary offerings (iii) Product enhancing: Facilitate wide use of revealed knowledge to increase value of complementary assets and likelihood of reciprocal behavior (iv) Niche creating: Build critical mass supporting firm's technology trajectory to attain buy-in from crucial actors in ecosystem	- Disclosure as a Strategic Decision - Holistic and Dynamic Trade Secret Management
Costas And Grey (2014)	Conceptual	N/A	The role of both formal and informal secrecy in organizations	Secrecy is a reality of day-to-day operations within firms of all sizes and natures and the role of secrecy within an organisation goes beyond its function in protecting valuable information, but also "about social aspects of organizational life, such as the cementing of group identity."	- Secrecy as a Structural Imperative - Employer/Employee Trust
Hannah And Robertson (2015)	Empirical	Semi-structured interviews with 55 employees at two	The factors which impact employees' behavior in breaking or bending their employers' rules	Employees are more likely to comply with rules that they perceive as justified. There are three types of tensions	- Holistic and Dynamic Trade Secret Management - Balanced Trade

Author/s (Year)	Type of Study	Sample & Method	Key Issue/s Examined	Results & Conclusions	Theme of Results/Conclusions
		companies to gather qualitative data	for the protection of confidential information	that precipitated rule breaking: (i) obstructions of work, (ii) disruptions of knowledge networks, (iii) threats to employees' identities. In these situations, there are several potential outcomes: - Rule Compliance, including: Tolerating (continuing to comply with the rules despite the tension they caused) Objecting (communicating dislike of a rule to management with the goal of having a rule changed, while still complying) - Rule Breaking or Bending, including: Shortcutting - circumventing the rules that slowed them down Conspiring - contact another employee and work together to get around the rules Selectively Disclosing - sharing certain aspects of the CI but not others	Secret Management - Central Role of Education and Awareness Building - Employer/Employee Trust
Bos, Broekhuizen And De Faria (2015)	Conceptual	Literature review	How secrecy can be employed as a mechanism for appropriating value from innovation	A dynamic framework that presents secrecy management as an ordered process across four stages with potential feedback loops that incorporate contingencies.	- Secrecy as a Structural Imperative - Holistic and Dynamic Trade Secret Management
Hannah, Mccarthy And Kietzmann (2015)	Conceptual	N/A	The strategic considerations that impact a firm's decision to deliberately leak secret information and impact of different methods of deliberate leaking	Provides a framework to help managers decide whether or not to strategically leal their trade secrets. Sets out four types of deliberate leaks: (i) Informing (Overt/Factual):	- Disclosure as a Strategic Decision - Holistic and Dynamic Trade Secret Management

Author/s (Year)	Type of Study	Sample & Method	Key Issue/s Examined	Results & Conclusions	Theme of Results/Conclusions
				Leaking secrets to be transparent, compliant and collaborative (ii) Dissembling (Overt/Concocted): Leaking secrets to misrepresent and deceive (iii) Misdirecting (Covert/Concocted): Leaking secrets to send others down the wrong path or course of action (iv) Provoking (Covert/Factual): Leaking secrets to stimulate and test reactions	
Robertson, Hannah, Lautsch (2015)	Conceptual	N/A	The impact of employees' perceptions of the policies, procedures, and practices implemented to protect trade secrets on the extent to which they willingly comply and how to cultivate a positive perceptions leading to maximum compliance.	Positive secrecy climates are defined as places where organizational secrets are strongly valued by employees and seen as a part of their formal role responsibilities.	- Secrecy's Impact on Productivity - Employer/Employee Trust - Central Role of Education and Awareness Building
Crittenden, Crittenden And Pierpont (2015)	Histographic	Primary and secondary sources where reviewed to catalogue 35 trade secrets held by different companies around the world	The nature and strategic intent behind the trade secrets catalogue with a view to expanding the range of narratives told about trade secrets in the extant literature	An in-depth database of various company trade secrets which provides more examples of strategic secrecy (beyond the oft cited examples of KFC, Coca-Cola, WD-40, and McDonald's).	- Secrecy as a Structural Imperative
Nelson (2016)	Empirical	Inductive, multiple-case study	The factors which impact researchers' decision to sharing scientific knowledge in a research setting - specifically how to manage the benefits of sharing (Reputation/prestige; Attracting collaborators; Recruiting employees) against the detriments (Erosion of competitive advantage; Enabling "scooping"	Identifies four tactics that researchers use to manage sharing/secrecy tensions: (i) Leveraging trust — i.e. trusting in the personal relationships with the recipient and their moral obligation not to disclose or steal the secret information (ii) Strategic withholding — i.e. to share some, but not all of the	- Disclosure as a Strategic Decision - Holistic and Dynamic Trade Secret Management

Author/s (Year)	Type of Study	Sample & Method	Key Issue/s Examined	Results & Conclusions	Theme of Results/Conclusions
			of academic credit or commercial success)	secret information (iii) Delaying — i.e. to hold back on sharing the secret information until such a time as the locus of control can be retained by the researcher (iv) Patenting — i.e. gaining a monopoly control position using IPRs	
Pedraza-Farina (2017)	Conceptual/ Doctrinal	N/A	How trade secret laws might be optimized to foster greater innovation in a highly networked and collaborative knowledge economy	Legal construction of trade secrets should be narrowed (i.e. limiting what is legally protected) in order to drive innovation. The current trend towards nation wide uniformity in the US (i.e. by federalizing trade secret law under the DFTA and UTSA), rather favoring state experimentalism in designing trade secret law and policy should be halted in favour of a more tailored state-by-state approach (so that different measures can be adopted depending on the nature of industry in a particular state/location.)	N/A
Sofka, De Faria And Shehu (2018)	Empirical	Hypothesis that firms that are legally required to share information with their shareholders will be more visible to potential imitators is tested using a representative sample of 683 firms in Germany between 2005 and 2013	The impact of a firm's visibility to potential imitators on the importance of secrecy as a mechanism for appropriating value from innovation	The importance of secrecy is influenced by the visibility of a firm's activities to potential imitators.The more visible a firm, the more vulnerable it is for imitation. This has a particularly significant impact on firms that are legally obligated to share information with shareholders in the form of financial reports, because such sharing increases the firm's visibility to competitors.	N/A

Author/s (Year)	Type of Study	Sample & Method	Key Issue/s Examined	Results & Conclusions	Theme of Results/Conclusions
Hannah, Parent, Pitt And Berthon (2019)	Conceptual	Literature review	The nature of 'Secrecy Appropriation Mechanisms' (SAMs) - i.e. how, when and why they can support innovation.	SAMs can have both positive and negative effects on a number of organizational dynamics - the key to realising the value of trade secrets is by identifying and managing the trade offs. SAMs can originate bureaucratically (from upper management) or normatively (from groups of insiders who are not typically the rule-makers). Three key characteristics of SAMs are identified as: (i) Permeability - "SAMs that have lowest permeability will be those that have become both bureaucratic and normative" (ii) Visibility - "Bureaucratic SAMs will be more visible than normative SAMs." (iii) Scope - "Bureaucratic SAMs will be more likely than normative SAMs to have broad scope."	- Secrecy's Impact on Productivity - Holistic and Dynamic Trade Secret Management - Balanced Trade Secret Management

Appendix C: Phase 1 Interview Template

INTRODUCTION

- Short description of the purpose of the study as well as the theoretical foundation.

"The purpose of this interview is to my Master Thesis dissertation — which is an academic research project on the topic of 'Trade Secret Management by Agile Technology Companies'."

- Short introduction of the author and their academic background.

"This project the final part of my Masters' degree in Intellectual Capital Management at the Chalmers University of Technology in Gothenburg, Sweden. The program is focused on how to evaluate Intellectual Assets and design IP based business strategies to leverage their value."

- Clarification of how the data gathered during the interview will be used and ensure that consent is given for use both internally & externally:

"Before we get started I want to clarify how the information you share during this interview will be used.

It will be used for my master thesis, which will be published at Chalmers University of Technology. In this capacity, your responses will be presented as anonymous qualitative data. Because it is a sensitive topic, the data that I collect during these interviews will be presented in my paper with a high level of abstraction and no attribution to a particular individual or company.

With that in mind, please let me know if there is anything you want me to specifically exclude. Otherwise, I will assume that I can use the information you share with me in this interview on that basis."

- Request to record the interview for ease of review

"If it is okay with you, I would like to record this interview. However, I want to stress that it is for my own personal review and reflection only. I will not share it, create any transcripts or publish any direct quotes. It is only so that I can focus on our discussion without worrying about capturing everything with copious note-taking. Is that okay?"

- Short overview of what a trade secret is and why it is an important means of controlling IAs at agile technology companies

"Can start by getting you to explain what, if anything do you understand are "trade secrets"?"

- Depending on the response, clarify/confirm that:

"A trade secret is a type of intellectual property. Other types include patents, trade marks, copyright. But it is the broadest type of IP because it can more or less protect anything as long as three criteria are filled:

1. *Secret;*
2. *Commercial value because it is secret; and*
3. *Subject to reasonable steps under the circumstance to keep it secret."*

QUESTIONS

About the Interviewee

Can you give me a short description of your role?

High-Level Questions

1. Do you see a need for a more formalized approach to trade secret protection at [COMPANY]?

2. Do you see any obstacles or challenges in implementing a more formalized approach to trade secret protection at [COMPANY]?

3. Have you worked in an organization earlier where there was a trade secret policy? If yes, can you provide any insight into how it was shaped?

4. Have you experienced that sensitive and valuable information within your team or department has leaked to third parties in an uncontrolled way?

Trade Secret Protection Measures

Internal Access Controls

5. Do you believe that some information is so commercially valuable and sensitive that it should be restricted with internal access controls, or do you believe that everyone should be able to access everything?

6. How do or would internal access controls you and your teams work at [COMPANY] — specifically your ability to work with speed and autonomy?

7. How about restricting remote access to files containing trade secret IAs, how do you think this would impact you and your teams work — specifically your ability to work with speed and autonomy?

Document Marking

8. One way of protecting trade secrets is by identifying and marking documents/files which contain the IAs to be protected. Is this something that you and your team already does?
    - If yes, how do you think it impacts your ability to get things done — specifically your ability to work with speed and autonomy?
    - If no, can you give your perspectives on how you think this would impact you and your teams work — specifically your ability to work with speed and autonomy?

Information Parsing

9. Another way of protecting trade secrets is by dividing or sectioning out trade secret IA into pieces such that no individual has access to/ability to reveal the whole thing (e.g. it is rumored that KFC's suppliers will only ever know half of the 11 secret herbs & spices that make up the original recipe, and the original handwritten recipe is stored in a safe in Kentucky). Can you think of any IAs that you or your team works with that could be divided up this way?
    - If yes, how do you think splitting knowledge of or access to them between different people would impact your ability to get things done — specifically your ability to work with speed and autonomy?
    - If no, move on.

Internal Communications

10. Another way of protecting trade secrets is by limiting the recipients of information via email distribution lists and other group communication channels. Is this something that you and your team already does?
    - If yes, how do you think it impacts your ability to get things done — specifically your ability to work with speed and autonomy?
    - If no, can you give your perspectives on how you think this would impact you and your teams work — specifically your ability to work with speed and autonomy?

11. Similarly, another way is to limit attendees at meetings concerning (potential) trade secret IAs on a need to know basis. Is this something that you and your team already does?
    - If yes, how do you think it impacts your ability to get things done — specifically your ability to work with speed and autonomy?
    - If no, can you give your perspectives on how you think this would impact you and your teams work — specifically your ability to work with speed and autonomy?

Physical Spaces

12. Another way of protecting trade secrets is by keeping shared physical spaces clear of confidential information (e.g. minimize signage laying out strategic plans or insights, erase whiteboards after team discussions etc.) How do you think this would impact you and your teams work — specifically your ability to work with speed and autonomy?

13. Another way is to prohibit employees from working on confidential documents in public spaces (e.g. in cafes, or on public transport). How do you think this would impact you and your teams work — specifically your ability to work with speed and autonomy?

Procurement Procedures

14. An important part of trade secret management is trying to minimize the risk of "trade secret tainting" (when another entities trade secret IAs could be revealed or leaked to [COMPANY] in a way which might open us up to a claim of IP theft or infringement). One way of managing this risk is by using external consultants or separate individuals or teams to inspect, analyse or trial acquisition or collaboration opportunities, from the actual individuals or teams who will work on the internal project. Is this something that you and your team have done or considered?
    - If yes, how do you think it impacts your ability to get things done — specifically your ability to work with speed and autonomy?
    - If no, can you give your perspectives on how you think this would impact you and your teams work — specifically your ability to work with speed and autonomy?

Employee Onboarding [Asked of People Managers Only]

15. Another way of minimizing the risk of trade secret tainting is by excluding lead engineers from active recruitment or background checks of new employees (because they could be tempted to recruit with a view to obtaining trade secrets from previous employers). As a manager, can you share your perspectives on this?

16. Similarly, one way of minimizing the risk of trade secret tainting is by asking hiring managers to monitor the contributions of new employees (or contractors and consultants) that may be at risk of exposing third party trade secrets. As a manager, can you share your perspectives on this?

Education & Training

17. Finally, a significant part of protecting trade secrets at any company is through education and training. Do you have any suggestions or ideas about how [COMPANY] could do this effectively?

Appendix D: Phase 2 Interview Template

INTRODUCTION

- Short description of the purpose of the study as well as the theoretical foundation.

"I am conducting this research to complete my Master Thesis dissertation on the topic of 'Trade Secret Management by Agile Technology Companies'."

- Short introduction of the author and their academic background.

"This project the final part of my Masters' degree in Intellectual Capital Management at the Chalmers University of Technology in Gothenburg, Sweden. The program is focused on how to evaluate Intellectual Assets and design IP based business strategies to leverage their value."

- Clarification of how the data gathered will be used and ensure that consent is given for publication.

"Before we get started I want to clarify how the information you share during this interview will be used.

Which is to say that it will be used for my master thesis, which will be published at Chalmers University of Technology. In this capacity, your responses will be presented as qualitative data on the perspectives of an IP professional working in the context of an agile technology company. Because it is a sensitive topic, the data that I collect during these interviews will be presented in my paper with a high level of abstraction - there will be no attribution to a particular individual (i.e. you) or company (i.e. [COMPANY]).

With that in mind, please let me know if there is anything you want me to specifically exclude from my thesis. Otherwise, I will assume that I can use the information you share with me in this interview on that basis."

- Request to record the interview for ease of review

"If it is okay with you, I would like to record this interview. However, I want to stress that it is for my own personal review and reflection only. I will not share it, create any transcripts or publish any direct quotes. It is only so that I can focus on our discussion without worrying about capturing everything with copious note-taking. Is that okay?"

QUESTIONS

About the Interviewee

Can you give me a short description of your role?

Substantive Questions

1. On a high level, how do you think about trade secret management at [COMPANY]?

2. What are the main challenges/obstacles to trade secret management at [COMPANY]?

3. How do you as an IP professional overcome/work around these challenges/obstacles with the teams that you serve?

4. Which (if any) trade secret protection measures are routinely implemented into product development practices at [COMPANY]? Or, on a more generalized level,

5. Can you reflect on any instances in your organization where trade secret management impacts upon the speed of execution which can be achieved by tech/product development teams?

6. Can you reflect on any instances in your organization where trade secret management impacts upon the autonomy of tech/product development teams?

7. Are you concerned about the impact of trade secret management on company culture — particularly feelings of trust and empowerment among employees? Does that impact your approach to trade secret management at [COMPANY]?

8. How is responsibility for trade secret management divided at [COMPANY]? Does it lay primarily with one team or is it viewed more cross-functionally? Which team/teams are involved?

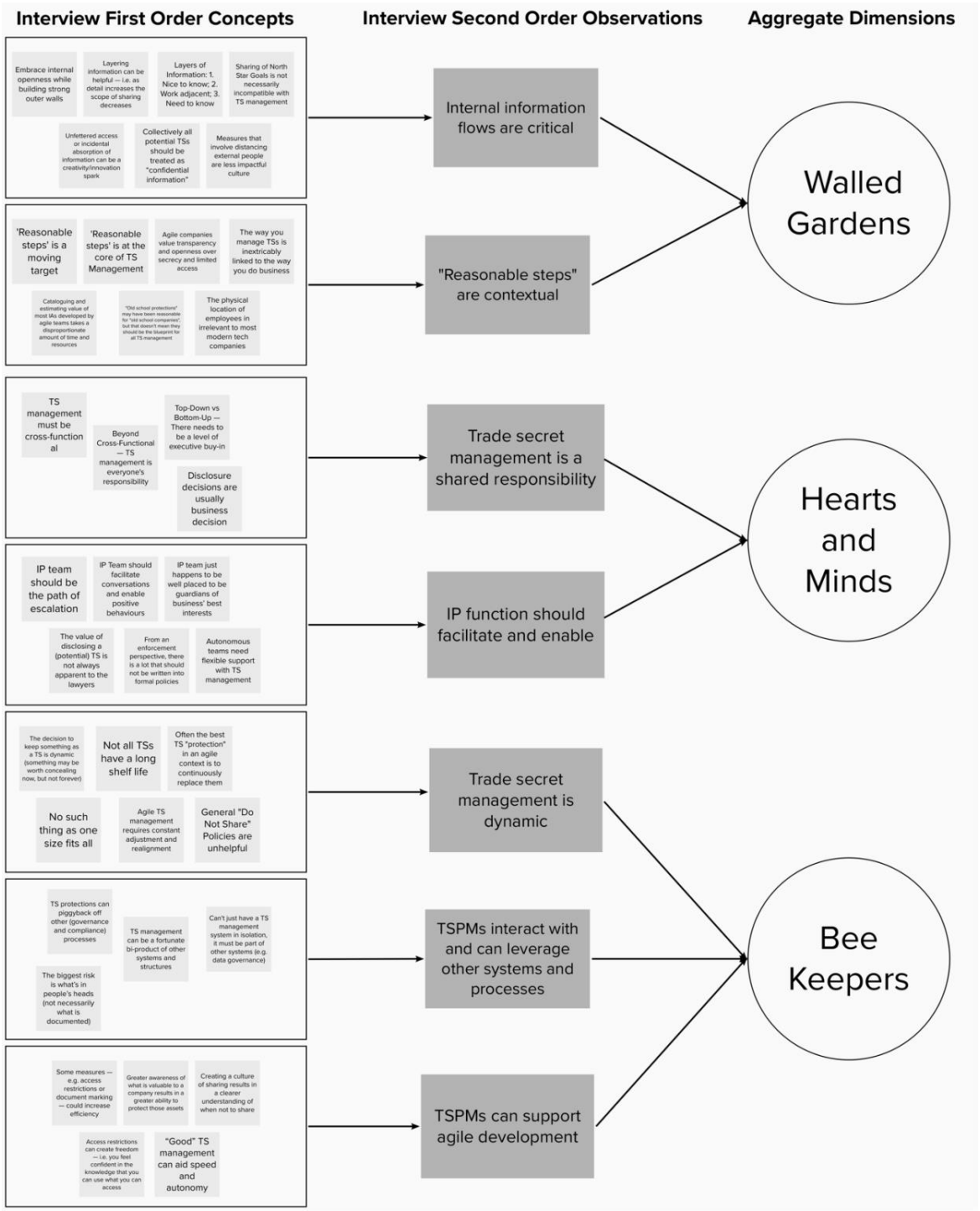
9. A significant part of protecting trade secrets at any company is through education and training — getting individuals to understand what trade secrets are, why they're important and what needs to be done to protect them. Can you share a bit about how you approach this at [COMPANY]? Or, on a more generalized level, do you have any ideas about how this can be done optimally?

10. On the whole, are you satisfied with the way that trade secrets are managed at [COMPANY] or are there room for improvement? If so, what are the key areas for improvement?

Appendix E: Anonymized List of Interviewees

Interviewee ID	Title	Role Description	Company Description	Interview Date
Phase 1 Interviews				
A	Chief Architect/VP, Engineering	Responsible for company's overall technology architecture and engineering processes	Agile Software Based Audio Streaming Technology Company	3-Apr-2020
B	Senior Director, Product	Resposible for overseeing development of one of the company's core product areas + related underlying platform technologies	Agile Software Based Audio Streaming Technology Company	6-Apr-2020
C	Product Manager	Responsible for managing a multifunctional team - including UX designers, product designers, data scientists and product managers - developing an exploratory additional product for the company	Agile Software Based Audio Streaming Technology Company	7-Apr-2020
D	Director, Research	Responsible for leading a team of research scienstists focused on pushing the company's core product area R&D processes beyond state-of-art	Agile Software Based Audio Streaming Technology Company	7-Apr-2020
E	Product Lead	Responsible for leading the development of a highly technical & external interfacing aspect of the company's product	Agile Software Based Audio Streaming Technology Company	16-Apr-2020
F	Program Manager	Responsible for overseeng the execution of a company wide cross-functional high priorty project	Agile Software Based Audio Streaming Technology Company	9-Apr-2020
G	Senior Product Manager	Responsible for managing a multifunctional team - including UX designers, product designers, data scientists and product managers - developing one of the company's core product areas + related underlying technologies	Agile Software Based Audio Streaming Technology Company	8-Apr-2020
H	Agile Coach Lead	Responsible for managing a team of agile coaches, focused on helping teams improve how they work and how they deliver value over time - including teaching agile and lean practices and mindset to leadership and teams	Agile Software Based Audio Streaming Technology Company	7-Apr-2020
I	Product Area Lead	Resposible for leading engineering outcomes for one of the company's core product areas + related underlying platform technologies (previously also an Agile Coach)	Agile Software Based Audio Streaming Technology Company	8-Apr-2020
J	Senior Patent Engineer	Responsible for prosecution of the company's patent applications globally, managing/reviewing invention disclosures, reviewing patent acquisition oppourtunities and supporting patent litigation matters.	Agile Software Based Audio Streaming Technology Company	16-Apr-2020
K	Patent Engineer	Responsible for all patent activities in company's European offices - including patent prosecution, innovation harvesting, FTO and clearance, patent portfolio management and IP training for company employees	Agile Software Based Audio Streaming Technology Company	16-Apr-2020
L	IP Counsel	Responible for assisting R&D teams across the company to manage and protect IAs	Agile Software Based Audio Streaming Technology Company	16-Apr-2020
Phase 2 Interviews				
M	Managing Counsel	Responseible for product counseling, privacy counselling and IP counselling at company (previously an experienced IP litigator)	Agile Software Based Media Streaming Technology Company	21-Apr-2020
N	IP Legal Director (Emerging Technologies)	Responsible for all IP matters related to company's emerging technologies	Agile Ride Sharing/Delivery Services Technology Company	22-Apr-2020
O	Legal Counsel (Litigation and IP)	Responsible for managing all patent (+ class action & partner) litigation and managing company's entire patent practice	Agile Cloud Computing Services Technology Company	8-May-2020

Appendix F: Interview Data Analysis Visualization



DEPARTMENT OF TECHNOLOGY MANAGEMENT AND ECONOMICS
Division of Entrepreneurship and Strategy
CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden
www.chalmers.se

CHALMERS
UNIVERSITY OF TECHNOLOGY